

Cleanroom Monitoring You Can Defend

Continuous environmental monitoring, local audit trails, and Part 11 / Annex 11 controls for sterile manufacturing

Fireball Industries · September 30, 2026 · 23 minute read

It is 02:40 on a filling night shift. The Grade A particle counter over the stopper bowl logs a cluster of 5 μm counts, below the action limit but above alert, three samples in a row. The operator acknowledges the alarm, writes "intervention, stopper jam" on the batch record, and the line keeps running. Four days later, QA is preparing batch disposition and has to answer a simple question: was that a real event, and which units did it touch? The answer is spread across the particle monitoring system, a separate differential pressure display, the building management system that logged an air handler fan restart at roughly the same time, a paper intervention log, and a historian whose clock runs 90 seconds ahead of the counter software. Nobody can say with confidence which happened first.

The excursion is usually manageable. Reconstructing it is what costs: investigator hours, batches held while the record is assembled, and sometimes an inspector asking for the audit trail of an alert limit changed last spring.

This paper is for the QA, validation, facilities, and metrology people who carry that work. It covers what EU GMP Annex 1 (2022) and FDA expect from continuous monitoring, which signals to connect, a reference architecture from sensor to signature, where these projects fail, and how Part 11 and Annex 11 controls map onto the design. Compliance belongs to your validated system and quality unit; the aim is a system that is easier to defend.

A self-check for your site

Answer these for one aseptic suite, from records alone.

1. For the last Grade A alert, can you show the raw particle counts, the alarm raise, acknowledge, and clear times, and the door and pressure state in the same five-minute window, all on one consistent clock?

2. If the network between the particle counter and the monitoring server dropped for 20 minutes during a fill, would the data be buffered and backfilled, or would there be a gap that has to be explained?
3. Who changed the Grade B alert levels most recently, when, and what reason did they record? Can you print that from the system?
4. Do any operators, engineers, or vendor service technicians log in to the monitoring system, the BMS, or the counter software with a shared account?
5. Are the alarm delays on your critical differential pressure alarms written down and justified in your contamination control strategy (CCS)?
6. When a counter or pressure transmitter goes out for calibration, how does the monitoring record show that the point was offline and which instrument replaced it?
7. If the vendor needs to troubleshoot the monitoring server remotely, what path do they use, and who can see what they did?

If more than two of these take a phone call to answer, start with the record before touching the instruments.

What the regulators expect the system to do

The revised Annex 1 came into operation on August 25, 2023, with one capping clause following in August 2024 [1]. For monitoring, sections 2, 4, and 9 matter most.

Section 2 requires a contamination control strategy (CCS) that defines critical control points and assesses every control and monitoring measure [1]. Clause 2.3 adds that well-managed existing control systems need not be replaced, but must be referenced in the CCS with their interactions understood [1].

Section 9 is where the monitoring program lives. Grade A must be monitored for the full duration of critical processing, including equipment assembly, continuously for particles of 0.5 μm and 5 μm , at a sample flow of at least 28 liters (1 ft^3) per minute, so that interventions, transient events, and system deterioration are captured (clauses 9.16 and 9.17) [1]. The system should compare each sample result against alert and action levels often enough to allow a timely response, and alarms should trigger when alert levels are exceeded. A similar system is recommended for Grade B, at a lower sample frequency (clause 9.18) [1].

The numbers your monitoring system has to keep up with

28 L/min

Minimum Grade A particle sample flow (Annex 1, 9.17)

10 Pa

Guidance minimum between adjacent grades (Annex 1, 4.14)

4 h

Maximum settle plate exposure, Grade A and B (Table 6)

< 20 min

Guidance clean-up to at-rest limits (Table 5, Note 1)

Figure 1. Four numbers from EU GMP Annex 1 (2022) that set the pace for a monitoring system. Source: EudraLex Volume 4, Annex 1, clauses 4.14 and 9.17, Tables 5 and 6.

Alert levels must be set from qualification data and reviewed against trend data, and they must be set so adverse trends are detected (clauses 9.9 and 9.10) [1]. Clause 9.11 lists what trending must cover, including consecutive excursions from alert levels and isolated excursions that share a common cause, such as single excursions that always follow planned maintenance [1]. Clause 9.13 requires a root cause investigation when action limits are exceeded, including an impact assessment on batches produced between monitoring and reporting [1]. Clause 3.2 requires monitoring excursions to be investigated before batch certification [1].

