System Architecture Overview

This page defines the **AOFS system architecture**, including all layers, their responsibilities, and interactions. It establishes **authority boundaries**, **offline operation rules**, and **federation/synchronization requirements** for AOFS controllers.

All AOFS-compliant systems **must conform** to the rules specified here.

1. Architecture Layers

AOFS defines four core layers:

- Field Controller Layer
- Farm Controller Layer (Local / Federated)
- HQ / Federated Controller Layer
- Human Interaction Layer

Each layer has a clearly defined role, authority, and interface.

—

1.1 Field Controller Layer

Purpose: Safety-critical, authoritative irrigation control.

Requirements (normative):

- Must execute irrigation schedules locally.
- Must read and enforce all sensor data (soil moisture, tank levels, rain, battery status).
- Must enforce fail-safe rules: prevent flooding, over-irrigation, pump damage.
- Must operate fully offline, without network connectivity.
- Must never accept remote commands that bypass safety logic.
- Must log all irrigation events and safety-triggered actions for audit purposes.

Examples of Field Controller hardware: ESP32, Arduino-compatible embedded controllers.

—

1.2 Farm Controller Layer (Local / Federated)

Purpose: Supervisory and management layer on-site; provides local operator interface and federation.

Requirements (normative):

- Must provide a full UI for field operators to monitor and configure the farm.

- Must operate fully offline with authoritative access to local data.
- Must aggregate telemetry from Field Controllers.
- Must support peer-to-peer federation with other Farm Controllers or HQ Controllers.
- Must enforce the rule that **Field Controllers remain authoritative** for all safety-critical actions.
- Must support pull/push synchronization of configuration, logs, and firmware updates.
- Must provide conflict resolution mechanisms for configurations (e.g., timestamp-based, operator approval).

Behavioral Rules:

- Offline operation: farm continues irrigation and monitoring normally if internet is unavailable.
- Sync: data and configuration propagate when connectivity is restored.
- Logging: all operator actions, sync events, and configuration changes must be logged.

Examples of Farm Controller hardware: NanoPi, Raspberry Pi, other industrial-grade single-board computers.

—

1.3 HQ / Federated Controller Layer

Purpose: Global oversight, analytics, and management of multiple farms.

Requirements (normative):

- Must receive telemetry and logs from multiple Farm Controllers.
- Must provide reporting, dashboards, and aggregated analytics.
- Must support configuration distribution to Farm Controllers when authorized.
- Must **never override Field Controller safety rules**.
- Must maintain full audit trails of all data exchanges and actions.

Behavioral Rules:

- HQ controller may act as a “central” sync point, but the architecture **remains decentralized**.
- Federation: HQ may push configuration updates or pull logs, but offline farms continue autonomous operation.

—

1.4 Human Interaction Layer

Purpose: Interface for humans to supervise, monitor, and optionally configure the system.

Requirements (normative):

- Must allow operators to monitor farm status, irrigation events, and alerts.
- Must allow operators to submit configuration changes, schedules, or manual requests.
- Must validate all requests against **Field Controller rules** before execution.
- Must integrate with Farm and HQ controllers as necessary, respecting authority boundaries.

—

2. Authority and Safety Rules

1. **Field Controller Authority:**

- Field Controller decisions are **authoritative** and cannot be overridden remotely.

2. **Supervisory Controller Rule:**

- Farm and HQ Controllers may propose changes, but **Field Controller safety rules cannot be bypassed**.

3. **Offline Operation:**

- Any controller layer on-site must maintain **full operational capability** without connectivity.

4. **Federation / Sync Rule:**

- Controllers may act as peers in a push/pull sync network.
- Conflict resolution must be deterministic and logged.

5. **Auditability:**

- All layers must log events, configuration changes, and synchronization actions.
- Logs must be preserved locally and transmitted to upstream controllers when possible.

—

3. Layer Interaction Summary

Layer	Primary Role	Connectivity Requirement	Authority
——-	————-	———————	———-
Field Controller	Execute irrigation & safety	None (offline)	Authoritative locally
Farm Controller	Local supervision & peer sync	Optional (for federation)	Supervisory
HQ Controller	Global oversight & analytics	Required for federation	Supervisory
Human Interface	Operator monitoring & configuration	Optional	Supervisory

—

4. Compliance Notes

- Any AOFS-compliant deployment **must implement all four layers** as defined, though multiple roles may be co-located on the same hardware. - Federated operations **must preserve local authority**. - Failure to respect authority boundaries **invalidates AOFS compliance**.