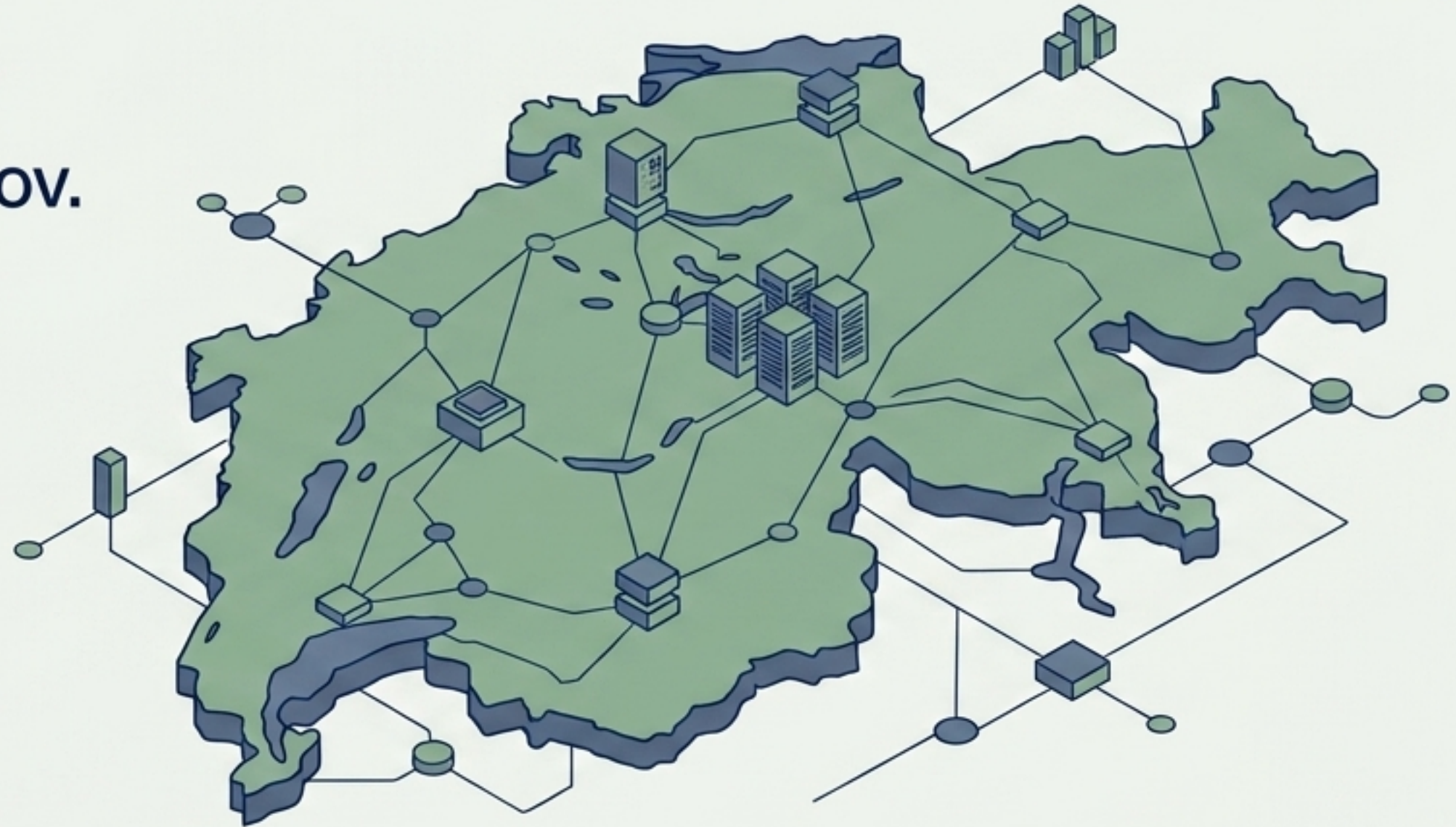
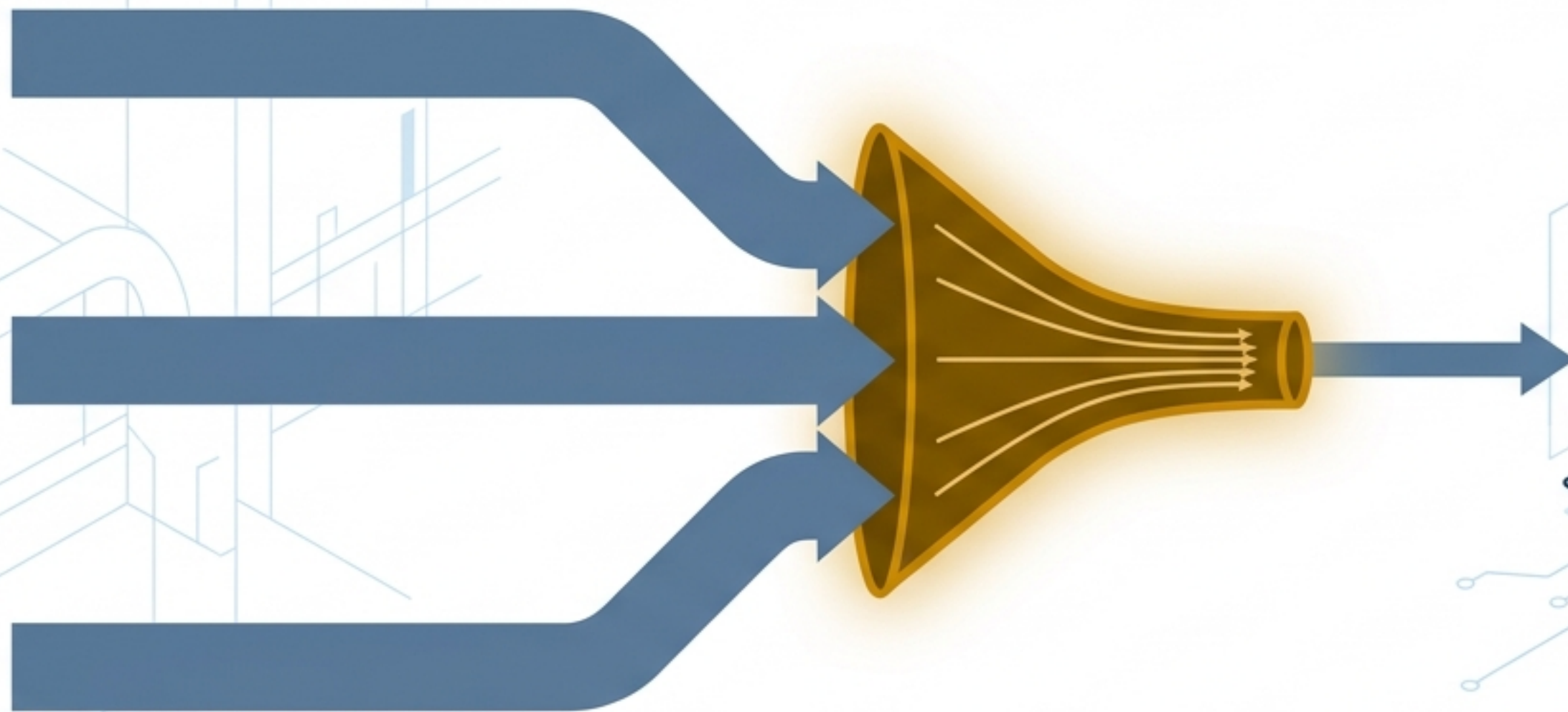