PARTICLES PER CUBIC METER

Annex 1 Table 5: maximum total particle limits for monitoring

Grade	$\geq 0.5 \mu\text{m}$ at rest	$\geq 0.5 \mu\text{m}$ in op.	$\geq 5 \mu\text{m}$ at rest	$\geq 5 \mu\text{m}$ in op.
A	3,520	3,520	29	29
B	3,520	352,000	29	2,930
C	352,000	3,520,000	2,930	29,300
D	3,520,000	Set by site	29,300	Set by site

Figure 2. Maximum total particle concentrations for routine monitoring, particles per cubic meter. Source: EudraLex Volume 4, Annex 1 (2022), Table 5.

Note 2 to Table 5 matters: occasional Grade A $5 \mu\text{m}$ counts may be false counts from noise or stray light, but consecutive or regular low-level counts may signal contamination, early filter failure, or poor set-up practice [1]. Single-sample limit checks miss that pattern.

Adjacent rooms of different grades should have a pressure difference of at least 10 Pa as a guidance value (clause 4.14) [1]. Critical pressure differences must be continuously monitored and recorded, a warning system must alert operators instantly, the warning must not be overridden without assessment, and any alarm delays must be justified in the CCS (clause 4.16) [1]. FDA's 2004 aseptic processing guidance says much the same for US sites, recommending 10 to 15 Pa between adjacent rooms of different classification and continuous monitoring of pressure differentials throughout each shift, with deviations investigated [6]. Under 21 CFR 211.42(c)(10), aseptic areas must have temperature and humidity controls and a system for monitoring environmental conditions [4]. Annex 1 clause 9.6 adds that temperature and relative humidity be held within ranges that support the defined cleanliness grade [1].

Annex 1 also requires continuous viable air monitoring in Grade A for all critical processing (clause 9.24), with Table 6 action limits of no growth in Grade A and 10 CFU/m³ for Grade B air [1]. For plates, the system must hold the metadata: location, exposure window, batch, and read result.

Under all of it sits ISO 14644. Part 1 (2015) classifies air cleanliness for particle sizes from 0.1 µm to 5 µm [9]; Part 2 (2015) sets minimum requirements for a monitoring plan [10]. The 2015 revision replaced fixed requalification intervals with a risk-based plan: annual reclassification, extendable when monitoring data supports it [11].

What needs to be measured and connected

Most sites already have every source below. The work is connecting them on one clock, with one audit trail.

SOURCE	TYPICAL SIGNALS	WHY IT MATTERS
Grade A remote particle counters	$\geq 0.5 \mu\text{m}$ and $\geq 5 \mu\text{m}$ counts per sample, flow status, laser and sensor health	Clause 9.17 continuous monitoring; flow faults invalidate samples
Grade B and C counters, portable counters	Counts, location ID, sample volume	Trending under 9.11; classification under ISO 14644-1
Differential pressure transmitters	Pa per room pair, alarm state	Clause 4.16 continuous recording and instant warning
Door contacts and interlocks	Open/closed, open duration	Explains pressure dips and transient counts
Temperature and RH probes	Per room and per critical zone	211.42(c)(10)(ii); Annex 1 9.6
BMS / AHU PLC	Fan status, supply and return flow, filter differential pressure, mode changes	Root cause for pressure and particle events
Isolator or RABS controller	Glove breach tests, decontamination cycle state, internal pressure	Context for interventions and Grade A conditions
Active air samplers and plate records	Start/stop times, volume, location, batch, CFU read	Clause 9.24 and Table 6
Filling line PLC	Batch ID, line state, intervention flags	Links excursions to units filled
Calibration system	Instrument ID, due date, as-found/as-left status	Shows the data came from a calibrated sensor

The BMS and filling line PLC usually sit outside the validated monitoring system, which is why their context ends up on paper. Reading their tags read-only into the record is integration work on each controller, with its

own risk assessment. The calibration link is cheap and often missing; better that you find an overdue counter than an inspector does.

