

CYBER-PHYSICAL ENFORCEMENT ARCHITECTURE

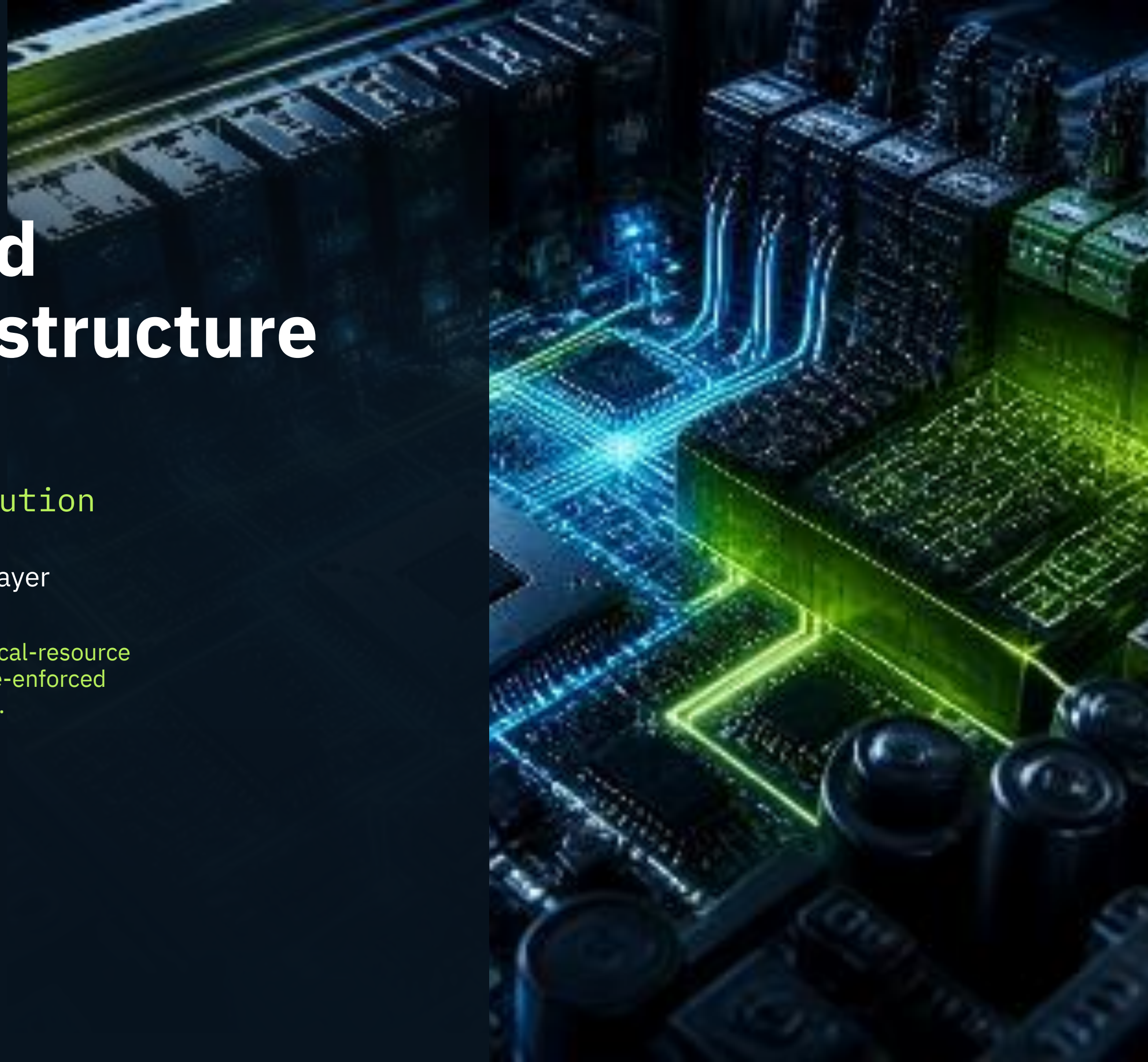
Hardware-Attested Autonomous Infrastructure Control System

with Resource-Bound Activity Execution

Defensible Cyber-Physical Control and Verification Layer

Patent scope centers on authenticated sensing, atomic physical-resource reservation, reservation-bound actuation authority, hardware-enforced release, protected metering and exclusive outcome evidence.

European Business Group – Dr. Wiegand Helmut FLEISCHER



Conventional control stops at the command

- 01 Authentication $\neq$ physical availability
- 02 Shared capacity can be overcommitted
- 03 Signed commands become stale
- 04 Cloud failure leaves infeasible dispatch
- 05 Logs cannot prove continuous linkage



From authentication to continuous proof

CONVENTIONAL

Origin only

Valid signature
Point-in-time check
Stale authority persists

Authentication proves origin. The patented architecture continuously proves current capacity, scope, freshness and usability at the point of actuation.

