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

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.

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 isolated spikes, inconsistent trends, or non-physical behavior that may indicate sensor noise, calibration drift, or hardware issues. These insights are observational only and do not affect detection or alerting.

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 informational, and configuration changes remain fully under human control.

Edge vs. Cloud

Detection and **alerting** run at the **edge**, close to the sensors, to ensure low latency and robustness under network failures. This includes signal preprocessing, anomaly detection, risk scoring, and alert triggering. The **LLM** runs in the **cloud** as an assistive component, handling explanations, historical analysis via RAG, reporting, and operator support. These tasks are non-real-time and do not affect detection correctness.

Risks & Mitigations

Hallucinations are mitigated by constraining the LLM to explain only structured data produced by the system and by basing responses in retrieved historical context.
Latency and **network** failures are mitigated by keeping all safety-critical logic on the edge; LLM outputs are optional and asynchronous.
Privacy and **security** risks are mitigated through strict access control and usage constraints. The LLM operates with read-only access, processes scoped data for analysis only, and cannot modify system state or perform external actions. All interactions can be logged and audited.

System flow:
Sensors → Edge (Detection & Alerts)
→ Cloud (Historical Storage + RAG retrieval)
→ LLM Assistant (Explanation & Operator Support)