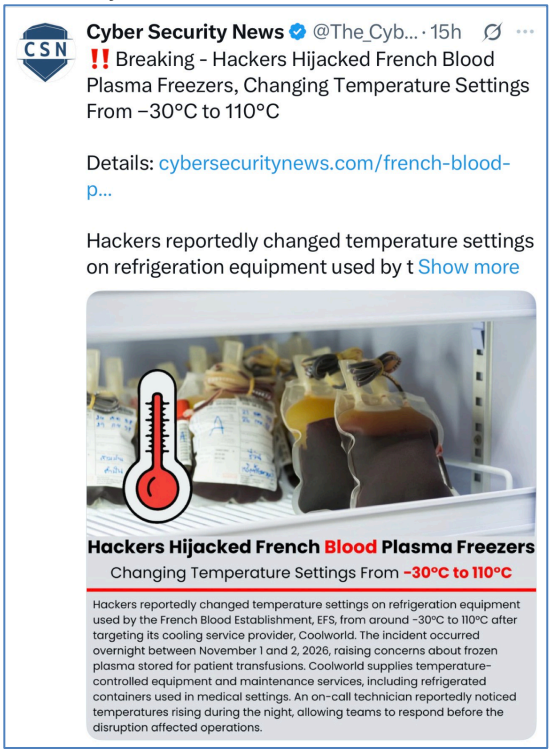
117-342-D CABOC-D and the 3-Layered SI-Economy

Cross-Layer Cascade Propagation, Physical Resource Protection, and Roving Observability

I. When a Digital Command Threatens a Physical Resource

A refrigeration unit holding blood plasma is not merely an IT asset. It is a physical preservation system whose operating state determines whether irreplaceable biological inventory remains suitable for clinical use. A digital command that changes its temperature setpoint crosses an important boundary: software instruction becomes a physical demand imposed upon matter.



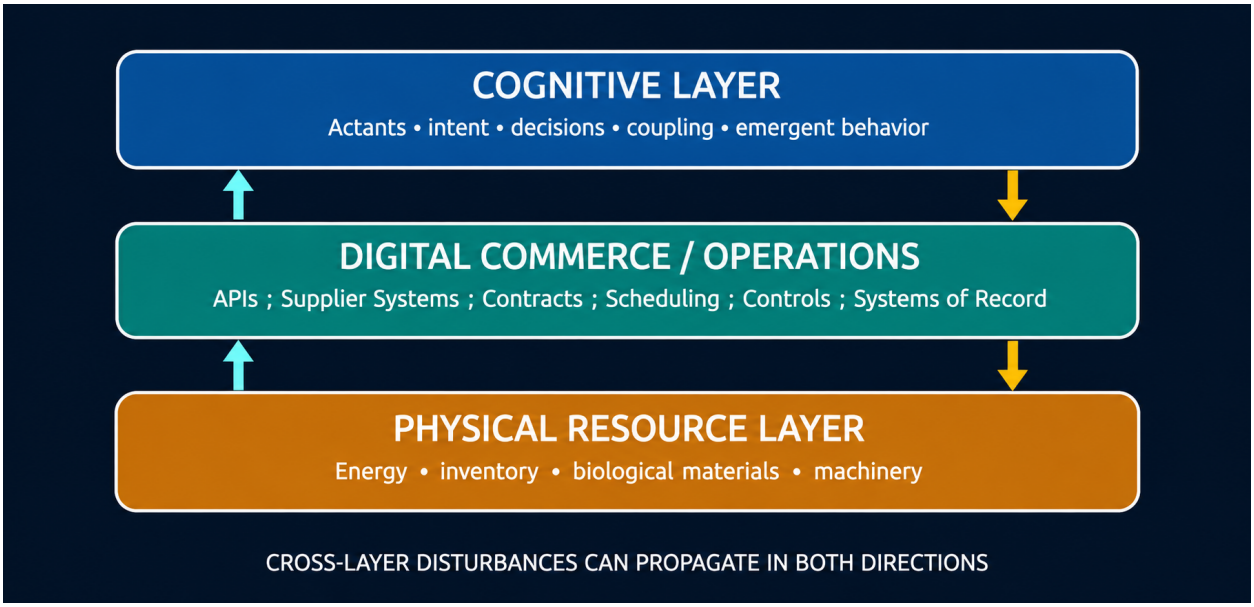
A reported incident involving French blood-plasma refrigeration systems in November 2026 described unauthorized changes to temperature setpoints from approximately −30°C toward +110°C through a supplier-related control pathway. The reported figures concern setpoints, not evidence that the stored material reached that temperature. Monitoring and intervention reportedly prevented product loss. The case is used here as an illustrative cyber-physical pathway; it is not evidence that autonomous SI agents participated in the intrusion.