Lokalna umetna inteligenca in kibernetska varnost

Arhitekturni premiki,
inženirski kompromisi in
varovanje Edge AI sistemov.





Status Quo:

Tradicionalno učenje in izvajanje UI modelov zahteva masivno centralizirano računsko moč (Cloud AI).

Katalizator sprememb:

EkspONENTNA rast količine podatkov na izvoru.

Sistemska omejitev:

Prenos surovih podatkov v oddaljene podatkovne centre ustvarja **nepremostljiva ozka grla v pasovni širini in latenci (zakasnitvi).**

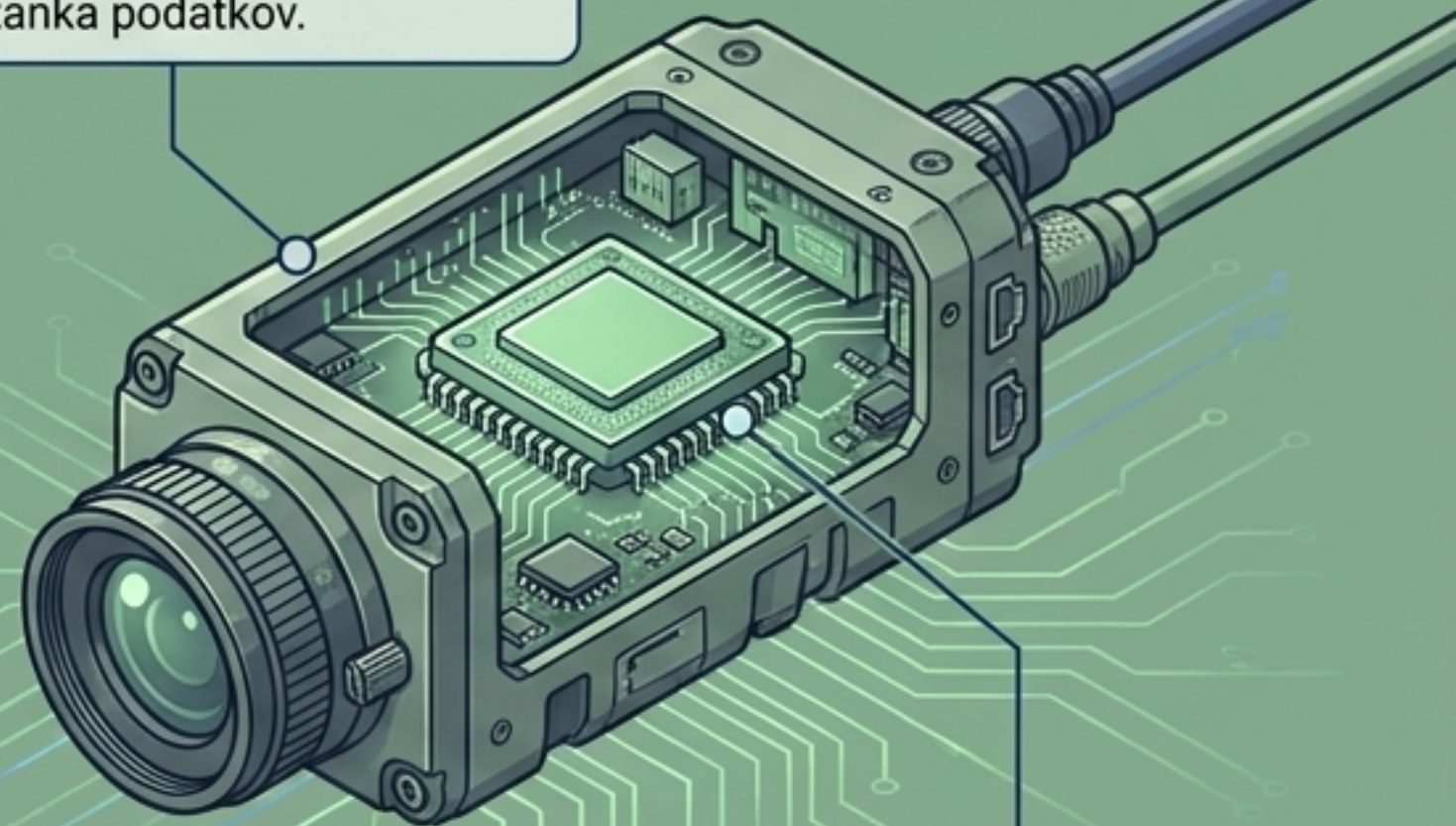
Paradigmski premik: Prehod na Edge AI



1

Definicija:

Edge (obrobje) ni abstrakten koncept, temveč fizična lokacija nastanka podatkov.



2

Izvajanje:

UI sistemi procesirajo podatke neposredno na napravi (lokalno).

3

Ključna prednost:

Odprava potrebe po prenosu surovih podatkov prek komunikacijskega omrežja.

	Training	Deployment
Level 0		Cloud AI
Level 1		
Level 2		
Level 3		Edge AI

Taksonomija hibridnih arhitektur (Stopnje 0–3)

Stopnja 0:

Popolni oblak. Učenje (training) in izvajanje (deployment) izključno v centralnem podatkovnem centru.

