Synthèse de validation logicielle

Axiospec, gestion des étalonnages Préparé pour le responsable qualité, le responsable de la validation ou l'évaluateur informatique qui évalue Axiospec comme système d'enregistrement de référence pour les étalonnages.

Version du document 1.0. Dernière revue le 19/08/2026. Publié par CaliTech LLC, Knoxville, Tennessee (États-Unis). Questions : support@axiospec.com, réponse sous un jour ouvré.

À lire en premier

Ce document est **une contribution à votre dossier de validation. Ce n'est pas un dossier de validation.**

Axiospec ne valide pas votre instance, ne certifie pas votre conformité et ne réalise pas votre qualification. La validation est une détermination que vous faites sur votre propre usage prévu, votre configuration, vos procédures et votre personnel. Votre organisme certificateur, votre évaluateur ou votre inspecteur décide si vous y avez satisfait.

Ce que ce document vous apporte : une déclaration d'usage prévu, une description des contrôles d'intégrité des données qui existent dans le produit et de la façon dont ils sont imposés, une liste de contrôle que vous pouvez exécuter et signer dans votre propre espace de travail, notre pratique de gestion des changements et une liste claire de ce que le logiciel ne fait pas.

Selon la catégorisation GAMP 5, un registre SaaS multilocataire configuré de ce type est normalement traité comme une Catégorie 4 (produit configuré). Cela signifie que votre effort de validation est fondé sur les risques et s'appuie sur la documentation de l'éditeur, complétée par vos propres tests de configuration et de processus. Confirmez cette catégorisation au regard de votre propre procédure.

1. Déclaration d'usage prévu

Axiospec est un système de gestion documentaire pour les équipements de mesure et d'essai. Son usage prévu est de :

- Tenir un registre des instruments, avec leur identification, leur fabricant, leur modèle, leur numéro de série, leur emplacement, leur site et les champs personnalisés définis dans l'espace de travail.
- Enregistrer les événements d'étalonnage et de vérification de ces instruments, y compris les relevés avant ajustage et après ajustage, la valeur nominale, la tolérance, le résultat, les conditions ambiantes, l'étalon de référence utilisé, le numéro de certificat, le prestataire et la référence de traçabilité.
- Enregistrer les champs métrologiques utilisés dans les processus ISO/IEC 17025 : incertitude de mesure, facteur d'élargissement, niveau de confiance, règle de décision, déclaration de conformité et numéro de certificat de l'étalon de référence lui-même.
- Identifier le statut d'étalonnage de chaque instrument et sa date de prochaine échéance, et faire ressortir les instruments en retard et ceux qui arrivent à échéance.

- Conserver ces enregistrements en ajout seul, sous une forme à intégrité vérifiable, avec attribution et horodatage.
- Faire passer les enregistrements d'étalonnage par une approbation facultative à deux personnes avant qu'ils prennent effet.
- Produire un export complet, lisible par l'humain et par la machine, du registre et de son historique pour l'audit.

Axiospec **n'est pas** un laboratoire d'étalonnage accrédité et ne réalise aucune mesure. Chaque document produit par le système porte textuellement cette mention :

> « Données d'étalonnage saisies par le personnel de l'espace de travail. Axiospec est un système de gestion documentaire, non un laboratoire d'étalonnage accrédité, et n'a pas réalisé cette mesure. »

Axiospec n'est pas un logiciel de dispositif médical, et aucune pertinence au regard de l'IEC 62304 n'est revendiquée ni suggérée. L'IEC 62304 s'applique aux logiciels qui sont un dispositif médical ou en font partie. Un registre d'étalonnages est un outil du système qualité.

Quels articles fixent les attentes envers un tel système

Le texte des articles des normes ISO est protégé par le droit d'auteur ; ce qui suit est donc une série de références d'articles avec paraphrase, et non des citations. Vérifiez-les dans votre propre exemplaire sous licence.

- **ISO 9001:2015, article 7.1.5.2** (traçabilité de la mesure) : équipements étalonnés ou vérifiés à intervalles spécifiés par rapport à des étalons traçables, identifiables quant à leur statut d'étalonnage, protégés contre les réglages qui invalideraient le résultat, et évaluation des résultats antérieurs lorsqu'un équipement est jugé inapte.
- **ISO 9001:2015, article 7.5.3** (maîtrise des informations documentées) : disponibilité, protection contre la perte d'intégrité, maîtrise de l'accès, stockage et préservation, maîtrise des modifications et des versions, conservation et élimination.
- **ISO 9001:2015, article 8.4** et **ISO/IEC 17025:2017, article 6.6** (produits et services fournis par des prestataires externes) : vous devez évaluer et enregistrer votre qualification d'Axiospec comme fournisseur. Ce document est conçu pour servir de preuve dans cet enregistrement.
- **ISO/IEC 17025:2017, article 6.4** (équipements), en particulier 6.4.6 (étalonnage lorsque l'exactitude ou l'incertitude influe sur la validité), 6.4.8 (étiquetage ou codage du statut pour que l'utilisateur identifie facilement le statut d'étalonnage ou la période de validité) et 6.4.13 (le contenu exigé des enregistrements relatifs aux équipements).
- **ISO/IEC 17025:2017, article 7.11** (maîtrise des données et gestion de l'information), en particulier 7.11.2 (le système de gestion de l'information est validé pour sa fonctionnalité, y compris les interfaces) et 7.11.3 (protégé contre l'accès non autorisé, sauvegardé contre l'altération et la perte, exploité conformément à sa spécification, entretenu pour garantir l'intégrité des données, avec enregistrement des défaillances et des actions correctives).
- **ISO 13485:2016, article 4.1.6** : procédures de validation des logiciels informatiques utilisés dans le SMQ, avant la première utilisation et après modification, avec une approche proportionnée au risque, et