For GUDIYA, the engineering lesson is that a disturbance originating in digital infrastructure can threaten physical resources. Those physical resources, in turn, may shape subsequent economic and cognitive activity. The incident need not remain confined to its originating layer.

II. The Three-Layer SI-Economy Is One Coupled System

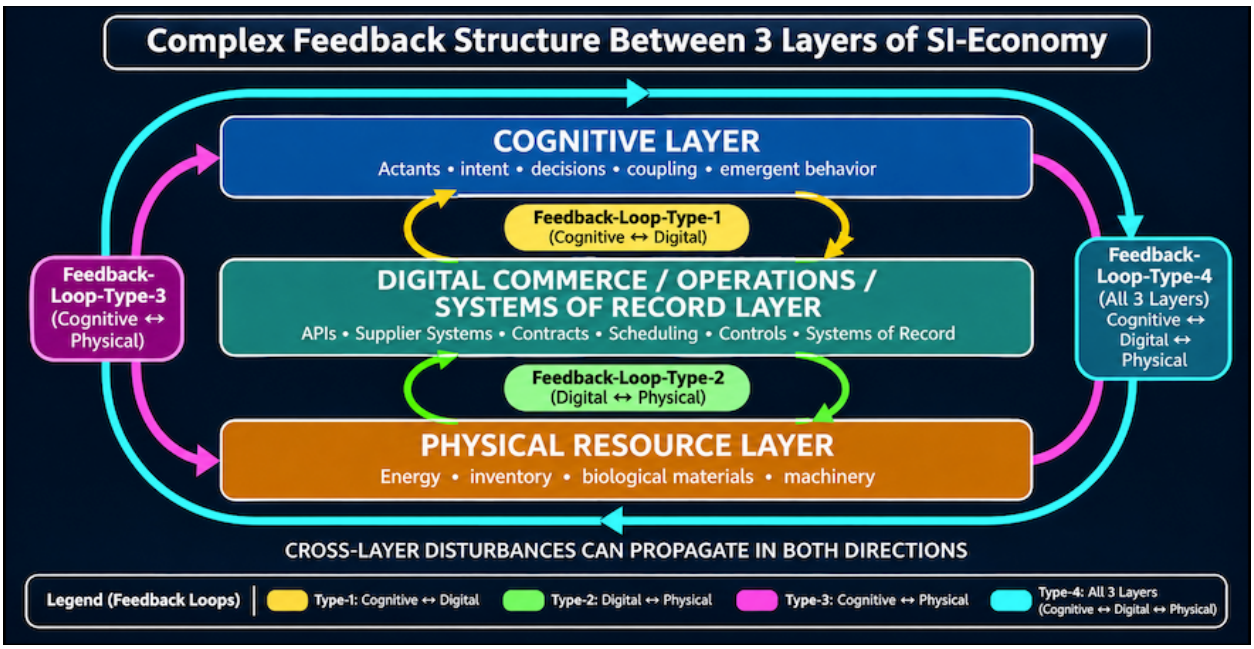
The proposed three-layer SI-Economy comprises a cognitive layer of intelligent actants and their decisions; a digital commerce and operational layer of platforms, transactions, tools, contracts, and control interfaces; and a physical resource layer containing energy, inventory, equipment, materials, logistics capacity, and other tangible assets.

