

Agentic AI at the Edge: The Security Frontier Worth Owning

Vriti Magee



Agentic AI at the Edge: The Security Frontier Worth Owning

1. The space and the market
2. The technology stack
3. Threat modelling

Where to go next..

The space and the market

“

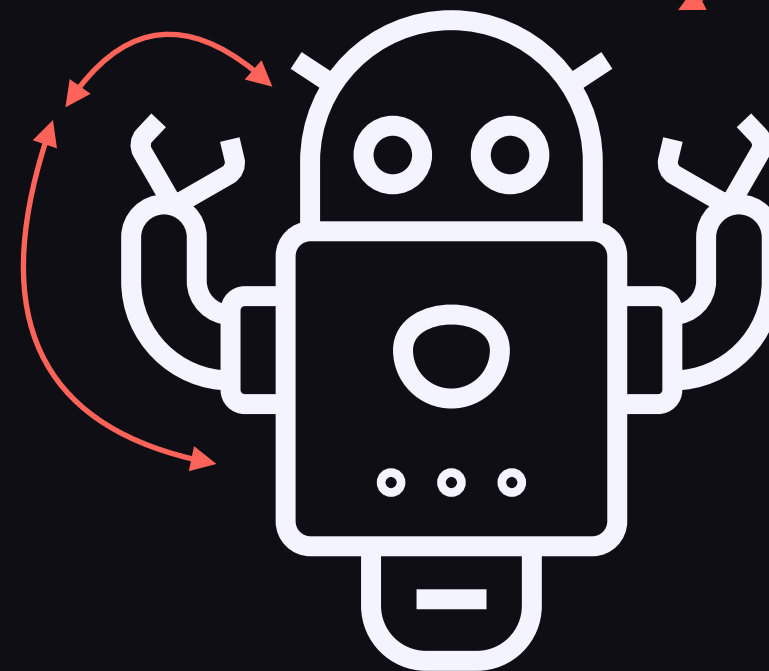
Local inference, turned into action

TEXAS INSTRUMENTS

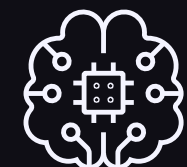
Increasing Intelligence at the Edge With Embedded Processors



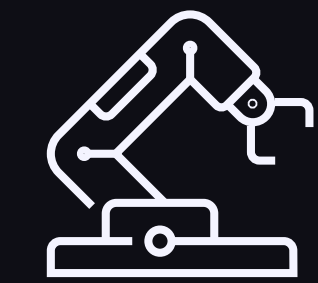
Physical AI



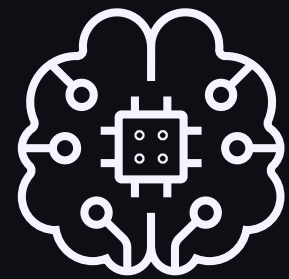
Edge AI



Three terms: edge AI, physical AI, agentic AI at the edge



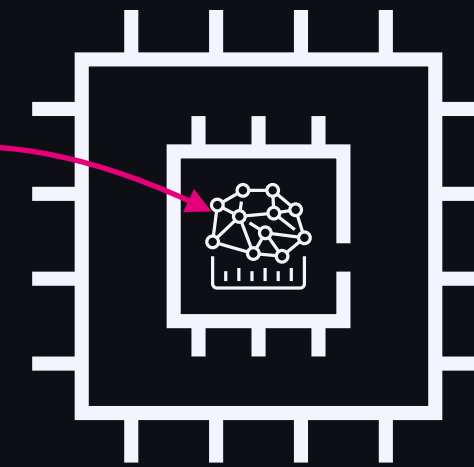
Physical AI



Edge AI



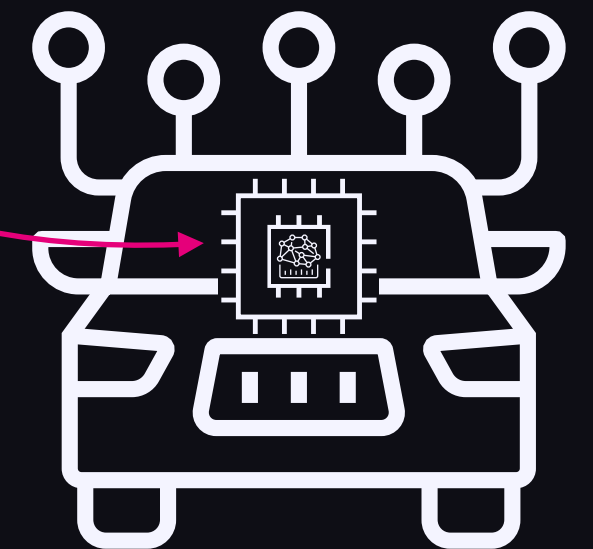
Agentic AI at the edge



Chip



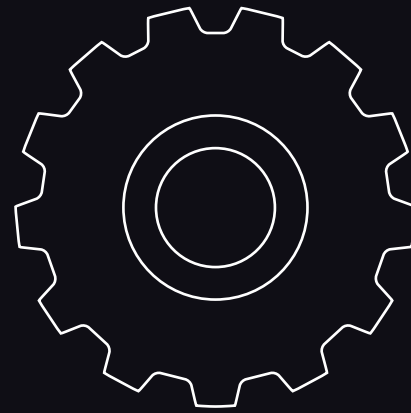
Cloud



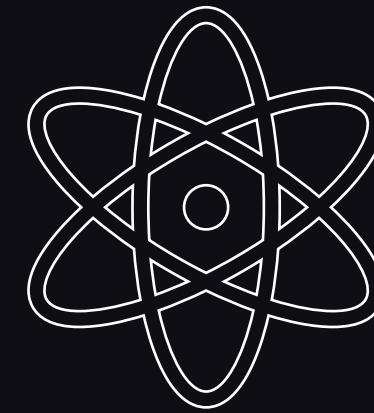
Advanced driver assistance systems (ADAS)

