

Secure Edge AI

JAAKKO ALA-PAAVOLA

Embedded Conference Finland

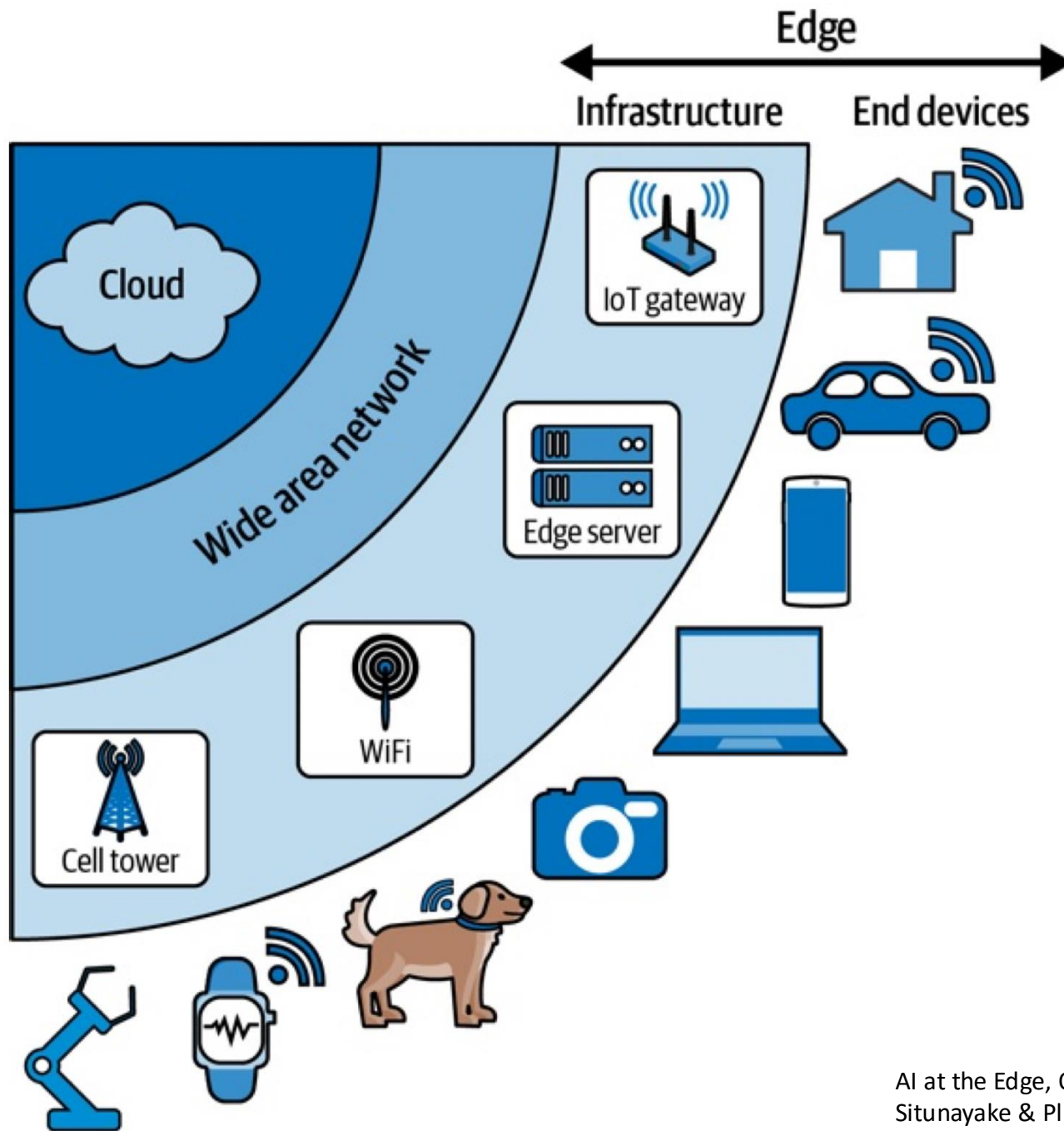
Helsinki 2025-09-16



Jaakko Ala-Paavola

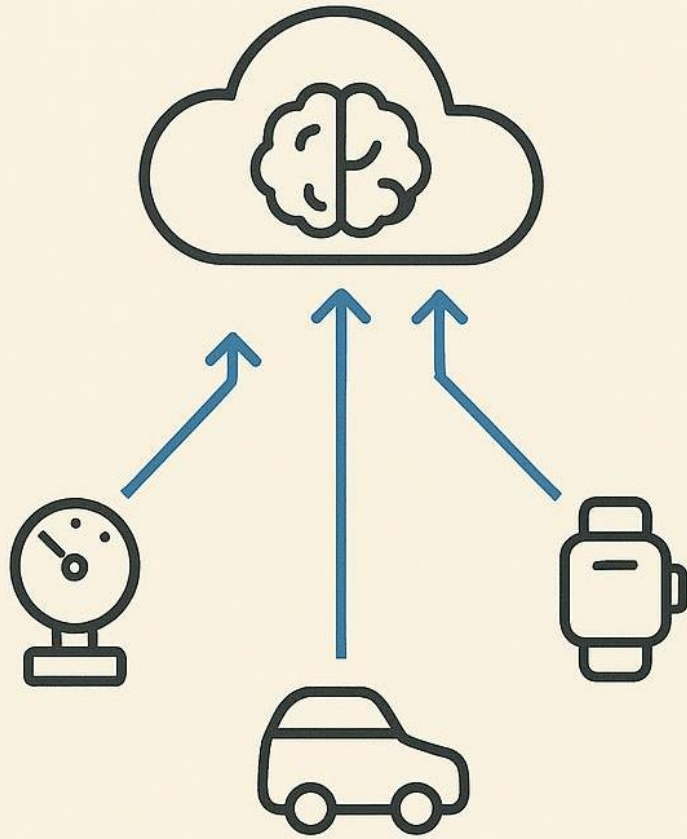
Technology Director, Etteplan



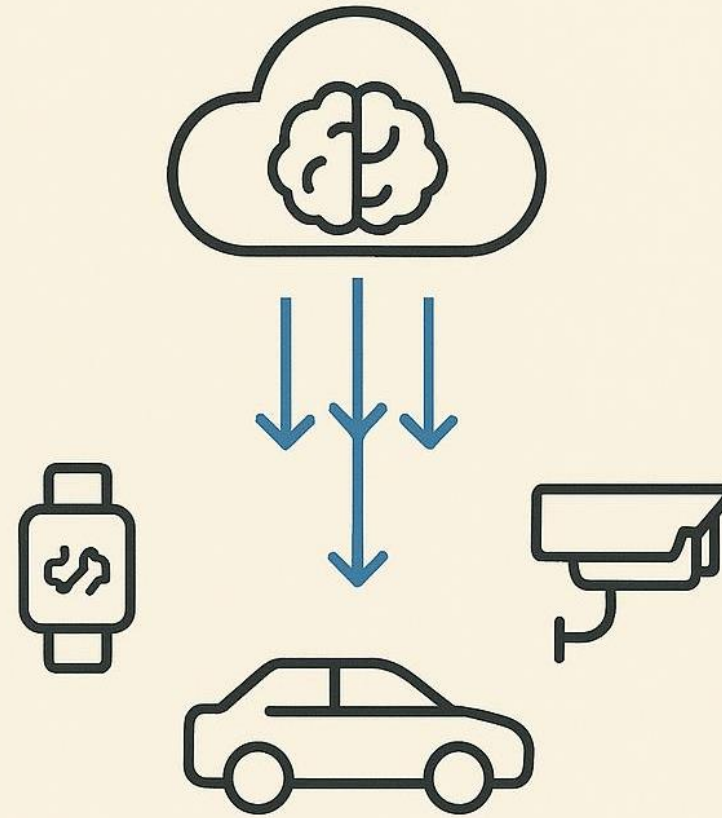


Edge

Edge AI



Traditional Cloud



Edge

Edge vs Cloud

Cloud :

It's just someone else's computer

Edge vs Cloud

Cloud :

It's just someone else's computer

Edge :

It's in someone else's hands



Fast Real-Time



Sensitive Data

Why Edge AI?

No Connectivity



Critical Infrastructure



New regulations on **Entities** and **Products** start applying

Secure-by-design becomes mandatory for products and operational systems in EU

Cyber security

NIS
Medical Devices
IVD Devices
Civil Aviation

GDPR

2016-2023

High risk AI safety

NIS2
General Product
Safety Regulation

Road Vehicles
Ships

Radio Equipment
Directive 3(3)def

EU CSA/EUCC

Data Act

2025

Use data sharing

**Cyber
Resilience Act**

Product Liability
Directive

Data Act

2026

**Cyber
Resilience Act**

**Machinery
Regulation**

AI Act

2027

AI Act



EU 2024/1689

2025/02

- Prohibitions
- AI Literacy

2025/08

- General purpose AI

2027/08

- High-risk AI systems

Exempts:

- Defense and national security, scientific research, non-professional

AI Act – Risk categories

Unacceptable – unethical – banned

- Analysis and manipulation of human behavior, social ranking, criminal offence risk assessment, emotion recognition, real-time remote biometric identification

High risk – fundamental rights – conformity assessment

- Safety component in products, critical infrastructure and transport, law enforcement and justice, health, education, recruitment, credit scoring, migration and border control

Limited risk – information alternation – transparency obligations

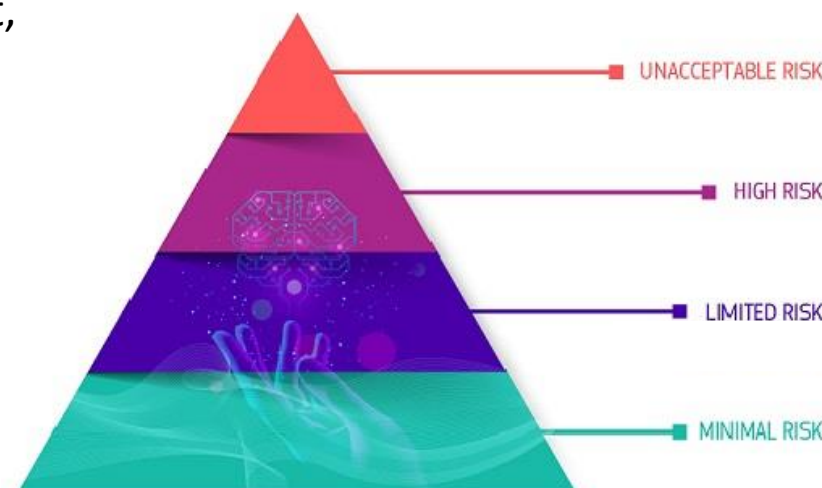
- Generate and manipulate data (image, video, sound), chatbots, informed decision making

Minimal risk – entertainment – no requirements

- Video games, content filtering

General purpose AI – reduced requirements

- Foundations models (LLM), free and open source licenses



<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

AI Act – High risk systems

Requirements

- Risk assessment & management system
- Data governance
- Technical documentation
- Record-keeping
