RUNSAFE
SECURITY

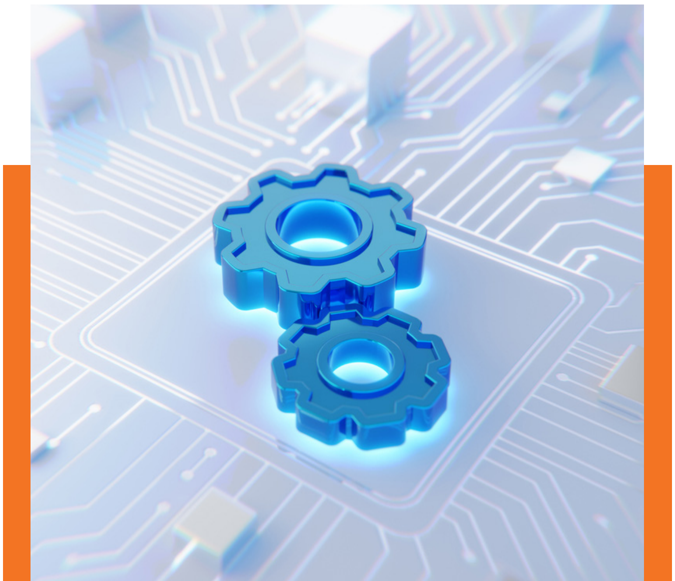
USE CASE

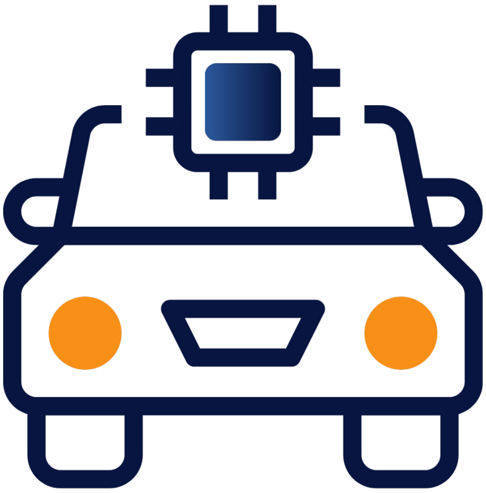
Securing Electronic Control Units (ECUs) in Autonomous Vehicles

INDUSTRY
Automotive

OVERVIEW

Electronic Control Units (ECUs) are critical components of autonomous vehicles (AVs) that control crucial systems, like braking, acceleration, and steering. These embedded systems communicate via Controller Area Network (CAN) bus or Ethernet and operate independently of an OS. Internal Combustion Engine (ICE) vehicles typically average about 70 ECUs, whereas AVs rely on hundreds of ECUs to process data from various sensors necessary to navigate and react to current road conditions.





CHALLENGE

ECUs are most commonly programmed in languages like C and C++, leaving these systems susceptible to memory safety vulnerabilities. One of the most prevalent memory safety issues in ECUs is buffer overflow vulnerabilities. These occur when data is written beyond the bounds of allocated memory, which can lead to unauthorized access and control. An attacker that exploits a memory-safety vulnerability in the ECU firmware could take runtime control and cause erratic vehicle behavior.

SOLUTION

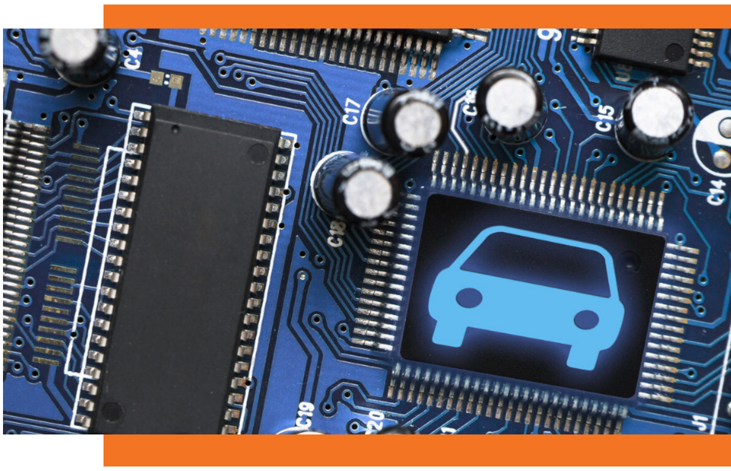
RunSafe offers a memory-based cybersecurity solution designed to keep ECUs in autonomous vehicle systems secure against known and unknown threats.

Key features of RunSafe's solution include:

- **Automated mitigation and code protection:** RunSafe's solution continuously monitors automotive embedded software systems for potential risks, identifying and mitigating risks before they can impact vehicle safety and operation.
- **Minimized attack surfaces:** By using unique technology to cyberharden vehicle components, RunSafe reduces opportunities for attackers to exploit memory safety vulnerabilities and take control of critical systems.
- **Seamless integration:** RunSafe's cybersecurity measures are easily integrated and align with existing automotive safety standards (such as ISO/SAE 21434 and ISO 26262), improving compliance and enhancing the overall safety of vehicle systems.
- **Futureproof from zero day threats:** By protecting against known and unknown vulnerabilities and denying the building blocks of zero days, RunSafe prevents future attacks by eliminating the entire class of memory safety vulnerabilities.

KEY FEATURES

- Automated Mitigation and Code Protection
- Minimized Attack Surfaces
- Seamless Integration
- Futureproof from Zero Days



Example

Enhancing autonomous vehicle safety: RunSafe offers collaboration with automotive companies to ensure the safety of autonomous vehicles. By implementing cybersecurity measures that comply with ISO 26262 standards, RunSafe can help protect autonomous systems from cyber threats, ensuring their safe operation.

Example Vulnerability: CVE-2022-42431: CVE-2022-42431 is a critical vulnerability discovered in Tesla Model 3 vehicles. The vulnerability is classified as a classic buffer overflow, specifically affecting the bcmdhd driver. The vulnerability allows local attackers to escalate privileges on affected Tesla vehicles and potentially execute arbitrary code on the target system.

RUNSAFE
SECURITY

🖥 www.RunSafeSecurity.com

☎ 571.441.5076

✉ Sales@RunSafeSecurity.com

ABOUT RUNSAFE SECURITY, INC.

RunSafe Security proactively protects embedded software for both commercial and defense deployments across critical infrastructure, with comprehensive risk identification, protection, and monitoring, ensuring robust, continuous security without affecting performance. Headquartered in McLean, Virginia, with an office in Huntsville, Alabama, RunSafe Security's customers span the aerospace, defense, energy, industrial, and national security verticals.