ARGUS
CYBER SECURITY

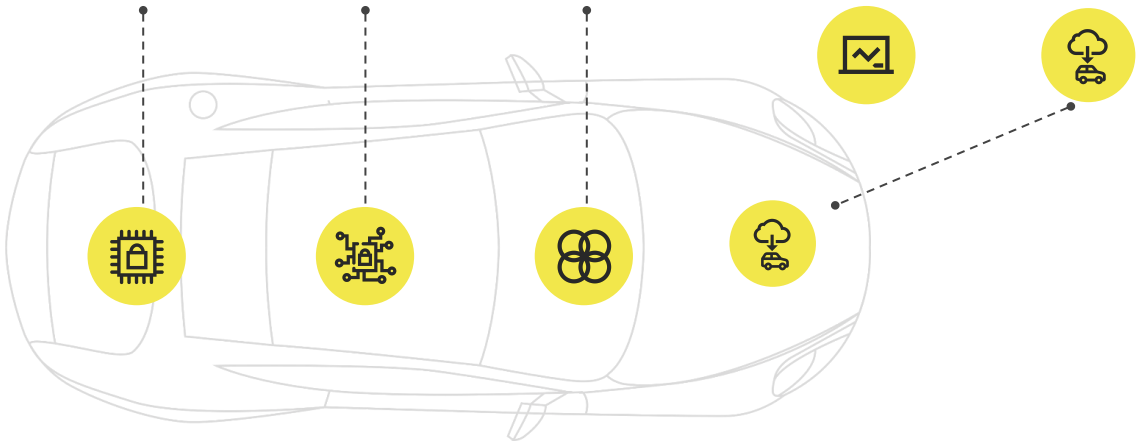
In-vehicle network의 사이버 보안

Yonghan Jeon, Simiao Wang

17th, NOV

Holistic Offering

IN VEHICLE			OUT OF VEHICLE			SERVICES
Core ECU Protection	Network Protection (CAN/Ethernet)	Connected ECU Protection	Fleet Protection	OTA Software Updates	Vehicle Vulnerability Management	Penetration Testing
						TARA
						Code Review
						Security Concept
						Security Requirements & Specifications
						Incident Response

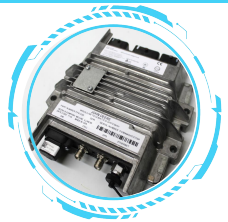


MAXIMUM SECURITY. GREATER VISIBILITY.