These are analytical layers, not independent worlds. A cognitive decision can produce a digital commitment; a digital control command can alter equipment; a physical shortage can modify market signals; and the changed signals can return to cognitive agents as new evidence. A closed causal loop may therefore span all three layers.



Importantly, the physical layer has irreversibility and conservation constraints. Destroyed biological material cannot be restored by resetting a database. Lost energy, wasted inventory, and damaged machinery impose physical and economic costs even after the initiating software defect is repaired.

The Complex Feedback Structure of the Three-Layered SI Economy



The three-layered SI economy is not merely a vertically integrated architecture consisting of the Cognitive Layer, the Digital Commerce-Operations-Systems of Record Layer, and the Physical Resource Layer. It is a dynamically coupled system containing multiple, overlapping, and potentially reinforcing feedback loops. As illustrated in the accompanying figure, four fundamental feedback structures can be identified.

- Feedback Loop Type 1 connects the Cognitive Layer with the Digital Commerce and Operations Layer, allowing autonomous decisions to influence transactions, contracts, schedules, and systems of record, whose changing states subsequently influence further cognitive decisions.
- Feedback Loop Type 2 connects the Digital Operations Layer with the Physical Resource Layer, where digital commands influence machinery, energy, inventory, and material flows, while changing physical conditions generate new operational signals.
- Feedback Loop Type 3 represents the coupling between the Cognitive and Physical Resource Layers, where cognitive decisions may influence physical resources through control pathways, and physical conditions may directly inform sensing, reasoning, and autonomous responses.
- Feedback Loop Type 4 traverses all three layers, forming an extended feedback circuit in which cognitive decisions produce digital actions, digital actions alter physical conditions, and the resulting physical consequences return through operational systems to influence subsequent cognition.

These loops are not necessarily independent; they may intersect, overlap, and dynamically modify one another. Under certain combinations of coupling gain, propagation delay, interaction topology, and insufficient damping, a localized disturbance may circulate repeatedly, amplify, and potentially contribute to Cognitive Cascade Saturation (CCSat). This is precisely why CABOC-D must treat the entire three-layered SI economy as an interconnected defensive object rather than as three separately protected domains. Its Cross-Layer Roving AWACS capability is proposed to follow disturbances across these feedback structures, identify their sustaining pathways, and provide the evidence necessary for timely stabilization and consequence-aware recovery.

The fundamental engineering implication is that a disturbance originating in any one layer may become self-sustaining through feedback involving the others. Protecting individual layers is necessary, but assuring ecosystem stability requires observing and governing the feedback relationships that connect them.

The Four Fundamental HCAS Stability Challenges

The GUDIYA Stability Engineering framework identifies four fundamental challenges that complicate the observation, governance, and stabilization of Hyper-Complex Adaptive Systems (HCAS), particularly within the interconnected three-layered SI economy.

Challenge 1 — Machine-Speed Time Compression

Autonomous intelligent actants can perceive, reason, decide, invoke tools, and interact with other actants at computational speeds. Consequently, disturbances may propagate through multiple decision chains and feedback circuits in milliseconds or seconds, compressing the available time for detection, interpretation, and corrective intervention. When the time required for human intervention exceeds the time available before unacceptable consequences occur, conventional human-in-the-middle supervision becomes insufficient as the primary stabilization mechanism. HCAS therefore requires appropriately authorized, locally executable, machine-speed stabilization capabilities.

Challenge 2 — Numerical Explosion of Intelligent Actants

The proliferation of autonomous SI introduces the possibility of enormous populations of simultaneously operating intelligent actants. These actants dynamically form teams, establish dependencies, exchange information, and create or dissolve interaction relationships. As the population grows, the number of possible coupling relationships and propagation pathways can increase dramatically, although actual connectivity depends on the system's topology. This hyper-scale expansion challenges centralized monitoring, coordination, computational capacity, and governance. HCAS therefore requires scalable, hierarchical, distributed, and risk-adaptive stabilization mechanisms.