Stopnje 1 do 3 (Hibridni modeli):

Resursno zahtevno učenje poteka v oblaku, medtem ko se izvajanje delno ali v celoti prenaša na lokalno napravo.

Inženirska opomba: To je trenutno najbolj prevladujoča oblika Edge AI aplikacij v industriji.

	Training	Deployment
Level 4	Cloud AI	Hybrid
Level 5	Cloud AI	Edge AI
Level 6	Hybrid	Edge AI
Level 7	Device AI	Device AI

Evolucija proti popolni lokalizaciji (Stopnje 4–7)

Stopnje 4 do 6 (Distribuirani modeli):

Učenje in izvajanje si delita oblak in lokalno obrobje.

Stopnja 7 (Popolna lokalizacija - On-Device):

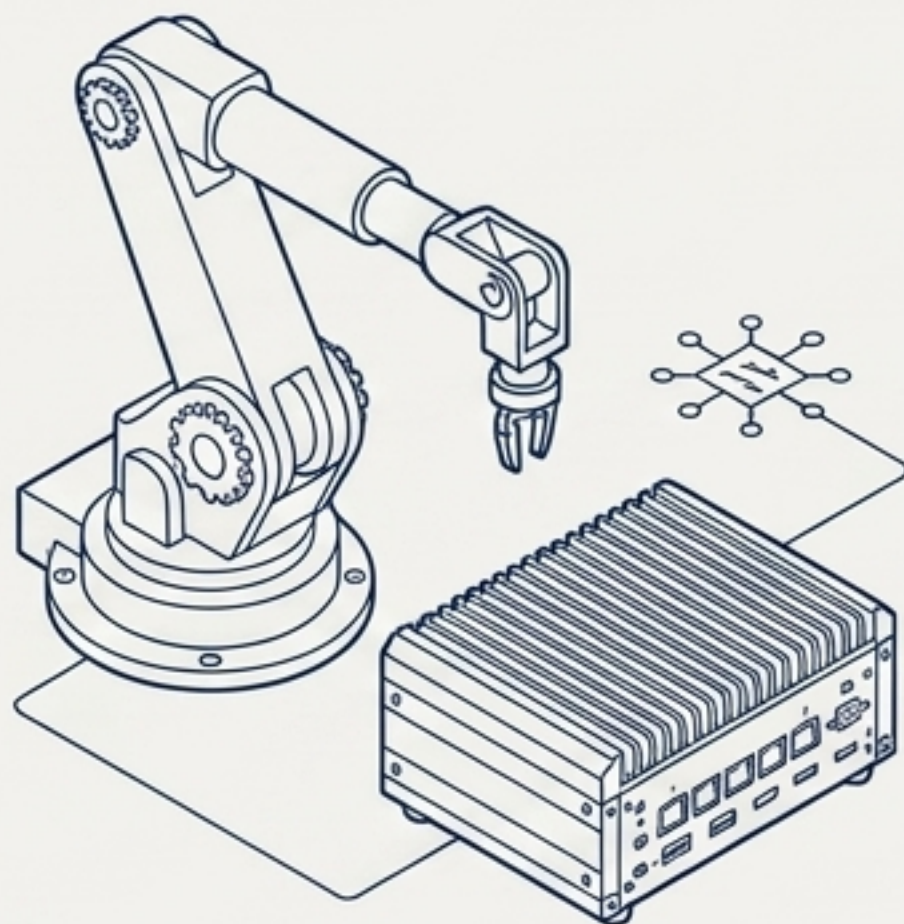
Učenje in izvajanje potekata izključno na napravi strojne opreme.

Inženirski izziv: Izvajanje kompleksnih nevronske mreže na čipih z močno omejeno porabo energije in pomnilniško kapaciteto.

Inženirska matrika: Oblak proti Obrobju

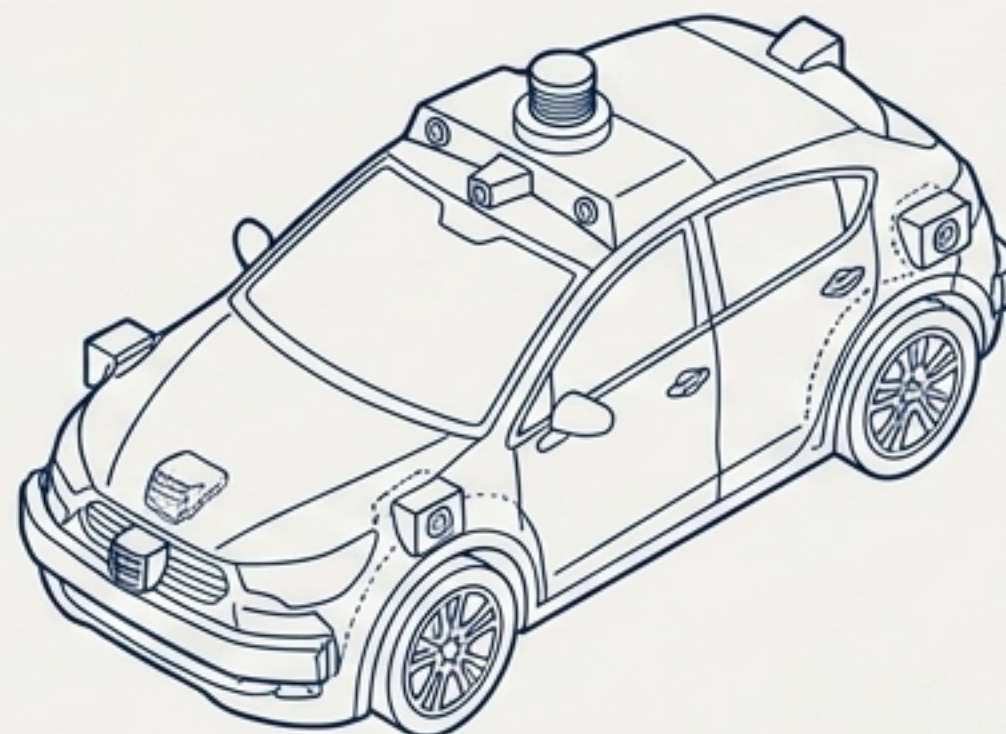
	Cloud AI		Edge AI	
Odzivni čas (Latency)	Visoka / Odvisna od omrežja		Nizka / Takojšnja	
Pasovna širina	Zahtevna		Minimalna / Deluje Offline	
Zasebnost (Privacy by design)	Podatki zapustijo vir		Podatki ostanejo na napravi	
Računska moč / Shranjevanje	Navidezno neomejena		Močno omejena	
Kakovost podatkov	Popolni, globalni nabori		Omejeni, lokalni podatki	