ARGUS CYBER SECURITY

Attack vectors connecting surfaces and end ECUs

V2X



Telematics & Cellular Devices

Bluetooth

WiFi

Infotainment

OBD II

Risky zone

TCU

BLM

IVI

OBD

Central Gateway

Secure zone

Domain Controller

Domain Controller

Domain Controller

ECU

ECU

ECU

ECU

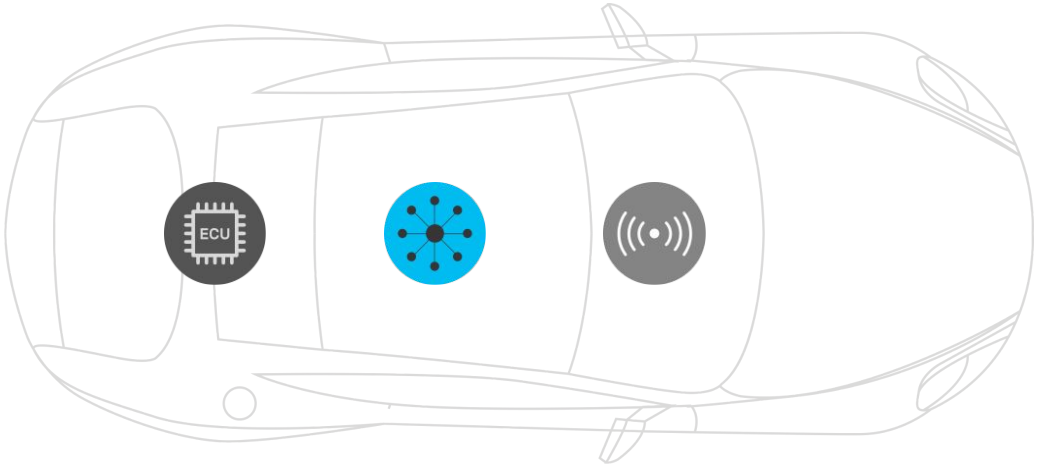
ECU

ECU

ARGUS CYBER SECURITY

Argus Network Protection

Argus provides network inspection logic designed to run in various platforms



As a Network IDS

Gateways Domain Controllers

Switch

HPC

As a Firewall

Connected ECUs

Endpoint Autosar ECUs

ARGUS CYBER SECURITY

Argus CAN IDS

Argus CAN IDS

- Software solution, designed for integration on classic Autosar / bare metal ECUs
- Detects attacks based on timing, context and deep packet inspection of CAN communication
- Rule-based
- Developed following extensive research and in-vehicle pen-tests
- Flexibility to support various security needs
- Detection only, Basic prevention only, Reaction approach and more
- Scalable and configurable to change modes in the future
- Ability to pinpoint malicious message, detailed information on each attack detected

Mapping to packages

Frame filtering

Frame Analysis

Diagnostics

Advanced analysis

Covering requirements from Global Regulations:

- **EU/Japan:** UNR 155 Annex 5
- **Chinese:** GB/T 40857 - 2021

Detection rule & Relevant Input

Detection rule of CAN is designed according to various inputs from **CAN DBC** and **Network recording**

CAN IDS Features	DBC Input					Network Recording
	CAN Header	CAN Payload		CAN Bus	Timing spec	
		CAN Data	Higher layer protocols (e.g. ISO-TP, UDS)			
Baseline	○			○		○
Specification Enforcement	○	○	○	○		
Diagnostic	○		○	○	○	○
Timing, Data and Timing	○	○	○	○	○	○

CAN IDS Ruleset

- Contains the vehicle specific security policy
- Easily updated without full firmware update
- Automatic generation process
- Enables modularity by using only specific parts
- Easy to use configuration tool
  - Change the required reaction per attack
  - Add specific rules (can be automated as well)
  - Remove / change parts

Use cases

Customer: Japanese OEM & Japanese Tier-1
Market: Global (Japan/Europe/North America)
Integrated ECU: CGW/C-BCM
Projects: 3 baseline projects +8 variants and still going on

Lessons learned from mass production projects:

- OEM & Tier-1 need more **security advices beyonds IDS**
  - Regulation Compliance check
  - E/EA, ECU Security Consulting
- Tuning for **0 False Positive** and **High Detection Rate** is challenging but mandatory
- **Expertise-Resources of various areas** is necessary to secure a mass production

Types of features implemented

Baseline	Specification Enforcement	Diagnostic	Timing, Timing and Data
• Header Filter • Busload Monitoring	• CAN DPI • Protocol Enforcement	• UDS Header Filter • UDS DPI • UDS DoS • UDS Vehicle Scenario Monitoring	• Frequency Monitoring • Minimal Interval Monitoring • Counter Monitoring

Key Tasks & Expertise-Resources for CAN IDS Production

Administration & Regulation

Regulation Compliance Check
- Regulation Expert

Regulation Compliance Check
- Regulation Expert

Regulation Update Track
- Regulation Expert

Life-time incident response
- P-SIRT
- Vulnerability Management

Planning → **Development** → **Validation** → **After production**

Feature & Deployment Plan
- Automotive Security Expert
- Product Expert

Product Development
- Product Expert

Network Research & Rule design
- Automotive Network Expert
- Security Researcher

Automotive Quality Validation
- ASPICE validator
- Automotive Functional Tester

Automotive Security Validation
- Fuzzing/Pentest Engineer

Continuous Product Improvement
- Product Expert
- Automotive Security Researcher

Engineering

THANK YOU

www.argus-sec.com

yonghan.jeon@argus-sec.com
simiao.wang@argus-sec.com

ARGUS
CYBER SECURITY