Source(s): ARM, Texas Instruments, McKinsey

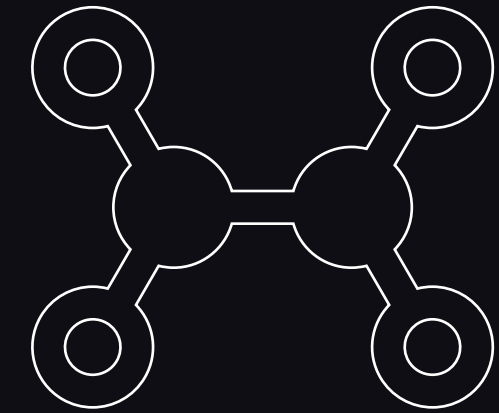
Why the edge



On-device AI
inference



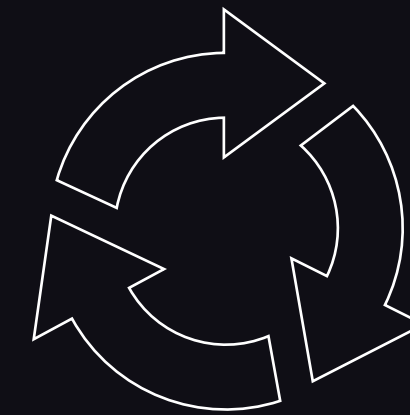
Low latency &
offline capability



Bandwidth & cost
efficiency



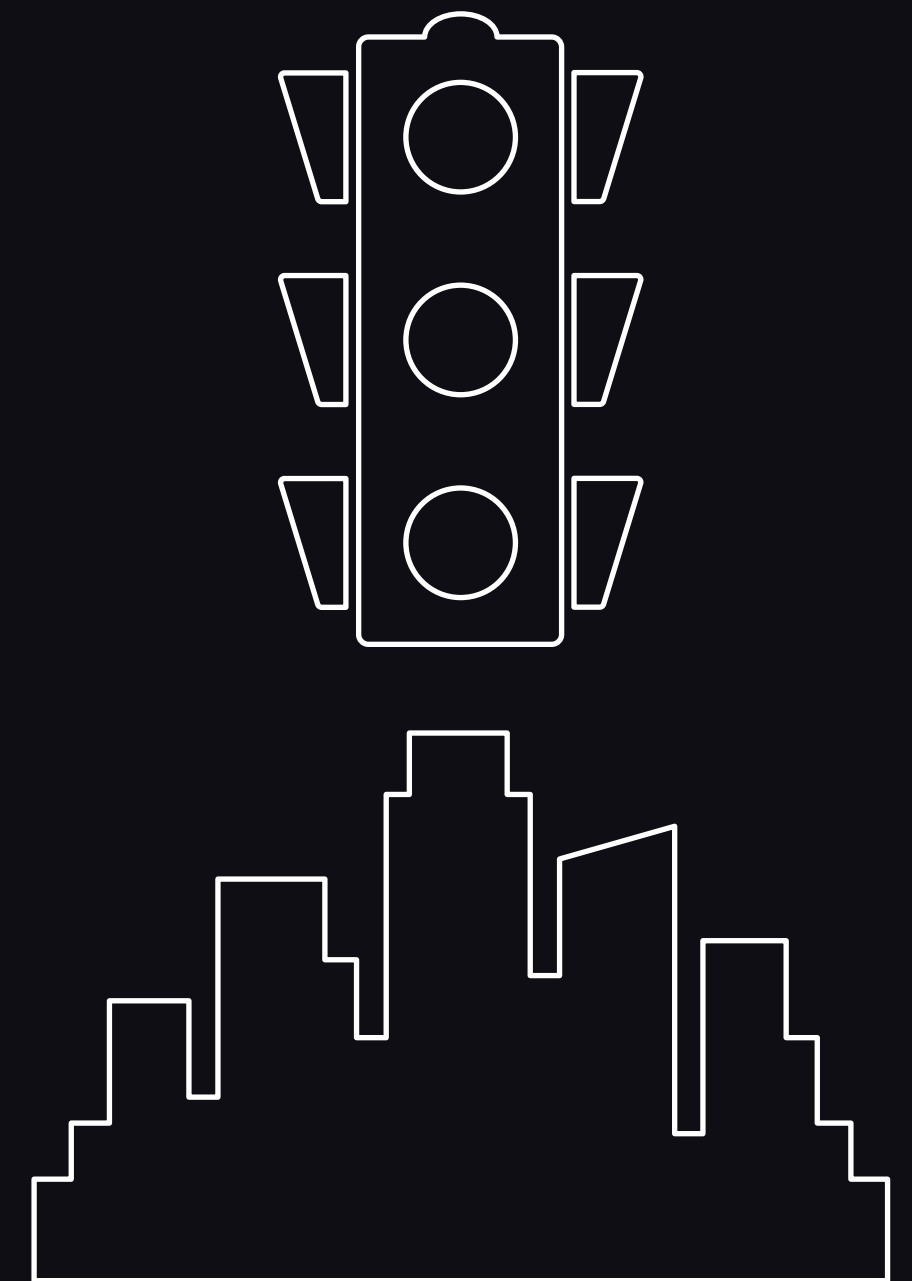
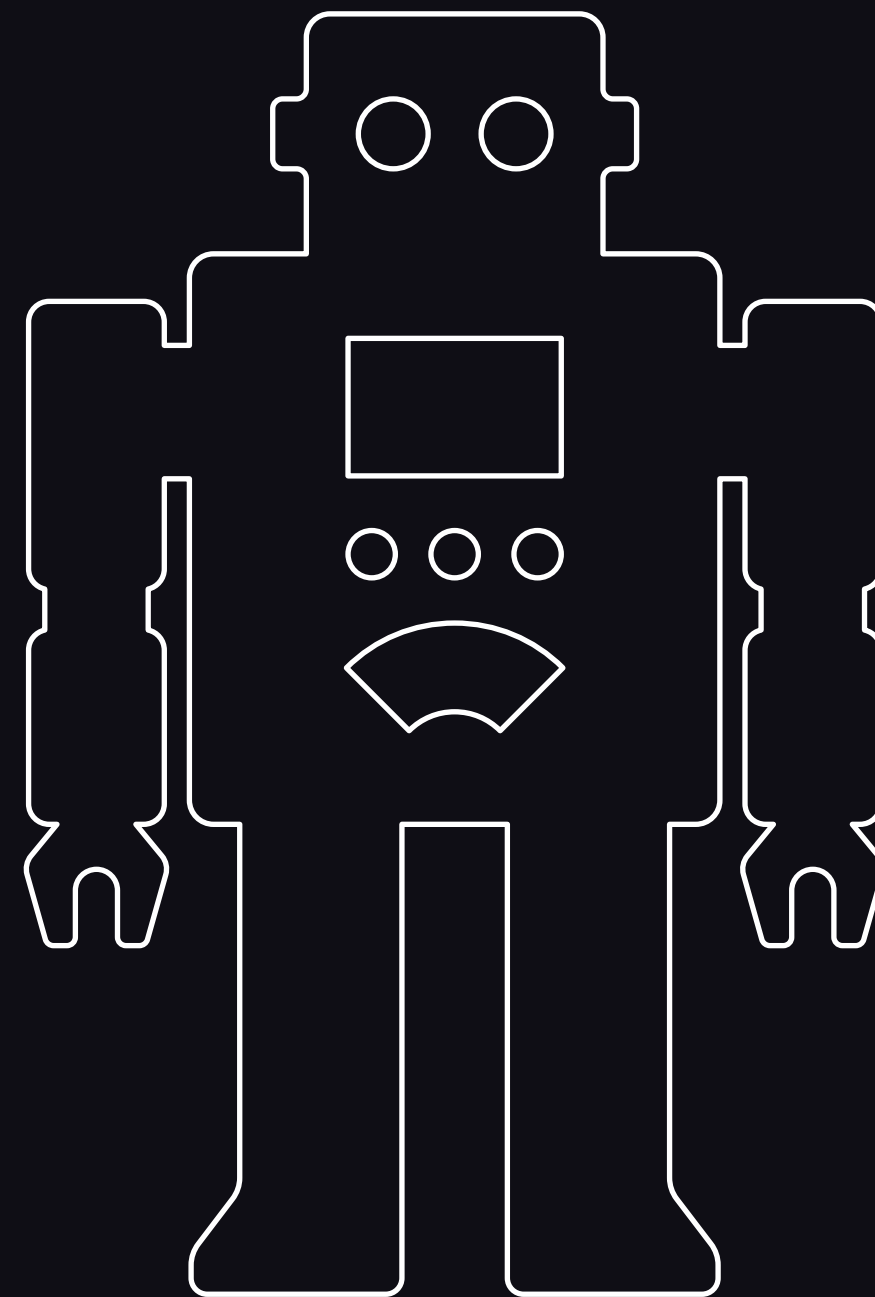
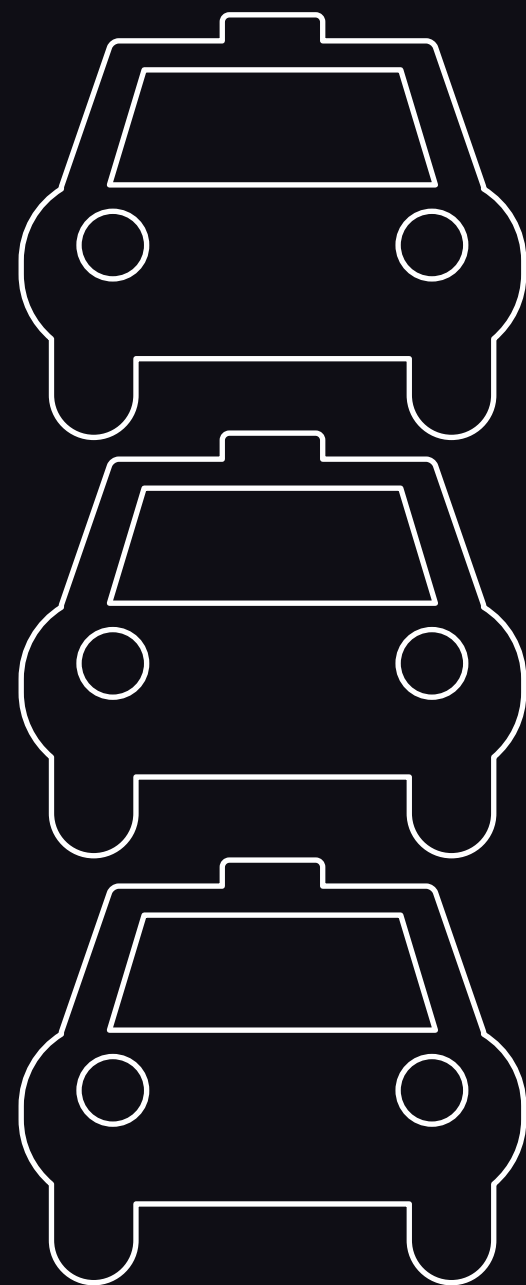
Improved privacy &
security