conservation des enregistrements.

- **21 CFR Part 11**, lorsque les enregistrements d'étalonnage sont vos enregistrements réglementés de référence : 11.10(a) validation, 11.10(b) copies exactes et complètes sous forme lisible par l'humain et sous forme électronique, 11.10(c) protection et récupération rapide, 11.10(d) limitation de l'accès aux personnes autorisées, 11.10(e) pistes d'audit sécurisées, générées par ordinateur et horodatées, où « les modifications d'enregistrements ne doivent pas masquer les informations précédemment enregistrées », 11.10(g) contrôles d'autorité, 11.50 manifestations de la signature, 11.70 liaison entre signature et enregistrement.

Notez que l'ISO 9001 ne contient pas d'article explicite sur la validation des logiciels. Pour une entreprise qui applique la seule 9001, l'obligation porte sur la maîtrise des informations documentées, pas sur un protocole de validation. Dimensionnez votre effort en conséquence.

2. Contrôles d'intégrité des données existants

2.1 Registre d'étalonnage en ajout seul, à intégrité vérifiable

Chaque événement d'étalonnage est écrit dans un registre. Dès qu'une entrée est confirmée (c'est-à-dire dès qu'elle quitte l'état de brouillon, DRAFT), elle ne peut plus être ni modifiée ni supprimée.

Comment toute altération devient détectable. Chaque entrée confirmée stocke un `record_hash` : une empreinte SHA-256 calculée sur une sérialisation JSON canonique, à clés triées, des champs de cette entrée, qui inclut le `record_hash` de l'entrée précédente sous le nom `prev_hash`. Les entrées sont chaînées par espace de travail dans l'ordre d'insertion, avec `created_at` forcé à être strictement croissant, de sorte que l'ordre est une relecture déterministe. Toute modification, insertion ou suppression d'un enregistrement change son empreinte et rompt la chaîne à partir de ce point, et la rupture est détectable.

Les champs pris en compte dans l'empreinte sont : l'équipement, le type d'événement, l'horodatage de réalisation, l'utilisateur qui l'a réalisé, le résultat de l'étalonnage, la valeur nominale, la tolérance, les relevés avant ajustage et après ajustage, la température, l'humidité, l'étalon de référence, les mesures, les notes, la référence de la pièce jointe, le numéro de certificat, le prestataire, la référence de traçabilité, le motif de correction et les champs métrologiques énumérés à la section 1.

Les fichiers de preuve entrent dans l'empreinte par leur contenu, pas seulement par leur référence. L'empreinte SHA-256 du certificat ou de la photo envoyés est calculée côté serveur et intégrée à l'empreinte de l'enregistrement. Remplacer le fichier derrière un lien inchangé rompt la chaîne.

L'immuabilité est imposée par la base de données, pas par le code de l'application. Un trigger PostgreSQL sur la table du registre bloque, au niveau de la base de données : la suppression d'une entrée confirmée, le retour d'une entrée confirmée à l'état de brouillon et la modification de toute colonne d'identité ou prise en compte dans l'empreinte d'une entrée confirmée. Cela signifie qu'une session SQL directe sur la base de données de production ne peut pas réécrire en silence un enregistrement d'étalonnage. C'est un contrôle plus fort qu'une vérification dans la couche applicative, et c'est précisément le point qui mérite d'être démontré à un évaluateur.

Les changements sont représentés par ajout, jamais par écrasement. C'est la réponse directe à l'exigence de la Part 11 selon laquelle les modifications d'enregistrements ne doivent pas masquer les

informations précédemment enregistrées.

- Une **correction** est une nouvelle entrée ajoutée qui fait référence à l'entrée qu'elle remplace et porte un motif de correction en texte libre. Le motif est obligatoire (l'API rejette une correction sans motif) et fait lui-même partie de l'empreinte. L'entrée remplacée reste dans l'historique, entièrement lisible.
- Une **annulation** est un événement marqueur ajouté au registre. L'original annulé reste dans l'historique avec l'étiquette annulé, et l'instrument revient à son étalonnage précédent ou à non étalonné. Une annulation ne peut jamais compter comme un étalonnage.