- Transparency
- Human oversight
- Robustness and Cyber security 

Obligations

- Quality management system
- Documentation keeping
- Automatically Generated Logs
- Processes for corrective actions and Duty of information
- Cooperation with authorities
- Authorized representatives
- Fundamental rights impact assessment

AI Act – High risk systems

Requirements

- Risk assessment & management system
- Data governance
- Technical documentation
- Record-keeping
- Transparency
- Human oversight
- Robustness and Cyber security 

Obligations

- Quality management system
- Documentation keeping
- Automatically Generated Logs
- Processes for corrective actions and Duty of information
- Cooperation with authorities
- Authorized representatives
- Fundamental rights impact assessment
 - Human and civil rights
 - Social and economical rights
 - Political rights
 - Cultural and linguistic rights
 - Environmental rights

Edge AI example

HIPE (Human-technology interoperability and artificial emotional intelligence) project, funded by Business Finland and lead by VTT Technical Research Centre of Finland (5/2022-11/2025).

Read the summary

- ▶ The HIPE project has developed a new technology platform that uses AI and data from cameras, sensors, and audio-visual analysis to monitor passenger mood, provide real-time feedback, anticipate disturbances and enhance safety in trams and buses.
- ▶ Ethical considerations have been prioritised during development to ensure passenger anonymity and responsible use of AI.
- ▶ The project aims to create more responsive and comfortable public transport systems.

This summary is written by AI and checked by a human.

Suomessa kehitetty tekniikka tunnistaa rähinöitsijät ratikassa jo ennen konfliktia

VTT:n johdolla kehitetään ”tunnelmanhaistajaa” raitiovaunuihin. Tässä jutussa kerromme, mihin sen toiminta perustuu.



Tarkkailua. Uudet tekniikat voisivat ennustaa rähinät raitiovaunussa. Kuvituskuva on Tampereen ratikasta. KUVA: TIINA SOMERPURO

Anturitekniikoiden avulla kyetään kenties jo muutaman vuoden kuluttua aistimaan tunnelmaa joukkoliikenteessä.

11.9.2025 08:30



Harri Repo

VTT:n vetämässä HIPE-projektissa on kehitetty palvelukonsepti, jossa video- ja äänitekniikan avulla kyetään analysoimaan matkustamossa vallitsevaa tunnelmaa. Tavoitteena on ennaltaehkäistä häiriökäyttäytymistä.

