Cascade Propagation: Refusal as First-Class Observation

by Nick Clark | Published April 25, 2026

Cascades Propagate Through Systems That Don't Coordinate

Smart-grid blackouts cascade because each utility's protective action (shed load, open breaker) is taken without coordination with adjacent utilities. The action protects the local system at the cost of pushing instability outward. The 2003 Northeast blackout, repeated in pattern at smaller scales since, is a textbook case.

Supply-chain disruptions cascade similarly: a single supplier's stockout produces protective actions (allocation, hoarding, alternative-source switching) that propagate to other tiers without structural coordination. Each tier protects itself; the cumulative protection becomes the cascade.

Joint operations face the same pattern: a coalition unit's protective action (perimeter expansion, force redistribution, mission re-prioritization) is taken without coordination with adjacent units. Each unit's local rationality contributes to system-level dysfunction.

1. The Primitive: Topology Graph + Refusal-as-Observation

Cascade propagation operates over a governance-credentialed topology graph. Nodes are participating systems (utilities, supply-chain participants, units, agencies); edges are credentialed coordination relationships with metadata (capacity, latency, criticality, authority).

Mitigation directives propagate over the topology with the same governance-credentialed structure as any other observation: a coordinating authority issues a credentialed directive; downstream nodes evaluate the directive through composite admissibility; nodes that admit the directive execute and broadcast acknowledgment; nodes that cannot admit produce a refusal observation that flows back upstream.

Refusal-as-observation is the load-bearing structural element. Refusal is not failure; it is a credentialed signal that the receiving node has evaluated the directive and determined it cannot or should not execute. The originator receives the refusal, updates its model of the topology's state, and re-plans accordingly.

2. Governance-Credentialed Topology Graph

The topology graph is itself a governed observation: each edge is signed by both endpoints' authorities, with metadata describing the coordination relationship. Edge taxonomy includes physical (transmission line, supply route), informational (data feed, telemetry), and authority (regulatory oversight, contractual commitment).

Multi-authority topology means different authorities maintain different edges: a utility-to-utility edge is signed by both utility authorities and the regional reliability authority (NERC); a supplier-to-supplier edge is signed by both companies and possibly an industry-association authority. The composite topology emerges from credentialed cross-recognition.

Topology updates flow as governance-credentialed observations: a new edge is proposed by both endpoints and admitted by the relevant authorities; an edge degradation is observed by either endpoint and credentialed; an edge removal is proposed and admitted through the same governance flow.

3. Refusal as Structured Feedback

When a node refuses a mitigation directive, the refusal observation carries a credentialed reason taxonomy: capacity exceeded, authority insufficient, prerequisite unmet, conflicting directive, policy violation, equipment unavailable, dependent system unavailable. Each reason category enables different upstream responses.

Capacity-exceeded refusal triggers the originator to redistribute the directive across additional nodes. Authority-insufficient refusal triggers escalation to a higher-authority issuer. Prerequisite-unmet refusal triggers issuance of the prerequisite. Conflicting-directive refusal triggers cross-authority resolution (next section).

Refusal with reason produces structured upstream re-planning rather than the binary success/failure of current architectures. The originator's model of the topology converges toward operating reality through accumulated refusal feedback.

4. Cross-Domain Cascade Composition

Real cascades cross domains. A cyber-attack triggers physical-system protective actions which trigger supply-chain disruptions which trigger financial-market reactions. Each domain has its own topology, authority, and propagation dynamics; the composite cascade flows across them.

Cross-domain composition is structural: each domain's topology is a credentialed observation; cross-domain edges are credentialed by authorities standing in both domains (a regulator straddling cyber and physical, an industry body spanning supply and finance); cascade observations flowing across domain boundaries are accepted under credential cross-recognition.

This enables modeling and response coordination that current single-domain architectures cannot: the cyber-physical cascade response is itself a coordinated topology operation, not a sequence of independent single-domain reactions.

5. Multi-Authority Cascade Resolution

Multiple authorities may issue cascading directives that conflict: a utility's load-shedding directive conflicts with a regional reliability authority's stability directive; a state's emergency-management directive conflicts with a federal regulator's compliance directive.

The primitive resolves multi-authority conflicts through the same composite admissibility framework that handles other multi-authority conflicts: each directive is a credentialed observation, the receiving node evaluates all admitted directives against its policy, conflicts surface as observable disagreement that propagate upstream, and resolution authorities (a coordinating authority credentialed to resolve cross-authority conflicts) issue dispositive directives.

Critically, the resolution process is itself audit-grade. Every directive, every refusal, every conflict, every resolution is recorded in lineage with credentials, supporting post-event reconstruction and accountability. The architecture produces structurally tamper-evident cascade responses.

6. Authority-Approval-Gated Topology Learning

Topology graphs evolve as systems are added, removed, or change capacity. Manual topology maintenance is the current state; the cumulative effort across utilities, agencies, and industries is enormous and chronically out-of-date.

The primitive supports topology learning: observed coordination patterns (which nodes consistently coordinate during which event types) produce credentialed proposals to add edges, modify edge metadata, or remove edges. The proposals require authority approval before becoming part of the operating topology.

Authority approval is the gate that prevents adversarial topology manipulation: an attacker cannot simply assert that two nodes are connected; the proposal must be

admitted by the relevant authorities. The learning mechanism is structurally aligned with regulatory oversight rather than working around it.

7. Preemptive Mitigation and Graduated Response

When forecasting (Article: forecasting-engine, plus the spatial-context cascade forecasting addressed here) predicts cascade onset, the topology graph supports preemptive mitigation: directives issued before the predicted cascade arrives, propagating ahead of the disruption to set up defensive postures.

Preemptive directives are structurally distinct from reactive directives: they carry the predicted disruption's time window, the forecaster's confidence, and the consequences of preemptive action versus reactive action. The receiving nodes evaluate the trade-off through composite admissibility.

Graduated response means the mitigation isn't all-or-nothing. Low-confidence forecasts produce light defensive postures (increased monitoring); high-confidence forecasts produce heavier postures (capacity reservations, alternative-routing pre-positioning); confirmed onset produces full response.

8. What This Is Not

This is not NERC reliability standards. Those are policy frameworks that prescribe utility behavior. The governed primitive is the architecture that could carry out those policies with structural feedback and cross-authority coordination.

This is not blockchain-based supply-chain visibility. Those provide tamper-evident records; the governed primitive provides credentialed coordination with structured refusal feedback and cross-domain composition.

This is not JADC2 / CJADC2. Those are coalition-operations programs whose architectures the governed primitive could implement; the architecture is broader

than any single-program scope.

Conclusion

Cascade propagation provides credentialed topology, refusal-as-observation upstream feedback, cross-domain composition, multi-authority resolution, authority-gated topology learning, and preemptive graduated response under composite admissibility.

Disclosed under USPTO provisional 64/049,409, the primitive serves smart-grid resilience, supply-chain coordination, joint-operations command, and other multi-stakeholder cascade-prone domains where current architectures rely on fire-and-forget mitigation.