Challenge 3 — Multiple Interacting and Interdependent Feedback Loops

Unlike systems characterized by a small number of relatively stable feedback circuits, HCAS may contain numerous dynamically evolving feedback loops that overlap, intersect, reinforce, or counteract one another. Within the three-layered SI economy, these loops may operate between

- Type 1 the Cognitive and Digital Layers,
- Type 2 Digital and Physical Resource Layers,
- Type 3 Cognitive and Physical Resource Layers, or
- Type 4 traverse all three layers.

Disturbances may migrate between these circuits, undergo amplification, and potentially establish recurrent propagation pathways that persist after the originating perturbation disappears. HCAS therefore requires ecosystem-level observability, coupling management, feedback-gain regulation, and mechanisms for detecting and interrupting self-sustaining cascades.

Challenge 4 — Nyquist-Related Limits on Observability

Every monitoring and stabilization system operates with finite sensing frequency, telemetry bandwidth, processing capacity, and communication latency. When consequential system dynamics evolve faster than the observation infrastructure can adequately resolve, rapid oscillations, transient deviations, and emerging instabilities may be missed or misrepresented through perceptual aliasing. Classical Nyquist sampling theory establishes precise reconstruction conditions for appropriately band-limited signals; nonlinear, asynchronous, and discontinuous cognitive processes require additional observability methods beyond those assumptions. HCAS therefore requires adaptive sampling, event-triggered telemetry, local high-resolution sensing, uncertainty-aware state estimation, and explicit recognition of observational blind spots.

The Combined HCAS Stability Challenge

These four challenges are mutually reinforcing.

- Machine-speed interactions compress the intervention window;
- numerical hyper-scale expands the population of interacting actants;
- multiple feedback loops create complex and potentially self-sustaining propagation pathways;
- and observability limitations may prevent the Grid from detecting instability before effective intervention becomes impossible.

Their interaction creates the possibility that the Cognitive Ecosystem's dynamics may exceed its available observation and stabilization capacity. The central GUDIYA engineering challenge is therefore to maintain sufficient observability, control authority, intervention speed, and survivability under the simultaneous pressures of time compression, hyper-scale, interacting feedback loops, and measurement limitations.

III. The Cross-Layer Cascade Mechanism

Consider a hypothetical sequence.

1. A supplier control pathway is compromised.
2. A refrigeration setpoint is changed. Inventory becomes unsafe or unavailable.
3. Logistics systems report scarcity.
4. Procurement agents order replacement supply.
5. Financial agents revise spending limits.
6. Production systems alter schedules.

These legitimate downstream responses may then affect other enterprises, causing a second round of scarcity signals and new decisions.

The initial compromise may have been local, but the consequential propagation becomes systemic. No second attacker is necessary once ordinary feedback relationships carry the disturbance onward. Equally, an autonomous-agent cascade can begin without a cyberattack: many authorized procurement agents may respond to the same signal and collectively generate a physical shortage.

The central research question is whether the combined system exhibits damping, transient propagation, reverberation, or persistent cascade saturation. These are different dynamical regimes, and CABOC-D must not treat them as interchangeable.

IV. From Elevated Awareness to Cross-Layer Roving AWACS

The original enterprise AWACS concept gave actants a localized view of the global GUDIYA Grid. Roving Cognitive AWACS extended that idea by redirecting observational attention across actants, Synchronization Zones, Intent Groups, and emergent behavior instances. The next extension is consequential: the disturbance may cross the three layers of the SI economy, so the observer must be able to follow its effects across those layers rather than remaining confined to cognitive telemetry.

Cross-Layer Roving AWACS (CL-RAC) is a proposed CABOC-D observational capability that follows a selected disturbance or consequence chain through cognitive decisions, digital operations and systems of record, and physical-resource measurements. Roving means reassignment of sensing and analytical attention—not unrestricted migration of executable code or privileged access into equipment.

A persistent local sensing baseline remains essential. Roving attention cannot recover events never recorded, and it cannot substitute for independent physical safety interlocks. Multiple concurrent observation missions may be needed when cascades branch faster than a single observer could traverse them.

