# Alert Design Spec

The Alert Design Spec defines every rule by which a fused telemetry output from e5-fusion-logic-map crosses into an alert: threshold definitions, false-positive suppression logic, warning-versus-critical separation, and the action link that connects an alert to a declared agent behavior or human escalation. This artifact is the C6 producer: every alert it fires emits a structured payload to s1-fallback-architecture-blueprint and s1-threshold-escalation-spec, and the S1 state machine — not this layer — owns the final fallback decision. The alert layer makes a recommendation; S1 acts on it within the reliability state machine.

## 1. Alert Anatomy

Every alert has the following mandatory fields:

```
alert:
  alert_id: <UUID v4; unique per event>
  rule_id: <resolves to an alert rule in §3>
  sensor_id: <resolves to a source_id in e5-telemetry-source-map>
  signal: <normalized, fused measurement that crossed the threshold; includes
measurement_type, fused_value, unit>
  severity: <critical|high|medium|low|info>
  confidence_band: <high|medium|low|unknown; inherited from fused_record>
  confidence_score: <optional; 0.0–1.0 numeric; never replaces band for control>
  suggested_fallback: <declared S1 fallback id or "none">
  timestamp_utc: <ISO 8601 Z>
  suppression_applied: <true|false>
  suppression_rule_id: <resolves to a suppression rule in §4 or null>
  action_link: <id of the linked agent action or escalation target; see §5>
```

The confidence_band field is authoritative for downstream control decisions. The optional confidence_score is observability-only; S1 and any downstream consumer must not let the numeric score alone change a pass/fail or go/no-go decision.

## 2. Severity Classification

Severity follows the locked glossary enum and maps directly to the S1 threshold-escalation tiers.

| severity | Meaning | S1 escalation tier |
|---|---|---|
| critical | Immediate risk to life, property, regulatory compliance, or irreversible environmental damage | Tier 3 (on-call / accountable exec) |
| high | Material harm, significant operational impact; recoverable with prompt action | Tier 2 (synchronous reviewer) |
| medium | Degraded performance or warning condition; time-sensitive but not immediately dangerous | Tier 1 (async review queue) |

| severity | Meaning | S1 escalation tier |
|---|---|---|
| low | Advisory signal; monitor trend | Log only; no escalation |
| info | Observability event; normal-range confirmation | Log only |

A critical or high alert routes into S1's s1-threshold-escalation-spec exactly as an internal low-confidence signal would. The S1 state machine decides whether to execute a fallback, raise a HITL gate, or escalate further.

## 3. Alert Rules Register

Each rule defines the threshold condition, the measurement type it applies to, and the severity triggered. Rules are evaluated against the fused_record from e5-fusion-logic-map, not against raw sensor readings.

### *3.1 Rule schema*

```
- rule_id: <kebab-case>
  measurement_type: <enum from e5-normalization-layer §2.1>
  condition: <expression using fused_value, confidence_band, stale_sources>
  severity: <critical|high|medium|low|info>
  description: <one sentence>
  suggested_fallback: <S1 fallback id or "none">
  action_link: <agent action id or escalation target>
  min_confidence_band_required: <high|medium|low|unknown>
  notes: <optional>
```

The min_confidence_band_required field is a hard gate: if the fused record's confidence_band is lower than this minimum, the rule is not fired and a suppression-confidence event is logged instead. This prevents a low-trust sensor composite from triggering a critical alert autonomously.