Lahjoita juttu

Tilaa tästä T&T:n maksuton uutiskirje - Kokoamme kiinnostavimmat artikkelit sähköpostiisi joka päivä.

”Matkustamon tunnelmaa arvioidaan analysoimalla matkustajien kasvonilmeitä, jonka perusteella tiedetään, onko tunnelma positiivinen, neutraali vai negatiivinen. Tieto

Edge AI example

“The system uses sensors to monitor passengers' movement and facial expressions, providing insights into passenger mood. This information can help operators anticipate disturbances, reduce safety risks, and create a more pleasant travel environment. Real-time data can be shared with traffic operators, drivers and security personnel.”

AI Act

Article 5: Prohibited AI Practices

1. The following AI practices shall be prohibited:
 - (d) the placing on the market, the putting into service for this specific purpose, or the use of an AI system for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence

Article 6: Classification Rules for High-Risk AI Systems

Annex III:

1. Biometrics
 - (c) AI systems intended to be used for emotion recognition.

Edge AI Security

Data Security

Algorithm Security

Platform Security

Edge AI Security

Data Security

- Quality
- Access

Algorithm Security

- Technology
- Tools

Platform Security

- Hardware
- Software

Edge AI Security - Platform

If you can't trust your device, how can you trust your data?

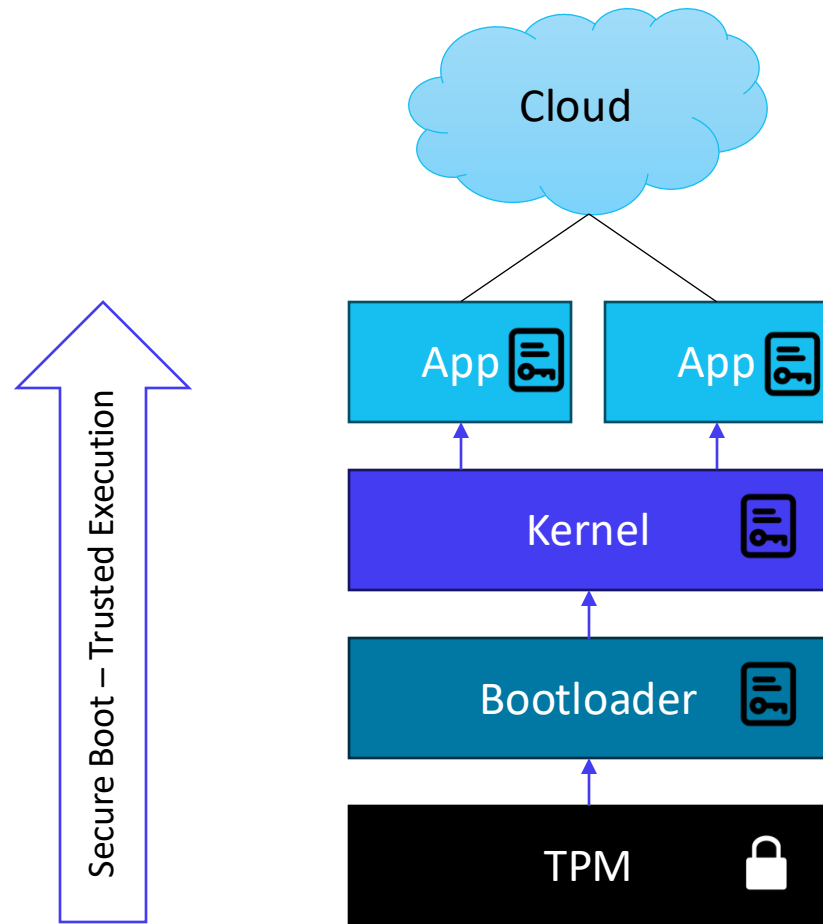
Extended attack surfaces, not only the Internet:

- Ports and services, physical connectors
- Hardware vulnerabilities, physical access
- Unused and unneeded features, testing interfaces
- Outdated software and legacy hardware
- Default credentials
- Unsecure interfaces to other field systems

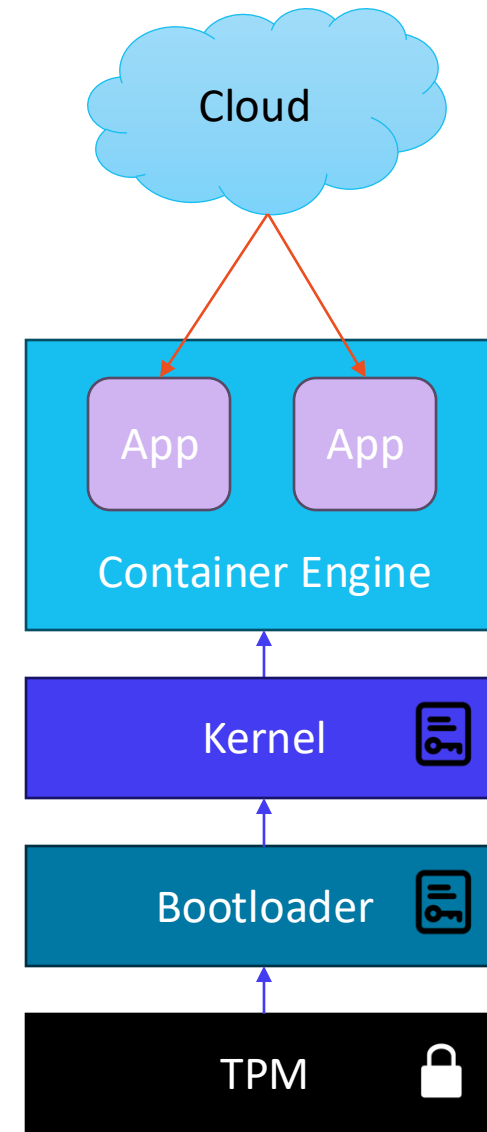
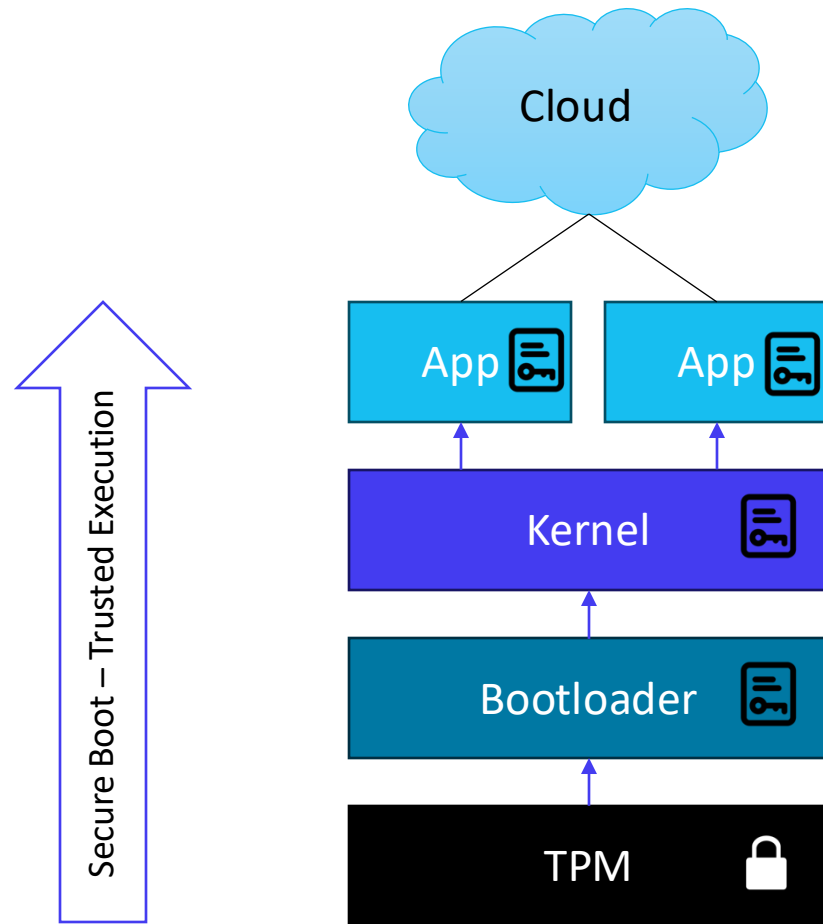
Advanced attack vectors:

- Deep Leakage from Gradients attacks
- Model Inversion attacks
- Membership Inference

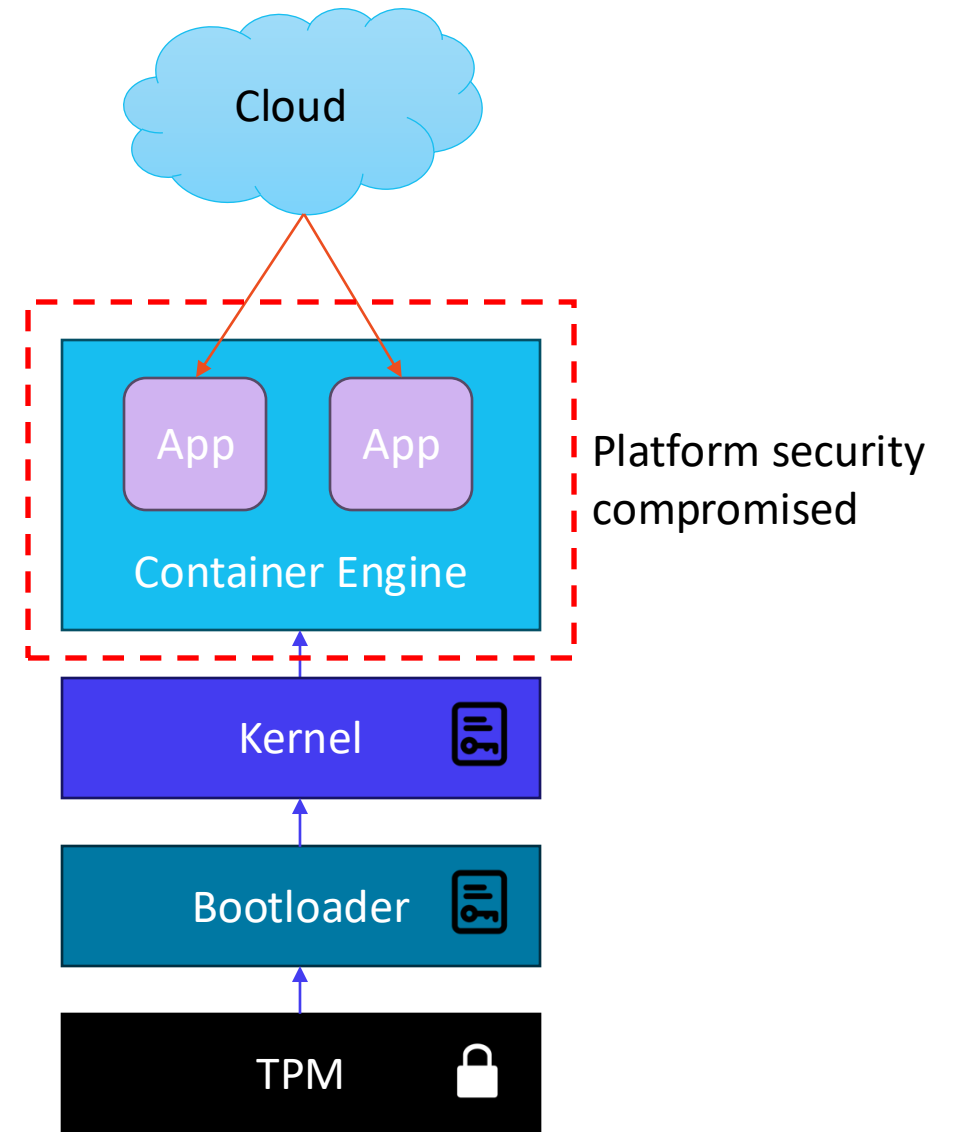
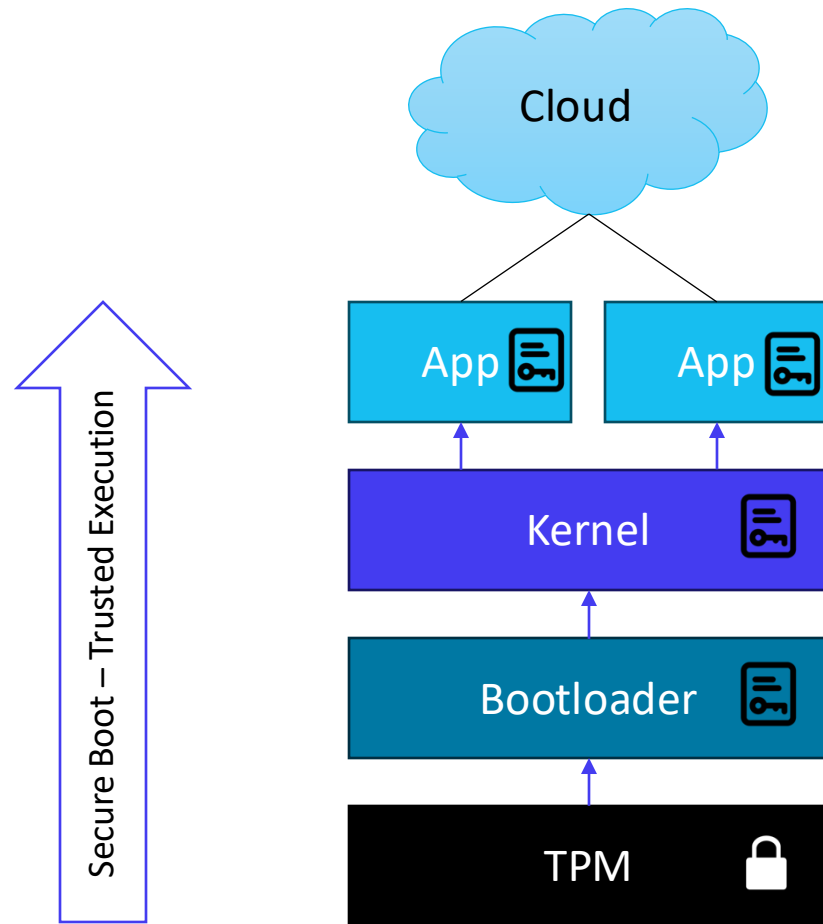
Platform Security



