LIVRE BLANC

Déclaration de conformité aux exigences de 21 CFR Part 11 et de l'Annexe 11 pour les laveurs et stérilisateurs pharmaceutiques conformes aux BPF

Utilisation du logiciel WinCC Unified

Objectif

Ce document fournit la déclaration de conformité de nos laveurs et stérilisateurs pharmaceutiques GMP controlés par le logiciel WinCC Unified conforme à 21 CFR Part 11 et Annexe 11.

- La conformité à 21 CFR Part 11 couvre les enregistrements électroniques et les signatures électroniques pour la FDA (FDA : Food and Drug Administration, CFR : Code of Federal Regulations, Titre 21 : Aliments et médicaments, Part 11 : Enregistrements électroniques et signatures électroniques)
- L'Annexe 11 porte sur le cycle de vie des systèmes informatisés relatifs aux médicaments à usage humain et vétérinaire fabriqués dans l'Union Européenne

Les sections suivantes décrivent la Sous-partie B de la Part 11 relative aux enregistrements électroniques et la Sous-partie C de la Part 11 relative aux signatures électroniques.

Définitions et terminologie

Terminologie de la règlementation

- Biométrie : méthode de vérification de l'identité d'un opérateur basée sur la mesure de ses caractéristiques physiques ou de ses actions répétables et mesurables, propres à cette personnes.
- Système fermé : environnement dans lequel l'accès au système est contrôlé par les personnes responsables du contenu des dossiers électroniques.
- Système informatisé : système comprenant la saisie de données, le traitement électronique, et la production d'informations utilisées à des fins de reporting ou de contrôle automatique.
- Enregistrement électronique : toute représentation sous forme de textes, graphiques, données, sons, images ou autres informations, créée, modifiée, conservée, archivée, récupérée ou distribuée par un système informatique.
- Signature électronique : ensemble de données informatiques constitué de symboles adoptés par un individu et ayant la même valeur juridique qu'une signature manuscrite.

Terminologie Getinge

- URS : Cahier des charges
- FS : Spécification fonctionnelle
- SDS : Spécification de conception logicielle
- AD : Répertoire central de contrôle
- QMS : Système de gestion de la qualité

Description

En Europe, les laveurs et stérilisateurs pharmaceutiques conformes aux BPF utilisent le logiciel WinCC Unified proposé par Siemens.
Les déclarations de conformité suivantes sont issues de la réponse de conformité ERES pour SIMATIC WinCC Unified V20.

Historique des versions

Date	Révision	Rédigé/Mis à jour par	Description
12 JUIN 2025	001	Amaury BRICOUT	Première publication

Validation interne

Nom	Service	Date	Signature
Marcus Persson	Stérilisateurs automatisés		
Manuel Samsom	Laveurs automatisés		

Validation client

Nom	Fonction	Date	Signature

Tableau 1 : Sous-partie B – Enregistrements électroniques

Exigences 21 CFR Part 11	Annexe 11	Conformité	Notes d'application
11.10 – Les personnes qui utilisent des systèmes fermés pour créer, modifier, conserver ou transmettre des enregistrements électroniques doivent mettre en œuvre des procédures et des contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confidentialité des enregistrements électroniques, ainsi que pour s'assurer que le signataire ne puisse pas facilement contester le caractère authentique de l'enregistrement signé. Ces procédures et contrôles doivent inclure les éléments suivants :	**7.1** – Les données doivent être sécurisées par des moyens physiques et électroniques afin de les protéger contre tout dommage. **7.2** – Des sauvegardes régulières de toutes les données pertinentes doivent être effectuées. **12.1** – Des contrôles physiques et/ou logiques doivent être mis en place afin de limiter l'accès aux systèmes informatisés aux seules personnes autorisées.	☒ Yes ☐ No ☐ N/A	La documentation Getinge est générée, maintenue, enregistrée et remise au client afin de décrire la conception du système (spécification fonctionnelle, spécification de conception matérielle, spécification de conception logicielle) ainsi que la validation (protocoles FAT/SAT). Toutes les données sont stockées dans une base de données et restent accessibles pour consultation, impression et exportation pendant toute la durée de conservation des enregistrements. Une procédure de sauvegarde est fournie au client dans le manuel de service. Une sauvegarde automatique de la base de données peut être configurée (en option). Les droits d'accès utilisateur aux rapports sont gérés par des droits de groupe. Les rôles des groupes sont définis dans la documentation de conception. Les accès utilisateurs locaux sont gérés par UMC. L'accès au répertoire central de contrôle via UMC est optionnel. Les contrôles physiques visant à restreindre l'accès au système relèvent de la responsabilité du client final.
11.10(a) – Validation des systèmes afin de garantir l'exactitude, la fiabilité, la cohérence des performances prévues et la capacité à détecter les enregistrements invalides ou altérés.	**4.1** – La documentation et les rapports de validation doivent couvrir les étapes pertinentes du cycle de vie. Les fabricants doivent être en mesure de justifier leurs normes, protocoles, critères d'acceptation, procédures et enregistrements sur la base de leur évaluation des risques.	☐ Yes ☐ No ☒ N/A	La validation des applications logicielles Getinge est réalisée conformément au système de gestion de la qualité (QMS) de Getinge. Une matrice de traçabilité est fournie (en option). Bien que le système soit conçu pour être conforme à la réglementation 21 CFR Part 11, l'utilisateur final reste responsable de la validation du système dans son ensemble. Getinge peut proposer un accompagnement pour la validation du système.