PATENTED

Reserved, sufficient and usable

Capacity • freshness • scope
Reservation-bound authority
Safe-state transition + terminal evidence

A narrow, explicit trusted computing base

INSIDE THE TRUSTED COMPUTING BASE

Authenticated sensing · secure controller state
Reservation engine/table · protected metering
Hardware-enforced actuator gateway · command counters
Inhibition path · secure time/monotonic state
Key material · evidence signing

OUTSIDE THE TRUSTED COMPUTING BASE

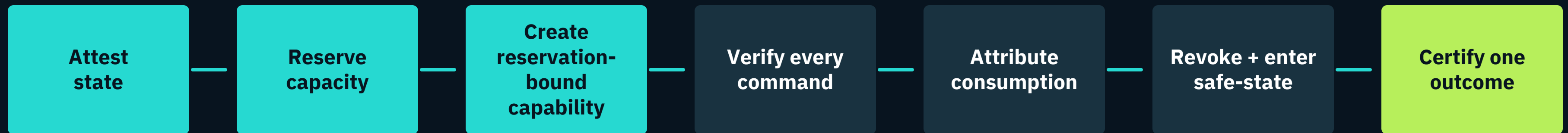
Cloud optimizer · coordinator
Enterprise scheduler · UI · analytics
Ledger · remote services

FAIL CLOSED

Loss of trusted time, freshness, authenticated sensing, metering integrity or gateway health revokes authority and fails closed.

Implementation obligations remain: calibration and plausibility, hazard-analysis adequacy, common-cause failure analysis and certification assessment.

End-to-end: evidence follows authority



Atomic admission → continuous reservation proof → bounded safe-state transition
→ exclusive evidence

No valid reservation, no actuation authority.

Conservation is the control law

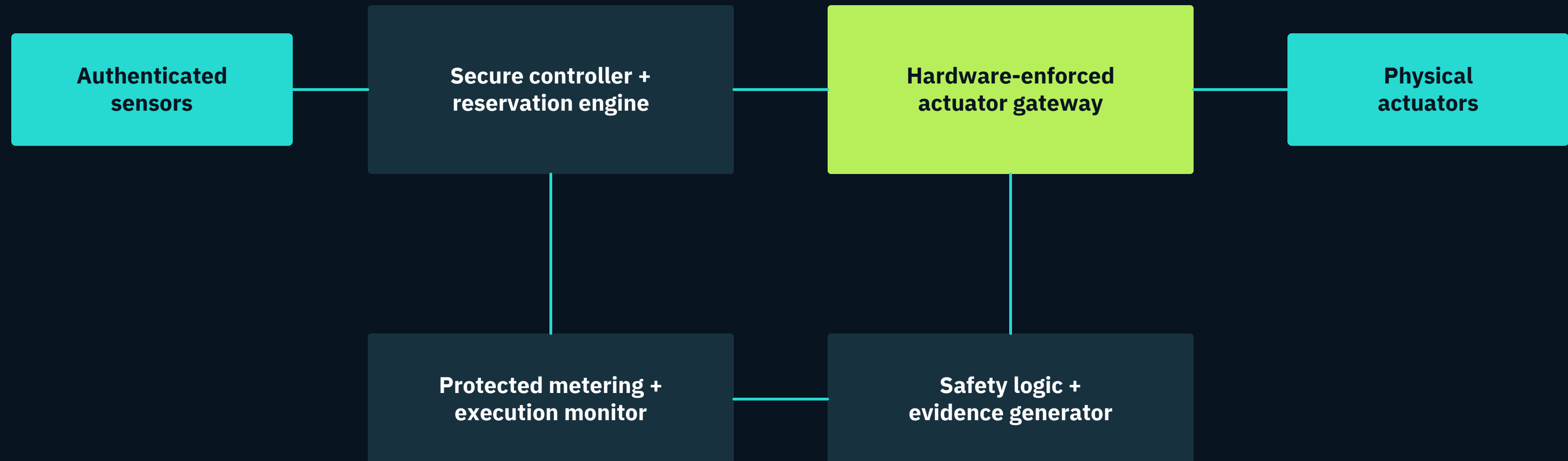
authenticated debit + certified remaining demand +
safe-transition reserve
 $\leq$ allocated capacity

UNIQUE RESOURCE ALLOCATION · CAPACITY CONSERVATION · AUTHORITY CONTINUITY
MONOTONIC EXECUTION · SAFE-STATE LIVENESS · OUTCOME EXCLUSIVITY · FRESH RESTART

Enforcement sits between intent and physics

EXTERNAL INTENT / ORCHESTRATION

TRUSTED LOCAL ENFORCEMENT CORE



Physical actuators are controlled only through the hardware-enforced actuator gateway.

Validation-to-use is one indivisible transaction



Any failed predicate → no actuator-control signal

**Reservation-bound capability · current
reservation-state root
Remaining-capacity certificate · actuator
scope/range
Expiry · monotonic command counter**

No maintenance, recovery, diagnostic or DMA path may bypass the actuator gateway.

Atomic gateway transaction: validation, state update and actuator release are indivisible.

Illustrative Use Case: Automotive Battery-Pack Testing

RESERVE

Power · thermal headroom · cooling
bench time · communications · safe-stop energy

VERIFY

Every charge, discharge and thermal command

REVOKE + ENTER SAFE STATE

Isolation loss · cooling degradation · over-consumption ·
replay · expiry

Loss of proof → capability revoked → bounded safe-state transition.