### *3.2 Example rules — 30A stormwater network (illustrative)*

```
- rule_id: pond-level-critical
  measurement_type: water-level
  condition: fused_value >= 1.20
  severity: critical
  description: Pond level has reached or exceeded the 1.20 m NAVD88 design-maximum; risk of
overtopping and uncontrolled discharge.
  suggested_fallback: activate-manual-bypass-valve
  action_link: notify-district-engineer-tier3
  min_confidence_band_required: medium
  notes: Do not fire on confidence_band=low alone; require corroboration from at least one
high-band source.

- rule_id: pond-level-high
  measurement_type: water-level
  condition: fused_value >= 1.00 AND fused_value < 1.20
  severity: high
  description: Pond level above 1.00 m NAVD88; approaching capacity; monitor closely.
  suggested_fallback: increase-monitoring-frequency
  action_link: notify-district-clerk-tier2
  min_confidence_band_required: medium

- rule_id: rainfall-rate-high
```

```
  measurement_type: rainfall-rate
  condition: fused_value >= 25.4
  severity: high
  description: Rainfall rate exceeds 1 in/hr (25.4 mm/hr); elevated runoff potential.
  suggested_fallback: none
  action_link: notify-district-clerk-tier2
  min_confidence_band_required: high
  notes: High-band required to avoid false alarms from gauge noise.

- rule_id: rainfall-rate-critical
  measurement_type: rainfall-rate
  condition: fused_value >= 50.8
  severity: critical
  description: Rainfall rate exceeds 2 in/hr (50.8 mm/hr); flash-flood advisory threshold.
  suggested_fallback: none
  action_link: notify-district-engineer-tier3
  min_confidence_band_required: medium

- rule_id: soil-moisture-saturation
  measurement_type: soil-moisture-volumetric
  condition: fused_value >= 0.45
  severity: medium
  description: Soil approaching field saturation; reduced infiltration capacity increases
runoff coefficient.
  suggested_fallback: none
  action_link: log-to-monitoring-queue
  min_confidence_band_required: medium

- rule_id: flow-culvert-elevated
  measurement_type: flow-rate
  condition: fused_value >= 0.85
  severity: high
  description: Culvert flow rate elevated above design normal; potential downstream
capacity issue.
  suggested_fallback: none
  action_link: notify-district-clerk-tier2
  min_confidence_band_required: medium
  notes: rule_id flow-culvert-elevated requires at least one corroborating source because
sw-flow-culvert-c4 is reliability-grade C.

- rule_id: tide-surge-watch
  measurement_type: tide-height
  condition: fused_value >= 0.75
  severity: medium
  description: Coastal tide height approaching 0.75 m MLLW; marine flooding watch per NOAA
guidance.
  suggested_fallback: none
  action_link: log-to-monitoring-queue
  min_confidence_band_required: high

- rule_id: feed-gap-sensor
  measurement_type: any
  condition: stale_sources contains source_id AND source.reliability_grade in {A, B}
  severity: medium
  description: A reliability-grade A or B source has gone stale within the fusion window.
  suggested_fallback: increase-monitoring-frequency
  action_link: notify-pipeline-ops
  min_confidence_band_required: low
```

## 4. False-Positive Suppression

False positives are the primary reason telemetry alert systems lose operator trust. This spec declares two layers of suppression, both logged as provenance events.

### *4.1 Confidence-gate suppression*

A rule is not fired if the fused record's confidence_band is below the rule's min_confidence_band_required. The non-firing is logged as suppression-confidence with the rule id and the actual band. This is not silence — it is an observable, auditable decision.

### *4.2 Hysteresis suppression*

A rule that fired in the previous fusion window is not re-fired unless either (a) the fused_value has changed by more than the hysteresis margin, or (b) a declared re-arm window has elapsed.

| severity | hysteresis margin | re-arm window (minutes) |
|---|---|---|
| critical | 5% of threshold value | 5 |
| high | 10% of threshold value | 10 |
| medium | 15% of threshold value | 30 |
| low | 20% of threshold value | 60 |

If hysteresis applies, the alert is not re-fired but a suppression-hysteresis event is logged with the current value, the threshold, and the elapsed time since the original alert.

### *4.3 Corroboration requirement*

For any rule with min_confidence_band_required: medium or higher, the alert may carry a corroboration_required: true flag in the rule definition. When set, the alert is held for one additional fusion window to confirm the signal persists before firing. A non-persistent signal generates a transient-suppressed event. This rule is particularly important for flow-culvert-elevated, which depends on a reliability-grade C source.