Exigences 21 CFR Part 11	Annexe 11	Conformité	Notes d'application
N/A	**4.2** – La documentation de validation doit inclure les enregistrements de gestion des modifications (le cas échéant) ainsi que les rapports relatifs à toute déviation observée au cours du processus de validation.	☒ Yes ☐ No ☐ N/A	Les déviations observées au cours du processus de validation sont suivies et tracées. Les exécutions de tests non conformes sont enregistrées et associées au plan de test. Si une modification est nécessaire, une procédure de gestion des changements Getinge est appliquée.
N/A	**4.3** – Une liste à jour de tous les systèmes pertinents et de leurs fonctionnalités BPF (inventaire) doit être disponible. Pour les systèmes critiques, une description actualisée du système doit détailler les configurations physiques et logiques, les flux de données et les interfaces avec d'autres systèmes ou processus, ainsi que les prérequis matériels et logiciels et les mesures de sécurité.	☒ Yes ☐ No ☐ N/A	La documentation Getinge est générée, maintenue, enregistrée et remise au client afin de décrire la conception du système (spécification fonctionnelle, spécification de conception matérielle et spécification de conception logicielle).
N/A	**4.5** – L'utilisateur réglementé doit prendre toutes les mesures raisonnables afin de garantir que le système a été développé conformément à un système de gestion de la qualité approprié.	☒ Yes ☐ No ☐ N/A	Une procédure est appliquée afin d'adapter le projet modèle au projet du laveur ou du stérilisateur. Une fiche d'adaptation logicielle, ou un document équivalent, est établie par un ingénieur en automatisation. Une revue du code source est réalisée par un autre ingénieur en automatisation.
N/A	**4.7** – Des preuves de l'utilisation de méthodes et de scénarios de test appropriés doivent être fournies. Les limites des paramètres système (processus), les limites des données ainsi que la gestion des erreurs doivent notamment être prises en considération. Les outils de test automatisés et les environnements de test doivent faire l'objet d'évaluations documentées attestant de leur adéquation.	☒ Yes ☐ No ☐ N/A	Les tests visant à valider le logiciel des laveurs et des stérilisateurs sont réalisés conformément au système de gestion de la qualité (QMS).