Platform Security



Platform Security



Platform Security

Open platform does not compromise security.
CRA-ready. IEC 62443-4-2 certified.



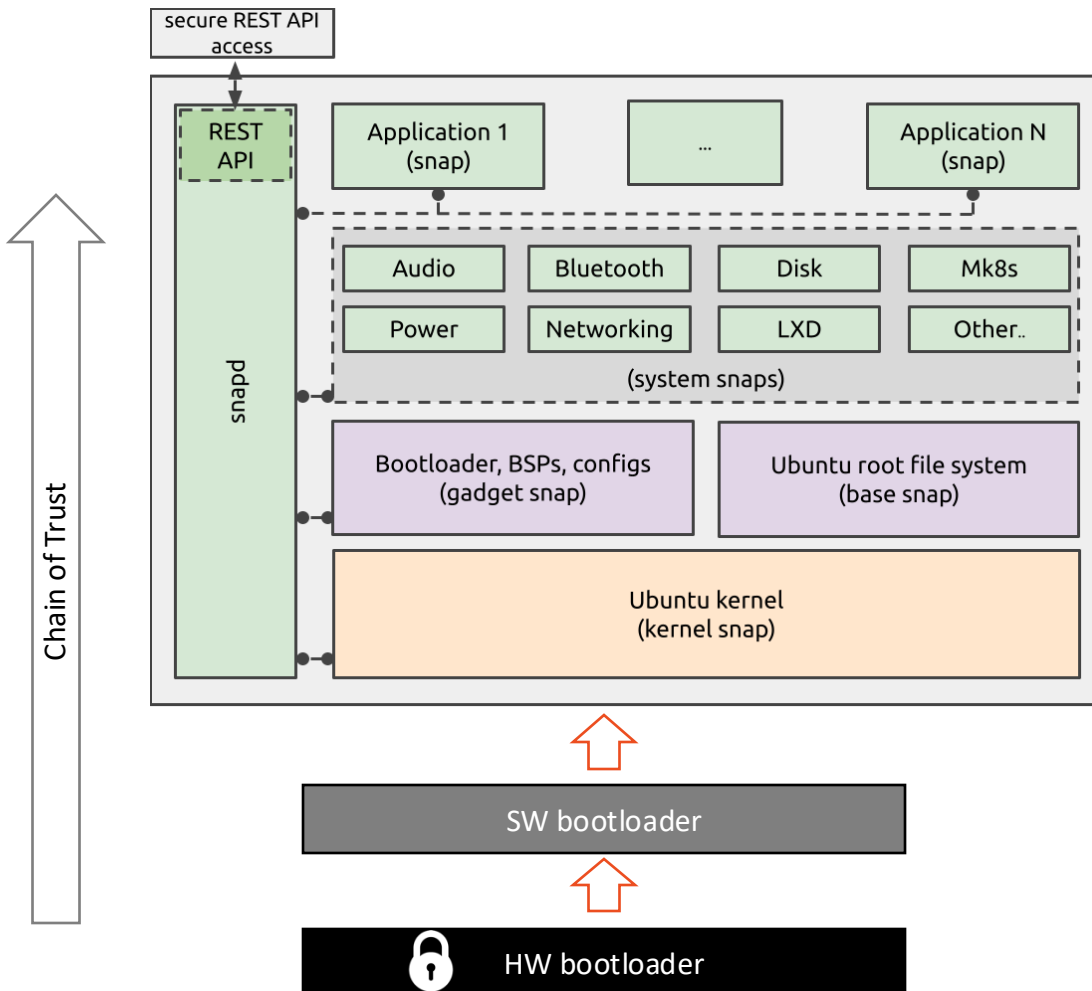
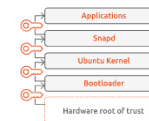
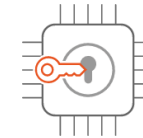
ctrlX OS
THE OPERATING SYSTEM FOR AUTOMATION

rexroth
A Bosch Company

Maintenance and Security Build-in:

Long-term commercial support

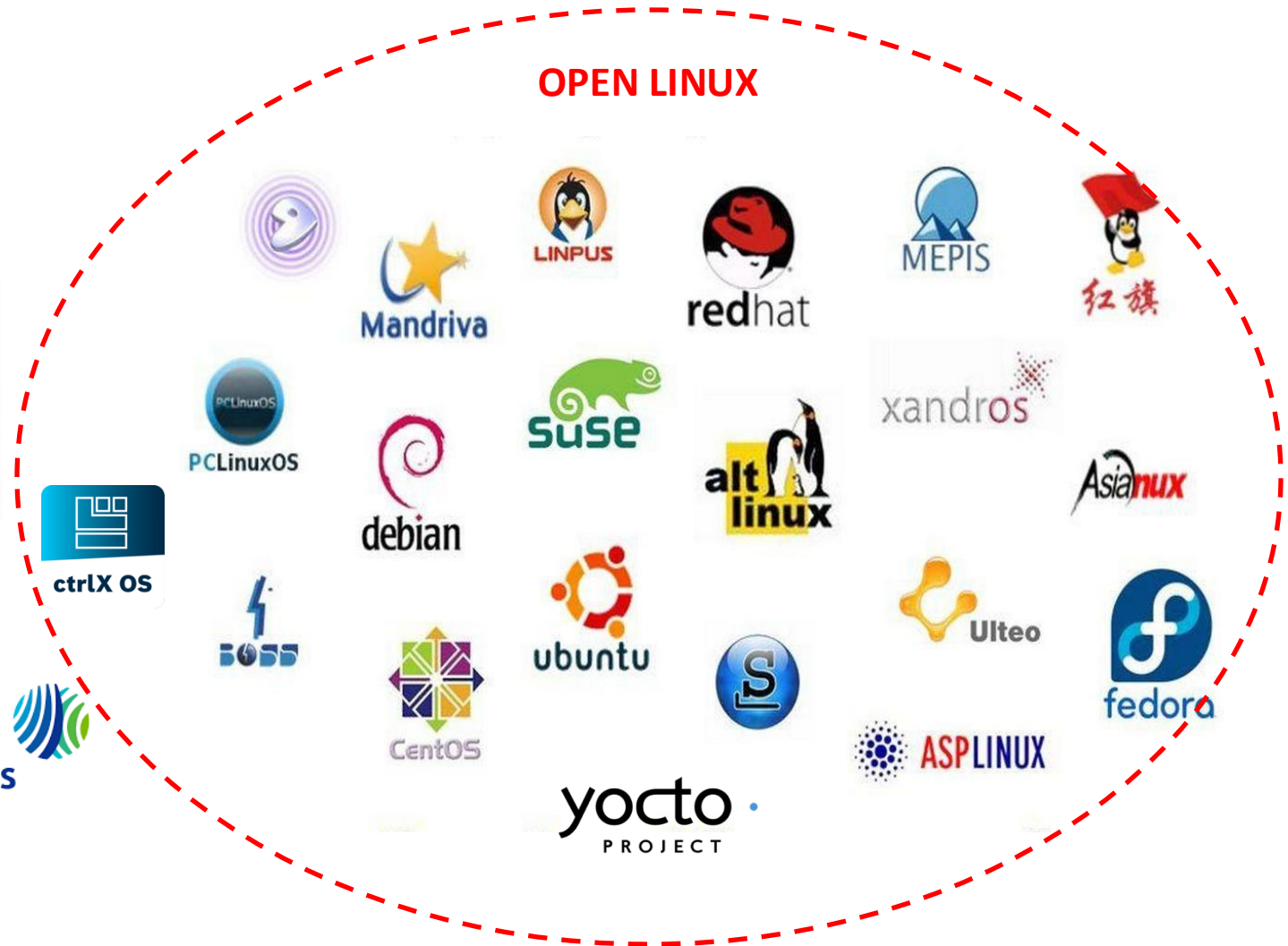
- Secure boot / Trusted execution
- Signed bootloader and snaps
- Secure element / Root of Trust
- Full disc encryption
- Snaps in compressed Read-Only FS
- Snaps are self-confined secure isolated dependency-free Linux packages
- Safe OTA upgrade / downgrade of applications and kernel snaps with fallback recovery.
- Device permission and interface security policies