Implementacija v kritičnih sistemih



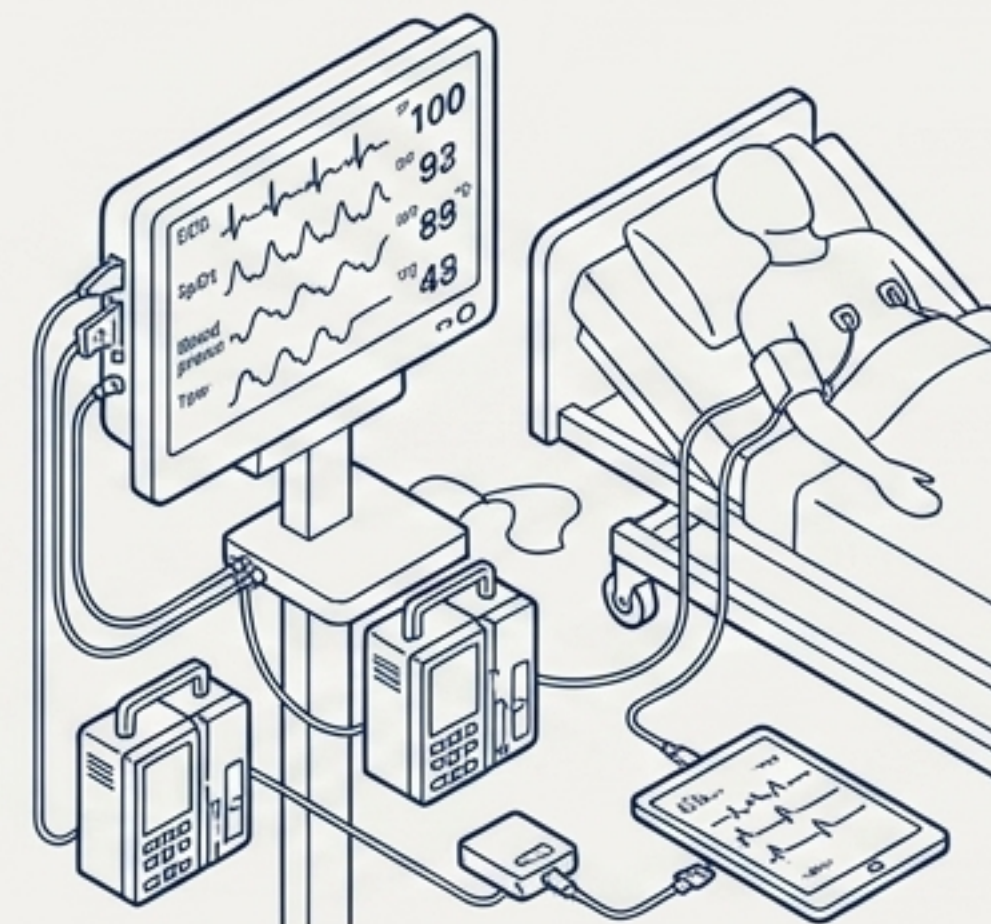
Prediktivno vzdrževanje (Industrija)

Analiza anomalij strojev v realnem času brez pošiljanja občutljivih tovarniških podatkov v zunanja omrežja.



Avtonomna mobilnost

Časovno kritične odločitve, ki ne smejo biti odvisne od stabilnosti in prepustnosti internetne povezave.

