Secure Autonomy at the Edge

AI Security + Computer Vision for Robots

Axelera® AI and Kudelski Labs demonstrate secure, low-latency computer vision on KLARQ, an autonomous robot dog, combining **Kudelski Labs' keySTREAM** AI-accelerated security stack with Axelera AI's Metis® AIPU for on-device inference.

Executive Summary

True autonomy in security robotics depends on perception, intelligence, and trust. Together, Axelera AI and Kudelski Labs enabled KLARQ, an autonomous robot dog that illustrates how embedded security and computer vision make real-world Edge AI autonomy possible. KLARQ pairs Kudelski Labs' AI-accelerated security stack, keySTREAM device lifecycle management, with Axelera AI's Metis® AIPU for on-device inference.

KeySTREAM supports secure activation, firmware and device integrity, real-time threat detection workflows, and compliance-ready lifecycle controls, helping ensure hardware identity and mission-critical firmware are authenticated and protected against tampering.

Metis is the on-device inference engine that makes KLARQ meaningfully autonomous. An external camera feeds live video into Metis so KLARQ can interpret its surroundings with low latency, running object detection, face detection, and face recognition in real-time to distinguish authorized "family" members from unfamiliar people.

Securing Autonomy at the Edge

Security robots often operate in "Mission Control" mode, receiving instructions and executing them in autonomous environments. This creates two primary business risks:

1) Robot Software Integrity: compromised firmware/pipelines and unauthorized control of the robot. Without a hardware-rooted security layer and lifecycle controls, edge devices are vulnerable to unauthorized firmware loading, model/pipeline manipulation, or hijacked mission protocols.

2) Inference Protection and Secure Execution: KLARQ combines a secure software layer with the Metis AIPU ensuring AI-driven actions are executed only after trust checks succeed, enforcing secure activation and integrity checks before inference pipelines run.

- **Root of Trust:** Establish device identity and trust before execution.
- **Firmware Integrity:** Verify firmware and critical components before mission start to reduce the risk of tampered code, altered pipelines, or unsafe behaviors.
- **Secure Execution:** Computer vision inference begins only once security checks pass, ensuring AI-driven behaviors are gated by trust, not just connectivity.

Architecture for Secure Intelligence

KLARQ's architecture is optimized for small form factor, low power, and low-latency reactions, pairing an edge host with an M.2 inference module and an AI-accelerated security stack.

- **AI Acceleration:** Axelera AI Metis AIPU (M.2 module with active cooling) with 214 TOPS running at 4-8 Watts of power.
- **Host Processor:** OrangePi single-board with a Rockchip processor and an M.2 slot.
- **Software:** Axelera AI's Voyager SDK; Ultralytics YOLOv5s v7.0 COCO ONNX model for object detection; RetinaFace Resnet50 widerface ONNX for face detection; FaceNet LFW for face recognition.
- **Security:** Kudelski Labs keySTREAM supports device lifecycle security and compliance management, from provisioning and secure activation through updates and retirement.

Achieved Results

KLARQ shows that on-device inference plus security gating enables autonomous AI while reinforcing security-first design principles for Edge AI robots.

- **Autonomous Object Tracking:** Autonomous Perception (low latency): Real-time object detection, face detection, and face recognition on-device ensuring the robot can assess its surroundings and react immediately without cloud round-trips. The AI models run in parallel across Metis' four independently programmable cores to support "sense → decide → react" behaviors without delay.
- **AI-Driven "Kill Switch":** The system features a visual safety protocol. When the AI recognizes a predefined symbol (for example, a stop sign), the robot immediately ceases activity and enters a safe state (for example, laying down).
- **Scalable Payload:** A repeatable external camera + M.2 AI accelerator + security stack package that can be adapted to other robotic and edge form factors.

Conclusion

The partnership between Axelera AI and Kudelski Labs demonstrates that high-performance AI innovation and uncompromising security can coexist at the edge. Metis provides the on-device computer vision inference that makes KLARQ responsive in real time, while Kudelski Labs' keySTREAM AI-accelerated security stack and lifecycle capabilities help ensure the device is securely activated, verified, and managed over time. Together, they provide a practical blueprint for secure autonomy: low-latency, on-device decision-making with trust controls that are foundational, not bolted on later.

About Axelera:

Axelera AI delivers high-performance, power-efficient AI acceleration for the edge. Its Metis AI platform combines the Metis AIPU with the Voyager SDK, which automatically compiles, optimizes, and deploys computer vision pipelines, using host processors (CPU, embedded GPU, or media accelerator) and the AIPU as required.

Visit us at Axelera.ai

About Kudelski Labs:

From pioneering the first portable audio recorder to driving the latest breakthroughs in artificial intelligence, data science, chipset security and quantum-resistant solutions, the Kudelski Group leads the development of cutting-edge and intelligent core security solutions.

For more details visit KudelskiLabs.com or LinkedIn

AXELERA
ARTIFICIAL INTELLIGENCE

Visit us at Axelera.ai