Scalable & robust
deployments

Source(s): ARM, IDC

Already running: vehicles, robots, cities



Source(s): Precedence

Market size: About USD 25bn today, over USD 150bn by the mid-2030s



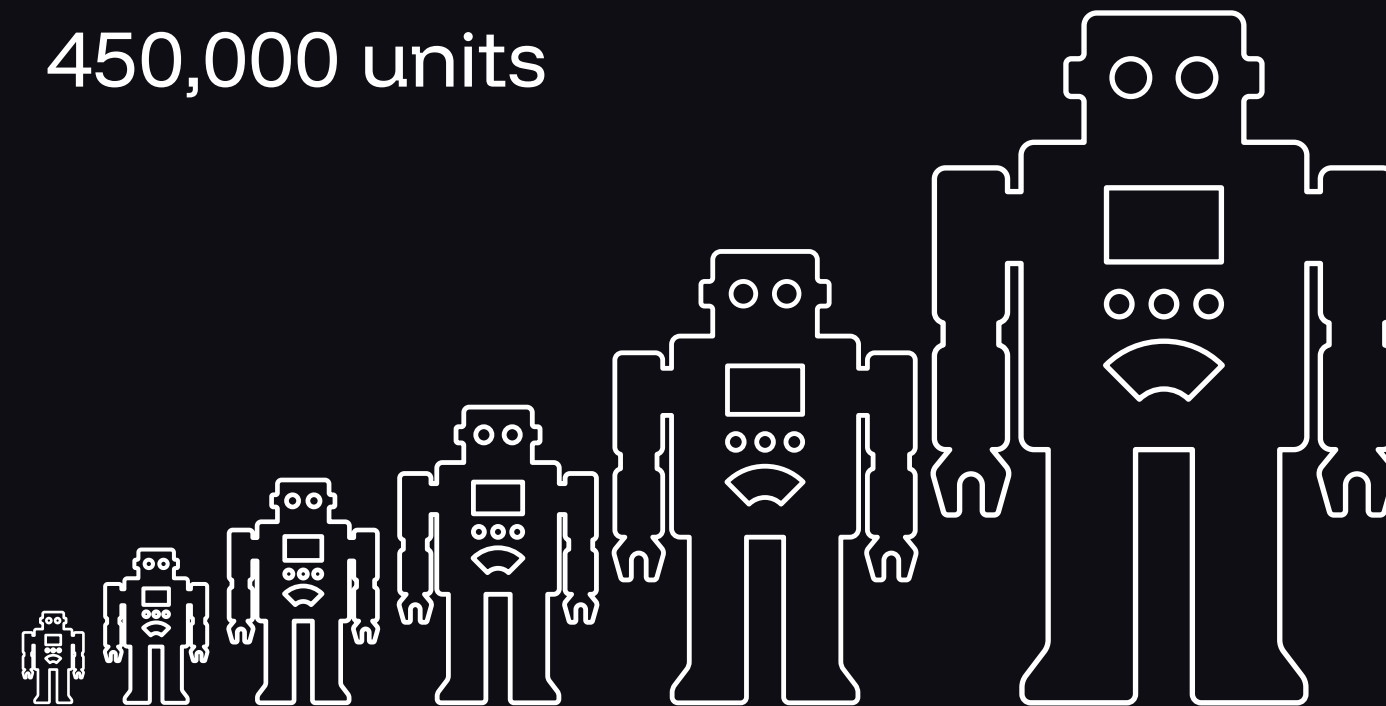
Automotive Fastest
growing segment

Source(s): Precedence

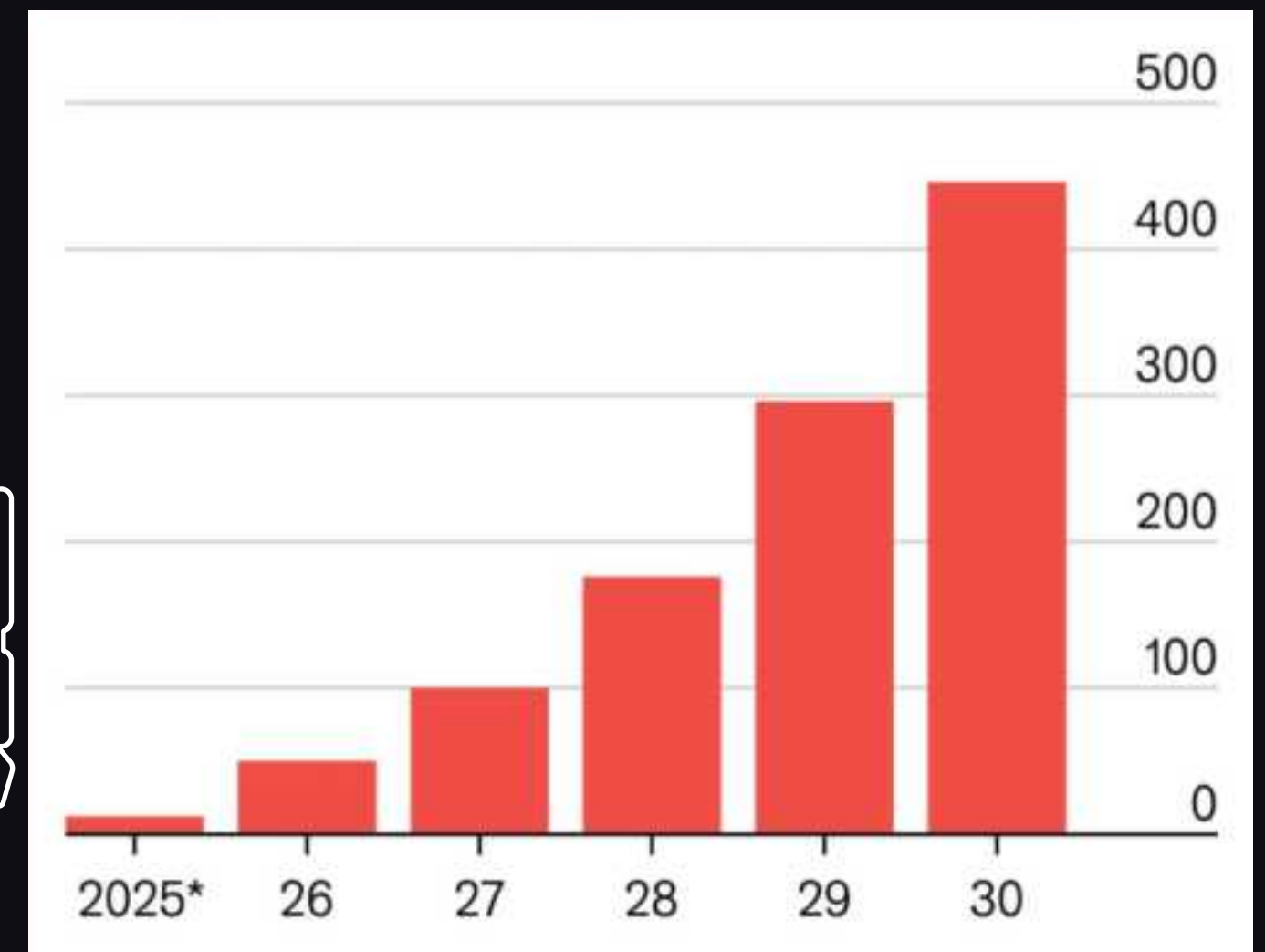
Beyond the silicon, a multi-trillion-dollar prize