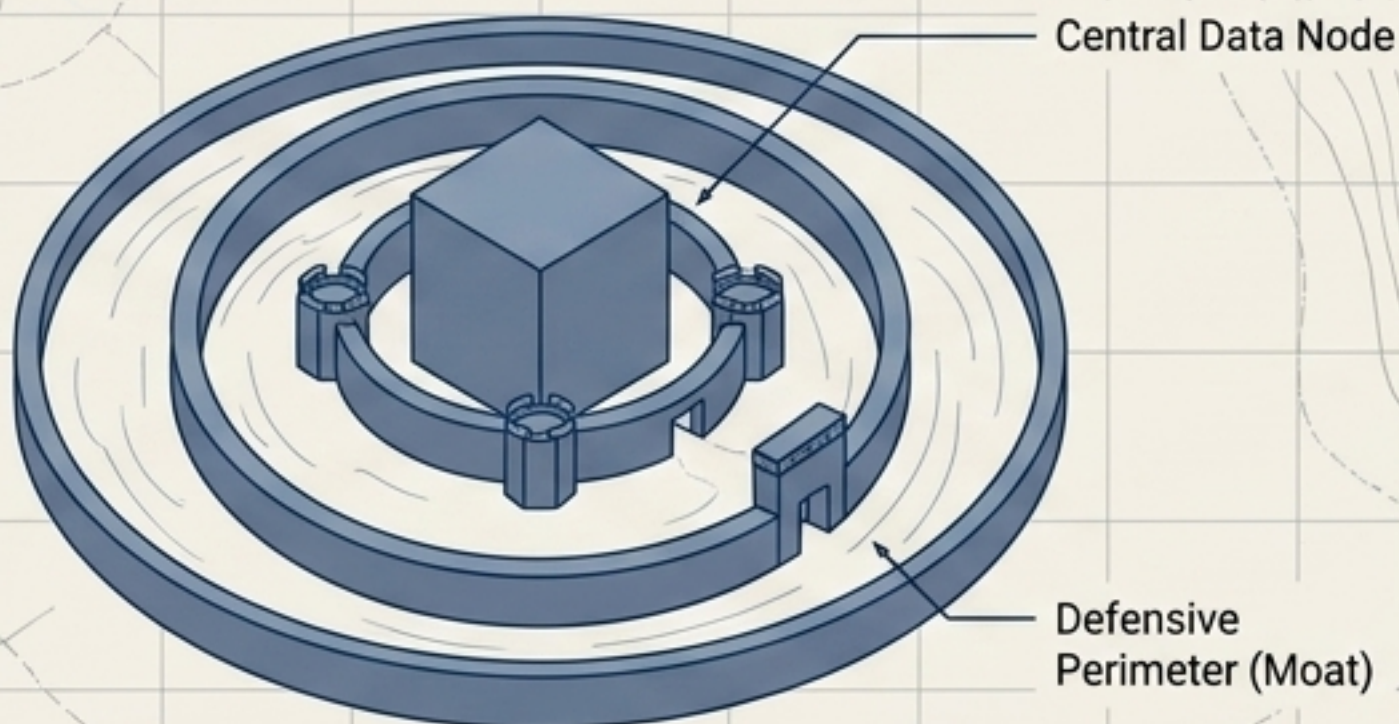


Zdravstvo in osebni podatki

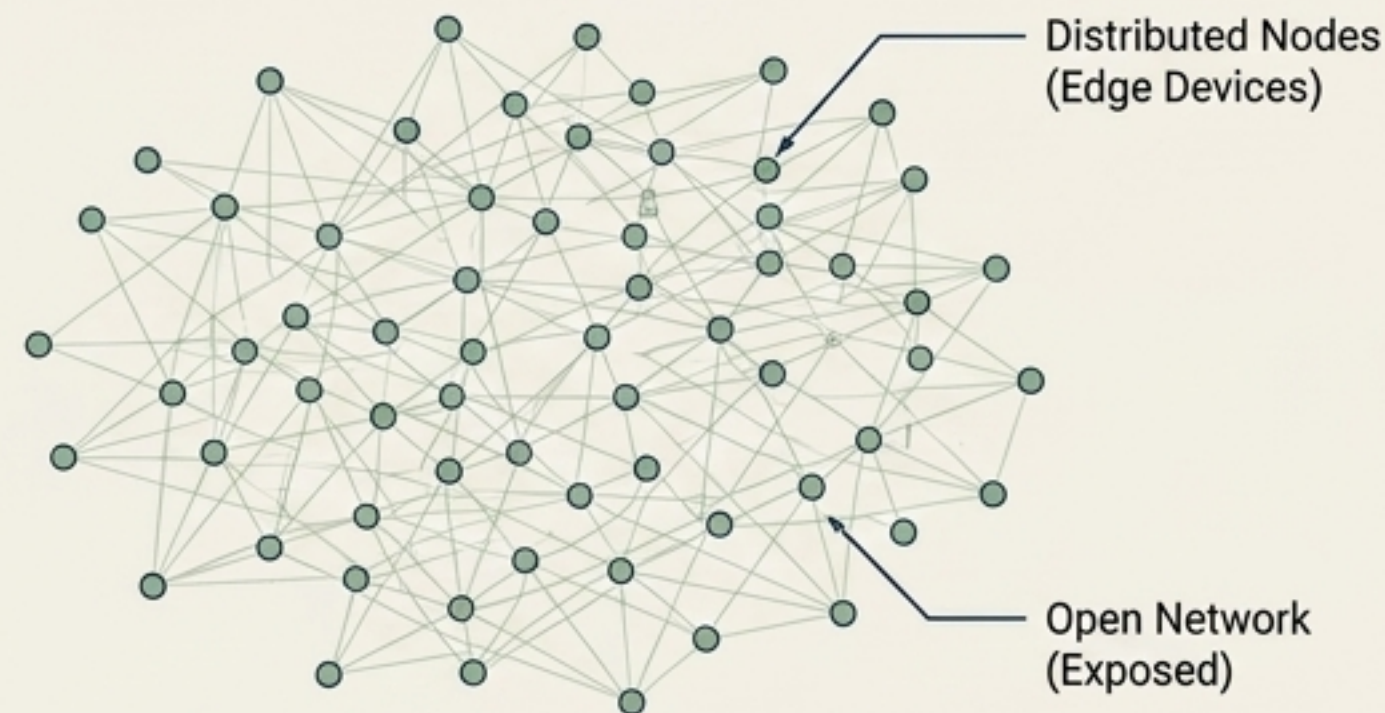
Lokalna analiza (npr. ob nujnih stanjih), ki strogo upošteva sistemsko zaščito občutljivih osebnih podatkov pacientov.

Sprememba varnostne paradigme

Castle and Moat Topology



Distributed Fortress Topology

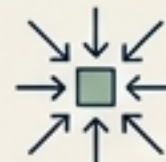


Decentralizacija tarče:



Porazdeljena obdelava zmanjšuje količino podatkov na enem mestu (odprava centralizirane tarče).

Eksplozija napadalne površine (Attack Surface):



