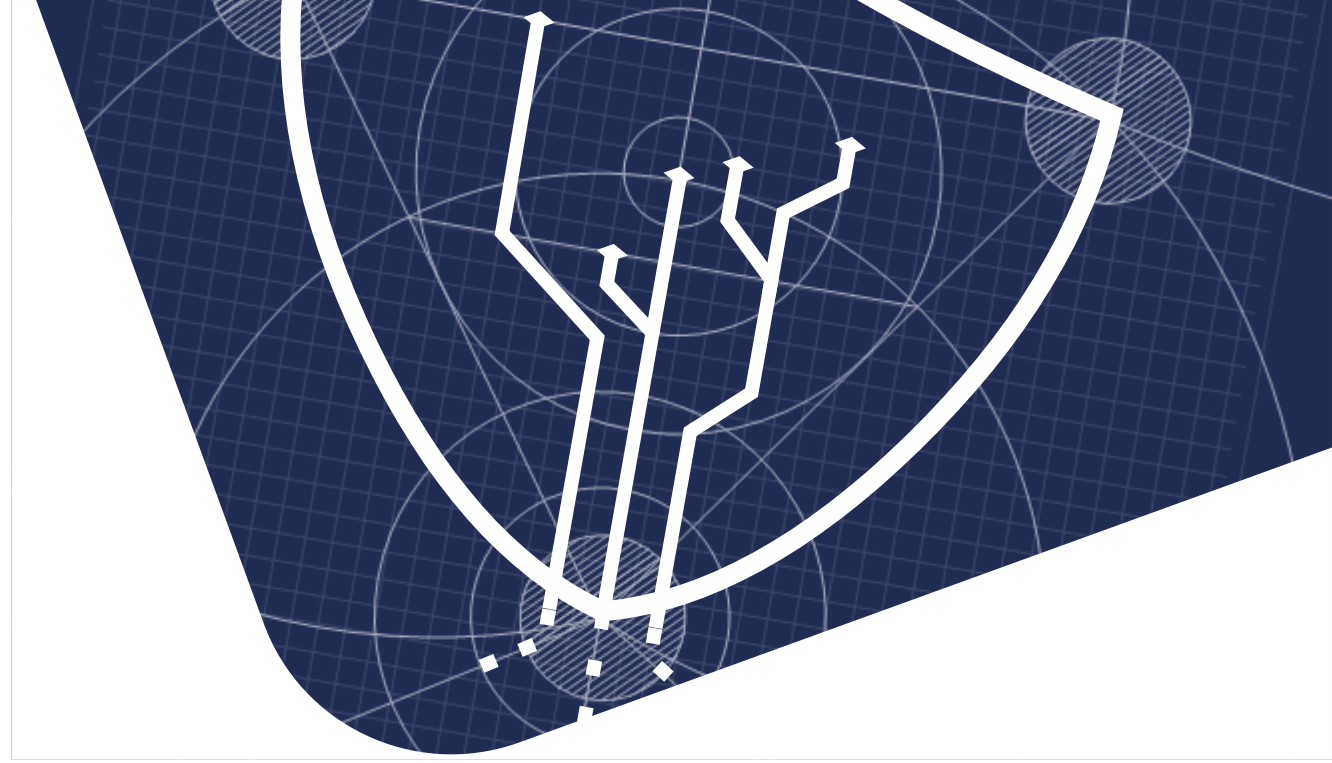




June 2026

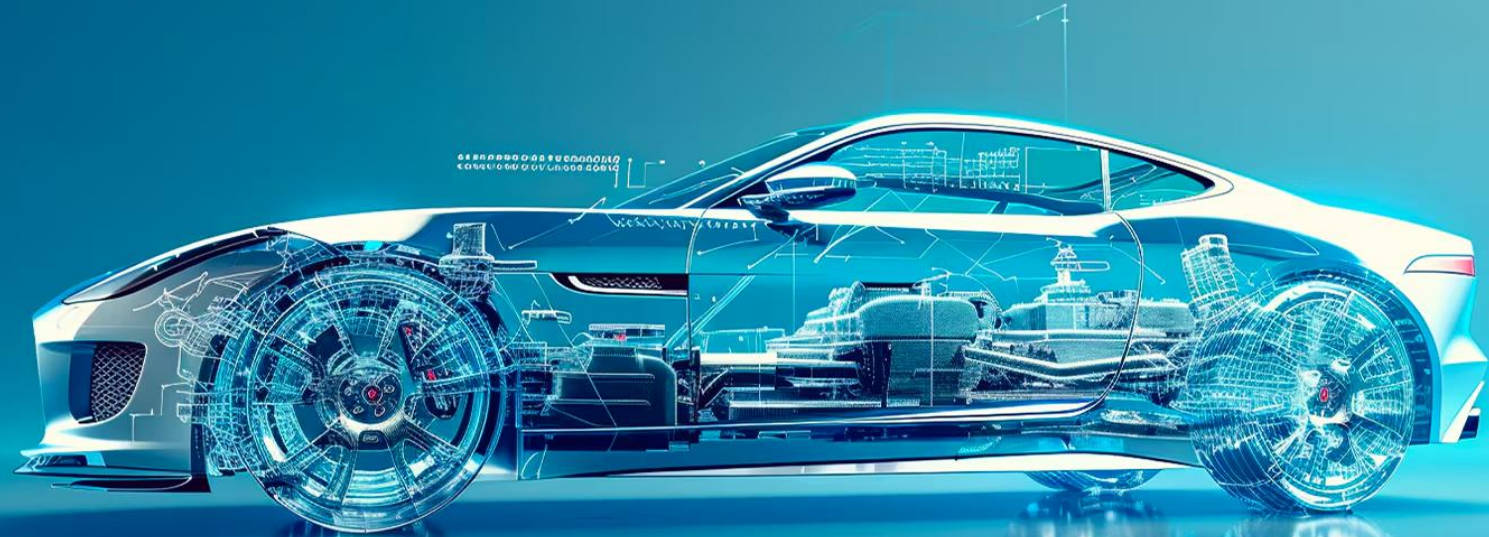
From Chip to Cloud: Securing AI Where It Meets Physical Reality

Closing the Gap: Semiconductors, AI, and Europe's Competitive Future

Christophe Nicolas, SVP Kudelski Labs & Group CIO, Kudelski Group

Münich stands at the heart of automotive innovation, bringing together world-leading OEMs, advanced engineering expertise and a thriving ecosystem driving the future of connected, software-defined mobility.

At the time AI is emerging into the Physical World...



The Automotive Industry Has Been Here Before

- The Model T didn't build a faster horse — it replaced the entire system of how we move
- Real innovation doesn't improve the existing. It reframes the problem
- Physical, autonomous AI-based vehicle is our “faster horses” moment

Every leap in mobility looked effortless — but it was built on engineering that no one saw



“If I had asked people what they wanted, they would have said faster horses.”

Henry Ford

AI Is Moving Into the Physical World

- Intelligence is migrating from the cloud — into remote physical devices, infrastructure and industrial systems
- Real-world systems now fuse software, hardware and AI into a single device full of sensors, but not without risk
- The Model T arrived before safety caught up. Innovation came first; security, governance and regulation came later

AI is today's Model T moment — capability racing ahead of broader governance



The Challenge Is Trust — Not Capability

- A self-driving car is the end-point: autonomous AI making real-time, life-or-death decisions at the edge
- When autonomous AI steers two tonnes of metal — a lack of security becomes a safety problem
- The barrier isn't capability — it's data integrity, system resilience, rising threats and 15-year+ lifecycles

Inadequate security means physical devices operating autonomously create a safety risk long before they create an IT risk



Cloud-Centric Software Security Is Not (good) Enough