Exigences 21 CFR Part 11	Annexe 11	Conformité	Notes d'application
N/A	**4.4** – Le cahier des charges des exigences utilisateur doivent décrire les fonctions requises du système, être fondées sur une analyse de risques documentée et sur l'impact BPF, et être traçables tout au long du cycle de vie.	☐ Yes ☐ No ☒ N/A	Les URS sont fournies par le client. Une matrice de traçabilité est fournie (en option).
N/A	**4.6** - Pour la validation des systèmes informatisés sur mesure ou personnalisés, un processus doit être mis en place afin de garantir l'évaluation formelle et le reporting des mesures de qualité et de performance à toutes les étapes du cycle de vie du système.	☐ Yes ☐ No ☒ N/A	Les tests visant à valider les logiciels des laveurs et des stérilisateurs sont réalisés conformément au système de gestion de la qualité (QMS). Bien que le système soit conçu pour être conforme à l'annexe 11, l'utilisateur final reste responsable de la validation du système dans son ensemble. Getinge peut proposer un accompagnement pour la validation du système.
N/A	**4.8** – En cas de transfert de données vers un autre format de données ou un autre système, la validation doit inclure des vérifications garantissant que les données ne sont pas altérées en termes de valeur et/ou de signification au cours de ce processus de migration.	☐ Yes ☐ No ☒ N/A	L'exploitation des données brutes dans le système Getinge relève de la responsabilité du client (table d'échange de données et base de données SQL). Les protocoles de communication OPC UA et Profinet sont disponibles en option.
11.10(b) – La capacité à générer des copies exactes et complètes des enregistrements, sous une forme à la fois lisible par l'homme et électronique, adaptées à l'inspection, à l'examen et à la copie par l'autorité compétente. Les personnes concernées doivent contacter l'autorité compétente en cas de question relative à sa capacité à effectuer cet examen et cette copie des enregistrements électroniques.	**8.1** – Il doit être possible d'obtenir des copies imprimées claires des données stockées électroniquement.	☒ Yes ☐ No ☐ N/A	Tous les enregistrements sont stockés dans une base de données. Le système permet de générer des rapports de lot, de recette, de piste d'audit et de journal des alarmes au format PDF.

Exigences 21 CFR Part 11	Annexe 11	Conformité	Notes d'application
11.10(c) – Protection des enregistrements afin de permettre leur récupération exacte et rapide pendant toute la durée de conservation des données.	**7.1** – Les données doivent être sécurisées par des moyens physiques et électroniques afin de les protéger contre tout dommage. L'accès aux données doit être garanti pendant toute la durée de conservation. **7.2** – Des sauvegardes régulières de toutes les données pertinentes doivent être effectuées. **8.1** – Il doit être possible d'obtenir des copies imprimées claires des données stockées électroniquement. **12.1** – Des contrôles physiques et/ou logiques doivent être mis en place afin de limiter l'accès aux systèmes informatisés aux seules personnes autorisées.	☒ Yes ☐ No ☐ N/A	Tous les enregistrements sont stockés dans une base de données et sont accessibles pour consultation, impression et exportation pendant toute la durée de conservation des données. Une procédure de sauvegarde est fournie au client dans la notice du manuel de service. Une sauvegarde automatique de la base de données peut être configurée (en option). Les droits d'accès utilisateur aux rapports sont gérés par des droits de groupe. Les rôles des groupes sont définis dans la documentation de conception. Les accès utilisateurs locaux sont gérés par UMC. L'accès au répertoire central de contrôle via UMC est optionnel.
11.10(d) – Limitation de l'accès au système aux seules personnes autorisées.	**2** – Tout le personnel doit disposer des qualifications appropriées, d'un niveau d'accès adapté et de responsabilités définies afin de pouvoir exercer les tâches qui lui sont attribuées. **12.1** – Des contrôles physiques et/ou logiques doivent être mis en place afin de limiter l'accès aux systèmes informatisés aux seules personnes autorisées. Des méthodes appropriées de prévention des accès non autorisés au système peuvent inclure l'utilisation de clés, de badges d'accès, de codes personnels associés à des mots de passe, de la biométrie, ainsi qu'un accès restreint aux équipements informatiques et aux zones de stockage des données. **12.3** – La création, la modification et la suppression des autorisations d'accès doivent être enregistrées.	☒ Yes ☐ No ☐ N/A	Seules les personnes autorisées disposant d'un nom d'utilisateur et d'un mot de passe valides peuvent se connecter au système. Une politique de mots de passe (complexité, durée de validité) est définie dans la spécification fonctionnelle (FS) et configurée dans le système. Seuls les administrateurs ont la possibilité de quitter l'application. Les accès utilisateurs locaux sont gérés par UMC. L'accès au répertoire central de contrôle via UMC est optionnel. La création, la modification et la suppression des autorisations d'accès au répertoire central de contrôle relèvent de la responsabilité du client.