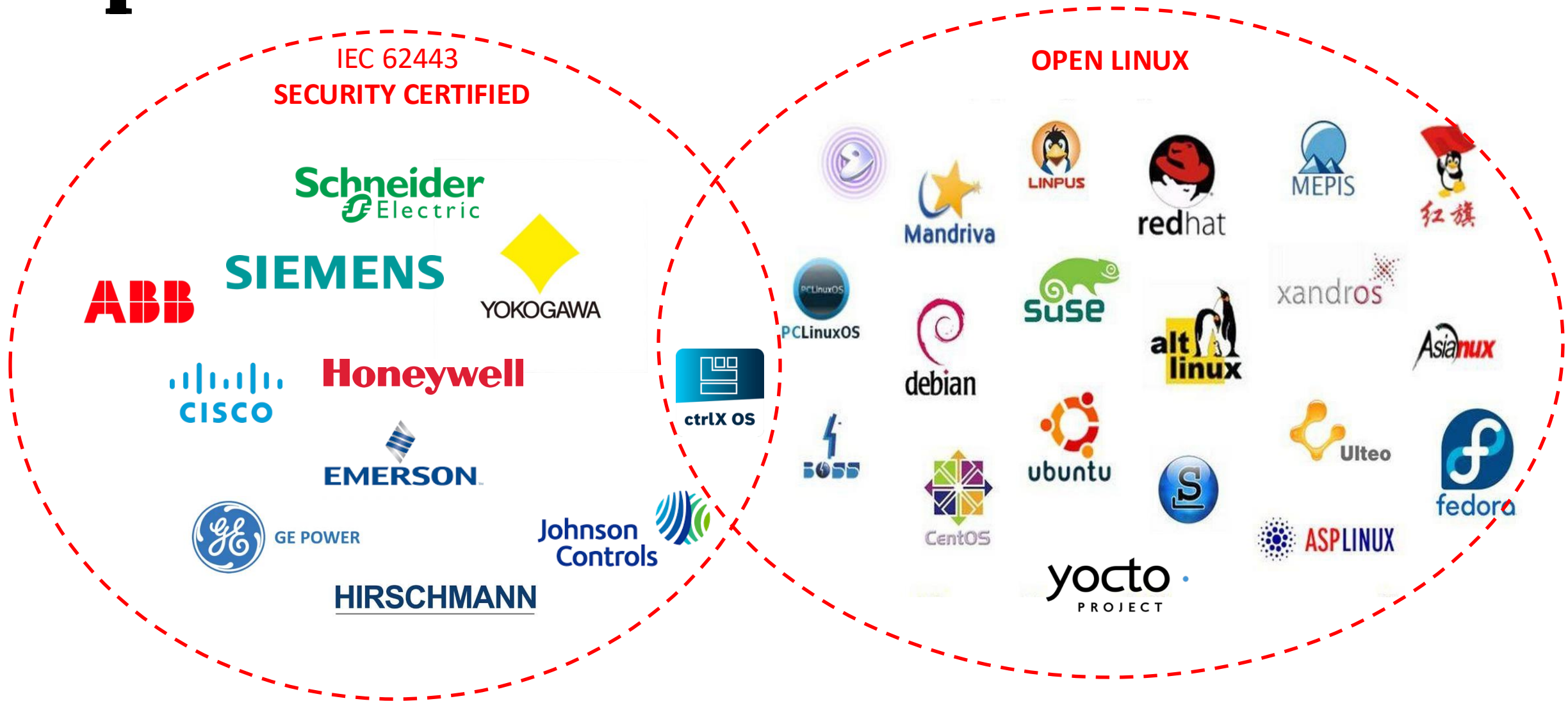
Open vs Secure



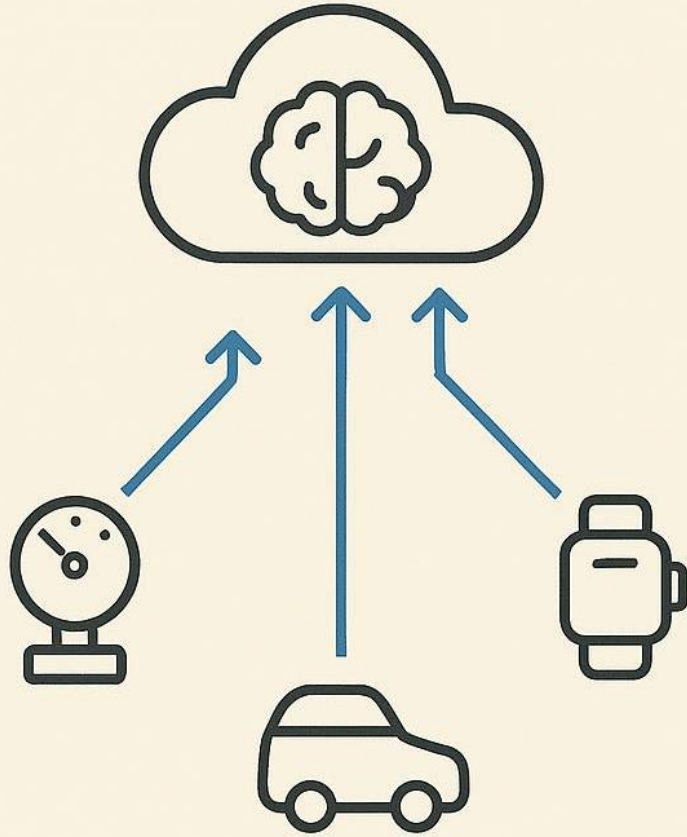
Open vs Secure



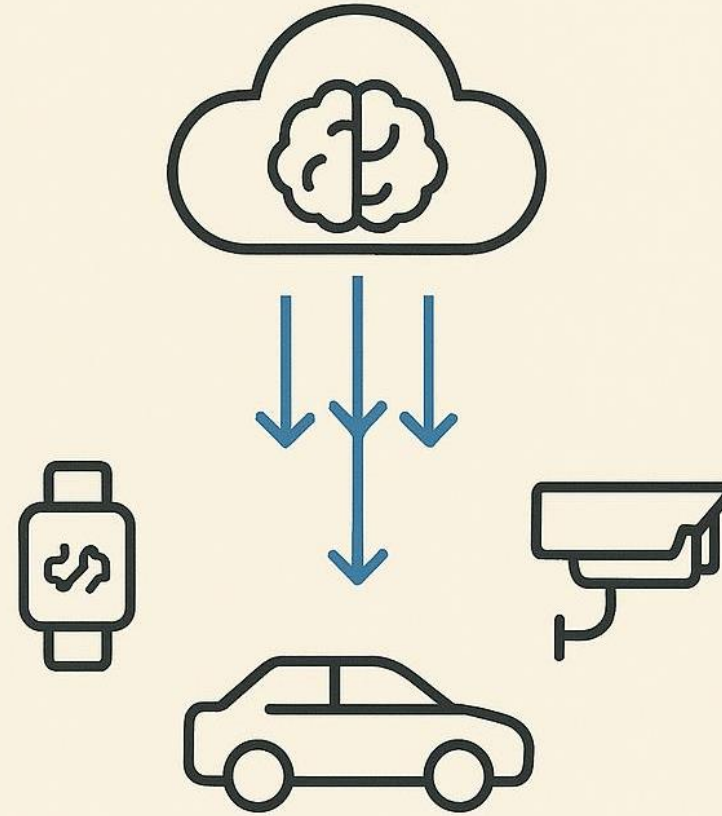
Open vs Secure



Algorithm & Data Security



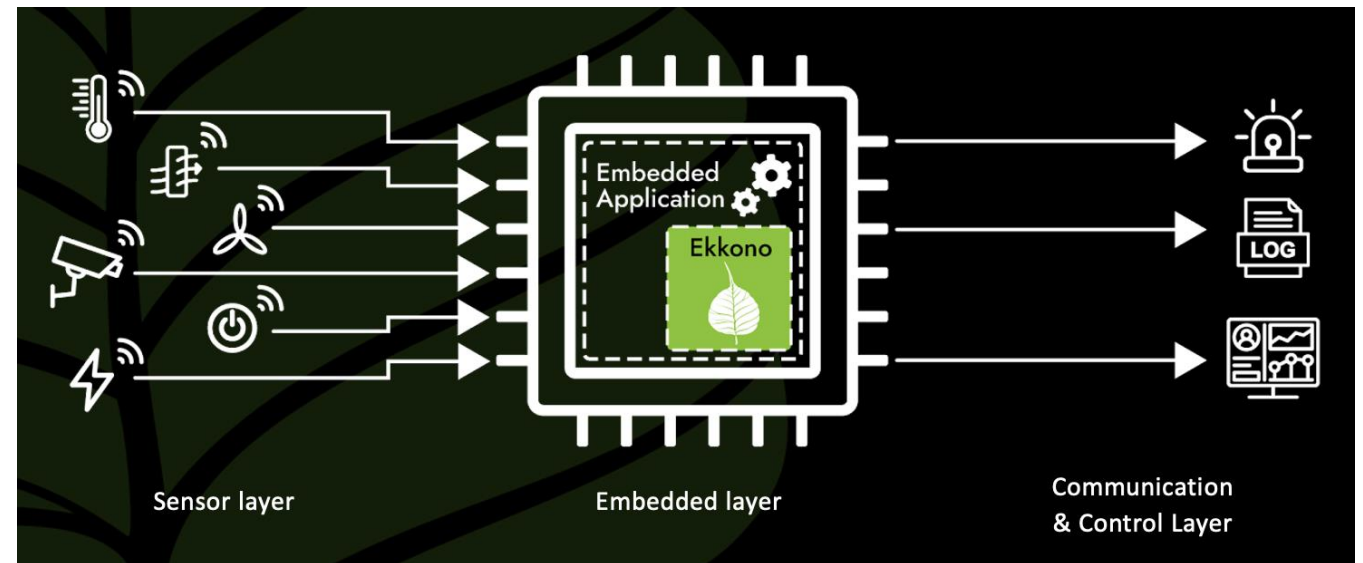
Deep Learning



Incremental Learning

Independent Incremental Learning

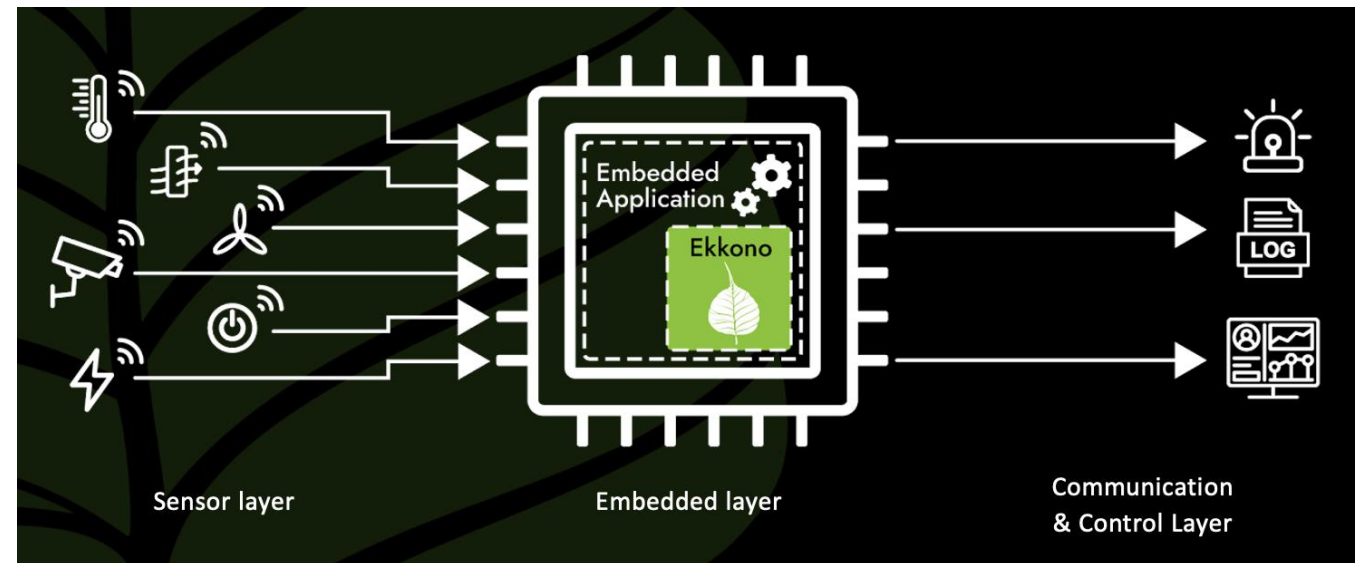
- Independent incremental learning of every unique point of deployment.
- Local machine learning for unique behavior and characteristics.
- Optimal for use cases where every deployment is unique.
- Data stay always on-site, never uploaded to cloud or other backend



Independent Incremental Learning

Use cases:

- ❖ Sensor data aggregation
- ❖ Condition monitoring
- ❖ Predictive maintenance
- ❖ Remaining usefull life
- ❖ Process optimization
- ❖ Product-as-a-Sensor
- ❖ Sensor virtualization & sensor condition monitoring



Etteplan Secure Edge AI

Industrial use-cases with