- Securing physical, autonomous AI from the cloud adds latency and enlarges the attack surface
- Security is having its **'Mythos' moment**". Defense is not about finding the fault, it's about making sure it doesn't hand over control
- Security needs to be **embedded** in the device where the decisions are being made
- Risks occur when physical devices, running in real-time, leave the network unexpectedly

Physical AI operates in unpredictable environments often without a reliable connection



A Strategic Moment for Europe

- Hyperscale platforms are dominated today by the US and China
- The growth and rollout of physical AI requires a semiconductor approach that supports supply chain sovereignty and control
- The ability to deploy trusted AI at the edge, at scale will define competitiveness

The winners won't build the smartest model. They'll deploy AI that is trusted, controlled and resilient



How Kudelski Labs Are Solving the Problem

- Embedding HW based secure enclave into autonomous robots to secure against malicious threats, evolving at the pace of Mythos enhanced AI model
- Combining embedded security directly into edge AI hardware for secure, on-device inference
- Enabling secure activation, lifecycle management, and continuous integrity for real-world operating environments

***This is secure, physical AI in action.
At the edge, in the real world***



Kudelski Labs – Securing Physical Edge AI at Scale



- Physical AI is our Ford T moment, transforming our ecosystem as never before
- Embedded security at the silicon level to establish a hardware root of trust
- Device identity and lifecycle management from provisioning through deployment and updates
- Security evaluation, design, certification and compliance
- End-to-end system security across devices, infrastructure, and connected ecosystems

The engineering discipline that turns secure, physical AI into scalable real-world applications





Thank You

Christophe Nicolas

SVP, Kudelski Labs & Group CIO
Kudelski Group

KUDELSKI
—  **LABS**
www.kudelskilabs.com