Three generations of AWACS

Enterprise AWACS	**Persistent localized enterprise or Sync Zone view of the Grid.**
Roving Cognitive AWACS	Risk-directed observation across actants, coupling neighborhoods and emerging behaviors.
Cross-Layer Roving AWACS	Evidence-led observation of causal pathways across cognitive, digital and physical layers.

V. Cross-Layer Observation Mission (CLOM) as a First-Class Object

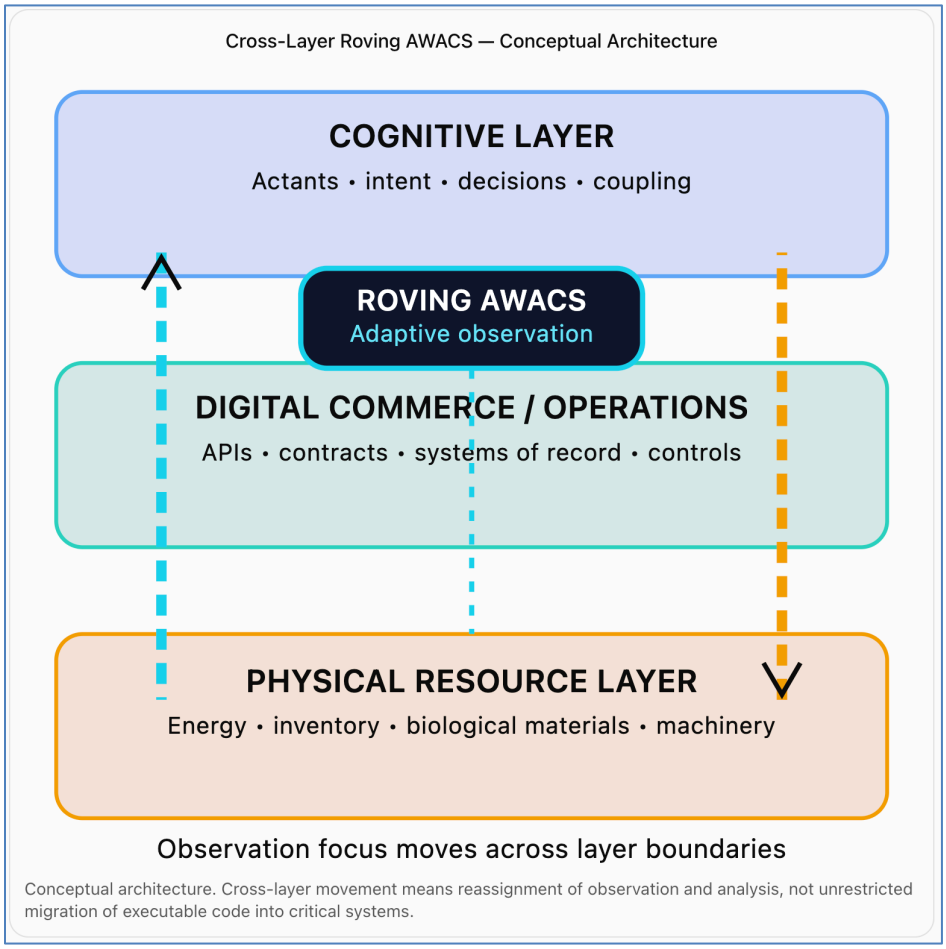
A Cross-Layer Observation Mission (CLOM) should itself be a first-class, auditable object. It follows a target such as an Emergent Behavior Instance, Cognitive Cascade Object, or Physical Resource Consequence even as the affected actants, records, machines and organizational boundaries change.

The mission record would include a persistent mission identifier, triggering evidence, target-object identity, authorized scope, observation adapters, frame and schema versions, time alignment, evidence provenance, uncertainty, compute and telemetry budget, escalation interfaces, and termination or handoff criteria. Every expansion into another enterprise or control domain requires fresh authorization, not an assumed right of passage.

Cross-Layer Causal Reference Model (CLCRM)

The three layers do not share one measurement language. Cognitive events describe intent, authority and coupling; digital systems describe transactions, contracts, APIs and records; physical systems describe temperatures, pressures, inventory and machinery states. CLCRM is the proposed evidence model connecting these heterogeneous observations through identities, timestamps, commands, measured effects and dependency relationships without pretending that their variables are interchangeable coordinates.