Vérification en un clic. Tout utilisateur authentifié de l'espace de travail peut lancer une vérification complète de la chaîne, qui parcourt chaque entrée confirmée, recalcule chaque empreinte, contrôle la continuité et indique soit un résultat sans anomalie avec le nombre d'entrées vérifiées, soit la première entrée divergente avec le repère de son instrument. Le résultat et l'utilisateur qui a vérifié sont enregistrés.

Vérification indépendante hors de la plateforme. L'export d'audit contient les valeurs `record_hash` et `prev_hash` dans le CSV du manifeste, ainsi qu'un README décrivant pas à pas comment vérifier hors ligne le **chaînage** sans Axiospec : le `prev_hash_hex` de chaque ligne doit être égal au `record_hash_hex` de la ligne précédente, si bien que tout enregistrement supprimé, inséré ou réordonné apparaît comme un lien rompu. Soyons précis sur la limite. Le manifeste ne contient pas tous les champs qui alimentent la fonction de hachage, il n'est donc pas possible de recalculer l'empreinte d'un enregistrement à partir du seul CSV. Le recalcul de l'empreinte d'un enregistrement individuel se fait côté serveur, dans l'application et au moment de l'export. Le chaînage est ce que vous pouvez prouver vous-même, sans nous, pour toujours.

2.2 Piste d'audit

Enregistrements d'étalonnage. Chaque entrée stocke l'identifiant de l'utilisateur qui l'a réalisée ainsi qu'un instantané figé de son nom, l'horodatage de réalisation et l'horodatage de création côté serveur. Lorsque l'entrée passe en revue, elle stocke aussi l'identifiant et l'instantané du nom du vérificateur, l'horodatage de la revue, les notes de revue et l'éventuel motif de rejet. Les valeurs antérieures sont préservées par construction : rien n'est écrasé, la « valeur précédente » est donc l'entrée remplacée, toujours lisible.

Administration de l'espace de travail. Un journal d'activité distinct enregistre les actions liées à l'équipe et à la configuration avec l'utilisateur à l'origine de l'action, la cible, un enregistrement JSON de ce qui a changé, l'adresse IP source et un horodatage. Les actions couvertes comprennent les invitations et révocations d'utilisateurs, les changements de rôle, l'archivage d'utilisateurs, les changements d'adresse e-mail, l'émission et la révocation de clés d'API, les modifications de la configuration SSO et les connexions SSO, les modifications d'abonnements aux webhooks et le début d'une période d'essai de la facturation. Les administrateurs de l'espace de travail peuvent le consulter dans l'application, strictement limité à l'espace de travail de la session authentifiée et non à un paramètre de requête.

Lacune connue, déclarée. Les modifications de la fiche principale d'un instrument (par exemple son intervalle d'étalonnage) ne sont pas encore consignées dans le journal d'audit du système. Les événements d'étalonnage eux-mêmes sont immuables et entièrement attribués. Il en va de même pour le repère, le numéro de série et l'emplacement d'un instrument. Si votre procédure doit savoir « qui a modifié l'intervalle de cet instrument et quand », vous devez le couvrir par votre propre contrôle jusqu'à ce que cette lacune soit comblée. Voir la section 6.

2.3 Approbations (auteur et vérificateur)

La revue à deux personnes est disponible par instrument ou pour tout l'espace de travail. Elle est **facultative et désactivée par défaut.**

Lorsque la revue est exigée, le système refuse que la personne qui soumet approuve son propre enregistrement. Le contrôle est inconditionnel au début des deux voies, approbation et rejet, et il échoue aussi en position fermée si l'identité de l'approbateur ne peut pas être résolue. L'approbation exige le rôle de responsable ou d'administrateur, vérifié à la fois au niveau de toute l'organisation et sur le site précis auquel appartient l'instrument, si bien qu'un responsable de toute l'organisation rétrogradé sur ce site y est refusé. La route générique de mise à jour des enregistrements refuse de fixer un statut approuvé ou rejeté, de sorte que le workflow ne peut pas être contourné. Les annulations suivent le même workflow, et une annulation en attente ou rejetée ne masque pas l'original.

Lorsque la revue **n'est pas** exigée, la soumission est approuvée automatiquement et la personne qui soumet est enregistrée comme approbateur. Une seule personne enregistre et l'enregistrement prend effet immédiatement. Indiquez-le clairement dans votre propre analyse des risques, et activez la revue pour les instruments où votre analyse des risques l'exige.