A reference architecture

Field instruments stay where they are. An edge layer near the cleanroom collects every signal on a disciplined clock, buffers it, and evaluates alarms without depending on the network. The site record layer holds the validated environmental monitoring system (EMS) or historian and its audit trail. People reach it through role-based views; nothing reaches into the cleanroom network from outside.

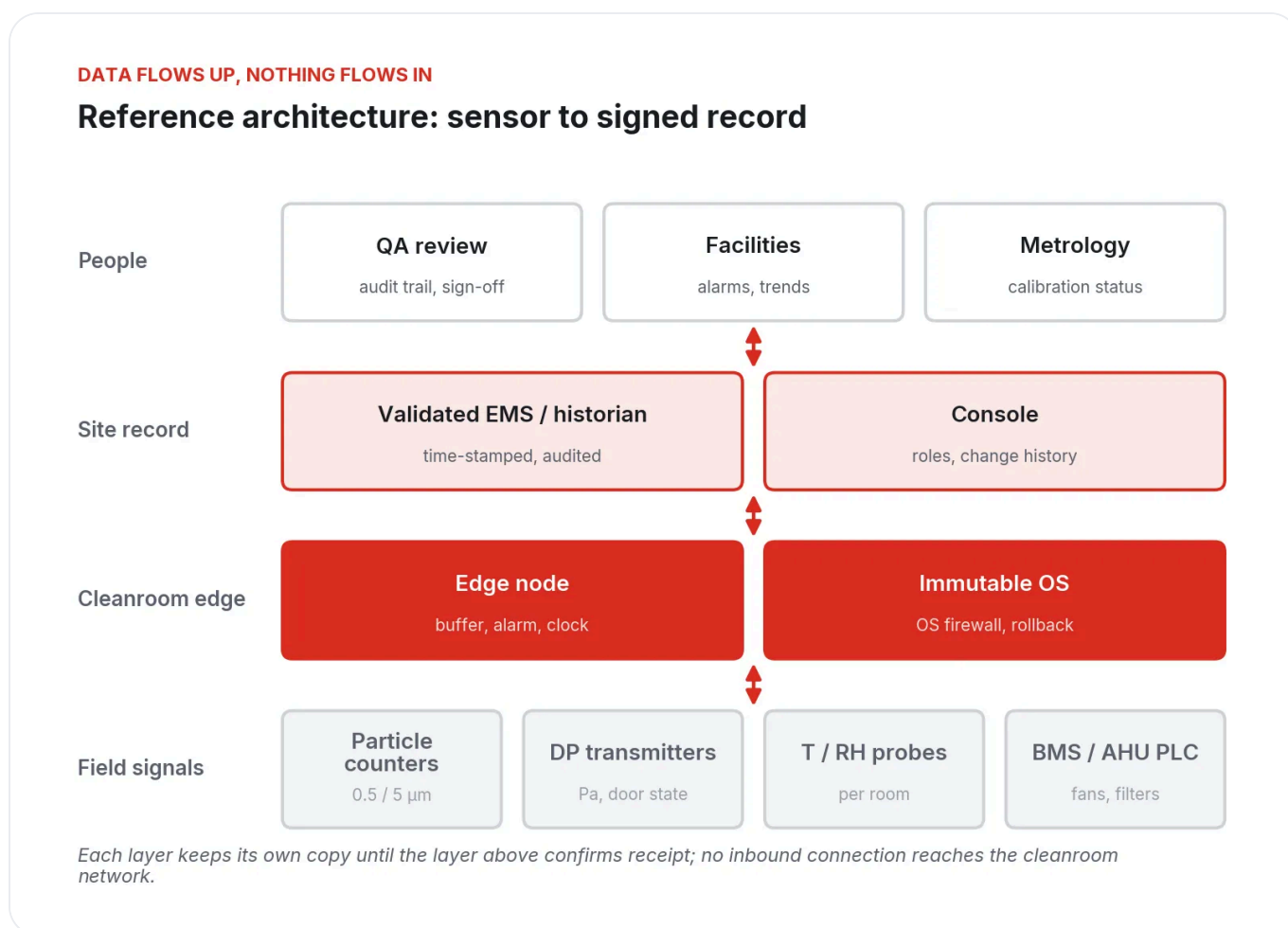


Figure 3. Reference architecture for a cleanroom monitoring record. Data moves upward from field instruments through a buffered edge layer to the validated record; no inbound connection reaches the cleanroom network.