A causal chain must distinguish a command from its physical effect and correlation from demonstrated causation. For example, a setpoint change, a temperature sensor reading and a subsequent inventory decision are three distinct observations; the linkage among them must be supported by evidence and uncertainty annotations.



VI. A Roving AWACS Patrol Through the Three Layers

Consider a hypothetical incident patterned after the reported refrigeration-control case. An abnormal command is detected at a supplier-connected control interface in the Digital Commerce/Operations layer. A CLOM is initiated and the AWACS directs attention to signed command logs, operator identities, access paths and the affected systems of record.

The mission next requests authorized telemetry from the Physical Resource layer: actual temperatures, setpoints, alarm histories, exposure duration and the status of biological inventory. It then moves analytical attention to the Cognitive layer, where logistics and procurement agents may be revising forecasts or commitments in response to perceived shortages. New purchase orders and schedules carry the investigation back into the digital layer; the resulting resource movements or shortages carry it back into the physical layer.

The AWACS does not merely collect five unrelated dashboards. It maintains the evolving, evidence-qualified causal hypothesis and follows its branches. This is how CABOC-D can investigate a feedback circuit that traverses all three layers, including a possible reentry loop in which physical scarcity triggers decisions that worsen scarcity.

Observation is not control

CL-RAC remains read-only by default. Local observation adapters enforce least privilege, time-limited credentials, data minimization and enterprise boundaries. Active probes require explicit authorization and isolation. RM, CACS, stabilization sidecars, industrial protection systems and human operators retain their separate intervention responsibilities. A compromised observer must not be able to override safety interlocks or alter physical control setpoints.

VII. Expanding CABOC-D's First-Class Defensive Objects

CABOC-D preserves the established cybersecurity objects:

- vulnerabilities,
- threats,
- assets,
- identities,
- events, and
- incidents.

It additionally proposes explicit representation of the Cognitive Ecosystem and Emergent Behavior Instances. Cross-layer analysis now motivates a further candidate object: the Physical Resource Consequence (PRC).

A PRC represents an observed or credibly threatened change to a physical resource arising through a digital, operational, or cognitive causal pathway. Its record could include resource identity, physical state, exposure duration, originating action, downstream dependencies, reversibility, uncertainty, responsible authority, and verified disposition.

A PRC is not simply another alert. It persists while consequential physical conditions remain unresolved. The object allows the Grid to connect security incident evidence, cognitive decision lineage, and the state of the resource itself without assuming that all three can be repaired by the same action.

Illustrative first-class object relationships

Cross-Layer Roving AWACS in BEFORE

During pre-attachment readiness, a CLOM can trace high-consequence dependency paths from Crown Jewels to supplier APIs, systems of record, control interfaces and physical resources. This supports risk-directed selection of SCWS inspections and independent physical safety checks. It must not imply that the Grid can

scan every third-party system: observation is limited to authorized surfaces and explicitly reported coverage gaps.

VIII. BEFORE — Mine-Clearing and Cross-Layer Readiness

The BEFORE phase extends the Standoff Cognitive Weapon Sweeper (SCWS) beyond a narrow search for malicious text. It combines the Grid repository of validated cognitive mines with authorized mapping of the digital-to-physical approaches to Crown Jewels. Relevant paths may include equipment-control APIs, vendor maintenance access, supplier documents, tool metadata, memory stores, and actant privileges.

The Grid should distinguish what it can inspect from what it cannot. It may assess an authorized enterprise integration but cannot presume permission to probe third-party infrastructure. Static inspection, synthetic-data behavioral testing, conventional vulnerability assessment, and safety-boundary review provide complementary evidence.

Pre-attachment approval should be risk-adaptive. Where a physical resource is high consequence, an actant may require restricted control authority, independent equipment interlocks, and human approval for changes to critical process parameters. A clean cognitive sweep cannot establish that physical controls are safe.

