Argus Core ECU Protection

Core ECUs, which do not have an operating system or are classic AUTOSAR-based, are at risk of high-impact attacks that can endanger passengers and lead to financial loss for OEMs and Tier 1s. Argus Core ECU Protection detects and mitigates attacks on these ECUs.

MINIMIZE EXPOSURE TO HIGH-IMPACT ATTACKS

Core ECUs may be considered safe from attacks, as they are internal, not connected, and located further away from the attack surface. However, these ECUs are also responsible for most vehicle functionalities, including safety-critical functions. A successful cyber-attack on core ECUs can have a high impact on car operation and place passengers’ safety at risk. Unlike connected ECUs, which run high-level operating systems (e.g., Linux, Android, QNX), core ECUs have minimal inherent security measures.

OPTIMAL SECURITY WITH MINIMAL EFFORT

Argus Core ECU Protection includes three independent modules that work individually, or together, to provide maximum host-based security, with minimal integration and configuration effort.

PROTECTING CORE ECUS

- Instrument Cluster
- Braking & Stability
- Body Control Module
- Gateway
- And more...

KEY BENEFITS

- Optimal balance between security and performance
- Flexible configuration from hardening to detection
- Cost-effective reusable software
- Seamless integration during development
- Detailed logging for future investigation
- Automotive-grade

Security Logger
Collects and securely stores security events for future investigation.

ECU Firewall
Prevents the ECU from receiving and sending malicious communications using Deep Packet Inspection.

Control Flow Integrity
Prevents exploitation of vulnerabilities by ensuring that the ECU software follows the expected execution flow.

Application Layer
AUTOSAR Runtime Environment (RTE)
Hardware
ATTRACTIVE TARGET FOR HACKERS

There are many reasons why malicious actors may target core ECUs:

- MANIPULATE SAFETY CRITICAL FUNCTIONS RISKING PUBLIC SAFETY
- CREATE NEW CAR KEYS AND STEAL VEHICLES FOR FINANCIAL GAIN
- EXTRACT ECU FIRMWARE TO PRODUCE COUNTERFEIT PARTS
- ACTIVATE PREMIUM FEATURES THAT ARE BLOCKED BY THE OEM

Example ECU:
- Braking & Stability
- Body Control Module
- Instrument Cluster
- Engine Control Module

SECURITY UNDER CONSTRAINT

Argus Core ECU Protection overcomes key challenges to integrating security in core ECU architecture:

- Limited resources
- No operating system or only low-level operating system
- Monolithic software architecture

KEY FEATURES

- Supports Classic AUTOSAR-based ECUs and bare metal.
- Easily configured throughout the development process
- Designed to fit any hardware architecture
- Reports events to a master ECU or logs events for future extraction
- Consumes minimal system resources

WHY ARGUS

- Multiple Production Projects
  Multiple SOPs in 2020 with OEMs & Tier 1s
- Acknowledged Automotive Vendor
  Partnerships with industry leaders
- Team of Experts
  Automotive & Cyber expertise - offering based on real world hacker expertise
- Leading Technology
  Outperforms competitors in 3rd-party evaluations
- Scalable Holistic Offering
  Protects connected high-performance ECUs to embedded ECUs throughout their lifespan

WE ARE ARGUS CYBER SECURITY

Argus, the global leader in automotive cyber security, provides comprehensive and proven solution suites to protect connected cars and commercial vehicles against cyber-attacks. With decades of experience in both cyber security and the automotive industry, Argus offers innovative security methods and proven computer networking know-how with a deep understanding of automotive best practices. Customers include car manufacturers, their Tier 1 suppliers, fleet operators and aftermarket connectivity providers. Founded in 2013, Argus is headquartered in Tel Aviv, Israel, with offices in Michigan, Silicon Valley, Stuttgart and Tokyo. Learn more at www.argus-sec.com.

Argus is an independent company of Elektrobit, a leading provider of automotive software products and services.

Tel Aviv, Israel – Global HQ and R&D Center
T. +972 77 899 5100
E. contact@argus-sec.com

Detroit, Michigan - North America HQ
T. +1 248 385 8781
E. usoffice@argus-sec.com

Stuttgart, Germany – EMEA HQ
T. +49 7021 8668 999
E. emea@argus-sec.com

Tokyo, Japan - APAC HQ
T. +81-80-5094-4562
E. japan@argus-sec.com

Redwood City, California - West Coast Office
T. +1 650 283 4402
E. westcoast@argus-sec.com

Shanghai, China - China Office
T. +86-21-60431951
E. china@argus-sec.com