AOFS Communication Protocols & Standards

AOFS systems rely on **robust, flexible communication protocols** to connect Field, Farm, and HQ controllers, as well as sensors and actuators. Protocols are selected based on **range, power requirements, reliability, and operational constraints**

1. Overview

- Communication is **layered**:
  - **Field Controller Layer:** short-range, low-power, real-time sensor and actuator connectivity
  - **Farm Controller Layer:** aggregation, supervisory control, and moderate-range communication
  - **HQ / Federated Layer:** long-range, optional cloud or networked data aggregation and research integration
- Protocols are **optional, configurable, and modular**
- All protocols must **respect AOFS principles**:
  - Offline-first operation
  - Safety-critical logic cannot be overridden remotely
  - Actions are auditable and logged

2. Recommended Protocols

- MQTT – lightweight publish/subscribe messaging for telemetry and asynchronous updates
- AMQP – robust messaging with guaranteed delivery, suitable for HQ/Farm Controller links
- Zigbee – low-power mesh networks for local sensors and actuators
- LoRa / LoRaWAN – long-range, low-power communication suitable for large farms and sparse sensor deployments
- Z-Wave – low-power mesh for home/farm automation devices and actuators
- EnOcean – energy-harvesting wireless sensors and switches

3. Layer Mapping Guidance

- **Field Controller Layer**
  - Zigbee, Z-Wave, EnOcean for sensor/actuator connectivity
  - MQTT for telemetry aggregation to Farm Controller
- **Farm Controller Layer**
  - MQTT or AMQP for Field→Farm aggregation
  - Optional Zigbee/Z-Wave for direct sensor integration
- **HQ / Federated Layer**
  - MQTT or AMQP for data sync
  - Optional internet-based services for forecasting, optimization, and research integration

4. Notes & Best Practices

- AOFS does **not mandate a specific protocol**; multiple protocols may coexist
- Protocol selection should consider **latency, reliability, power, and range**
- Offline-first principle: all safety-critical functions **must function without network connectivity**
- Optional online connections (e.g., for forecasts, research data) must **never override safety-critical rules**
- Protocols should be **auditable and loggable** to maintain operational traceability