Cross-Layer Roving AWACS in DURING

When an EBI or CCO begins propagating, CL-RAC can follow the disturbance across layer boundaries and request higher-resolution evidence where risk-weighted uncertainty is greatest. Its findings inform RM restrictions, CACS local controls, breakwater isolation and physical-system operators. Under machine-speed time compression, these roving investigations complement preauthorized local controls; they cannot become a mandatory centralized step before urgent containment.

An active-observability policy should balance expected risk-weighted information gain against telemetry cost, sampling delay, privacy exposure and observer-induced load. Persistent local event capture remains necessary because Nyquist-related aliasing cannot be repaired by an observer arriving after the evidence was lost.

IX. DURING — Detecting and Constraining Cross-Layer Propagation

The DURING phase treats the physical consequences of cognitive and digital actions as part of the ecosystem state. GUDIYA could correlate GCID-linked decisions, Rendezvous Management events, equipment-control requests, sensor readings, and resource-state changes. This permits a distinction between an authorized command and an authorized command producing an unsafe collective outcome.

When a developing cascade threatens the resource layer, the Grid may restrict new actant commitments, damp coupling gain, isolate unsafe rendezvous relationships, or request escalation. These controls must be pre-authorized, proportionate, and timed against the physical process. They cannot replace equipment-level safety systems, whose independent interlocks must remain effective even if the Grid is unavailable.

The four HCAS constraints matter simultaneously: machine speed compresses intervention deadlines; hyper-scale multiplies propagation paths; unbounded domains obscure dependencies; and sampling or observability gaps may conceal rapidly changing conditions. A physical process may become irreversible before a centralized human-in-the-middle review can complete.

Cross-Layer Roving AWACS in AFTER

After containment, the same CLOM can preserve an evidence trail across GCID-linked decisions, digital records, equipment histories and physical resource assessments. The mission helps investigators separate Security Incident Closure, Cognitive Consequence Closure and Physical Resource Consequence Closure. It also identifies unresolved branches that require reinspection, compensating transactions, quality assurance or restricted reauthorization.

X. AFTER — Three Forms of Consequence Closure

Closing the original vulnerability is necessary but may be insufficient. CABOC-D proposes distinct assurance outcomes: Security Incident Closure (SIC) for the initiating compromise; Cognitive Consequence Closure (CCC) for decisions, memories, authority changes, and propagated actions; and Physical Resource Consequence Closure (PRCC) for material losses, equipment condition, and safety disposition.

PRCC requires evidence from the physical domain. For temperature-sensitive biological materials, that may include validated sensor history, quality-control decisions, product quarantine or disposal, and authorization by competent operators. A software rollback cannot certify material safety.

The Cognitive DVR and decision ledgers should preserve a chain from originating artifact through decisions and tool invocations to physical effects. Missing observations and uncertain causal links must remain explicitly marked. Recovery should proceed through containment, evidence preservation, physical assessment, state reconciliation, independent validation, and controlled reauthorization.

XI. Resource-Layer Reverberation and Cognitive Cascade Saturation

Cross-layer propagation becomes especially challenging when physical resource scarcity itself acts as a new stimulus. A shortage can cause autonomous agents to increase demand, producing further shortages. Under some feedback structures, the original initiating disturbance may disappear while the ecosystem continues to generate harmful activity.

This resembles, by analogy rather than physical equivalence, reentrant cardiac excitation or self-organized traffic waves. The proposed Cognitive Cascade Saturation (CCSat) hypothesis asks whether recurrent, overlapping disturbances can consume stabilization capacity and sustain an unstable operating regime.

The engineering objective is to characterize the gain, latency, topology, and resource constraints that determine whether a disturbance decays or persists. A strong claim requires simulation and empirical evidence; the analogy alone cannot establish the phenomenon.

Comparative CL-RAC experiment

A controlled testbed should compare fixed-layer monitoring against cross-layer roving observation using the same compute and telemetry budget. Inject a bounded disturbance that moves from digital command to physical effect to cognitive reaction and back into digital transactions. Measure time to detect cross-layer transition, causal-chain reconstruction precision and recall, time to containment, cascade reach, resource loss, false-positive disruption and recovery assurance. Include missing sensors, delayed timestamps, partitions and maliciously misleading records. A null or negative result would constrain the architectural claim.