2050 Global TAM =
USD 5,000,000,000,000

2030 China humanoid sales=
450,000 units

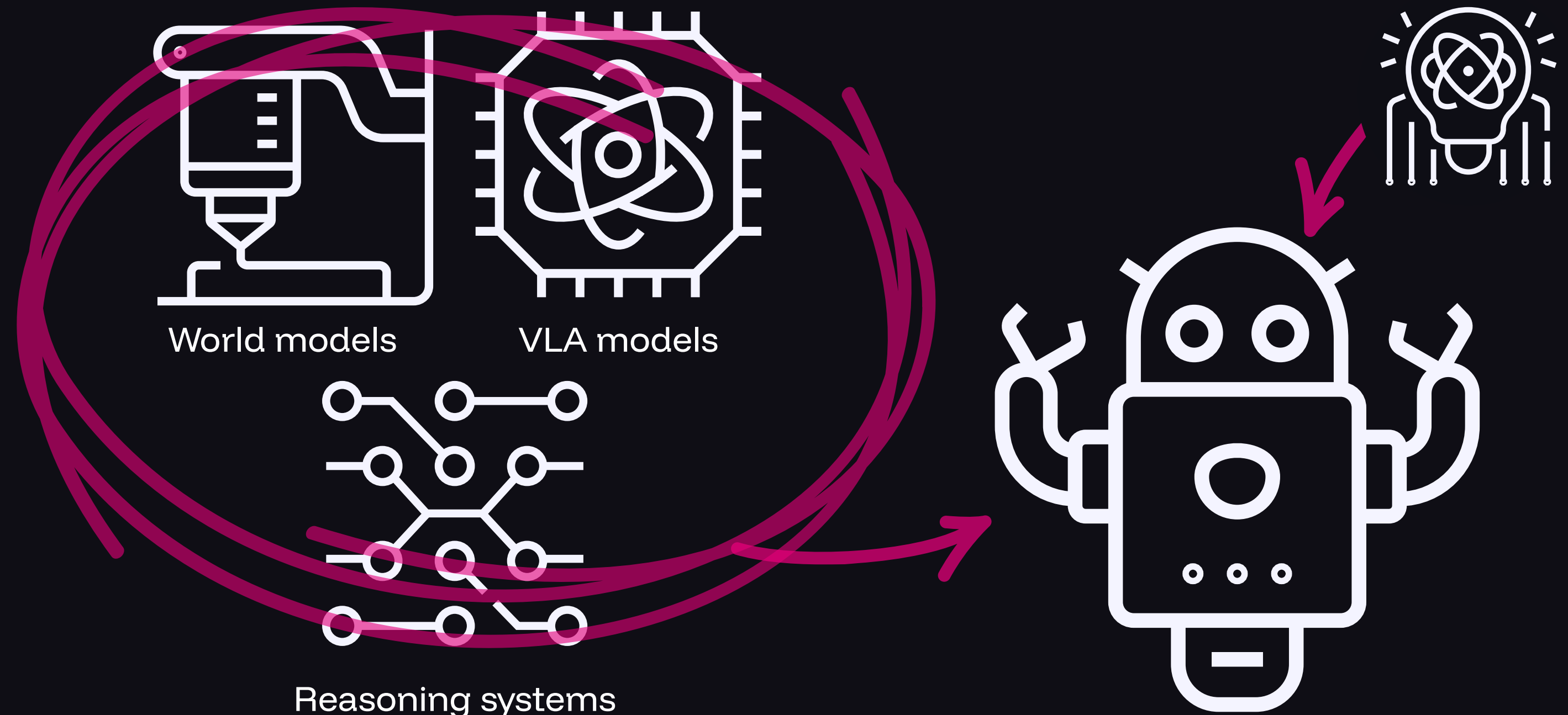


Training season: China, humanoid robots, unit sales forecast, '000



Source(s): Morgan Stanley Research, The Economist

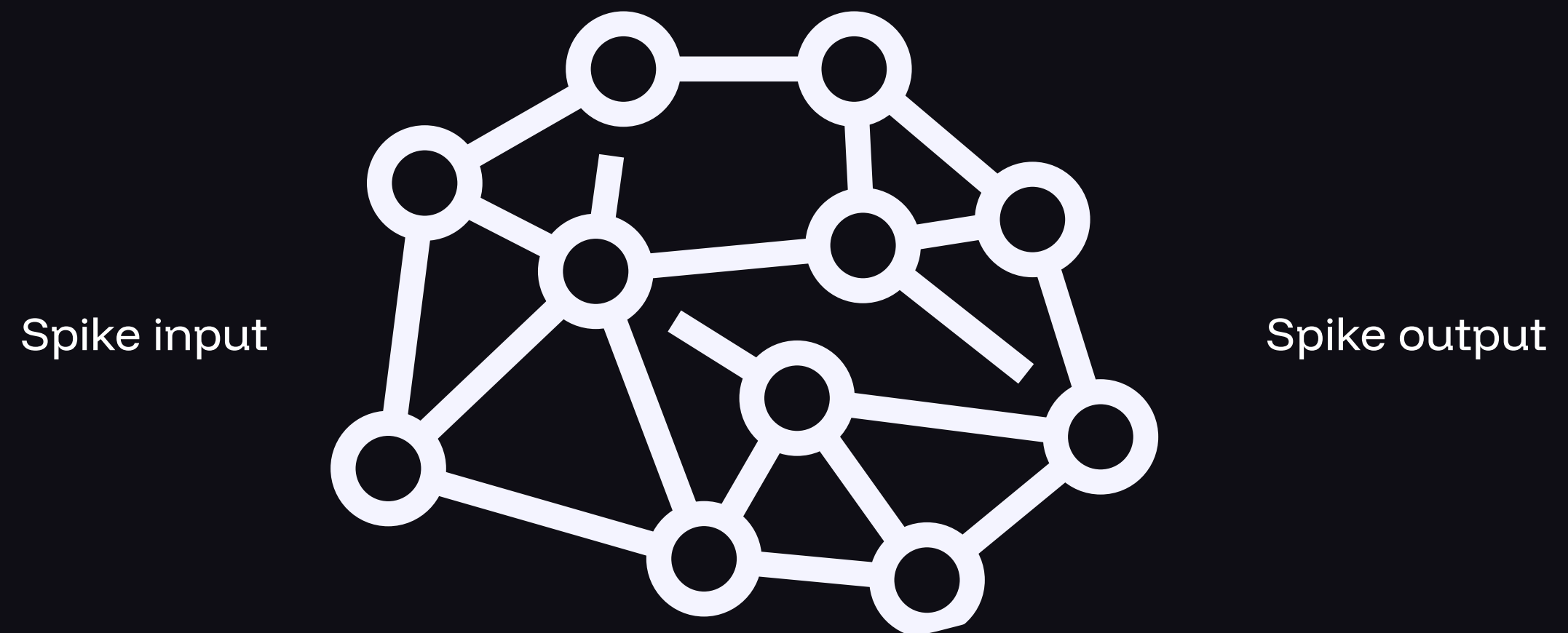
From perception to anticipation



Source(s): McKinsey, IDC

Embedded intelligence

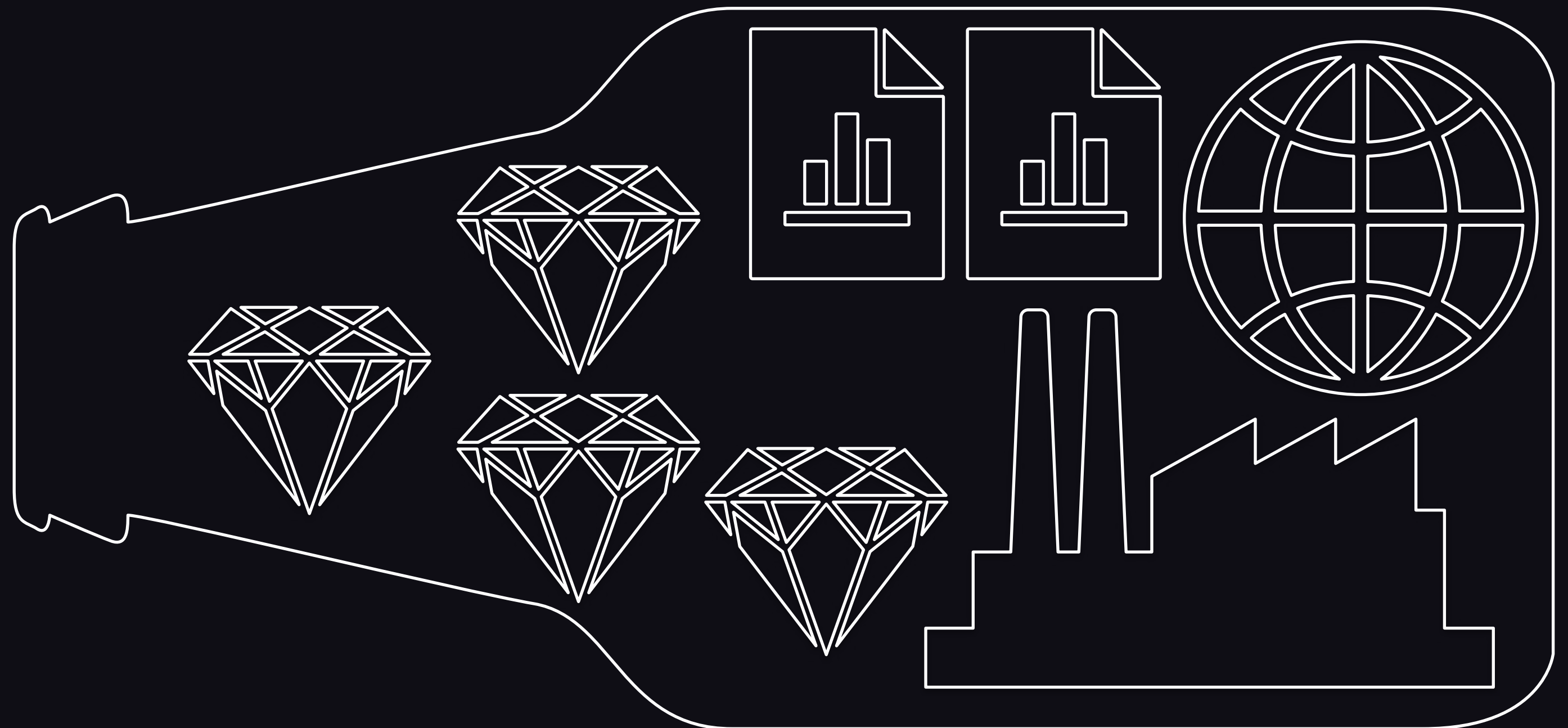
Neuromorphic Architecture



Neurons and synapses for both processing and memory

Source(s): McKinsey, IDC

