LLM (RAG-Based) Integration in the Wildfire Detection System

1. Use cases

Event Reasoning, Historical Context & Incident Summarization

The LLM helps operators understand why alerts or near-miss events occurred and how they evolved over time, grouping related data points into a single incident summary. Using RAG, it compares the current event to similar historical incidents to assess how unusual the situation is and whether comparable patterns escalated in the past.

Identify Potential Sensor Data Quality Issues

The LLM assists by flagging sensor behavior that appears unreliable or meaningless. By inspecting signal patterns over time, it identifies inconsistent trends, or non-physical behavior that may indicate sensor noise or hardware issues.

Operator Decision Support & System Understanding

Beyond individual events, the LLM helps operators understand how algorithmic parameters influence system behavior. By reasoning about the detection logic, it can provide environment-specific advisory insights, such as suggesting parameter review when the system appears consistently over- or under-sensitive. All suggestions are only informational.

2. Data flow

The LLM receives read-only, structured inputs including raw sensor data, computed statistics, detected events and summaries, historical event data, and configuration metadata, provided primarily as structured JSON for explanation and analysis.

3. Edge vs. Cloud

Drone-mounted in hazardous areas, the lightweight edge device's primary role is collecting sensor data and transmitting raw readings as structured JSON to the cloud. The cloud handles the detection logic, alert, historical storage, and edge device orchestration. The cloud aggregates data from drones to correlate regional alerts and centralize system coordination. The cloud-based LLM offers explanations, historical analysis (via RAG), reporting and operator support without impacting real-time detection accuracy.

4. Risks & Mitigations

To mitigate **hallucination**, the LLM is restricted to explaining only structured system outputs and historical data. **Latency and network** risks are managed by designing the cloud to handle small, periodic data payloads. Processing in secure cloud environments mitigates the physical and **security risks** inherent in hazardous, distributed edge devices, providing superior security, access control, and monitoring capabilities thanks to modern cloud platforms. The LLM maintains read-only access, which prevents it from modifying system state or initiating any actions.

In harsh environments with unavailable cloud connectivity, a fallback deployment can enable the core detection logic to run locally on the edge device.

System flow: Sensors → **Edge** (Data Collection & Transmission)
→ **Cloud** (Detection, Alerts, Historical Storage, RAG retrieval)
→ **LLM** Assistant (Explanation & Operator Support)