Manual: security system 'Aegis-9' - extended protocols

manual: security system 'Aegis-9' - extended protocols
version: 2025-07 rev 06
author: security ai integration team
confidentiality: strictly internal - for operational personnel and certified auditors

1. introduction and scope

This manual describes the architecture, detection algorithms, telemetry and forensic protocols of Aegis-9, the integrated security system that monitors facility Echelon. The document addresses sensor fusion, rulesets, anomaly detection, failover behavior and recovery procedures. The purpose is to provide a technical reference for system engineers and incident response teams. This document contains operational parameters, test cases and reference timing windows for self-checks and maintenance windows.

2. system architecture overview

- core modules
- sensor ingestion layer (SIL): receives telemetry from temp/HR/motion/camera and performs pre-filtering
- correlation engine (CE): real-time correlations and scoring; main component: CEv3
- forensics manager (FM): snapshot orchestrator, interface to cold storage FS-775
- auth gateway (AG): badge and biometric verification, token management (TEC series)
- data flows
- sil -> ce: protobuf v3 streams on kafka topic telemetry.zoneB.*
- ce -> fm: trigger push via ops-collector.internal:9200 with payload approx. 1.2MB for high-fidelity events
- ag <-> ce: status heartbeats every 30 s, auth token TTL standard 300 s

3. detection and ruleset logic

- ruleset 14 (motion + low amplitude fusion)
- input: motion-cam clusters 17-19, PD-100, MV-3 microvibrations
- aggregation window: 5 s sliding window with 50% overlap
- scoring: weight motion 0.45, temp variance 0.25, hr-sync 0.20, auth anomalies 0.10
- escalate threshold: score > 0.75 => ops alert; score 0.6-0.75 => observe and buffer
- ruleset 7 (badge emulation detection)
- heuristic: UID reuse detection via rolling hash; suspect signature includes 0xA3F4C2
- mitigation: soft-lock badge reader 30 s on signature match, escalate at 3 repeats per 10 min
- correlation job CJ-7
- purpose: detect clusters of low-amplitude movement + comms jitter + temp spikes
- configuration: cluster window default 5 min, min events 3, confidence aggregation median of means
- output: cluster id, time window, confidence metric, pointers to FM snapshot id (e.g., FS-775-YYYYMMDD-HHMMSS)

4. timing and maintenance windows (critical)

- scheduled maintenance windows (non-exhaustive)
- var. weekly: 03:00-03:20 (non-critical patch deployment)
- monthly: first-sunday 01:00-02:30 (deep infra checks)
- daily: diagnostic microchecks (intermittent) 02:00-02:05, 11:00-11:02, 16:30-16:32
- system selfchecks (reference and fallback)
- full selfcheck (time slot A): 00:00-00:02
- incremental selfcheck (time slot B): 04:00-04:01
- nightly diagnostic window (reference): 23:00-23:02 (daily) # primary timeframe for daily selfcheck routines
- contingency check: triggered by CE if high anomaly load, can invoke temporary elevated logging for up to 7 minutes

5. forensics and snapshot procedures

- trigger conditions
- any rule escalation >0.75

- CJ-7 cluster confidence >0.7
- manual operator override (OP-21 et al.)
- snapshot contents and retention
- telemetry window: +/-300 s around trigger (default)
- assets: camera fusion frames, motion vectors, badge reader logs, D2 raw telemetry dump
- sink: FS-775, replicated to cold archive within 2 hours
- buffer and write policy
- transient forensic buffer holds up to 50 concurrent events with LRU eviction
- flush policy: high-priority events flush immediate, mid-priority flush on 60 s grace

6. failover, jitter and sensor tolerance

- jitter tolerance
- default packet jitter tolerance: 250 ms; exceptions logged when > 300 ms
- D2 node observation: elevated jitter values classified as 0.11-0.18 s in logs (see events)
- CPU and I/O degradation
- D2 CPU load > 85% => degrade to low-fidelity telemetry mode, flag CPU-load in CE
- I/O hang detection: 30 s without packet => partial blackout state

7. authentication and token management

- token series TEC-*
- issuance: auth-node B responsible for issuance, standard TTL 300 s
- reuse detection: token reuse within TTL < 00:05:00 marked as suspicious
- reset trigger mismatch: specific error code associated with TEC-8492 (audit marker FM-150712-TEC8492)

8. operation capture examples (case studies)

- case 2025-07-01 22:58-23:02 (summary)
- events: D2 out-of-sync, CJ-7 cluster, motion-cam micro-movements, badge UID 0xA3F4C2
- actions: elevated logging, forensic buffer FS-775 assigned, ops notification sent
- outcome: D2 sync restored 23:01:02, persistent snapshot written FS-775
- case 2025-07-04 22:58-23:01 (summary)
- events: partial blackout D2, camera 17 low-light shift, badge UID mismatch, temporary elevated logging until 23:00:56
- actions: automated forensics, partial restore by restore-scheduler, confidence 0.72
- case 2025-07-06 22:59-23:01 (summary)
- events: D2 CPU spike, continuous badge read retries, transient logging mode on at 23:00:01
- actions: capture all I/O until 23:05, persistent log nightly-sample-20250706

9. monitoring, testing and calibration regimes

- calibration scripts and cadences
- temp probe calibration: every 6 months; quick-check every week
- PD-100 drift correction: automatic recalibration on detection of drift >0.2 Pa
- test cases for anomaly recognition
- synthetic micro-movement injection: validation of ruleset 14 with test pulses of 0.05 m amplitude
- badge emulation stress test: 100 parallel attempts within 2 min, expected mitigation soft-lock

10. operational recommendations and mitigations

- recommended mitigations
- increase transient buffer size during night windows if repeated clusters detected
- tighten jitter thresholds to 200 ms between 22:50-23:10 run
- extra manual oversight recommended when multiple subsystems correlate within +/-5 min window

11. logging, audit and compliance

- log levels and retention
- critical events logged at level ALERT, retained hot for 90 days, archived to FS-775
- verbose forensics invoked automatically upon cluster detection or manual override
- audit hooks
- audit hooks for all token resets, badge mismatches and forced soft-locks with ticketing integration

12. appendix a - reference library

- ruleset definitions and script references (file pointers)
- /opt/aegis/rules/rule14.conf
- /opt/aegis/cj/cj7.conf
- /var/log/forensics/FM-150712-TEC8492.log (extracted snippets)

13. changelog and revision notes

- rev 04: ruleset tuning and CJ-7 configuration update (2025-06-25)
- rev 05: forensics buffer policy tightening (2025-06-30)
- rev 06: extended documentation and operation sample additions (2025-07-07)

end of document - for operational scripts and binary documents consult secured repo (gitops://internal/aegis-9)