RUNSAFE SECURITY

USE CASE

Defending Advanced Driver Assistance Systems (ADAS)

INDUSTRY
Automotive

OVERVIEW

Advanced Driver Assistance Systems (ADAS) enhance safety using sensors, cameras, radar, and complex software. Examples of ADAS include lane keeping assist, which centers the vehicle in its lane; traffic jam assist, which manages speed and steering in slow traffic; and automated emergency braking, which prevents collisions. Specific safety features such as Forward Collision Warning with Autobrake have reduced front-to-rear collisions by 50% and injuries by 56%.

CHALLENGE

Advanced Driver Assistance Systems that are written in languages like C or C++ are at risk of memory safety vulnerabilities like buffer overflows, dangling pointers, and potential exploitation and software crashes due to improper memory handling. Memory safety vulnerabilities in an automotive software pose a significant safety risk because a successful attack could alter sensor data or decision-making algorithms, endangering the vehicle's safety. For example, memory corruption in sensors could result in incorrect object detection, leading to collisions or other dangerous situations.

SOLUTION

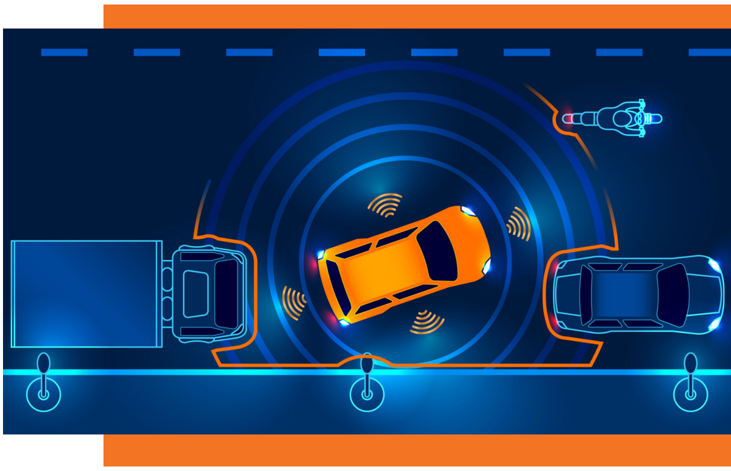
RunSafe offers a memory-based cybersecurity solution designed to keep ADAS safe and secure against known and unknown vulnerabilities.

Key features of RunSafe's solution include:

- **Protect Vehicle Safety and Security**
  Fortify critical systems like braking and steering against cyber attacks. Millions of lines of code create a large attack surface. RunSafe provides automated cybersecurity protection from source to runtime, reducing vulnerabilities and enhancing vehicle safety.
- **Comply with Automotive Regulations**
  Accelerate compliance with increasing regulatory requirements. RunSafe's cybersecurity measures are easily integrated and support existing automotive safety standards (such as ISO/SAE 21434 and ISO 26262), improving compliance and enhancing the overall safety of vehicle systems.
- **Enable New Automotive Technologies**
  Strong cybersecurity measures are essential for implementing emerging automotive technologies at scale. RunSafe's solution continuously monitors automotive embedded software systems for potential threats, identifying and mitigating risks before they can impact vehicle safety and operation.

KEY FEATURES

- Protect Vehicle Safety and Security
- Comply with Automotive Regulations
- Enable New Automotive Technologies



Example

Enhancing 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.

Securing telematics and communication systems: RunSafe stands ready to partner with automotive manufacturers to secure telematics and communication networks within connected vehicles. By implementing RunSafe's advanced cybersecurity solutions, automotive manufacturers can protect against potential cyber threats, ensuring the safe and efficient operation of their fleets.

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.