Business Interpretation for Anomaly Detection

Use-case and outcome

- Detect anomalous sensor behavior to reduce unplanned downtime and scrap, improving OEE and throughput.

Rarity of events

- If Alarm.ItemDroppedError is rare, unsupervised methods (Isolation Forest, optional Autoencoder) help surface early-warning signals.

Alerting strategy

- Define severity tiers from model scores (e.g., Info/Warning/Critical with score thresholds).
- Route Critical alerts to on-call maintenance; batch lower tiers into daily summaries to reduce noise.

Dashboards and monitoring

- Show anomaly rate over time, top contributing sensors/features, and recent incidents.
- Include filtering by machine, shift, product, operator, and recipe.

Maintenance workflow integration

- Create tickets automatically when Critical anomalies persist for N minutes or recur within T hours.
- Attach context windows (pre/post anomaly) and sensor snapshots to work orders.

Root-cause triage

- Display top deviating features per anomaly instance to guide initial inspection.
- Correlate anomalies with changeovers, maintenance logs, and environmental/utility data (e.g., air pressure, temperature).

KPIs and targets

- Track precision@K for alerts, MTTR, avoided downtime, scrap reduction, and alert acknowledgment latency.
- Set acceptance criteria (e.g., precision ≥ 0.6 on Critical alerts, acknowledgment < 10 min).

False positives/negatives handling

- Provide one-click feedback (Valid issue / False alarm) to retrain and recalibrate thresholds.
- Suppress alerts during planned maintenance or known transient states.

Feedback loop (HITL)

- Capture maintainer feedback and resolution codes; use them to label data and improve models.
- Periodically review the most frequent false-alarm patterns and adjust features or rules.

Model monitoring and governance

- Monitor data drift (feature distributions), performance drift (AP, precision), and data quality (nulls, ranges).
- Establish retraining cadence (e.g., monthly or after N validated incidents) and change management approvals.

Explainability and auditability

- Log model version, features, thresholds, and explanations per alert for traceability.
- Provide simple reason codes (e.g., 'Vacuum pressure variance above baseline').

Rollout plan

- Start in shadow mode (no-alert) → pilot line with few Critical alerts → plant-wide.
- A/B compare with current rules or thresholds to quantify incremental value.

SLA and on-call

- Define alerting windows, response SLAs, and escalation paths.
- Document an incident playbook for repeated anomaly types.

Security, privacy, compliance

- Control access to anomaly data and explanations; log access for audits.
- Ensure compliance with data retention and regulatory standards.

Performance and scaling

- Specify latency and throughput targets (e.g., scoring within 1s per batch of N rows).
- Use batch scoring for high-volume sensors; stream only KPIs needed for alerting.

Data enrichment

- Join with contextual data (maintenance logs, BOM/recipe, operator rosters, environmental sensors) to improve precision.

Next steps checklist

- Finalize alert thresholds with operations; define SLAs and escalation.
- Build dashboard panels (anomaly trend, top features, recent incidents).
- Instrument feedback capture in CMMS/ticketing and wire back to training data.
- Stand up drift/data-quality monitors and schedule retraining.