Zero Trust. Zero Compromise. Embedded Security.

Automotive

Robotics

Maritime

Medical

Railway

Protecting critical embedded systems, IoT, and infrastructures

acce/erat

c/are

Hypervisor-Centric Software Stack for Mixed-Criticality Applications

Validation and Performance Measurements

User requirements

CLARE-Toolkit

Configuration output

Schedulers

QoS Regulators

Resource partitioning

Domains

Middleware

APPLICATION

CLARE-Middleware

Guest Bare-metal	Guest RichOS/GPOS	Guest RTOS	Guest RTOS
Low Critical	**Mid Critical**	**Mid Critical**	**High Critical**

CLARE-Hypervisor

EDGE HW PLATFORM
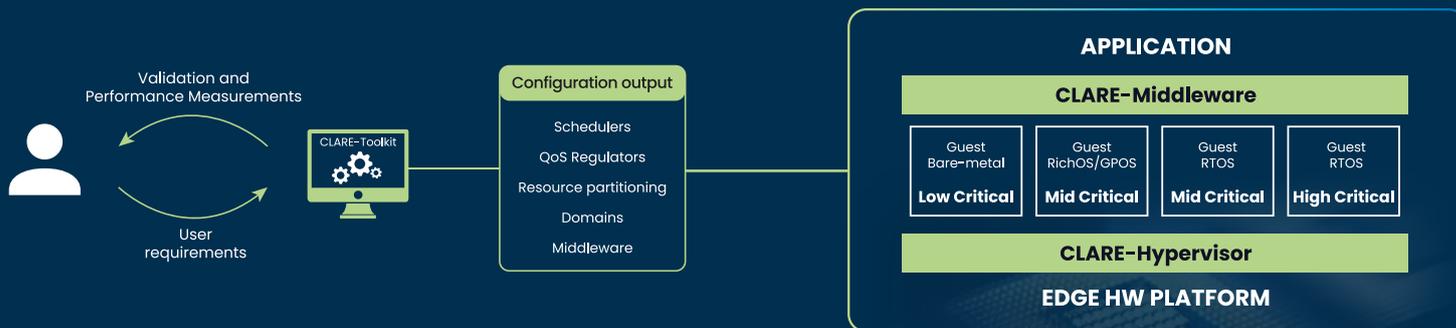
- ✓ **Next-Generation Proprietary Hypervisor Technology**
- ✓ **Multi-Security Classification**
- ✓ **Strong Isolation and Security Capabilities**
- ✓ **Best-in-class Event Latency and Minimal Overhead**
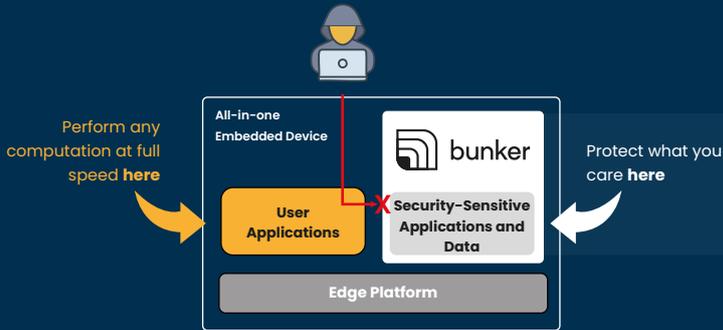- ✓ **Automatic Optimization of Configuration**

Functional-Safety & Cyber-security

ISO/IEC/EN

10K +
Secured Devices

bunkers

powered by c/are

The Ultimate Fusion of **Zero-Trust Security** and **Performance** at the Edge under the **Cyber Resilience Act (CRA)**

Perform any computation at full speed here

All-in-one Embedded Device

bunker

User Applications

Security-Sensitive Applications and Data

Edge Platform

Protect what you care here

- Robust Against Zero-Day Attacks
- Confidentiality, Integrity, and Availability
- Attack Monitoring, Recovery, and Secure Update
- Simplified CRA/ISO/IEC Compliancy
- Reduced Total Cost of Ownership (TCO) and Time-To-Market

Some Use Cases

Secure AI-Powered Intelligent Edge Device

AI bunker

embeddedaward2025
winner: Start-up

- AI Models Protected from Theft
- Secure Model Storage in Isolated Partitions
- Seamless Model Invocation
- Real-time Inference Performance

High Performance Linux-based Control System

bunker for linux

- Secure and Isolated Linux Applications
- Maximing Performance and Security
- Pay Performance Overheads when Needed
- Inter-Partition Seamless Communication

Supporting CRA Compliancy

embeddedaward2025
winner: Start-up