Exigences 21 CFR Part 11	Annexe 11	Conformité	Notes d'application
11.10(e) – Utilisation de pistes d'audit sécurisées, générées par ordinateur et horodatées, afin d'enregistrer de manière indépendante la date et l'heure des saisies et actions des opérateurs qui créent, modifient ou suppriment des enregistrements électroniques. **Les modifications apportées aux enregistrements ne doivent pas masquer les informations précédemment enregistrées.** **Cette documentation de piste d'audit doit être conservée pendant une durée au moins équivalente à celle requise pour les enregistrements électroniques concernés et doit être disponible pour examen et copie par l'autorité compétente.**	**7.1** – L'accès aux données doit être garanti pendant toute la durée de conservation. **9** – Sur la base d'une analyse de risques, il convient d'envisager l'intégration dans le système d'un enregistrement de toutes les modifications et suppressions pertinentes au regard des BPF (piste d'audit générée par le système). Pour toute modification ou suppression de données pertinentes au regard des BPF, la raison doit être documentée. Les pistes d'audit doivent être disponibles, convertibles dans un format généralement compréhensible et faire l'objet d'une revue régulière. **12.4** – Les systèmes de gestion des données et des documents doivent être conçus de manière à enregistrer l'identité des opérateurs effectuant la saisie, la modification, la confirmation ou la suppression des données, ainsi que la date et l'heure correspondantes.	☒ Yes ☐ No ☐ N/A	SIMATIC WinCC Unified prend en charge l'exigence relative à la piste d'audit des actions opérateur pertinentes au regard des BPF en enregistrant ces actions de manière appropriée (qui, quoi, quand et, le cas échéant, pourquoi). Ces enregistrements électroniques sont sécurisés grâce à des mécanismes de sécurité intégrés au système. Les horodatages sont enregistrés au format UTC. Voir l'annexe 1 relative à la piste d'audit pour plus de détails.
11.10(f) – Utilisation de contrôles opérationnels du système afin de garantir, le cas échéant, le respect de l'enchaînement autorisé des étapes et des événements.	**N/A** (aucun équivalent direct dans l'annexe 11).	☒ Yes ☐ No ☐ N/A	Les logiciels sont validés avant d'être remis au client.

Exigences 21 CFR Part 11	Annexe 11	Conformité	Notes d'application
11.10(g) – Utilisation de contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroniquement un enregistrement, accéder aux dispositifs d'entrée ou de sortie du système ou de l'application, modifier un enregistrement ou réaliser l'opération en cours.	**2** – Tout le personnel doit disposer des qualifications appropriées, d'un niveau d'accès adapté et de responsabilités définies afin d'exercer les tâches qui lui sont attribuées. **12.1** – Des contrôles physiques et/ou logiques doivent être mis en place afin de limiter l'accès aux systèmes informatisés aux seules personnes autorisées. Les méthodes appropriées de prévention des accès non autorisés peuvent inclure l'utilisation de clés, de badges d'accès, de codes personnels associés à des mots de passe, de la biométrie, ainsi qu'un accès restreint aux équipements informatiques et aux zones de stockage des données.	☒ Yes ☐ No ☐ N/A	Seules les personnes autorisées disposant d'un nom d'utilisateur et d'un mot de passe valides peuvent se connecter au système. Une politique de mots de passe (complexité, durée de validité) est définie dans la spécification fonctionnelle (FS) et configurée dans le système. Seuls les administrateurs ont la possibilité de quitter l'application. Les accès utilisateurs locaux sont gérés par UMC. L'accès au répertoire central de contrôle via UMC est optionnel.
11.10(h) – Utilisation de contrôles au niveau des dispositifs (par exemple, terminaux) afin de vérifier, le cas échéant, la validité de la source des données saisies ou des instructions opérationnelles.	**6** – Pour les données critiques saisies manuellement, un contrôle supplémentaire de l'exactitude des données doit être effectué. Ce contrôle peut être réalisé par un second opérateur ou par des moyens électroniques validés.	☒ Yes ☐ No ☐ N/A	L'équipement fait l'objet de tests réalisés en présence du client sur le site de production(FAT) avant son installation sur le site du client. Lors de cette validation, les entrées/sorties sont vérifiées.
11.10(i) – Vérification que les personnes qui développent, maintiennent ou utilisent des systèmes d'enregistrements électroniques/signatures électroniques disposent de la formation, de l'éducation et de l'expérience nécessaires pour accomplir les tâches qui leur sont assignées.	**2** – Tout le personnel doit disposer des qualifications appropriées, d'un niveau d'accès adapté et de responsabilités définies afin d'exercer les tâches qui lui sont attribuées.	☐ Yes ☐ No ☒ N/A	Getinge vérifie que les personnes respectent les procédures opératoires standard (SOP) et les règles de codage de Getinge. L'utilisateur final est responsable du recrutement et de la formation de personnel qualifié disposant de l'éducation, de la formation et de l'expérience nécessaires pour accomplir les tâches qui lui sont assignées. Getinge peut proposer des formations et un accompagnement tout au long du cycle de vie du système.