The design choices that make this hold up:

- 1. Buffer at the edge.** Each layer keeps its copy until the layer above confirms receipt. A switch reboot during a fill becomes a backfill, with the backfill itself logged, instead of a data gap and a deviation.

- 2. Alarm at the edge.** Clause 4.16 asks for a warning that is instant. Alert evaluation for Grade A counts and critical pressures should run close to the instrument, so a server outage cannot silence it.
- 3. One clock.** PIC/S expects operating system clocks to be synchronized with connected systems and access to clocks to be restricted to authorized people [7]. MHRA asks for controlled, synchronized clocks and a stated time zone where data crosses sites [8]. The edge layer is the natural place to discipline time for instruments that cannot do it themselves.
- 4. Outbound only.** The cleanroom network should accept no inbound connections. Vendors, corporate systems, and remote engineers connect through an authenticated, logged path that the site controls.
- 5. Immutable base.** The software on edge devices should change only through a controlled, recorded change, with a known-good version to return to. Annex 11 clause 10 asks for exactly this discipline for configurations [2].

On EmberNet. An EmberNode sits in front of the existing counters, transmitters, and BMS controller and microsegments them; the instruments and the AHU PLC keep running unchanged. The node runs EmberRTOS, an immutable operating system with a firewall built into the OS and automatic rollback patching, so the edge layer changes only through a recorded update and can return to the prior image. Collection, buffering, and alarm apps run side by side as containers on the node, and a crashed app does not take the node down.

Walking through the work

The order below puts the cheap, high-value fixes first. Each step stands on its own and can be done with the systems you have.

Step 1: Fix the clocks and the accounts

List every system that time-stamps environmental data: counter software, EMS, BMS, historian, and isolator and line HMIs. Record each clock's source and offset, point them all to one site time source, and restrict who can change time settings [7].

Then list every account, vendor service accounts included. FDA states that shared logins prevent attribution; shared read-only accounts are acceptable for viewing only [5]. Administrator rights should

sit with people independent of those responsible for record content [5].

Step 2: Write the alarm philosophy into the CCS

Annex 1 requires alarm delays on critical pressures to be justified in the CCS (clause 4.16) [1], and alarm events to be acknowledged and evaluated for trends, with critical alarms reviewed immediately (clause 5.2) [1]. For each alarm, record the limit, the delay, the reason for the delay, who acknowledges it, and the required response. For Grade A 5 µm counts, decide how consecutive low-level counts will be detected, since a single-sample check cannot see them (Table 5, Note 2) [1].