2.4 Signatures électroniques

Ce qui est réel et disponible. La signature électronique est un paramètre par espace de travail. Elle est facultative, pas obligatoire. Lorsqu'un espace de travail l'active, l'approbation exige que le mot de passe du propre compte de l'approbateur soit revérifié au moment de la signature, côté serveur, par rapport à l'empreinte du mot de passe stockée, avant que l'approbation ne se poursuive. Un mauvais mot de passe est toujours refusé avec une erreur 403, quel que soit le réglage de configuration. L'application mobile demande le mot de passe lors de l'enregistrement d'un étalonnage. Les mots de passe sont stockés en PBKDF2-HMAC-SHA256 avec 260 000 itérations et un sel aléatoire de 16 octets par mot de passe, et la vérification se fait en temps constant. Un endpoint de réauthentification distinct existe dans le même but. L'utilisateur qui approuve et l'horodatage de l'approbation sont consignés dans l'enregistrement immuable du registre, figés par le trigger de base de données décrit à la section 2.1.

Deux limites à connaître avant de vous y fier.

1. **Elle est facultative par espace de travail et n'est pas imposée strictement aujourd'hui.** Si le client n'envoie aucun mot de passe de signature, l'approbation aboutit actuellement et consigne un avertissement, au lieu d'être refusée. Seul un mauvais mot de passe est refusé. L'interrupteur d'application stricte existe dans le code, mais n'est pas activé dans l'environnement de production.
2. **Il n'existe pas de liaison cryptographique de signature stockée.** Ne vous attendez pas à un artefact de signature distinct et récupérable sur l'enregistrement d'étalonnage, ni à un indicateur « signé » dans l'API. La preuve durable est l'enregistrement d'approbation lui-même : l'identité de l'approbateur, l'instantané de son nom, l'horodatage de l'approbation et les notes de revue, tous figés par le trigger d'immuabilité.

Par conséquent, Axiospec **ne satisfait pas** aujourd'hui aux articles 11.50 et 11.70 du 21 CFR, et l'exigence de deux composants d'identification distincts pour les sessions non continues ne peut pas être satisfaite, car le produit ne dispose pas d'authentification multifacteur. Si les signatures électroniques au sens de la

Part 11 sont une exigence ferme pour vous, traitez ce point comme une lacune et soulevez-le avec nous avant d'acheter.

2.5 Contrôle d'accès fondé sur les rôles

Cinq rôles : super-administrateur, administrateur, responsable, technicien, auditeur. L'application des droits se fait **côté serveur**, sur chaque route, au moyen des dépendances FastAPI. Le rôle de l'utilisateur est redéterminé à partir de la base de données au moment de la requête au lieu de faire confiance au jeton de session, si bien qu'un jeton périmé ne peut pas conserver des privilèges élevés. Des restrictions existent aussi côté client, mais elles sont cosmétiques ; le serveur est le point d'application.

Comportements pertinents pour 11.10(d) et (g) et pour l'ISO/IEC 17025 7.11.3 :

- Le pouvoir de modifier les rôles est encadré. Un responsable ne peut gérer que des techniciens. Les droits d'invitation sont limités selon le rôle.
- **Le rôle d'auditeur est imposé en lecture seule dans tout le système.** Toutes les méthodes HTTP d'écriture sont bloquées pour les auditeurs, avec exactement deux exceptions autorisées : demander un export de la piste d'audit et révoquer son propre jeton de flux de calendrier (ce qui retire un accès et n'en accorde jamais). C'est le rôle à attribuer à votre organisme certificateur ou à un évaluateur externe.
- Une **frontière d'accès par site** s'ajoute au rôle. Un utilisateur peut détenir un rôle à l'échelle de l'organisation et se voir quand même refuser l'accès sur un site précis, et cela est vérifié lors de la soumission, de l'annulation et de l'approbation d'étalonnages.
- Seuls les responsables et les administrateurs peuvent annuler un étalonnage. Les techniciens ne peuvent corriger que leurs propres enregistrements ; les responsables et les administrateurs peuvent corriger n'importe lequel.

Les enregistrements sont stockés avec un cloisonnement par espace de travail au niveau des lignes, imposé dans la couche d'accès aux données, l'espace de travail étant tiré d'une revendication de session dont la signature est vérifiée, jamais d'un en-tête fourni par le client. Notez la description honnête : il s'agit d'un cloisonnement par espace de travail **imposé par l'application**, pas de la sécurité au niveau des lignes de PostgreSQL, ni d'une base de données distincte par client. L'immuabilité du registre, en revanche, est imposée par la base de données.

3. Ce que vous devriez vérifier dans votre propre environnement

Ce qui suit est un protocole suggéré, que vous exécutez et enregistrez. Rien ici n'a été exécuté pour vous. Pour chaque étape, enregistrez la date, la personne qui l'a exécutée, le résultat attendu, le résultat obtenu, la conformité ou non, et joignez une capture d'écran. Au sens de l'ISO/IEC 17025 7.11.2, c'est la vérification fonctionnelle qui vous revient.