Exigences 21 CFR Part 11	Annexe 11	Conformité	Notes d'application
11.10(j) – La mise en place et le respect de politiques écrites qui rendent les individus responsables et redevables des actions effectuées sous leur signature électronique, afin de prévenir toute falsification des enregistrements et des signatures.	**N/A** (aucun équivalent direct dans l'annexe 11).	☐ Yes ☐ No ☒ N/A	L'exigence relative aux politiques rendant les individus responsables des actions effectuées sous leur signature électronique relève des procédures du client.
11.10(k) – Utilisation de contrôles appropriés sur la documentation du système, incluant : **(1) des contrôles adéquats sur la diffusion, l'accès et l'utilisation de la documentation relative à l'exploitation et à la maintenance du système ;** **(2) des procédures de révision et de gestion des modifications afin de maintenir une piste d'audit documentant le développement et les modifications successives, dans l'ordre chronologique, de la documentation du système.**	**N/A** (aucun équivalent direct dans l'annexe 11 au 21 CFR 11.10(k)(1)). **10** – Toute modification apportée à un système informatisé, y compris à sa configuration, doit être réalisée de manière contrôlée, conformément à une procédure définie.	☐ Yes ☐ No ☒ N/A	Getinge fournit la documentation projet et le logiciel pour revue par le client. Toute modification du logiciel est décrite dans une procédure, et un document est établi afin d'enregistrer l'ancienne et la nouvelle version du logiciel et de la documentation. Ce formulaire ainsi que la nouvelle version du logiciel/de la documentation sont remis au client. Les utilisateurs finaux sont responsables de la mise en place de contrôles procéduraux concernant l'accès, la diffusion et l'utilisation des documents pendant toute la durée de vie du système. Les utilisateurs finaux doivent définir des procédures appropriées de gestion des changements pour l'exploitation et la maintenance de la documentation.

Exigences 21 CFR Part 11	Annexe 11	Conformité	Notes d'application
11.30 – Les personnes qui utilisent des systèmes ouverts pour créer, modifier, conserver ou transmettre des enregistrements électroniques doivent mettre en œuvre des procédures et des contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confidentialité des enregistrements électroniques, depuis leur création jusqu'à leur réception. **Ces procédures et contrôles doivent inclure ceux identifiés au §11.10, selon le cas, ainsi que des mesures supplémentaires telles que le chiffrement des documents et l'utilisation de normes appropriées de signature numérique afin de garantir, lorsque nécessaire, l'authenticité, l'intégrité et la confidentialité des enregistrements.**	**5** – Les systèmes informatisés échangeant des données électroniquement avec d'autres systèmes doivent intégrer des contrôles appropriés afin de garantir la saisie et le traitement corrects et sécurisés des données, dans le but de minimiser les risques. **7.1** – Les données doivent être sécurisées par des moyens physiques et électroniques afin de les protéger contre tout dommage. **7.2** – Des sauvegardes régulières de toutes les données pertinentes doivent être effectuées. **12.1** – Des contrôles physiques et/ou logiques doivent être mis en place afin de limiter l'accès aux systèmes informatisés aux seules personnes autorisées.	☐ Yes ☐ No ☒ N/A	Les laveurs et stérilisateurs disposent de connexions limitées avec d'autres systèmes : La connexion au répertoire central de contrôle du client est optionnelle et sa gestion relève du client. L'échange de données via une table d'échange de données est également optionnel. Getinge utilise des protocoles industriels (Ethernet/IP, OPC UA) afin de sécuriser les communications. Une procédure de sauvegarde est fournie au client dans le manuel de service. Une sauvegarde automatique de la base de données peut être configurée (en option). Seules les personnes autorisées disposant d'un nom d'utilisateur et d'un mot de passe valides peuvent se connecter au système. Une politique de mots de passe (complexité, durée de validité) est définie dans la spécification fonctionnelle (FS). Les accès utilisateurs locaux sont gérés par UMC. L'accès au répertoire central de contrôle via UMC est optionnel. Les utilisateurs finaux sont responsables de l'établissement de politiques et de procédures internes afin de garantir des contrôles appropriés lorsque le système est classé comme système ouvert.