Step 3: Bring the context onto the same record

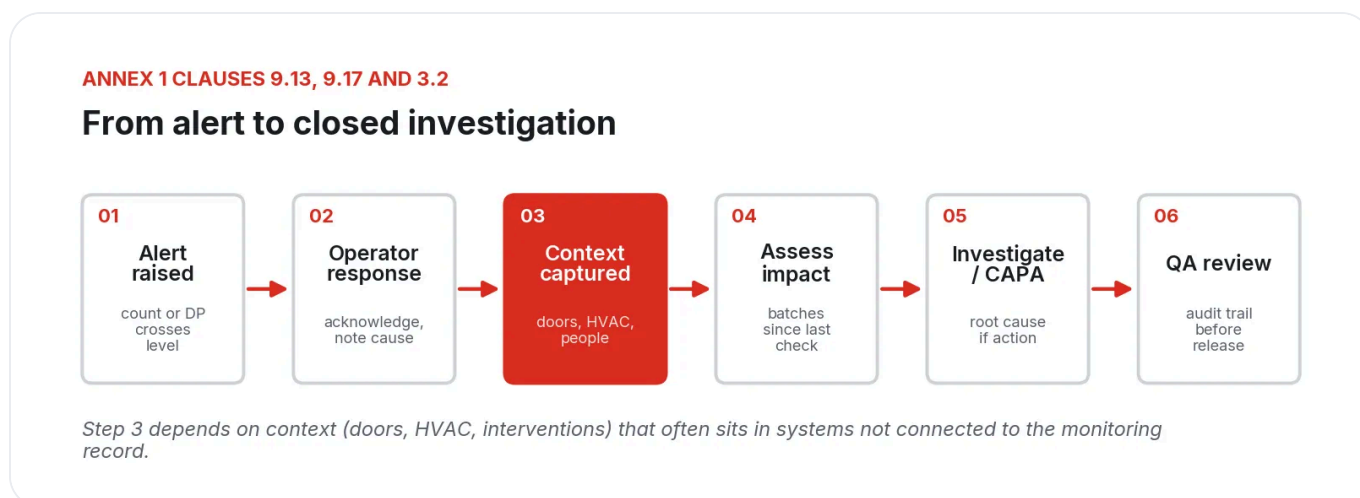


Figure 4. The excursion workflow implied by Annex 1 clauses 3.2, 9.13, and 9.17. Step 3 is the one that depends on context held outside the monitoring system.

Door states, AHU fan status, filter differential pressure, and isolator state separate a stopper-jam intervention from a failing HEPA filter. Read them, read-only, into the same time-aligned record as particle and pressure data, so the investigator opens one window instead of four systems.

On EmberNet. Apps run as containers or full virtual machines on the same node, orchestrated by k3s and deployed, updated, or rolled back from EmberCORE. A site can run an MQTT broker, Node-RED, or Ignition Edge for tag collection and InfluxDB for local buffering next to its own validated EMS connector, each as a separate, versioned app. Connectors are not limited to one vendor's instruments.

Step 4: Buffer locally and prove the backfill

Annex 11 clause 7 asks that stored data be checked for accessibility, readability, and accuracy, and that the ability to restore be checked during validation and monitored periodically [2]. FDA says a backup must be a true copy kept securely through the retention period, and that temporary copies kept for a computer crash do not count [5]. In practice: pull the network cable from an edge device during a qualification run, record for 30 minutes, reconnect, and show that every sample arrived with its original time stamp and that the gap and backfill were both logged.

Step 5: Make the audit trail reviewable

PIC/S expects audit trail functions to be enabled and locked so they cannot be deactivated, deleted, or modified; if an administrator can switch them off, the system should log that it happened [7]. Critical audit trails should be reviewed with the other records before the operation is complete, for example before batch release, and PIC/S allows review by exception focused on anomalous or unauthorized activity [7]. FDA ties audit trail review frequency to the review frequency of the underlying data, or to a documented risk assessment when CGMP does not specify one, and names alert records and instrument communication logs as examples [5].

