8D Swarm Safety Kit and Topological Flocking (Concept & Roadmap)

Purpose and Scope

This document sketches how AethergenPlatform's 8D manifold control and non-linear algebraic methods can enable large-scale, resilient drone swarms (1k–15k+) with evidence-backed safety. It is an architectural and research plan to be shelved until core models are shipped; it also seeds a future public case-study/blog.

Problem Statement

Current shows and industrial swarms can fail catastrophically when command/control or a subset of agents misbehave. We aim to design decentralized, topology-aware control with strong safety guarantees so that local failures do not cascade.

8D State Manifold (agent state)

An agent's control state lives on an 8-dimensional manifold M capturing kinematics and mission/safety context. Example coordinates (choose 8 based on use-case):

- Position: x, y, z
- Velocity: vx, vy, vz
- Health/risk: h (battery/IMU confidence/ESC thermal)
- Link/latency/role: ℓ (QoS tier, comm health, role index)

Alternative dimensions: local density estimate, goal progress, formation slot, altitude band, airspace rule mode.

Behavioral Fields and Topology

- Topological neighborhood (not purely metric): each drone tracks k≈7 nearest neighbors by graph connectivity, improving resilience in variable density (starling heuristic).
- Potential/field design via non-linear functions and SDFs:

    - Cohesion/Alignment/Separation terms
    - Goal/formation fields, geofences as hard SDF constraints
    - Density regulation (avoid crowding), turbulence/wind compensation
- Control follows negative gradients on M, combined with hard safety constraints (below).

Safety Layer (hard constraints)

- Control Barrier Functions (CBFs): enforce $h_i(x) \geq 0$ for min-separation, altitude bands, geofence and no-fly constraints.
- Real-Time Assurance (RTA) supervisor: overrides learned/heuristic commands when constraint violation is imminent; degrades to safe mode (hover/rise/land) based on context.
- Resilient consensus (W-MSR): filters outliers/Byzantine agents from neighbor sets to avoid cascading failures.
- Fault isolation: local graph repairs “holes”; role reassignment maintains connectivity and coverage.

Communications & Graph Model

- ROS 2/DDS or equivalent pub/sub with bounded message sizes; periodic heartbeat; local broadcast range limits.
- Neighbor graph: dynamic k-NN in topological sense; timeout and packet-loss handling; link quality contributes to ℓ.
- Compliance hooks: geofence updates, ATC directives, remote ID integration where applicable.

Simulation & Training (NVIDIA Omniverse / Isaac Sim)

- Physics: 3D kinematics, wind gusts, GNSS bias/drift, sensor latency; domain randomization across weather and time of day.
- Failure injection: motor loss, GPS dropouts, comm partitions, sensor spikes.
- Policy learning: multi-agent RL + imitation (murmuration traces/expert), GNN/attention for decentralized policies atop the safety layer.
- Curriculum: scale agents 100 → 1k → 10k with staged constraints and tighter latency budgets.

Evaluation & Evidence (for procurement and audit)

- Safety: violations per flight-hour, minimum separation breaches, geofence intrusions (target: zero with RTA), recovery time from k failures.
- Connectivity & resilience: component of the largest connected subgraph over time; mission completion score under partitions.
- Efficiency: energy per mission, trajectory smoothness, task throughput.
- Packaging: signed evidence bundle with metrics, seeds, config, and hashes (ties into platform evidence system).

Edge Packaging & Deployment

- Export compact policies and safety controllers for Jetson/PC GPUs (INT8/Q4/FP16). Use Aethergen Edge Bundle (GGUF/ONNX/LoRA options) with device profiles.
- Offline policy packs: default CBFs, geofences, RTA thresholds, and logging toggles; checksum/SBOM inclusion.
- On-device watchdog and flight-mode selection to ensure fail-safe degradation.

Governance, Security, Compliance

- Airspace: configurable geofencing, altitude limits, restricted zones per locale.
- Logging: append-only offline logs; periodic signed digests.
- Supply chain: SBOM for artifacts, checksums, optional signatures; license controls and adapter watermarking.

Risks and Mitigations

- Multi-agent scalability: use topological neighbor limits, sparse comms, and GNN policies for linear scaling.
- Sensor/comms unreliability: RTA dominance with conservative fallbacks; robust estimators.
- Adversarial/Byzantine nodes: W-MSR filtering; authenticated comms; anomaly detection on behaviors.
- Regulatory variance: policy profiles per jurisdiction; verifiable audit trails.

Roadmap (shelved until core models ship)

- MVP (R&D):
  - Baseline topological boids + CBF/RTA in Isaac for 1–3k agents; wind and GPS noise; failure injection.
  - Evidence kit v1: violation histograms, resilience curves, signed report.
- Beta:
  - GNN decentralized policy; domain randomization; device-aware quantization; on-device watchdog.
  - Policy pack and offline deploy guides; procurement-grade evidence bundle.
- GA:
  - Expanded airspace compliance features, operator tools, and field telemetry integrations.

Mathematical Sketch (high-level)

- CBF constraint: $h_j(x) \geq 0$ (e.g., min-sep − $||p_i - p_n||$). Find u minimizing $||u - u_{ref}||$ s.t. $\dot{h}_j(x,u) + \alpha\, h_j(x) \geq 0$ for all j.
- Topological neighbor set: $N_k(i)$ via robust k-nearest using connectivity/quality score.
- Reward (RL): w_safety·penalty(violations) + w_cohesion·cohesion + w_goal·goal − w_energy·usage − w_latency·delays.

Public Case Study (future blog outline)

- Title: “From Starlings to Swarms: 8D Safety for Thousands of Drones”
- Story beats: problem, 8D state, safety layer, simulation campaigns, resilience results, edge deployment, evidence.
- CTA: contact for regulated pilots; downloadable red-team prompts and eval snippets.

Status: concept complete, implementation shelved. When resumed, start with the MVP simulation harness and evidence kit v1.