Exigences 21 CFR Part 11	Annexe 11	Conformité	Notes d'application
11.50(a) – Les enregistrements électroniques signés doivent contenir les informations associées à la signature indiquant clairement les éléments suivants : (1) le nom imprimé du signataire ; (2) la date et l'heure d'exécution de la signature ; (3) la signification associée à la signature (par exemple : revue, approbation, responsabilité ou attribution) ; (4) les éléments définis aux paragraphes (a)(1), (a)(2) et (a)(3) du présent article doivent être soumis aux mêmes contrôles que les enregistrements électroniques et doivent être inclus dans toute forme lisible par l'homme de l'enregistrement électronique (telle qu'un affichage électronique ou une impression).	**14** – Les enregistrements électroniques peuvent être signés électroniquement. Les signatures électroniques sont censées avoir la même valeur que les signatures manuscrites, être liées de manière permanente à l'enregistrement correspondant et inclure la date et l'heure de leur application.	☒ Yes ☐ No ☐ N/A	Les informations listées sont disponibles. Voir l'annexe 2 relative à la signature électronique pour plus de détails.
11.70 – Les signatures électroniques et les signatures manuscrites apposées sur des enregistrements électroniques doivent être liées à leurs enregistrements électroniques respectifs, afin de garantir qu'elles ne puissent pas être extraites, copiées ou autrement transférées par des moyens ordinaires dans le but de falsifier un enregistrement électronique.	**14** – Les signatures électroniques doivent être liées de manière permanente à leur enregistrement respectif.	☒ Yes ☐ No ☐ N/A	Les signatures électroniques ne peuvent pas être supprimées ni utilisées d'une autre manière. Voir l'annexe 2 relative à la signature électronique pour plus de détails. L'utilisateur final doit établir des procédures opératoires standard (SOP) afin d'assurer l'application de cette exigence pour les enregistrements archivés.

Tableau 2 : Sous-partie C – Signatures électroniques

Exigences 21 CFR Part 11	Annexe 11	Conformité	Notes d'application
11.100(a) – Chaque signature électronique doit être propre à une seule personne et ne doit être ni réutilisée par une autre personne, ni réattribuée à quelqu'un d'autre.	**N/A** (aucun équivalent direct dans l'annexe 11).	☒ Yes ☐ No ☐ N/A	La signature électronique utilise les identifiants uniques associés aux comptes utilisateurs. La réutilisation ou la réattribution des signatures électroniques est ainsi efficacement empêchée.
11.100(b) – Avant qu'une organisation n'établisse, n'attribue, ne certifie ou n'autorise de toute autre manière la signature électronique d'une personne, ou tout élément de cette signature électronique, elle doit vérifier l'identité de cette personne.	**N/A** (aucun équivalent direct dans l'annexe 11).	☐ Yes ☐ No ☒ N/A	Le client doit mettre en place des contrôles procéduraux appropriés afin de vérifier l'identité d'une personne avant l'attribution d'un compte utilisateur et/ou d'une signature électronique.
11.100(c) – Les personnes utilisant des signatures électroniques doivent, avant ou au moment de leur utilisation, certifier auprès de l'autorité compétente que les signatures électroniques utilisées dans leur système, à compter du 20 août 1997, sont destinées à avoir la même valeur juridique que les signatures manuscrites traditionnelles.	**14.a** –Les signatures électroniques doivent avoir la même valeur et les mêmes effets que les signatures manuscrites.	☐ Yes ☐ No ☒ N/A	Les clients sont responsables d'informer la FDA de leur intention de reconnaître la signature électronique comme l'équivalent juridiquement contraignant d'une signature manuscrite traditionnelle.