Qualification d'installation (IQ), configuration enregistrée

N°	Contrôle	Enregistrement
IQ-1	Nom de l'espace de travail, URL de l'application et date de première utilisation en production	

N°	Contrôle	Enregistrement
IQ-2	Utilisateurs nommés, leurs rôles et leurs droits par site	
IQ-3	Paramètres de l'espace de travail enregistrés : approbations exigées oui/non, signature électronique activée/désactivée, modules activés, champs personnalisés définis	
IQ-4	Sites et emplacements configurés, conformes à votre liste d'installations	
IQ-5	Registre des instruments chargé, nombre rapproché de votre registre source	
IQ-6	Dossier de qualification fournisseur ouvert pour CaliTech LLC, avec ce document en pièce jointe	
IQ-7	Votre procédure maîtrisée désignant Axiospec comme système d'enregistrement des étalonnages, émise et approuvée dans le cadre de votre maîtrise documentaire	

Qualification opérationnelle (OQ), tests fonctionnels

N°	Test	Résultat attendu
OQ-1	Enregistrer un étalonnage sur un instrument de test	L'entrée apparaît dans l'historique de cet instrument avec votre nom, la date de réalisation et les relevés saisis
OQ-2	Tenter de modifier cet enregistrement confirmé	Le système refuse et vous invite à émettre une correction
OQ-3	Tenter de supprimer cet enregistrement confirmé	Le système refuse en indiquant que le registre est en ajout seul
OQ-4	Émettre une correction sans motif, puis avec un motif	Refusée sans motif ; acceptée avec un motif ; l'entrée d'origine reste visible dans l'historique
OQ-5	En tant que responsable, annuler un étalonnage	L'original reste dans l'historique avec l'étiquette annulé ; le statut de l'instrument revient à l'étalonnage précédent ou à non étalonné
OQ-6	En tant que technicien, tenter d'annuler un étalonnage	Refusé
OQ-7	Activer l'approbation pour un instrument. Soumettre un étalonnage en tant qu'utilisateur A, puis tenter de l'approuver en tant qu'utilisateur A	Refusé, en invoquant la séparation entre auteur et vérificateur
OQ-8	L'approuver en tant qu'utilisateur B	Le nom de l'approbateur et l'horodatage de l'approbation sont consignés sur l'entrée et visibles dans l'historique

N°	Test	Résultat attendu
OQ-9	Se connecter avec un utilisateur ayant le rôle d'auditeur et tenter une modification quelconque	Toutes les écritures sont refusées
OQ-10	Affecter un utilisateur au seul Site 1, puis tenter d'agir sur un instrument du Site 2	Refusé
OQ-11	Lancer la vérification de la chaîne depuis l'espace d'audit	Indique « vérifiée », avec le nombre d'entrées vérifiées. Enregistrez la date, le nombre et l'utilisateur qui a vérifié
OQ-12	Générer un export d'audit sans périmètre	Un fichier ZIP est téléchargé, contenant audit_manifest.csv, audit_summary.pdf, le guide de vérification README et les fichiers joints
OQ-13	Suivre la procédure du README pour vérifier le chaînage hors ligne	Le `prev_hash_hex` de chaque ligne est égal au `record_hash_hex` de la ligne précédente
OQ-14	Enregistrer un résultat hors tolérance	L'instrument est signalé ; l'évaluation de l'impact du hors tolérance peut être saisie une fois, puis elle est verrouillée
OQ-15	Confirmer que le statut d'étalonnage et la date de prochaine échéance s'affichent correctement pour un instrument connu (ISO/IEC 17025 6.4.8)	Le statut et l'échéance correspondent à ce que vous attendez
OQ-16	Changer le rôle d'un utilisateur, puis ouvrir le journal d'activité de l'espace de travail	Le changement apparaît avec l'utilisateur à l'origine de l'action, la cible et l'horodatage
OQ-17	Modifier l'intervalle d'étalonnage d'un instrument, puis consulter le journal d'activité	**Aucune entrée n'apparaît. C'est la lacune connue de la section 2.2.** Enregistrez-la comme lacune de contrôle et documentez votre contrôle compensatoire
OQ-18	Imprimer ou exporter un certificat d'étalonnage pour un enregistrement approuvé, puis tenter la même chose pour un enregistrement annulé	Le certificat est produit pour l'enregistrement approuvé ; il est refusé pour l'enregistrement annulé

Qualification de performance (PQ), votre processus avec votre personnel

N°	Activité
PQ-1	Définir la période (un cycle d'étalonnage complet est préférable ; un mois est un minimum courant)
PQ-2	Fonctionner en parallèle avec votre registre actuel pendant cette période. Rapprocher à la fin le nombre d'instruments et les échéances
PQ-3	Confirmer que les avis d'échéance et de retard parviennent aux bonnes personnes selon le calendrier prévu
PQ-4	Confirmer que vos techniciens peuvent compléter un enregistrement d'étalonnage selon votre procédure, sans contournement