ALCOA+ IN PRACTICE

What an inspector reconstructs from one excursion

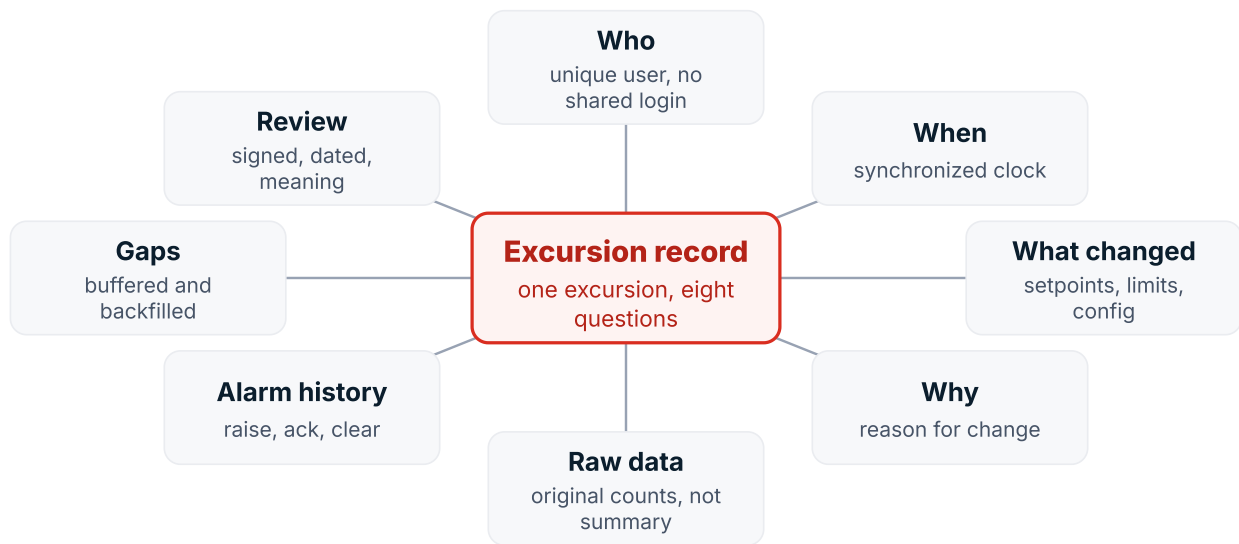


Figure 5. The questions an inspector can answer from one well-formed excursion record. Drawn from FDA data integrity guidance (2018), PIC/S PI 041-1 (2021), and MHRA guidance (2018).

Build a per-batch exception report: limit and setpoint changes, late alarm acknowledgements, gaps and backfills, calibration-overdue points, and service-account logins. The reviewer signs that report.

Where these projects go wrong

These come from public FDA warning letters and guidance.

- 1. Probes in the wrong place.** In a February 2025 warning letter, FDA found non-viable particle probes positioned well above the level where sterile materials were exposed, and operators placing mobile counters in locations other than those in procedures [15]. Annex 1 clause 9.7 requires sampling locations and probe orientation to be justified [1].
- 2. Pressure recorded by hand.** FDA cited one manufacturer for recording room differential pressures manually at intervals rather than through an integrated system, and for lacking a building management system able to monitor and record them [17]. Another firm lacked an adequate integrated system for frequently recording differential pressure, with excursions including reversals [16].
- 3. Alarm delays used to avoid investigations.** In a 2020 letter, the same firm required an investigation of particle action-level excursions only when the excursion lasted beyond a set duration, which FDA treated as inadequate [16]. Annex 1 now expects alarm delays to be justified in the CCS [1].

- 4. Raw data and audit trails not reviewed before release.** The 2025 letter cited production and quality staff who did not review electronic raw data and audit trails before batch release, and repeated testing where only the passing result was reported [15].
- 5. Audit trails switched off or never switched on.** MHRA expects audit trails to be on and not amendable by users [8]. One monitoring vendor lists inactive audit trails and undocumented changes among common failures [18].
- 6. Validation that tests the wrong things.** Scripted protocols often exercise every screen and miss the backfill, clock, and alarm path. GAMP 5 (second edition, July 2022) asks for critical thinking by experienced subject matter experts and greater use of supplier documentation [12], and focusing effort on functions that affect patient safety, product quality, and data integrity [13].
- 7. Remote access nobody can see.** Vendor support through an unmanaged remote desktop tool on the EMS server breaks access control and attribution at once. PIC/S lists remote vendor updates and network exposure among the risks to computerized system settings, and asks for least-privilege firewall rules [7].

Security and data integrity controls

The site's validation, quality agreements, and procedures decide whether a system meets these controls; the architecture's job is to make each one easy to implement and test.

21 CFR Part 11 and FDA data integrity

Part 11 §11.10 lists the controls for closed systems [3]. The ones that bear directly on monitoring are: validation (a); the ability to produce accurate and complete copies (b); protection of records through the retention period (c); limiting access to authorized individuals (d); secure, computer-generated, time-stamped audit trails that record creation, modification, and deletion without obscuring prior entries (e); operational and authority checks (f, g); device checks (h); and controls over system documentation (k) [3]. Electronic signatures must show the signer's name, date and time, and the meaning of the signature (§11.50), and must be linked to their records so they cannot be copied or transferred (§11.70) [3]. FDA's 2018 guidance defines data integrity through ALCOA (attributable, legible, contemporaneous, original or true copy, accurate) and treats data generated to satisfy CGMP as CGMP records from the moment of creation [5].

EU GMP Annex 11

Annex 11 applies risk management through the system life cycle (clause 1), and requires validation (4), data storage and backup with tested restore (7), audit trails for GMP-relevant changes and deletions with reasons documented (9), controlled change and configuration management (10), periodic evaluation (11), physical and logical access control with recorded changes to access rights (12),

incident management with root cause (13), electronic signatures permanently linked to records with date and time (14), and tested business continuity arrangements (16) [2]. PIC/S PI 041-1 extends ALCOA to ALCOA+ by adding complete, consistent, enduring, and available [7].