Exigences 21 CFR Part 11	Annexe 11	Conformité	Notes d'application
11.200(a)(1) – Les signatures électroniques qui ne sont pas fondées sur la biométrie doivent : **(i) utiliser au moins deux éléments d'identification distincts, tels qu'un identifiant et un mot de passe.** **(ii) lorsqu'une personne effectue une série de signatures au cours d'une même période continue d'accès contrôlé au système, la première signature doit être réalisée en utilisant l'ensemble des composants de la signature électronique ; les signatures suivantes doivent être réalisées à l'aide d'au moins un composant de la signature électronique qui ne peut être utilisé que par cette personne et qui est conçu à cette seule fin.** **(iii) lorsqu'une personne effectue une ou plusieurs signatures en dehors d'une même période continue d'accès contrôlé au système, chaque signature doit être réalisée en utilisant l'ensemble des composants de la signature électronique.**	**12.1** – Des contrôles physiques et/ou logiques doivent être mis en place afin de limiter l'accès aux systèmes informatisés aux seules personnes autorisées. Des méthodes appropriées pour prévenir tout accès non autorisé au système peuvent inclure l'utilisation de clés, de badges d'accès, de codes personnels associés à des mots de passe, de dispositifs biométriques, ainsi qu'un accès restreint aux équipements informatiques et aux zones de stockage des données.	☒ Yes ☐ No ☐ N/A	La réalisation d'une signature électronique nécessite l'identifiant utilisateur ainsi que le mot de passe de l'utilisateur. Voir l'annexe 2 relative à la signature électronique pour plus de détails.
11.200(a)(2) – Les signatures électroniques qui ne sont pas basées sur la biométrie doivent être utilisées uniquement par leurs propriétaires légitimes.	**12.1** – Des contrôles physiques et/ou logiques doivent être mis en place afin de limiter l'accès aux systèmes informatisés aux seules personnes autorisées. Les méthodes appropriées de prévention des accès non autorisés au système peuvent inclure l'utilisation de clés, de badges d'accès, de codes personnels associés à des mots de passe, de la biométrie, ainsi qu'un accès restreint aux équipements informatiques et aux zones de stockage des données.	☐ Yes ☐ No ☒ N/A	Le client est responsable de s'assurer que le propriétaire légitime est bien celui qui appose la signature électronique et que le mot de passe n'est pas divulgué à des tiers.

Exigences 21 CFR Part 11	Annexe 11	Conformité	Notes d'application
11.200(a)(3) – Les signatures électroniques qui ne sont pas fondées sur la biométrie doivent être administrées et exécutées de manière à garantir que toute tentative d'utilisation de la signature électronique d'une personne par une autre personne que son propriétaire légitime nécessite la collaboration de deux personnes ou plus.	**12.1** – Des contrôles physiques et/ou logiques doivent être mis en place afin de limiter l'accès aux systèmes informatisés aux seules personnes autorisées. Les méthodes appropriées pour empêcher les accès non autorisés au système peuvent inclure l'utilisation de clés, de badges d'accès, de codes personnels associés à des mots de passe, de la biométrie, ainsi qu'un accès restreint aux équipements informatiques et aux zones de stockage des données.	☐ Yes ☐ No ☒ N/A	Le client doit mettre en œuvre des procédures appropriées pour gérer les situations nécessitant une signature électronique par une personne autre que le propriétaire légitime. La signature électronique utilise les identifiants uniques des comptes utilisateurs. La réutilisation ou la réattribution des signatures électroniques est ainsi efficacement empêchée. La réalisation d'une signature électronique nécessite l'identifiant utilisateur ainsi que le mot de passe de l'utilisateur. Chaque signature est composée de deux éléments (identifiant utilisateur et mot de passe). Il n'est pas possible de falsifier une signature électronique lors de sa réalisation ou après son enregistrement. De plus, l'utilisateur réglementé doit mettre en place des procédures empêchant la divulgation des mots de passe.
11.200(b) – Les signatures électroniques basées sur la biométrie doivent être conçues de manière à garantir qu'elles ne puissent être utilisées par personne d'autre que leur propriétaire légitime.	**12.1** – Des contrôles physiques et/ou logiques doivent être mis en place afin de limiter l'accès aux systèmes informatisés aux seules personnes autorisées. Les méthodes appropriées pour empêcher les accès non autorisés au système peuvent inclure l'utilisation de clés, de badges d'accès, de codes personnels associés à des mots de passe, de la biométrie, ainsi qu'un accès restreint aux équipements informatiques et aux zones de stockage des données.	☐ Yes ☐ No ☒ N/A	Les mécanismes de connexion basés sur la biométrie ne sont pas disponibles dans le système.