What could slow it: supply of raw materials, politics, data



Source(s): The Economist, Morgan Stanley Research

The technology stack

“Unlocking the next wave of
innovation and value at the edge

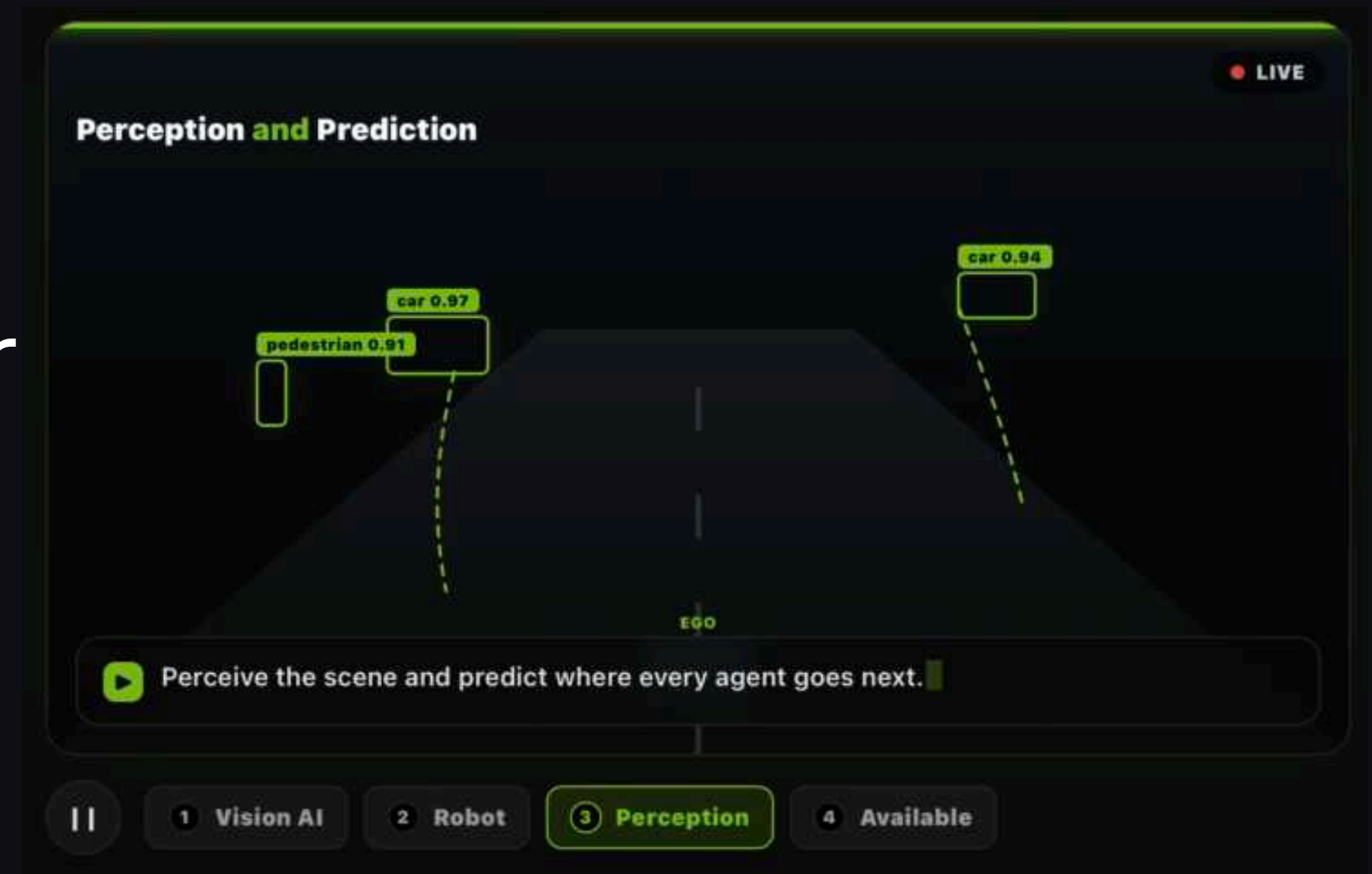
IDC

EDGE AI: Paving the Way for Intelligent, Resilient Deployments with a
Systems Mindset

Small models that reason on the device

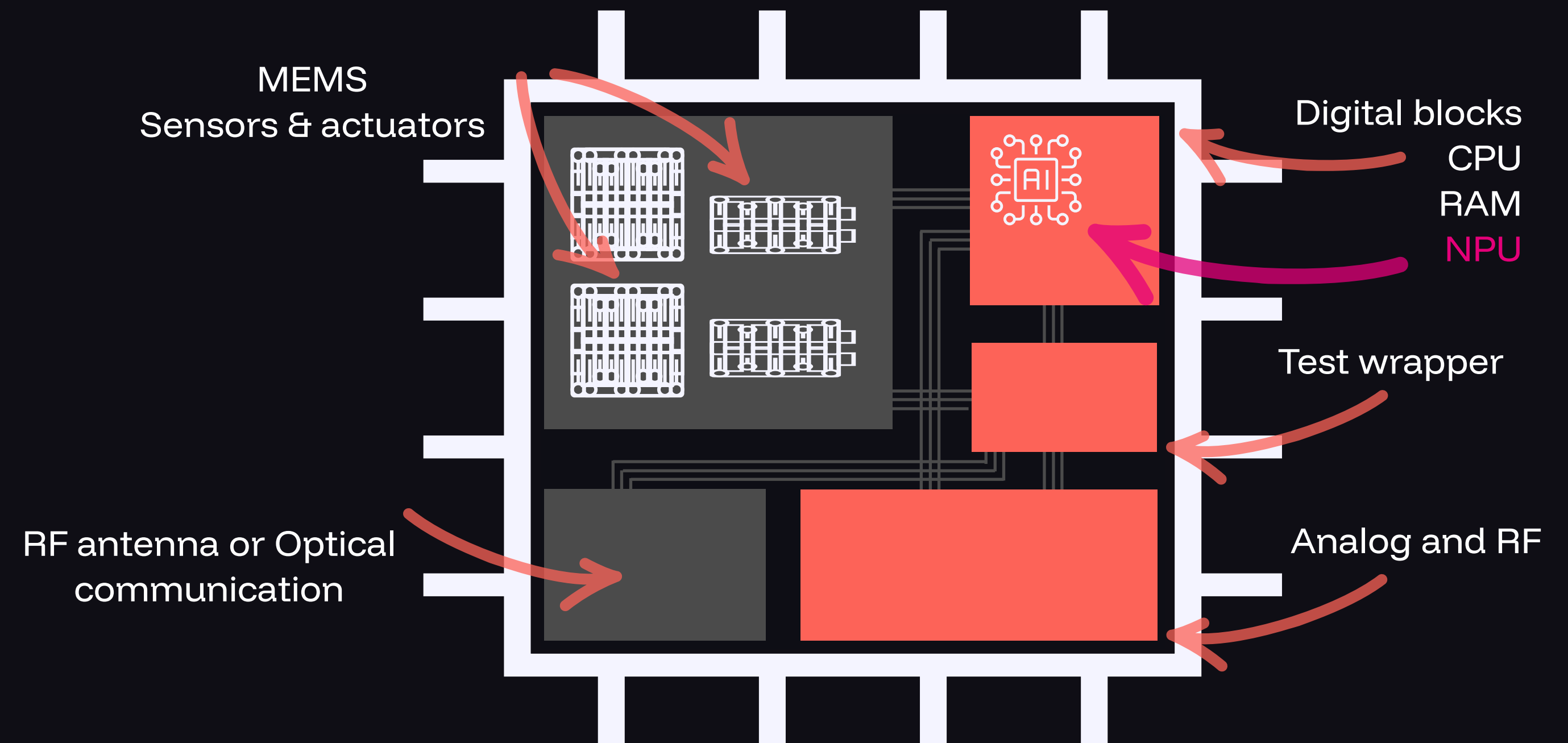
Cosmos
4 billion
parameter
world
model

built to run on an
edge module



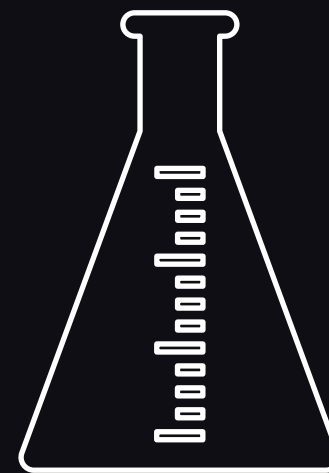
Source(s): NVIDIA (Jetson, Cosmos 3 Edge), Mistral, IDC