How the architecture supports the controls

CONTROL	REQUIREMENT	ARCHITECTURAL SUPPORT
Access (11.10(d); Annex 11 cl. 12)	Authorized individuals only; access changes recorded	Named accounts and role-based views; identity-based device access; no shared logins
Audit trail (11.10(e); Annex 11 cl. 9)	Time-stamped, independent, reasons for change	Audit trail kept on site with the record; edge changes recorded as versioned deployments
Time (PIC/S PI 041-1; MHRA)	Synchronized clocks, restricted access	Edge layer disciplines time for instruments; clock settings restricted
Change control (Annex 11 cl. 10)	Changes made only through a defined procedure	Immutable OS; apps deployed and rolled back as versioned units
Backup and restore (Annex 11 cl. 7; FDA Q&A)	True copy, restore tested	Local buffering with logged backfill; restore exercised in qualification
Business continuity (Annex 11 cl. 16)	Tested alternative arrangements	Alarms evaluated at the edge; the node keeps running when an app or the WAN fails
Network security (PIC/S PI 041-1)	Least-privilege firewall, protection from external attack	OS-level firewall and microsegmentation; outbound-only connections

On EmberNet. EmberFLUX makes outbound connections only, on port 443, and opens no inbound ports at the plant; there is no VPN to configure, traffic is encrypted, and devices are reached by identity. EmberNet does not require the cloud and can run entirely on premises, so the monitoring record and its audit trail stay at the site. EmberCORE provides role-based views, tenant scope, and an audit trail of platform actions across every node.

On validation approach: FDA finalized its Computer Software Assurance guidance in September 2025. It is written for medical device production and quality system software under 21 CFR 820, and it replaces section 6 of the older General Principles of Software Validation with a risk-based approach built on intended use, risk, proportionate assurance activities, and objective evidence [14]. Many pharmaceutical quality units now apply the same thinking through GAMP 5 second edition [12][13]. For monitoring, that means scripted tests of the alarm path, audit trail, backfill, and clock, and lighter testing of reports.

On EmberNet. Maintenance is the part of remote access that usually breaks attribution. The EmberFLUX maintenance tunnel reaches a specific device by identity, without an inbound port. On September 29, 2026, an engineer in Austin, Texas, downloaded a PLC application from the CODESYS IDE to a virtual PLC on an industrial PC in Cleveland, Ohio, over EmberNet, with no VPN and no inbound port opened.

A phased rollout

ILLUSTRATIVE PLAN

Phased rollout for one filling suite



Figure 6. An illustrative phased plan for one aseptic filling suite. Durations depend on the site's validation approach and change control cycle.

- 1. Assess (weeks 1 to 4).** Inventory every monitoring point, clock, account, and interface for one suite. Score each against the self-check questions and against the CCS. Out of this comes a gap list and a user requirements specification grounded in a risk assessment, as Annex 11 clause 4 expects [2].
- 2. Connect (weeks 5 to 10).** Install edge devices in front of the counters, pressure transmitters, BMS, and isolator controller, read-only. Run them in parallel with the existing EMS, and do not use them as the record yet.
- 3. Qualify (weeks 11 to 16).** Test the intended use: alarm path at the edge, backfill after a network loss, clock discipline, audit trail entries for limit changes, access control, restore. Use the supplier's documentation where it is adequate.
- 4. Operate (second quarter).** Move to the new record. Run monthly trend reviews against clause 9.11 and audit trail review by exception before each batch release.
- 5. Extend (third quarter onward).** Add the next suite, then support areas. Feed the accumulated monitoring data into the ISO 14644-2 argument for your requalification interval [11].

What to do Monday

Pick the suite with the most investigations. Pull its last three Grade A or B alert events and reconstruct the five minutes around each: counts, pressures, doors, AHU status, who acknowledged what, on one time base. Note how long each took and which systems you had to open. Then record the clock offset on every system that time-stamps environmental data, and list every shared or vendor account. That one table (events, time to reconstruct, clock offsets, shared accounts) is your business case and your first CAPA, and it needs no new equipment.

About Fireball Industries

Fireball Industries is EmberNet's master integrator. Its engineers design, build, and support monitoring systems like this one with the site's QA, validation, and facilities teams, connecting the instruments and controllers a site already runs and supporting the system through qualification and operation.