### *4.4 What suppression does NOT do*

Suppression never silently discards a signal. Every suppression event is logged to the pipeline monitoring channel and to the provenance record. An operator reviewing the alert history must be able to see every suppressed near-miss alongside every fired alert.

## 5. Alert-to-Action Links

An alert does not automatically execute an action. The action link in the alert payload names the declared response; the S1 state machine and e5-decision-support-layer determine whether the action is executed autonomously or gated.

| action_link | Description | S1 gate required |
|---|---|---|
| notify-district-engineer-tier3 | Synchronous page to district engineer via SMS + Slack | HITL gate |
| notify-district-clerk-tier2 | Async notification to clerk ops queue | Post-hoc review |
| log-to-monitoring-queue | Append to pipeline monitoring log only | None |
| notify-pipeline-ops | Alert the pipeline operations team | Async |
| activate-manual-bypass-valve | Recommended physical action; always requires human authorization | HITL gate (irreversible-impact) |

Actions classified as HITL gate required are never executed autonomously regardless of confidence_band. The activate-manual-bypass-valve action crosses the irreversible-impact boundary and is always human-authorized per s1-fallback-architecture-blueprint §6.

## 6. Reliability Emission — C6 Producer

This section is the C6 contract implementation. Every alert fired by this spec emits the following payload to s1-fallback-architecture-blueprint (for fallback state-machine intake) and s1-threshold-escalation-spec (for tier routing).

### *C6 payload schema*

```
c6_emission:
  sensor_id: <source_id from e5-telemetry-source-map; may be "composite" if multiple
sources>
  signal: <fused_value, measurement_type, unit, fusion_window_end_utc>
  severity: <critical|high|medium|low|info>
  confidence_band: <high|medium|low|unknown>
  confidence_score: <optional; 0.0–1.0; omit if not available>
  suggested_fallback: <declared S1 fallback id or "none">
```

Routing rule (verbatim from interface-contracts C6): A critical or high alert routes into S1's threshold-escalation spec exactly as an internal low-confidence signal would; the S1 state machine — not the sensor layer — owns the fallback decision. Telemetry alerts MUST obey S1 fallbacks; a sensor layer that silently overrides the S1 state machine is gate-failing.

Band authority: The confidence_band field is the authoritative control signal. The optional confidence_score is observability metadata. If a downstream consumer promotes the numeric score above the band in any control decision, that is a contract violation.

Emission rule: Every fired alert produces exactly one C6 emission record. Suppressed alerts produce a suppression-event but no C6 emission. Drops are gate-failing.

### *C6 worked example — pond-level-critical (illustrative)*

Alert fires when sw-water-level-j1 fused record reaches 0.596 m and is on a rising trend crossing 1.00 m threshold (illustrative scenario with different input values):

```
c6_emission:
  sensor_id: sw-water-level-j1
  signal:
    measurement_type: water-level
    fused_value: 1.03
    unit: meters above NAVD88
    fusion_window_end_utc: "2026-05-29T19:33:00Z"
  severity: high
  confidence_band: medium
  confidence_score: 0.72
  suggested_fallback: increase-monitoring-frequency
```

The S1 state machine receives this C6 payload, looks up confidence_band: medium plus severity: high, and applies the Tier 2 escalation path from s1-threshold-escalation-spec. The sensor layer does not decide the escalation tier; it only recommends increase-monitoring-frequency as the fallback.

## 7. Alert Rule Versioning

Adding a new rule_id is MINOR. Changing a threshold value, severity, or min_confidence_band_required on an existing rule is MINOR but requires a documented rationale (false-positive rate, incident report, or calibration update). Removing a rule is MINOR but must not orphan any action_link still referenced by e5-decision-support-layer. Changing the C6 payload schema shape is MAJOR and governed by interface-contracts.