The silicon that makes agentic AI fit on the edge: SoC, NPU



Source(s): Synopsys

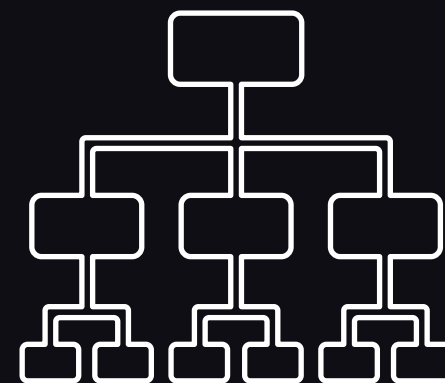
Model optimisation & future outlook



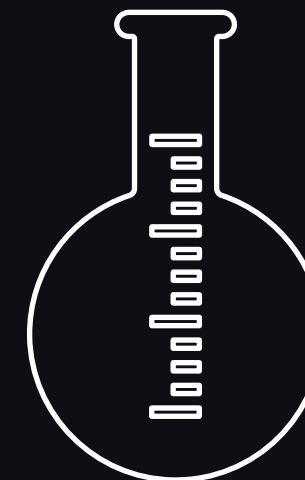
Quantization



Pruning



Structured sparsity



Knowledge distillation

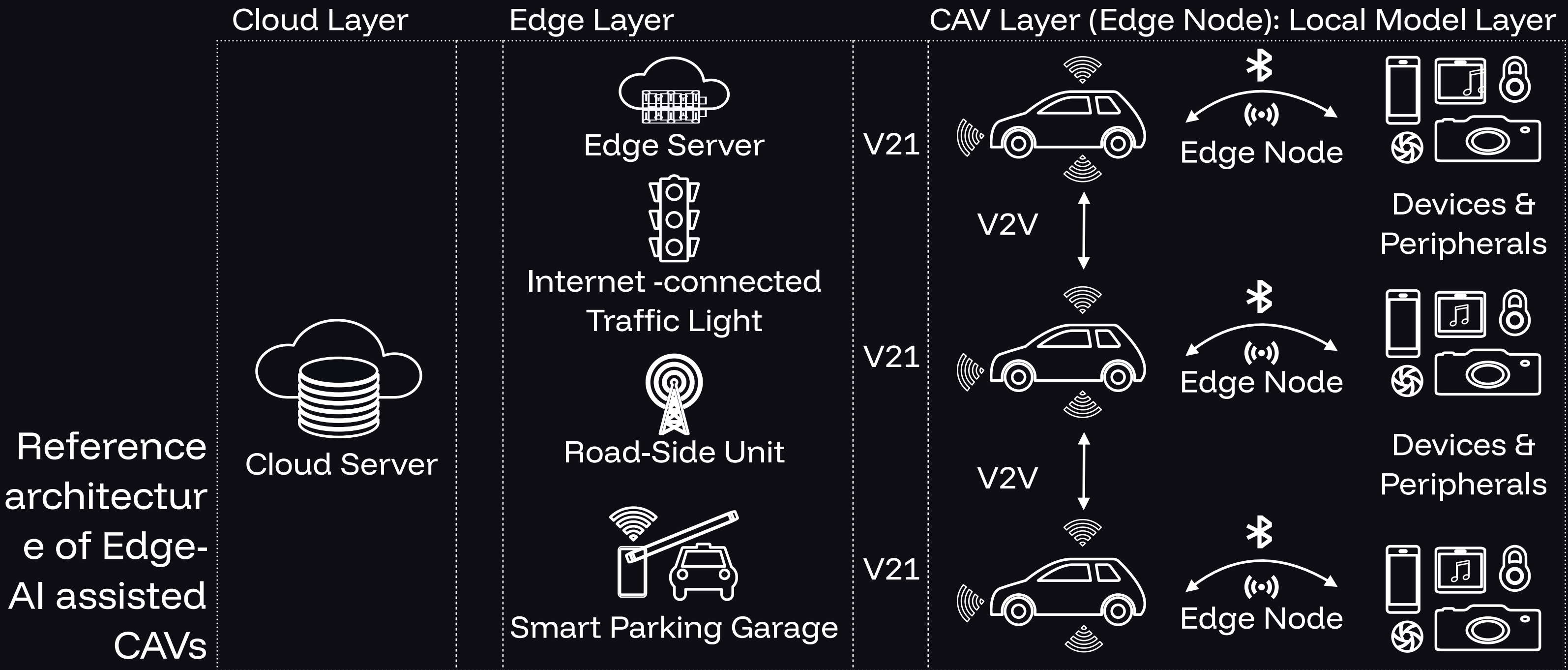
By 2030,
50%

of enterprise AI
inference workloads
will be processed
locally on endpoints
or edge nodes,
reducing cloud
traffic and latency
while supporting
greater control over
sensitive data.

Source(s): IDC, McKinsey

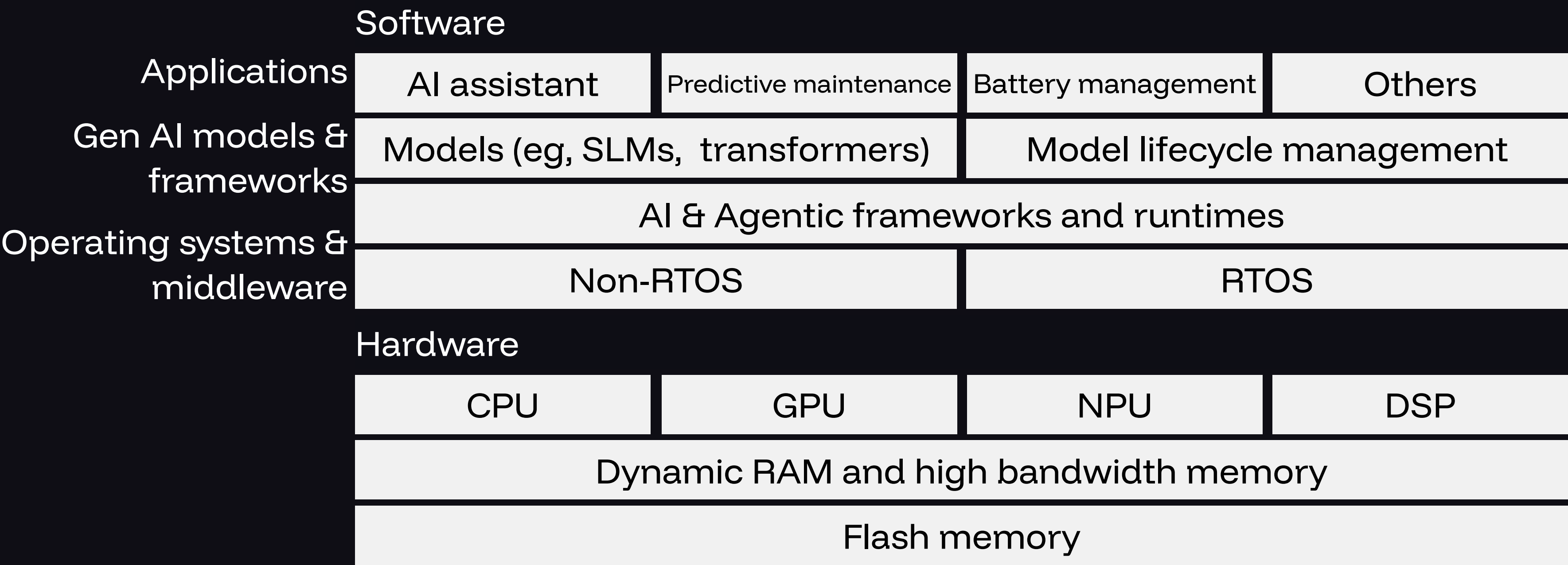
will be processed locally on endpoints or edge nodes, reducing cloud traffic and latency while supporting greater control over sensitive data.

The emergence of Connected Autonomous Vehicles (CAVs)



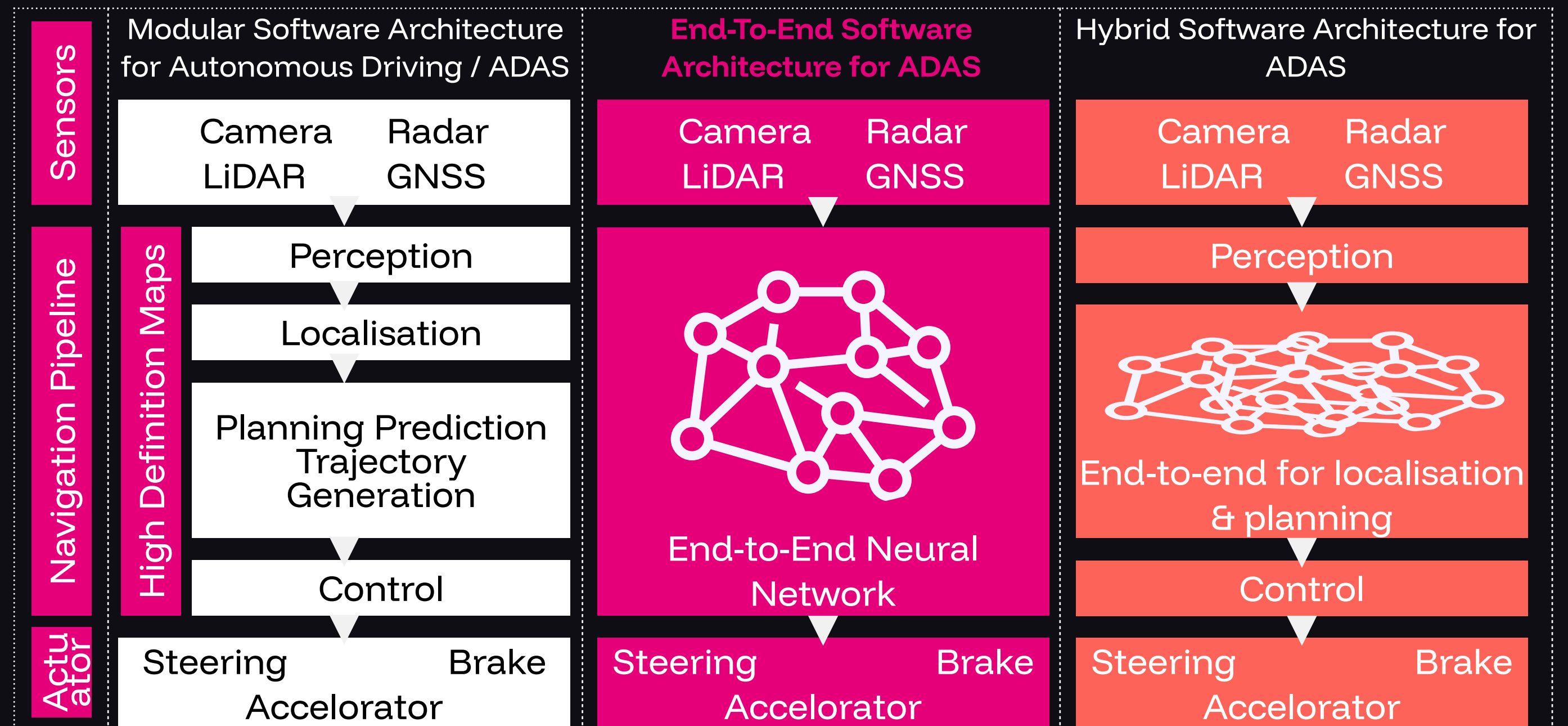
Source(s): Research paper, Threat landscape of edge-AI-assisted connected autonomous vehicles (CAV)

