KARAMBA AND WIND RIVER

Karamba Runtime Integrity Technology and Wind River Certifiable Operating System and Virtualization Platform Combine to Secure Connected Cars

Karamba, with its runtime integrity technology, and with its certifiable OS and virtualization platform—part of the Wind River Chassis portfolio of safe and secure automotive software—have partnered to secure the future of connected cars.

The joint solution from Karamba and Wind River will support original equipment manufacturers (OEMs) and Tier 1 suppliers in their improvement of in-vehicle security by hardening ECUs to preserve original factory settings. During development, Karamba's Autonomous Security® automatically defines the full image golden behavior as a secure profile and then assures, via control flow integrity (CFI), that there are no deviations from the secure profile in runtime. As connected and autonomous cars evolve, this collaboration will allow automakers to ensure customer trust by preventing the most pervasive fileless attacks that can take control of the car.

KEY ADVANTAGES OF THE SOLUTION

Leveraging this safe, secure, and reliable consolidated compute platform from Wind River, Karamba's runtime integrity technology can secure in-vehicle systems, from infotainment and TCUs to autonomous driving and V2X ECUs. With low-performance impact, both in latency and footprint, the combined technologies allow automakers and suppliers to deploy turnkey, automotive-grade solutions with fast time-to-market.

Key benefits include:

- A preventive solution against advance attacks, with continuous runtime ECU protection
- Minimization of the security overhead normally associated with security solutions:
  - No false positive
  - No need for lengthy and expansive investigation of detected anomalies
  - No need for constant over-the-air updates
- Seamless integration into the build process, with no impact on development processes or time-to-market
- Negligible impact on ECU performance, making it suitable for demanding embedded systems

KARAMBA SECURITY

Karamba algorithms and policy enforcement processes enable manufacturers of connected devices to meet security requirements using minimal resources, without affecting real-time operations.

Karamba Security

Ecosystem Component

Runtime integrity technology

Solution

Automotive security

Value

- Preventive solution against in-memory attacks and zero-day threats
- No false positive alerts, no OTA updates, no development intervention

MORE INFORMATION

Detailed information about Karamba Security can be found at www.karambasecurity.com.

Information about the runtime integrity technology and the autonomous security approach can be found at www.karambasecurity.com/approach.

Detailed information about Wind River Chassis can be found at www.windriver.com/automotive.

Karamba Security has developed award-winning, patented, and patent-pending technology that blocks automotive attack vectors on multiple levels, including at exploits in the ECUs themselves (via Carwall®) and at authentication loopholes in the in-car networks through which the ECUs exchange information (via SafeCAN®).

Initially introduced to the automotive market, Karamba Security enhanced and extended its unique security technology to embedded and networking devices. The deterministic approach eliminates false positives, as security decisions are not based on heuristic predictions using statistics calculations.

Karamba Security was founded in 2016. It has offices in the U.S. (Detroit and San Francisco), Israel, and Europe (including an office in Munich), as well as a representative in Japan.

WIND RIVER CHASSIS

Chassis brings together software, technologies, tools, and services to help automotive manufacturers unify, simplify, and maintain the software systems within vehicles and help manage their connectivity to IoT. It incorporates all the components needed to define and integrate systems for controlling the entertainment, navigation, drivetrain, safety, and connectivity systems throughout intelligent, connected, and autonomous vehicles.

Leveraging its proven technologies that deliver software for devices subject to the highest standards of safety, security, and performance, the Wind River Chassis portfolio of automotive software includes VxWorks®, Wind River Drive, Wind River Edge Sync, and Wind River Diab Compiler, along with complimentary tools and services. The Chassis portfolio provides OEMs with a software framework for the next-generation automobile that includes tested and certified virtualization technologies that allow the secure consolidation of computing workloads.

VxWorks is the market-leading real-time operating system (RTOS), tuned for both determinism and responsiveness, with a proven track record in safety- and security-certified environments across multiple industries. VxWorks is also ISO 26262–certified to ASIL-D by TÜV. The market's most tested and certified virtualization solution, VxWorks allows for workloads to be consolidated with static and dynamic configuration options for heterogeneous mixed criticality OSes, with safety-critical and noncertified applications sharing a common platform.

SUMMARY

As cybersecurity becomes a priority for the future of smart mobility, the partnership between Wind River and Karamba is putting forward a strong, combined solution that can prevent cyberattacks while offering simple deployment for connected ECUs. The companies are providing the industry with a state-of-the-art, secure platform that contributes to the evolution of the connected and autonomous vehicle.

WIND

Wind River is a global leader in delivering software for IoT. Its technology is found in more than 2 billion devices and is backed by world-class professional services and customer support. Wind River is accelerating digital transformation of critical infrastructure systems that demand the highest levels of safety, security, performance, and reliability.