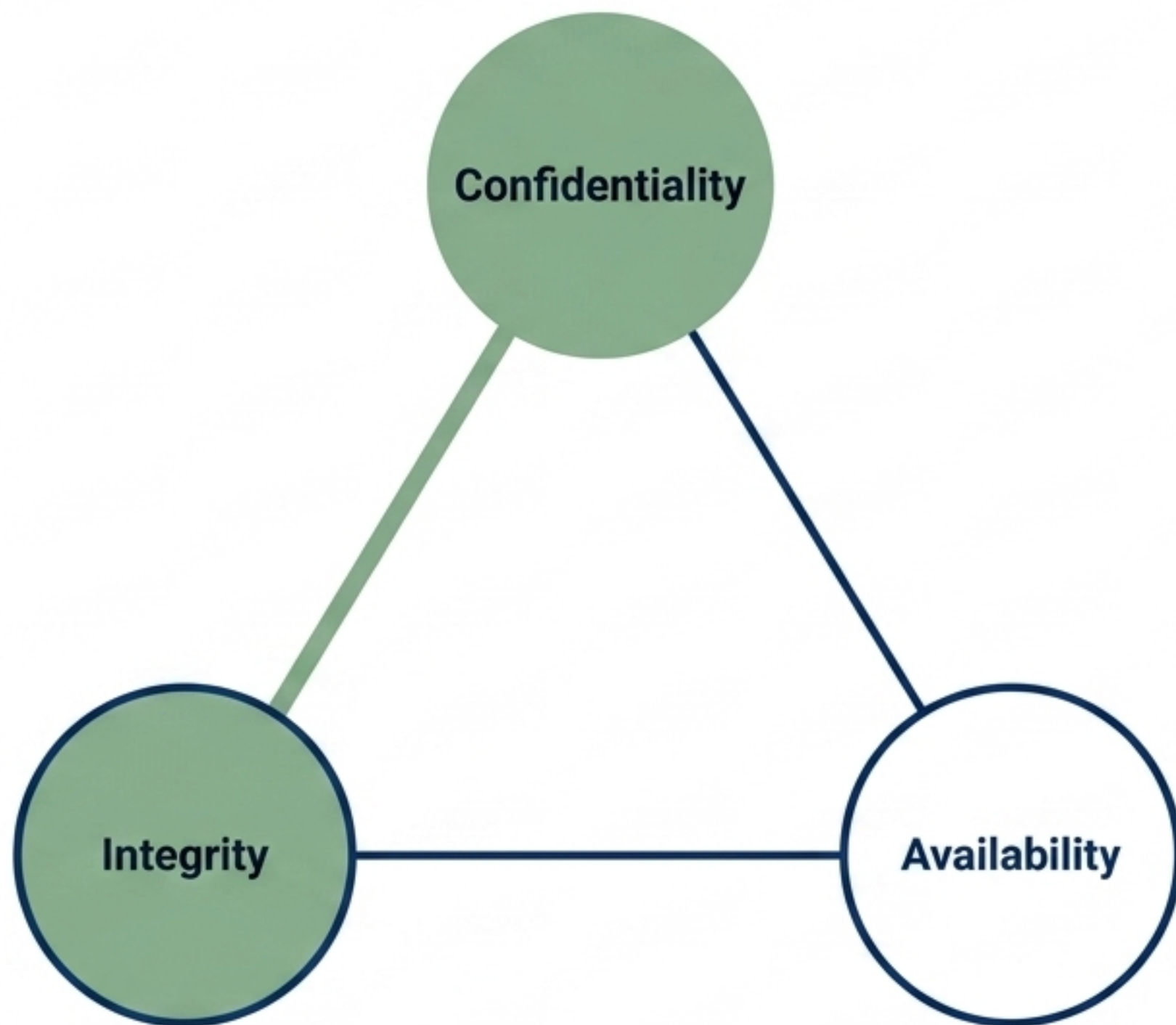
Fizična in logična bližina podatkov, modelov in strojne opreme masovno poveča število vstopnih točk.

Novi vektorji napada:



Prehod zahteva premik odgovornosti s ponudnika oblčnih storitev neposredno na operaterja Edge naprave.

Analiza CIA triade: Zaupnost in Integriteta



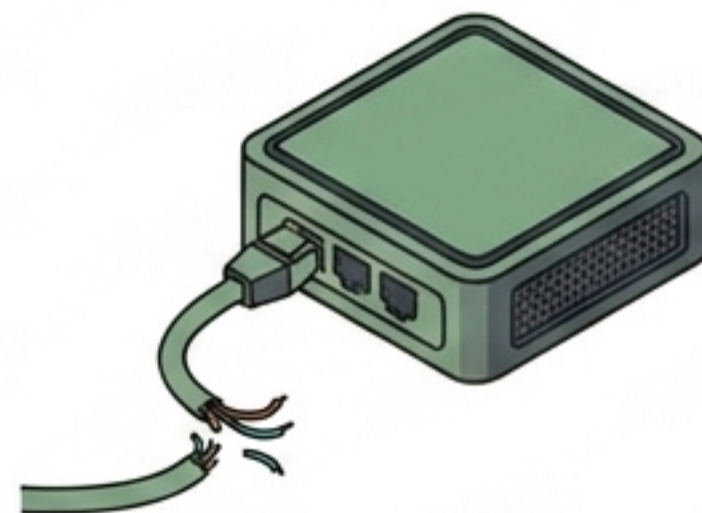
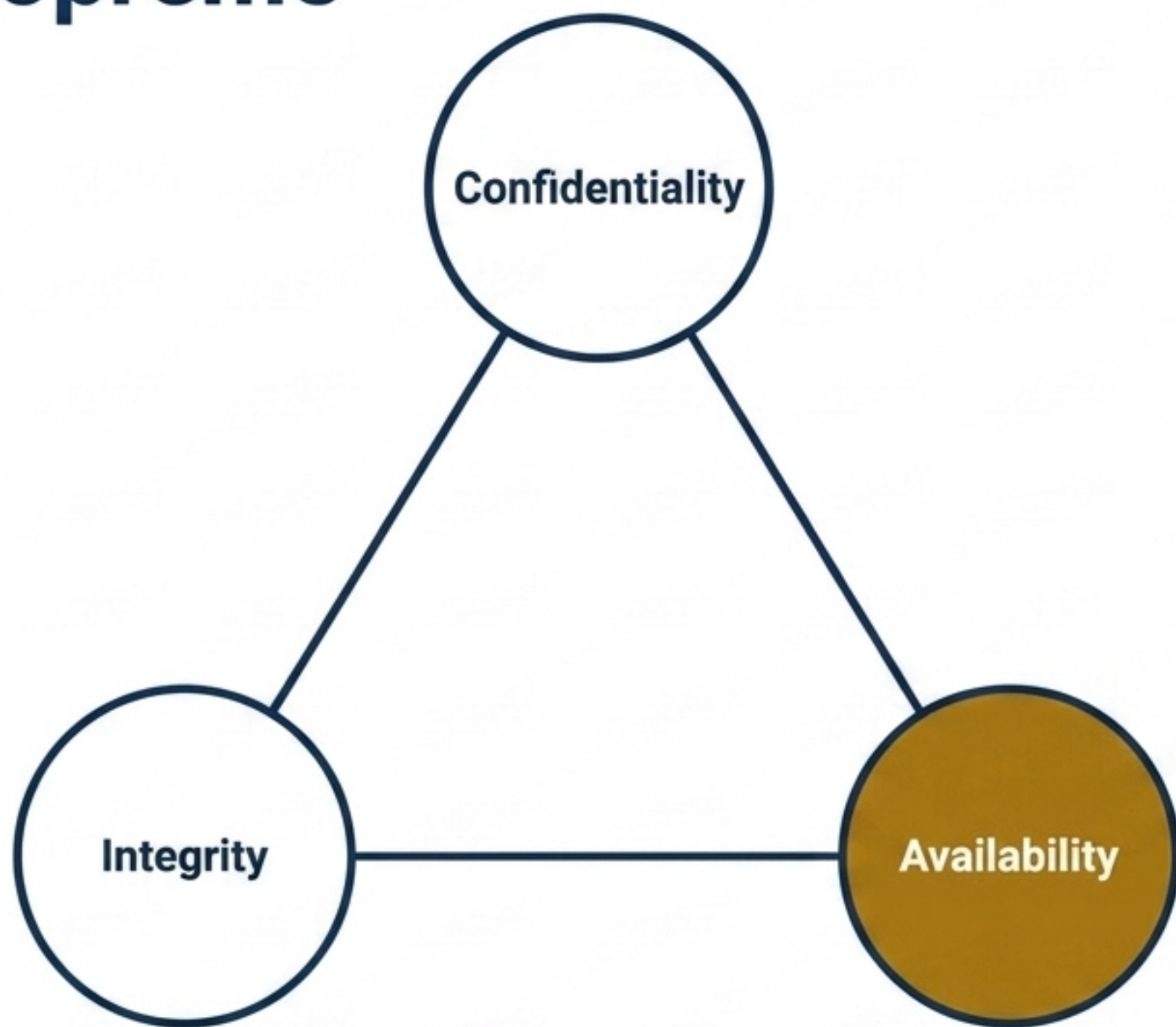
Zaupnost (Confidentiality):