Evolution of the in-car technology stack



Source(s): McKinsey, Synopsis, IDC, research papers

Advanced Driver Assistance Systems (ADAS)



Source(s): IDTechEx Research

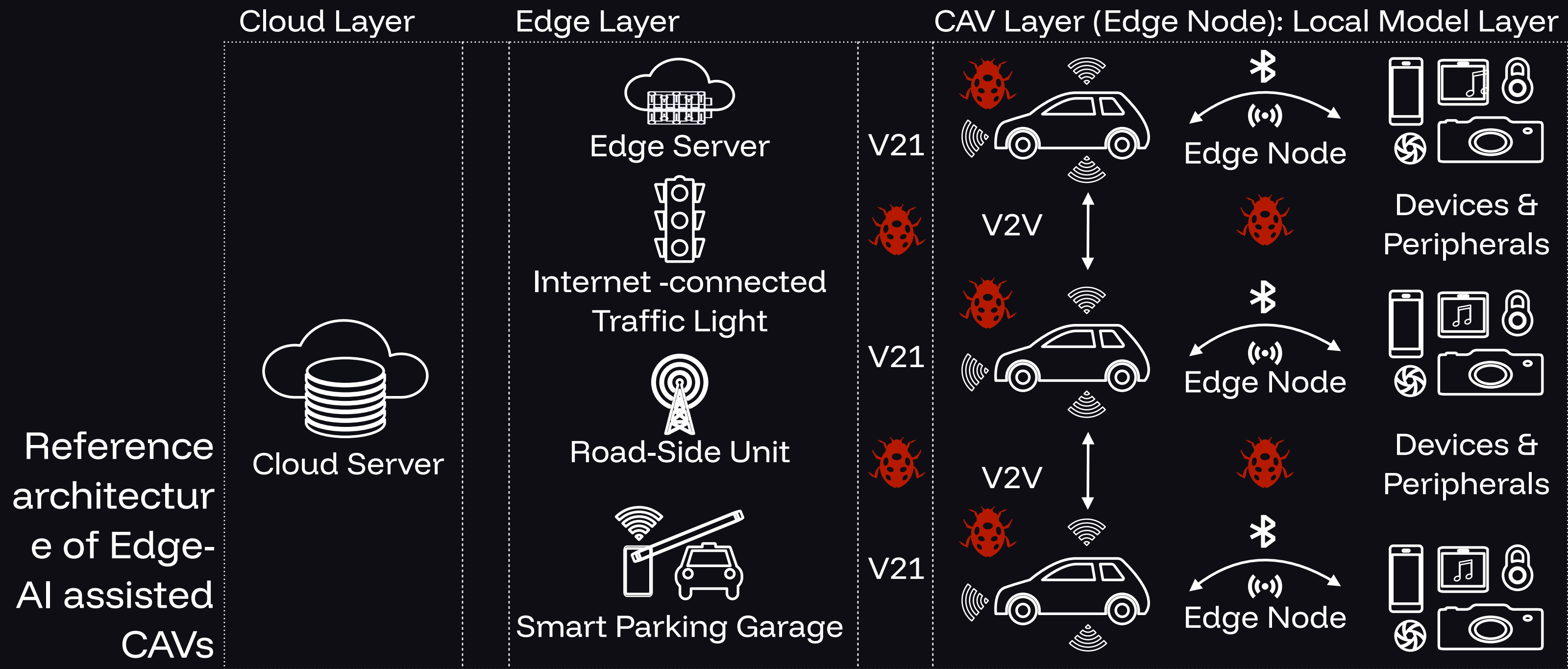
Threat modelling

“ Model the loop, not the components

Exein

Threat modelling physical AI

Threat landscape of edge-AI-assisted connected autonomous vehicles (CAV)



Source(s): Adapted from research paper, Threat landscape of edge-AI-assisted connected autonomous vehicles (CAV)

Threat modelling frameworks



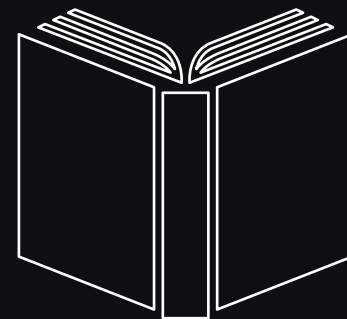
Spoofing



Tampering



Repudiation



Information
Disclosure



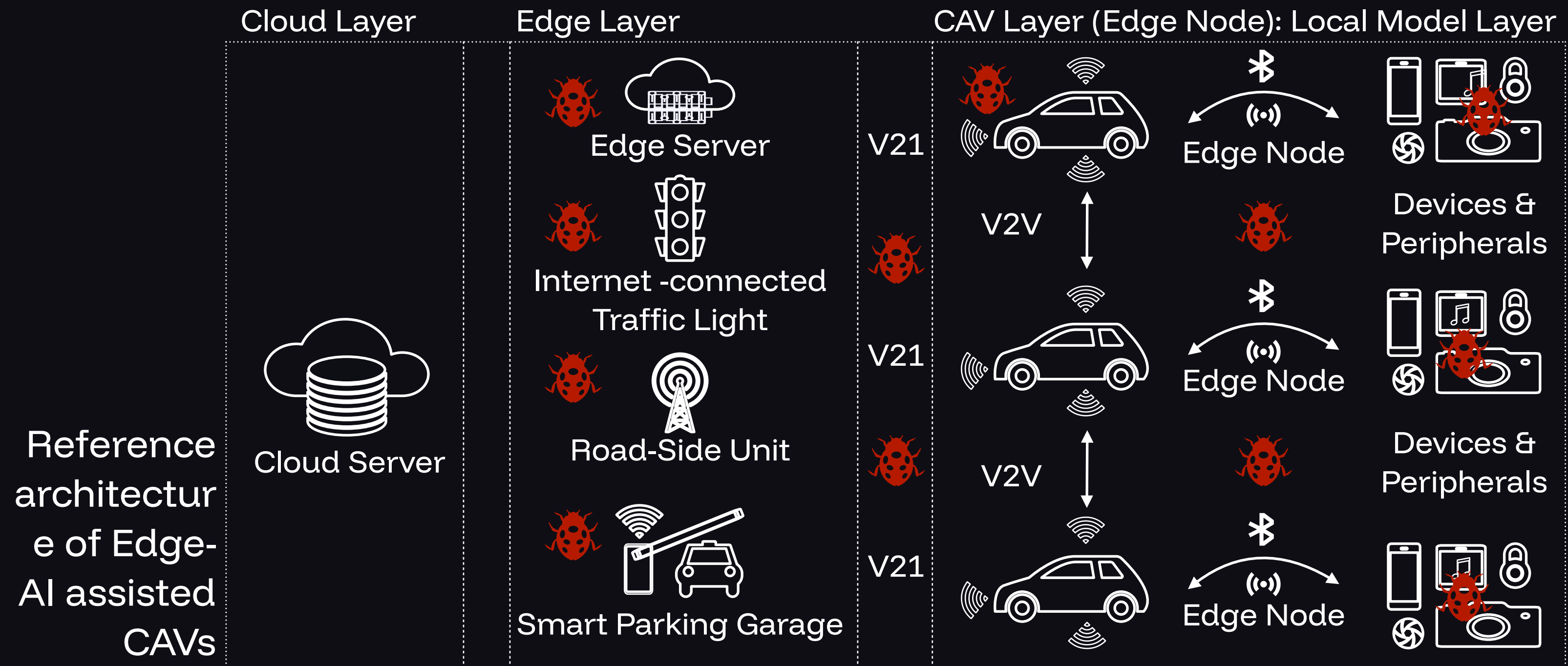
Denial of
Service



Elevation of
Privilege

Source(s): Adam Shostack

Threat landscape of edge-AI-assisted connected autonomous vehicles (CAV)



Source(s): Adapted from research paper, Threat landscape of edge-AI-assisted connected autonomous vehicles (CAV)