highest security requirements



Security build-in:

- Local data processing at the Edge, no cloud
- Incremental independent self-learning
- Build from secure components
- Full stack security with no compromise

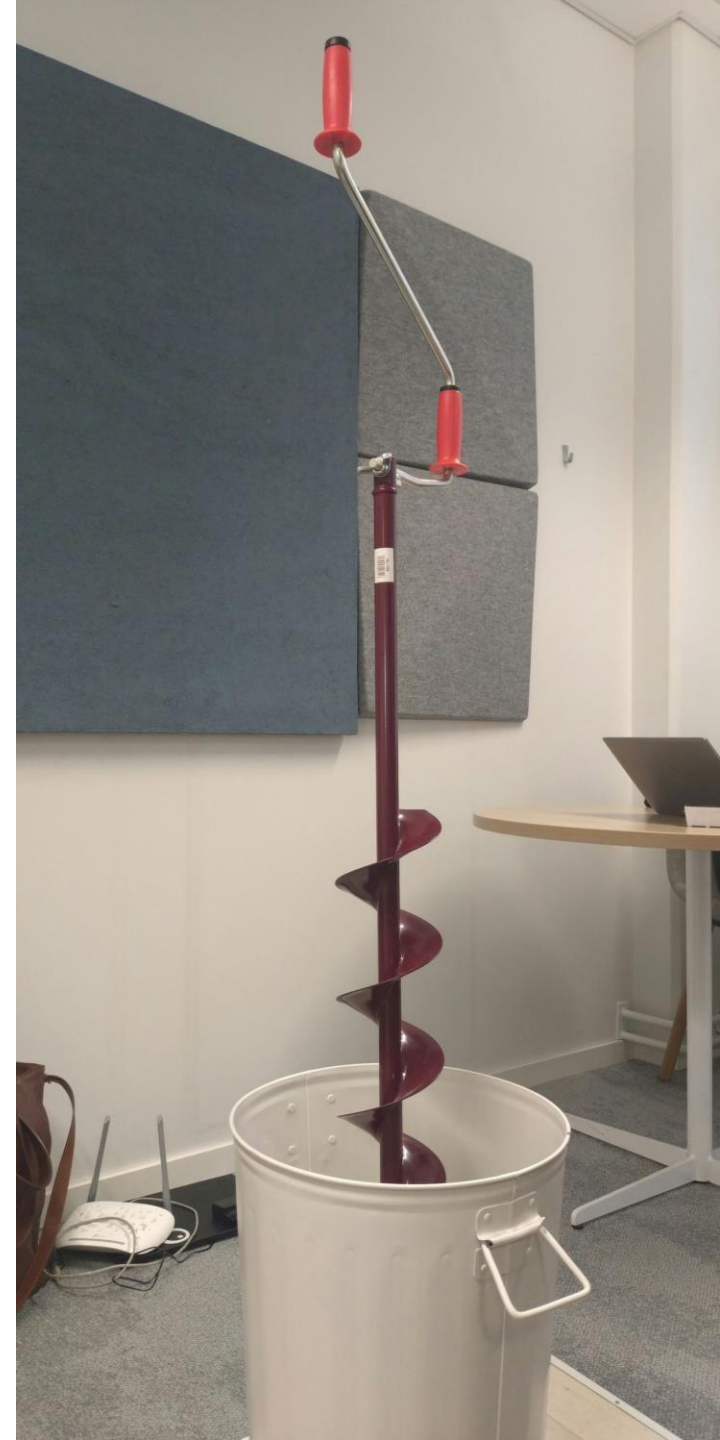
Regulation:

- ✓ AI Act
- ✓ CRA
- ✓ NIS2
- ✓ GDPR

Etteplan Demo 1: Independent incremental learning

Demo:
Learn drilling style
(ice fishing)

- **Local learning and model execution**
 - No data to cloud
- **Use case: Anomaly detection**
 - What's normal / abnormal
- **Secure Edge AI**
 - Open and cyber-security certified Linux platform (SW+HW)



Etteplan Demo 2: Vision AI at the Edge



Demo: Soft drink brand detection

- Deep learning in the cloud
 - Learning data set uploaded
 - ML model downloaded
- Use case: Object classification
 - This or that
- ML model execution in the local hardware
 - No cloud, no internet, no computer
 - Low cost, low power, low memory



For the better



etteplan