N°	Activité
PQ-5	Réaliser un audit à blanc. Choisir un instrument au hasard et produire : l'historique complet, la référence de traçabilité, l'étalon de référence utilisé, les pièces jointes de preuve et la preuve que l'enregistrement n'a pas été modifié
PQ-6	Traiter de bout en bout un véritable événement hors tolérance, y compris l'évaluation de l'impact sur les mesures antérieures (ISO 9001 7.1.5.2)
PQ-7	Vérifier la voie de secours prévue par votre procédure en cas d'indisponibilité du système
PQ-8	Rédiger et approuver le rapport de synthèse de validation. Le signer

Requalification. Définissez ce qui déclenche un nouveau test. Une règle pratique pour un SaaS de Catégorie 4 : réexécuter le sous-ensemble de l'OQ qui touche toute fonction sur laquelle vous vous appuyez chaque fois que vous modifiez sensiblement votre configuration (paramètres d'approbation, rôles, sites, champs personnalisés, adaptation aux normes), ainsi qu'à un intervalle de revue périodique que vous fixez. Voir la section 5 pour le fonctionnement des changements côté éditeur.

4. Conservation et export des enregistrements

L'export est en libre-service, complet, et ne dépend ni d'une formule payante ni d'une demande au support. Les responsables, administrateurs et auditeurs peuvent le générer. Les techniciens conservent l'historique par instrument dans l'application, mais pas l'export de tout l'espace de travail.

L'export est un fichier ZIP unique qui contient :

- `audit_manifest.csv` : une ligne par fiche d'instrument, puis une ligne par événement d'étalonnage confirmé. Environ 45 colonnes, dont l'identification de l'instrument, le site et l'emplacement, tous les champs d'étalonnage, les champs métrologiques, les champs d'approbation et de vérificateur, l'impact du hors tolérance, les champs personnalisés de l'espace de travail en JSON, et les valeurs `record_hash_hex` et `prev_hash_hex`. Les colonnes d'empreinte sont volontairement exclues de la protection contre l'injection de formules CSV, afin d'être exactes à l'octet près pour la comparaison du chaînage.
- `audit_summary.pdf` : un rapport lisible avec un tableau de bord de conformité, une section de vérification d'intégrité qui rend toute altération détectable et indique le verdict sur la chaîne, le nombre d'entrées vérifiées, l'algorithme de hachage et les empreintes de l'enregistrement initial et du plus récent, puis la piste d'audit des étalonnages, le registre des instruments et le détail des hors tolérance. Le tableau des exceptions liste les 20 événements concernés les plus récents ; l'ensemble complet se trouve dans `audit_manifest.csv`.
- `assets/<tag>/...` : les fichiers de preuve eux-mêmes, dans leur format d'origine, regroupés par repère d'instrument.
- Un guide de vérification README avec le périmètre de l'export, les nombres couverts, l'explication de la chaîne d'empreintes et la procédure de vérification hors ligne du chaînage.

L'archive est conçue pour étayer votre détermination au titre de 11.10(b) : elle fournit les enregistrements à la fois sous forme lisible par l'humain (PDF) et sous forme électronique (CSV). Savoir si elle satisfait à 11.10(b) pour vos enregistrements relève de votre détermination. C'est aussi la réponse pratique aux questions sur la continuité de l'éditeur : le dossier est autonome, au format ouvert, et son chaînage est vérifiable sans nous.

Périmètre et une limite importante. Les exports peuvent être restreints par site, emplacement, instruments précis, plage de dates et statut, et le périmètre est toujours croisé avec les droits par site de la personne qui fait la demande, il ne peut donc que se resserrer. **Un export restreint ou limité à une plage de dates revérifie l'empreinte propre à chaque enregistrement exporté, mais n'affirme pas la continuité de la chaîne entre enregistrements, car un ensemble filtré est un sous-ensemble délibéré de la chaîne.** Seul un export sans périmètre, couvrant tout l'historique, parcourt la chaîne complète. Utilisez un export sans périmètre lorsque vous avez besoin de la preuve de continuité. Le README l'indique également.

Conservation tant que le compte est actif : les enregistrements sont conservés pendant toute la durée de vie de l'espace de travail. Aucun enregistrement d'étalonnage confirmé ne peut être modifié ou supprimé individuellement par qui que ce soit, nous compris.

Conservation après fermeture : lorsqu'un compte est fermé, les données sont conservées **730 jours (environ 24 mois)** pour que vous puissiez vous reconnecter et exporter. La facturation est annulée dès la demande, rien n'est donc facturé pendant cette période. À son terme, une purge définitive supprime les données de l'espace de travail dans toutes les tables et efface les fichiers de preuve stockés. Cette purge est la **seule** voie autorisée par laquelle des lignes confirmées du registre sont supprimées, et c'est une opération portant sur tout l'espace de travail, jamais une suppression enregistrement par enregistrement.