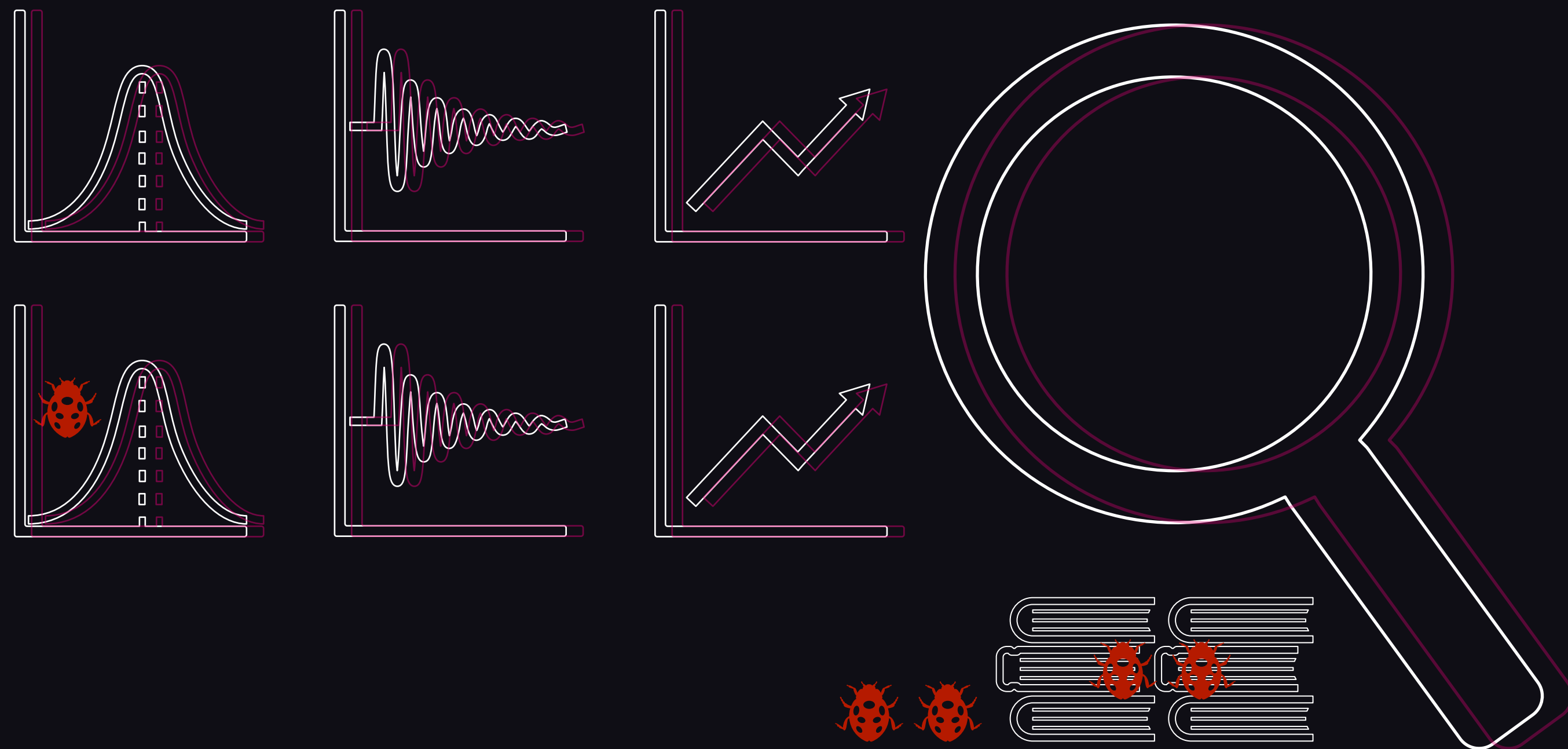
Threat modelling of edge-AI-assisted connected autonomous vehicles (CAV)

- 1. Threats to input data level in Edge-AI-assisted CAVs (Compromise).
- 2. Threats to model training level in Edge-AI-assisted CAVs,
- 3. Threats to model aggregation level in Edge-AI-assisted CAVs.
- 4. Threats to inference level in Edge-AI-assisted CAVs.

Attack	Description	Impact	Type of Compromise	Entry Point	STRIDE	Attack Vector
Data Poisoning Backdoor	Injecting manipulated or mislabeled data into a CAV's local dataset to bias the model's training	Misleading behaviour. In local and aggregated models	Data integrity sensors (e.g. LiDAR, cameras), Peripheral devices	Tampering	Physical access to sensors	Physical access to sensors

Source(s): Research article, Threat landscape of edge-AI-assisted connected autonomous vehicles (CAV)

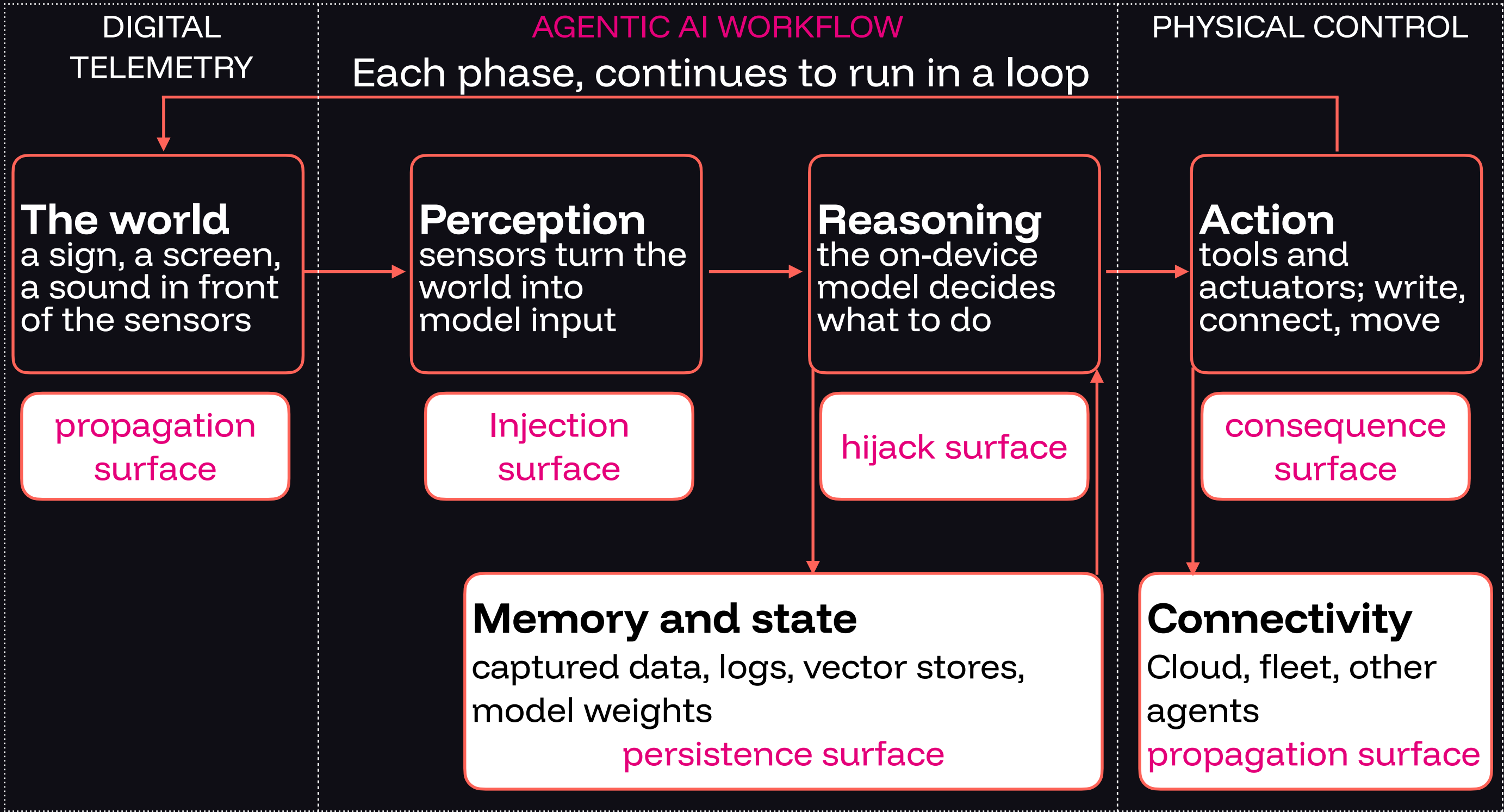
The urgent need for adaptive, resilient countermeasures



Source(s): Adam Shostack, Research article, Threat landscape of edge-AI-assisted connected autonomous vehicles (CAV)

The value of the loop

The infinite loop every physical AI device runs. Each stage is a distinct attack surface.



Source(s): Adam Shostack, exein

AI stack: principles for defence



Compromise at the model layer, containment at the layers below it.
One device's blocked attempt is the fleet's early warning.

Scan

the AI stack before it ships

Before Shipping

- SBOM of the AI stack
- CVEs in model runtimes
- poisoned or tampered model artefacts

Enforce

below the model on the device

The device

AI agent + model
steerable by anything it perceives
assumed compromised



Exec. connect . open

Kernel enforcement
default-deny allowlist, keyed to the agent's own identity a prompt cannot reach here

hardware / OS

Monitor

the boundary across the fleet

Runtime

- in the field
- Every blocked action becomes an incident
- correlated across the whole fleet

Source(s): exein

Where to go next..

ARM, [Edge AI glossary](#)

Texas Instruments, [Increasing Intelligence at the Edge](#)

Precedence, [Edge AI Market Size, Share and Trends 2026 to 2035](#)

McKinsey, [The rise of edge AI in automotive](#)

Research Article, [Threat landscape of Edge-AI-assisted connected autonomous vehicles \(CAV\)](#)

IDC, [Edge AI: Paving the Way for Intelligent, Resilient Deployments with a Systems Mindset](#)

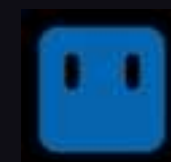
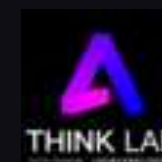
Adam Shostack, [Threat Modeling: Designing for Security in an AI World](#)

Exein, [Threat modeling physical AI](#)

Research article, [Threat landscape of Edge-AI-assisted connected autonomous vehicles](#)



[Awesome-LLM4AD](#) | [azaro-infra](#)



[Mistral](#)



[NemoClaw](#)



Contact

Vriti Magee

<https://www.linkedin.com/in/vriti>