Izboljšana. Ker ni prenosa v oblak, se tveganje za prestopanje podatkov močno zmanjša. Digitalna suverenost je okrepljena.

Integriteta (Integrity):

Mešano. Ni tveganja manipulacije med prenosom, vendar fizični dostop do Edge naprave omogoča neposredno manipulacijo lokalnih podatkov ali uteži UI modela (Model Poisoning).

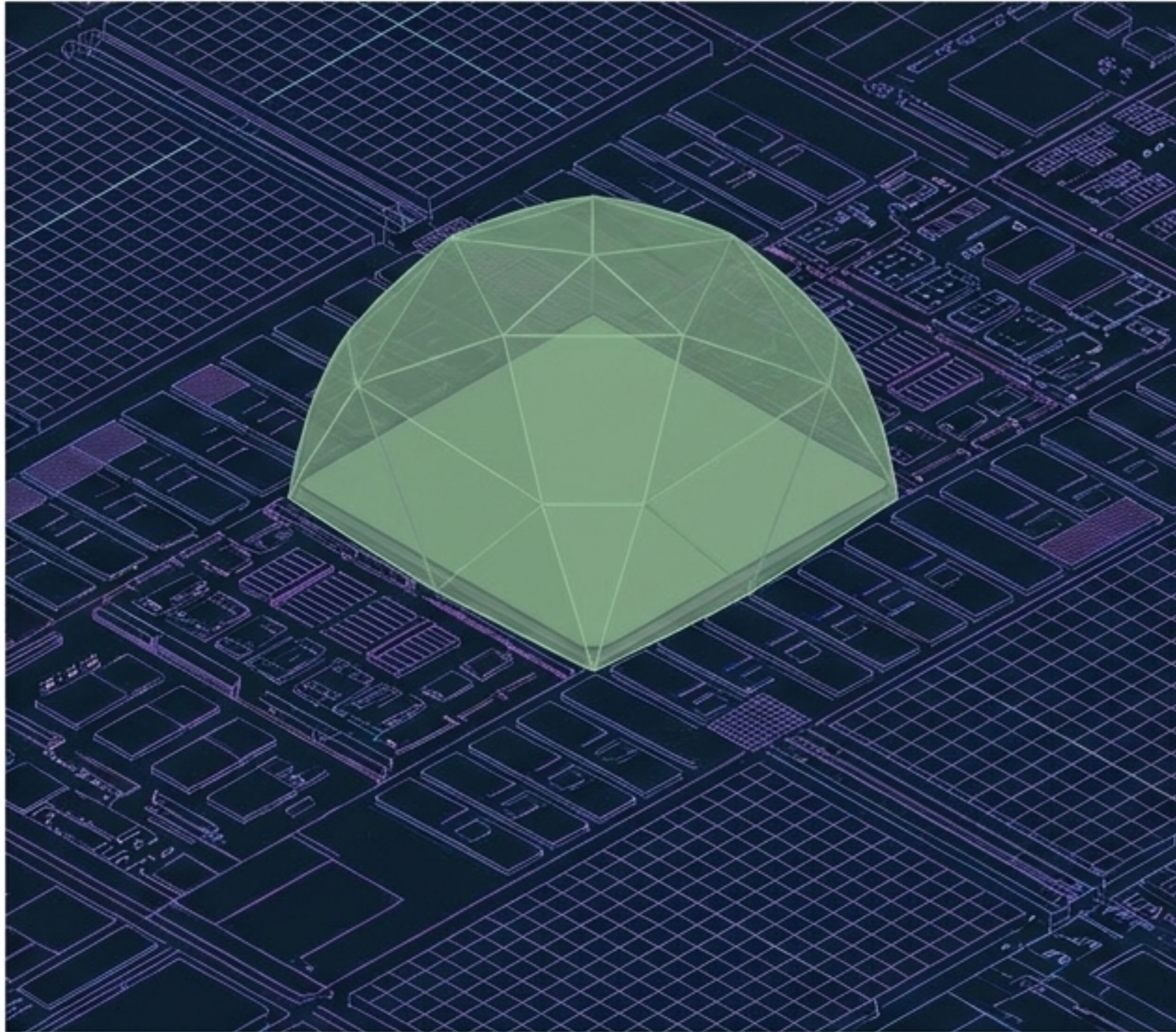
Analiza CIA triade: Razpoložljivost in tveganja strojne opreme



Odpornost omrežja: Delovanje je neodvisno od internetne povezave (velika prednost za kritično infrastrukturo).

Single Point of Failure (SPOF): Enotna točka odpovedi. Pri visoki stopnji lokalizacije izpad posamezne naprave pomeni popolno nedostopnost lokalnega UI modela, saj ni redundantnega sistema, ki bi prevzel proces.

Strojna izolacija: Trusted Execution Environments (TEE)

**Problem:**

Programska zaščita pri lokalno izpostavljenih napravah ne zadostuje.