Sauvegardes : la base de données de production dispose de sauvegardes quotidiennes automatiques avec une durée de conservation de 14 jours, d'une protection contre la suppression activée et d'un instantané final lors de tout démantèlement d'instance. Voir la section 6 pour ce que nous n'affirmons pas sur la reprise.

Hébergement : la production fonctionne sur Amazon Web Services, dans us-east-1, aux États-Unis. La base de données est chiffrée au repos et n'a aucun accès depuis l'internet public. L'application et l'API sont servies uniquement en HTTPS, avec TLS 1.2 au minimum. AWS CloudTrail est activé sur tout le compte avec validation de l'intégrité des fichiers journaux et une durée de conservation de 365 jours. Une présentation distincte de la sécurité est publiée sur axiospec.com/security.

5. Gestion des changements

Comment les changements sont réalisés et encadrés.

- Les déploiements en production sont **déclenchés uniquement à la main**. Il n'existe aucune mise en production automatique.
- Un déploiement en production est bloqué tant que trois tâches n'ont pas réussi : la suite complète de tests du backend, une tâche de validation du schéma OpenAPI et un audit des vulnérabilités des dépendances. Une suite de tests en échec arrête le déploiement.

- La suite de tests du backend compte **2 465 fonctions de test réparties dans 197 fichiers de test**. Il existe en outre 233 fichiers de test pour le frontend web. Ce sont des tests de non-régression automatisés qui s'exécutent à chaque changement.
- Chaque build de production est publié sous une étiquette d'image immuable par commit, ce qui donne une cible de retour arrière définie pour chaque version.
- La préproduction et la production sont des environnements distincts, avec une infrastructure distincte. Les changements arrivent d'abord en préproduction.

Soyons clairs sur ce que c'est et ce que ce n'est pas. Une suite de tests automatisés de cette taille est une mesure de maîtrise du développement logiciel réelle et citable, et une bonne matière première pour un argumentaire de qualification opérationnelle. Ce **n'est pas** un dossier de validation. Elle n'est pas écrite à partir d'une spécification fonctionnelle formelle, il n'existe pas de matrice de traçabilité des exigences vers les tests et il n'existe pas d'enregistrement de mise en production signé. Un évaluateur en validation de systèmes informatisés ne l'acceptera pas comme tel, et nous ne la présenterons pas comme telle.

Comment vous savez que quelque chose change.

Axiospec est un logiciel en tant que service multilocataire. Tous les clients utilisent une seule version de production. **Vous ne pouvez pas figer une version, différer une mise à jour ni exploiter une version antérieure.** C'est une contrainte réelle pour un environnement validé, que vous devriez consigner dans votre analyse des risques.

Il n'existe aujourd'hui **ni journal des modifications publié, ni page de notes de version, ni engagement écrit de notification des changements.** Si votre procédure exige un préavis pour les changements apportés à un système validé, demandez-nous cet engagement par écrit avant d'acheter, à support@axiospec.com. Nous préférons vous dire qu'il n'existe pas plutôt que vous le laisser découvrir pendant un audit.

Ce que nous vous suggérons de faire, compte tenu de ce qui précède : définissez dans votre procédure un intervalle de revérification périodique (par exemple, réexécuter le sous-ensemble de l'OQ chaque trimestre et après tout changement que vous remarquez sur une fonction dont vous dépendez), et relancez la vérification de la chaîne en enregistrant le résultat au même intervalle. La vérification de la chaîne se fait en un clic et produit un résultat daté et attribuable.

6. Limites de ce que fait ce logiciel

Énoncées clairement, parce qu'un petit éditeur qui nomme ses limites est plus facile à qualifier qu'un éditeur qui les esquive.

Certifications et évaluations que nous ne détenons pas. Aucun SOC 2, ni Type I ni Type II. Aucune ISO/IEC 27001. Aucun test d'intrusion réalisé par un tiers. Aucun accord d'associé commercial HIPAA, et nous n'acceptons pas d'informations de santé protégées. Aucun FedRAMP, StateRAMP, CMMC, NIST 800-171, ITAR, EAR ou DFARS 252.204-7012. Si vous traitez des informations non classifiées contrôlées ou des données soumises au contrôle des exportations, Axiospec ne vous convient pas aujourd'hui. Aucun avenant relatif au traitement des données publié, aucune clause contractuelle type et aucune résidence des données dans l'UE ; toutes les données se trouvent aux États-Unis.

Aucun dossier de validation de l'éditeur. Il n'existe ni dossier IQ/OQ/PQ, ni protocole de validation, ni matrice de traçabilité, ni rapport de synthèse de validation produits par nous. La section 3 est une liste de contrôle que vous exécutez, pas la preuve que quoi que ce soit a été exécuté.