Sources

1. European Commission. EudraLex Volume 4, EU GMP Guidelines, Annex 1: Manufacture of Sterile Medicinal Products. Published August 25, 2022; in operation August 25, 2023.
https://health.ec.europa.eu/system/files/2022-08/20220825_gmp-an1_en_0.pdf
2. European Commission. EudraLex Volume 4, Annex 11: Computerised Systems. In operation June 30, 2011.
https://health.ec.europa.eu/system/files/2016-11/annex11_01-2011_en_0.pdf
3. U.S. Code of Federal Regulations. 21 CFR Part 11, Electronic Records; Electronic Signatures. Current eCFR text, accessed September 2026. <https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11>
4. U.S. Code of Federal Regulations. 21 CFR 211.42, Design and construction features. Current eCFR text, accessed September 2026. <https://www.ecfr.gov/current/title-21/chapter-I/subchapter-C/part-211/subpart-C/section-211.42>
5. U.S. Food and Drug Administration. Data Integrity and Compliance With Drug CGMP: Questions and Answers, Guidance for Industry. December 2018. <https://www.fda.gov/media/119267/download>
6. U.S. Food and Drug Administration. Sterile Drug Products Produced by Aseptic Processing: Current Good Manufacturing Practice, Guidance for Industry. September 2004.
<https://www.fda.gov/media/71026/download>
7. Pharmaceutical Inspection Co-operation Scheme (PIC/S). PI 041-1, Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments. July 1, 2021. <https://picscheme.org/docview/4234>
8. Medicines and Healthcare products Regulatory Agency (MHRA). GXP Data Integrity Guidance and Definitions, Revision 1. March 2018.
https://assets.publishing.service.gov.uk/media/5aa2b9ede5274a3e391e37f3/MHRA_GxP_data_integrity_guide_March_edited_Final.pdf
9. International Organization for Standardization. ISO 14644-1:2015, Cleanrooms and associated controlled environments, Part 1: Classification of air cleanliness by particle concentration. December 2015.
<https://www.iso.org/standard/53394.html>
10. International Organization for Standardization. ISO 14644-2:2015, Cleanrooms and associated controlled environments, Part 2: Monitoring to provide evidence of cleanroom performance related to air cleanliness by particle concentration. December 2015. <https://www.iso.org/standard/53393.html>
11. PharmOut. What does the recent ISO 14644-2:2015 update mean for pharmaceutical cleanroom monitoring? Accessed September 2026. <https://www.pharmout.net/iso-14644-12015-update-cleanroom-monitoring/>
12. ISPE. GAMP 5 Guide: A Risk-Based Approach to Compliant GxP Computerized Systems, Second Edition. July 2022. <https://ispe.org/publications/guidance-documents/gamp-5-guide-2nd-edition>

- 13.** Walia, G. and Neri, D. Computer Software Assurance and the Critical Thinking Approach. ISPE Pharmaceutical Engineering, March/April 2024. <https://ispe.org/pharmaceutical-engineering/march-april-2024/computer-software-assurance-and-critical-thinking>
- 14.** U.S. Food and Drug Administration. Computer Software Assurance for Production and Quality Management System Software, Guidance for Industry and FDA Staff. Finalized September 24, 2025, as "Computer Software Assurance for Production and Quality System Software"; current version issued February 3, 2026. <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/computer-software-assurance-production-and-quality-management-system-software>
- 15.** U.S. Food and Drug Administration. Warning Letter 701671, Aspen Pharmacare Holdings Limited. February 24, 2025. <https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/aspen-pharmacare-holdings-limited-701671-02242025>
- 16.** U.S. Food and Drug Administration. Warning Letter 607837, Panacea Biotech Limited. September 24, 2020. <https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/panacea-biotech-limited-607837-09242020>
- 17.** U.S. Food and Drug Administration. Warning Letter 654986, KC Pharmaceuticals Inc. August 3, 2023. <https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/kc-pharmaceuticals-inc-654986-08032023>
- 18.** Vaisala (vendor). GxP data integrity for environmental monitoring systems: ALCOA+ and regulatory expectations. Accessed September 2026. <https://www.vaisala.com/en/gxp-environmental-monitoring-systems-for-data-integrity>