Rešitev (TEE): Strojno podprta izolacija znotraj samega procesorja.

Mehanizem: Kriptografsko ločuje področje, kjer se obdelujejo podatki in izvaja koda UI modela, od preostalega operacijskega sistema in morebitnih zunanjih vdorov.

Arhitekturni ukrep: Zero-Trust načela



NIST SP 800-207:

Zanašanje na princip:
Nikoli ne zaupaj, vedno
preveri.

Odsotnost perimetra:

V Edge omrežjih varno
notranje omrežje ne
obstaja več.

Mehanizem žetonov:

Za vsak dostop do vira (UI
model, dataset, senzor) se
generira ločen žeton (access
token), ki ga je mogoče
v primeru varnostne grožnje
v realnem času preklicati.

Industrijski standardi in varnostne zahteve

Grožnje modelom

- Data poisoning (učni podatki)
- Model poisoning (uteži)
- Adversarial attacks (vhodni podatki)

IEC-62443

Standard za industrijsko avtomatizacijo zahteva strogo definicijo varnostnih con in ločevanje komunikacijskih kanalov.

EU AI Act (Člen 15)

Visoko tvegani sistemi (kritična infrastruktura) obvezujejo k 'Security by Design' – varnost mora biti vgrajena v arhitekturo od prvega dne, vključno z obveznimi 'Red Team' napadalnimi simulacijami pred implementacijo.

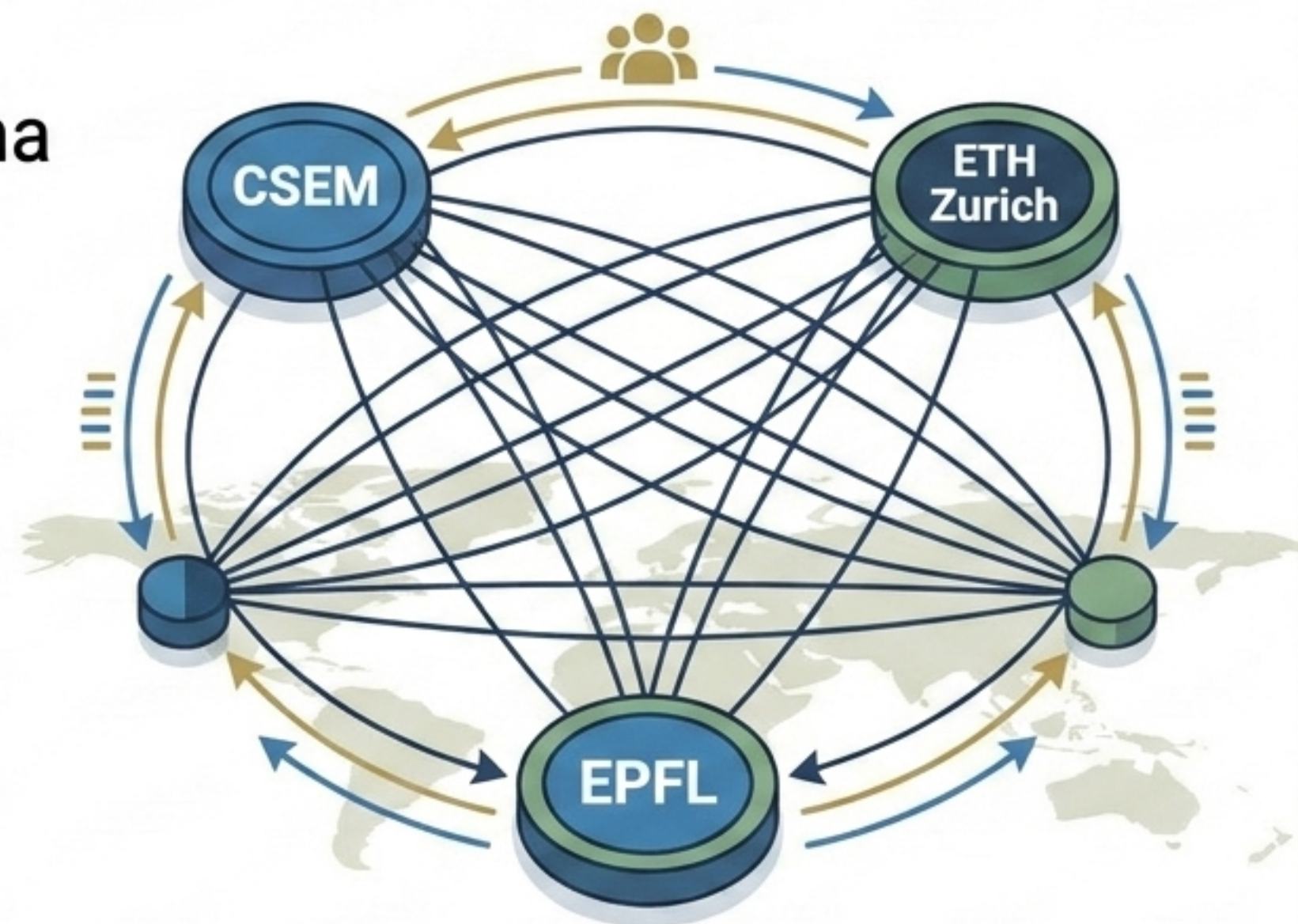
Strateški kontekst in raziskovalni ekosistem

Digitalna suverenost:

Zmanjšanje odvisnosti od tujih oblačnih storitev je prepoznano kot ključna strateška prioriteta (SATW).

Vodilne iniciative:

- Hardware za Edge AI: CONVOLVE (vključuje ETH Zurich, načrtovanje nanoelektronike/EPFL).
- Razložljivost in zaupanje: EdgeAI-Trust konzorcij (osredotočen na transparentnost sistemov in IoT).



Sinteza: Varnost kot temelj arhitekture



- Prehod na Edge AI rešuje fizikalne omejitve oblaka (latenca, pasovna širina), a drastično razširi površino kibernetских napadov.
- Prihodnost inženirstva ni le v optimizaciji učinkovitosti algoritmov, temveč v popolni integraciji koncepta Security by Design.
- Varnost in robustnost ne smeta biti naknadni dodatek – vsebovani morata biti v sami strojni in programski arhitekturi lokalne umetne inteligence.