Aucune déclaration de conformité. Axiospec ne certifie, n'assure ni ne garantit votre conformité à aucune norme. Il soutient et documente les enregistrements d'étalonnage et les maintient prêts pour l'audit. La conformité est déterminée par votre service qualité, votre organisme certificateur, votre organisme d'accréditation ou votre inspecteur.

Nous ne revendiquons pas la conformité au 21 CFR Part 11. Les éléments qui fondent l'intégrité des enregistrements sont réellement solides : immuabilité imposée par la base de données, chaîne d'empreintes SHA-256, entrées attribuées et horodatées, corrections en ajout seul qui ne masquent pas les informations antérieures, et revue à deux personnes. Les contrôles de signature ne sont pas encore là. Voir la section 2.4 : la signature électronique est facultative par espace de travail plutôt qu'obligatoire, il n'y a pas de liaison de signature stockée sur l'enregistrement, pas de champ indiquant la signification de la signature et pas d'identification multifacteur. Nous publions une correspondance des fonctionnalités avec les lacunes signalées ; nous ne publions pas de déclaration de conformité.

Aucune authentification multifacteur. Il n'existe ni TOTP intégré, ni application d'authentification, ni WebAuthn, ni SMS, ni codes de secours. Aujourd'hui, la seule voie vers un second facteur est la connexion via Google, où votre propre fournisseur d'identité l'impose. Le SSO d'entreprise par espace de travail via OIDC et SAML est développé et testé dans le backend, mais il n'est pas activé en production et doit être considéré comme disponible sur demande, et non comme une fonctionnalité livrée. Si votre politique informatique exige une MFA imposée pour tous les systèmes du SMQ, c'est aujourd'hui un point bloquant. Demandez-nous où en sont les choses avant d'acheter.

Les modifications de la fiche principale des équipements ne sont pas journalisées. Section 2.2 et test OQ-17. Les événements d'étalonnage sont entièrement couverts par le registre. Les modifications de la fiche descriptive de l'instrument, y compris son intervalle d'étalonnage, ne sont pas attribuées dans le journal d'activité.

Les exports filtrés ne prouvent pas la continuité de la chaîne. Section 4. Utilisez pour cela un export sans périmètre.

Aucun engagement de disponibilité. Il n'existe ni SLA de disponibilité, ni page d'état, ni historique de disponibilité publié. La base de données de production est une instance unique dans une seule zone de disponibilité, si bien qu'une panne de zone de disponibilité exige une restauration plutôt qu'une bascule. Nous ne publions pas d'objectif de délai de reprise ni de point de reprise, et aucun exercice de restauration n'a été documenté. Les sauvegardes sont configurées et conservées 14 jours ; c'est une affirmation vraie sur les sauvegardes, pas une affirmation prouvée sur la reprise. Votre procédure devrait prévoir une solution de secours en cas d'indisponibilité du système, ce que les évaluateurs ISO/IEC 17025 demandent de toute façon.

Aucun plan documenté de réponse aux incidents ni délai contractuel de notification des violations. Des alarmes d'infrastructure sont configurées dans CloudWatch et envoyées à une adresse e-mail d'astreinte. C'est de la surveillance, pas un programme de réponse aux incidents.

Aucune clé de chiffrement gérée par le client. Le chiffrement utilise des clés gérées par AWS.

Les enregistrements ne peuvent être supprimés que d'une seule façon. Aucun enregistrement confirmé ne peut être modifié ou supprimé individuellement par qui que ce soit. La seule voie de suppression est une purge de tout l'espace de travail demandée par le client, après la durée de conservation de 730 jours.

Nous ne réalisons pas d'étalonnage. Axiospec est un système de gestion documentaire, pas un laboratoire d'étalonnage accrédité, et n'a réalisé aucune des mesures de vos enregistrements.

Comment utiliser ce document. Joignez-le à votre dossier de qualification fournisseur pour CaliTech LLC (ISO 9001, article 8.4 ; ISO/IEC 17025, article 6.6). Citez-le dans votre plan de validation comme description fonctionnelle et des contrôles fournie par l'éditeur. Exécutez la section 3 dans votre propre espace de travail et conservez le résultat signé comme preuve de qualification. Consignez les limites de la section 6 dans votre analyse des risques, avec vos contrôles compensatoires.

Si une affirmation de ce document ne correspond pas à ce que vous observez dans le produit, dites-le-nous à support@axiospec.com et nous corrigerons le document.

Axiospec est édité par CaliTech LLC, Knoxville, Tennessee (États-Unis). Axiospec soutient et documente votre programme d'étalonnage et le maintient prêt pour l'audit. Il ne certifie, n'assure ni ne garantit la conformité à aucune norme ; cette décision vous appartient, à vous et à votre auditeur. Questions : support@axiospec.com