XII. Engineering Demonstration and Measurements

A reproducible testbed should model a small supply network with cognitive procurement agents, digital ordering and equipment-control interfaces, and a constrained physical inventory. Researchers can inject a bounded digital-control fault or a nonmalicious demand perturbation, then observe propagation across layers.

Candidate measures include time to physical consequence, propagation fan-out, resource loss, coupling amplification, time to containment, stabilization capacity utilization, false-positive intervention cost, recovery time, and unresolved consequence backlog. The experiment should compare conventional security controls alone against a configuration that additionally implements CABOC-D-style ecosystem observability and stabilization.

Controls should be tested separately and in combination: SCWS inspection, provenance validation, interaction-rate limiting, Rendezvous Management restrictions, CACS local correction, breakwater isolation, and independent physical interlocks. A failed experiment is informative; the purpose is to discover where the proposed controls work and where they do not.

XIII. Survivability and Institutional Accountability

When physical assets are involved, survivability is more than continuity of computing. Essential services, legitimate authority, safe physical states, and verified resource quality must persist through disruption. The Greenbrier-inspired continuity doctrine is relevant because emergency governance and alternate operating arrangements must exist before the crisis begins.

No single Grid operator should be able to override all physical safety constraints. Local operators, equipment protection systems, enterprise owners, and appropriate regulators retain distinct responsibilities. Federated evidence sharing should reveal actionable threat patterns without exposing confidential process data unnecessarily.

Cross-layer recovery also requires clear authority to quarantine materials, stop machinery, cancel commitments, or restart production. CABOC-D should support these decisions with evidence and bounded controls, not assume authority that has not been granted.

XIV. The Cross-Layer Consequence Principle

In the three-layer SI-Economy, disturbances originating in cognitive or digital systems may propagate into the physical resource layer and create material consequences that cannot necessarily be reversed through software remediation. Physical consequences may subsequently propagate upward through scarcity, operational disruption, economic commitments, and autonomous actant interactions.

CABOC-D therefore proposes that cross-layer propagation and physical resource consequences become explicit objects of observation, containment, investigation, and verified recovery. Closure of the initiating cybersecurity incident shall not be presumed to establish closure of its cognitive, operational, or physical consequences.

XV. Closing — Protecting the Whole SI-Economy

The three-layer SI-Economy is not stable merely because its software is patched, its agents are authenticated, or its transactions are authorized. Its physical resources, digital operations, and cognitive relationships form a coupled system whose behavior must be examined as a whole.

CABOC-D does not replace cybersecurity, industrial control-system safety, or human institutional responsibility. It proposes an additional engineering discipline that connects them through continuous BEFORE–DURING–AFTER defense and consequence-aware recovery.

The governing proposition is simple: a Cognitive Ecosystem cannot be considered stable if the physical resource system on which it depends is becoming unstable. The ultimate engineering test is whether cross-layer disturbances can be measured, contained, and resolved before their consequences become self-sustaining.

XVI. Source and Research Qualification

The French plasma-freezer incident is discussed as a reported cyber-physical example based on the conversation's supplied news account. Specific forensic details and the absence of product loss should be independently verified against primary reporting before formal external publication. No SI-agent involvement is claimed. PRC, PRCC, CCSat and the proposed GUDIYA control mechanisms remain research constructs requiring specification and validation.

Engineering Doctrine — Cross-Layer Roving Observability

CABOC-D shall support dynamically directed, scoped observation missions capable of following consequential disturbances across the Cognitive, Digital Commerce/Operations, and Physical Resource layers. Such missions shall preserve target identity, evidence provenance, uncertainty, and authorization boundaries while supplying timely observations to independently governed stabilization and recovery functions. Cross-layer mobility shall be achieved through authorized observation interfaces, not unrestricted executable access.

The disturbance does not respect architectural layers. The observer must be capable of following it across them.