One control primitive, many constrained systems

01

Automotive plants

02

Factories

03

Microgrids

04

Charging depots

05

Buildings

06

Data centers

07

Farms

08

Water facilities

09

Mines

10

Remote sites

Technical control becomes independently verifiable evidence

Prevent conflict

Atomic reservation blocks shared-capacity overcommit.

Reduce exposure

Deterministic inhibition bounds unsafe-state duration.

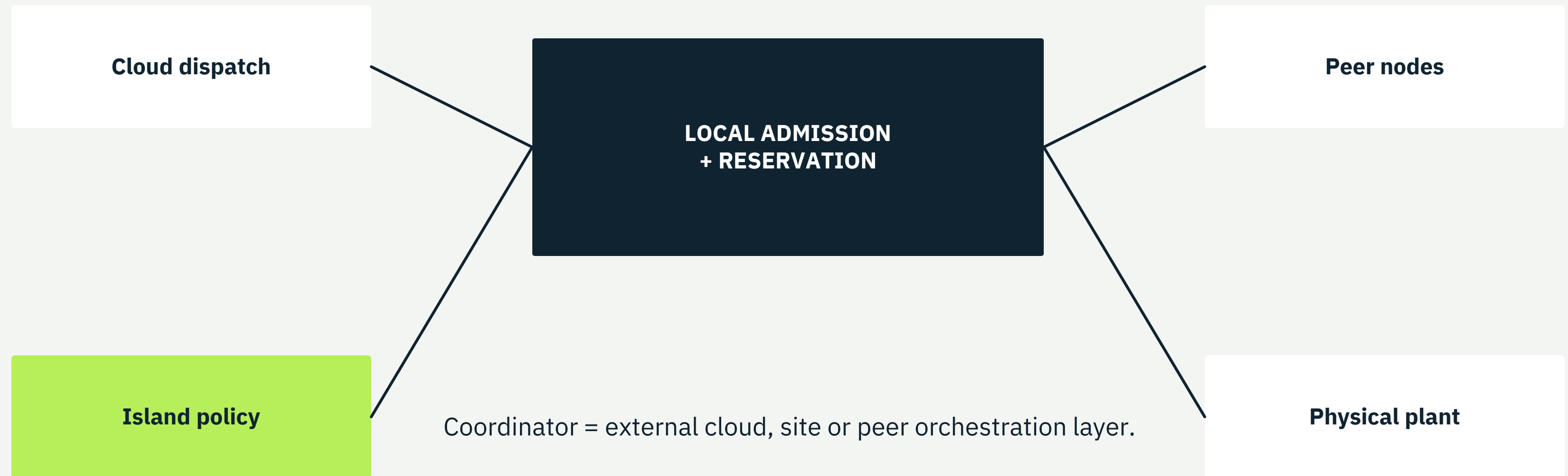
Prove attribution

Consumption and outcomes remain tamper-evidently linked.

Operate locally

Coordinator loss does not erase feasible authority.

Federated by policy. Islandable by physics.



Local admission and reservation remain authoritative; physically unreservable dispatch is rejected, and authenticated island policy persists through communication loss.

Assurance scales with the enforcement substrate

FPGA / ASIC

Preferred enforcement substrate; strongest physical mediation

Secure MCU

Alternative enforcement substrate where timing and assurance targets are met

TPM / HSM

Supporting root of trust; not a substitute for actuator-path enforcement

TEE

Optional isolation layer; not a substitute for the gateway

Redundant safety

Independent inhibition path

Distributed nodes

Scale and resilience across sites

ASSURANCE EVIDENCE READINESS

ISA / IEC 62443

Industrial cybersecurity lifecycle



IEC 61508

Functional safety evidence

ISO 26262

Automotive safety cases

The architecture can support implementation-specific evidence for ISA/IEC 62443, IEC 61508 and ISO 26262. It does not itself confer or guarantee certification. Hazard analysis, validation, process evidence, configuration control and independent assessment remain implementation- and deployment-specific.

Acceptance is binary, measurable and adversarial

01

No double allocation

02

No stale actuation

03

Atomic validation-to-use

04

Bounded inhibition latency

05

Capacity conservation

06

Outcome exclusivity

07

Coordinator independence

08

Recovery freshness

Attest → authenticated freshness | Reserve → no double allocation | Bind → reservation-bound authority | Execute → atomic validation-to-use | Revoke → bounded inhibition latency | Certify → outcome exclusivity.

INVESTOR TAKEAWAY

**Authority exists only while reserved physical conditions remain continuously provable.
Loss of proof revokes authority and triggers a bounded safe-state transition.**

A defensible cyber-physical enforcement and verification layer for autonomous infrastructure—beyond command authentication.

INVEST IN THE ENFORCEMENT LAYER

Hardware-attested · resource-bound · independently verifiable

European Business Group
Dr. Wiegand Helmut FLEISCHER
wiegandhelmut.fleischer@gmsil.com