Exigences 21 CFR Part 11	Annexe 11	Conformité	Notes d'application
11.300(a) – Les personnes utilisant des signatures électroniques basées sur des codes d'identification associés à des mots de passe doivent mettre en œuvre des contrôles garantissant leur sécurité et leur intégrité. Ces contrôles doivent inclure le maintien de l'unicité de chaque combinaison code d'identification/mot de passe, de sorte qu'aucune paire identique ne soit attribuée à deux individus différents.	**12.1** – Des contrôles physiques et/ou logiques doivent être mis en place afin de limiter l'accès aux systèmes informatisés aux seules personnes autorisées. Les méthodes appropriées pour prévenir les accès non autorisés au système peuvent inclure l'utilisation de clés, de badges d'accès, de codes personnels associés à des mots de passe, de la biométrie, ainsi qu'un accès restreint aux équipements informatiques et aux zones de stockage des données.	☒ Yes ☐ No ☐ N/A	La sécurité de la gestion des utilisateurs est assurée par les outils d'administration WinCC Unified. La gestion des utilisateurs peut être liée à l'Active Directory du client (en option). L'unicité des utilisateurs et des rôles relève de la responsabilité du client.
11.300(b) – La vérification périodique, la révocation ou la révision de l'attribution des codes d'identification et des mots de passe doivent être assurées (par exemple, pour prendre en compte des mécanismes tels que l'expiration des mots de passe).	**11** – Les systèmes informatisés doivent être évalués périodiquement afin de confirmer qu'ils demeurent dans un état validé et qu'ils sont conformes aux BPF. Ces évaluations doivent inclure, le cas échéant, les aspects liés à la sécurité. **12.3** – La création, la modification et la suppression des autorisations d'accès doivent être enregistrées.	☒ Yes ☐ No ☐ N/A	Une politique de mots de passe (complexité, durée de validité) est définie dans la spécification fonctionnelle (FS) et configurée dans le système. La gestion des utilisateurs et des rôles relève de la responsabilité du client.
11.300(c) – Mise en œuvre de procédures de gestion des pertes afin de désactiver électroniquement les jetons, cartes et autres dispositifs portant ou générant des informations de code d'identification ou de mot de passe en cas de perte, de vol, de disparition ou de compromission potentielle, et d'émettre des remplacements temporaires ou permanents en appliquant des contrôles appropriés et rigoureux.	**12.3** – La création, la modification et la suppression des autorisations d'accès doivent être enregistrées.	☐ Yes ☐ No ☒ N/A	Des procédures clients doivent être mises en place afin de satisfaire à cette exigence. Getinge n'utilise pas de jetons, cartes ou autres dispositifs portant ou générant des informations de code d'identification ou de mot de passe.

Exigences 21 CFR Part 11	Annexe 11	Conformité	Notes d'application
11.300(d) –Utilisation de mécanismes de protection des transactions afin de prévenir l'utilisation non autorisée des mots de passe et/ou des codes d'identification, ainsi que de détecter et de signaler de manière immédiate et urgente toute tentative d'utilisation non autorisée à l'unité de sécurité du système et, le cas échéant, à la direction de l'organisation.	**12.1** – Des contrôles physiques et/ou logiques doivent être mis en place afin de limiter l'accès aux systèmes informatisés aux seules personnes autorisées.	☒ Yes ☐ No ☐ N/A	Toute entrée de journal (réussie ou échouée) est enregistrée dans la piste d'audit. Une politique de mots de passe (complexité, durée de validité) est définie dans la spécification fonctionnelle (FS) et configurée dans le système. Un seuil de verrouillage de compte est également paramétré.
11.300(e) – Essais initiaux et périodiques des dispositifs, tels que les jetons ou cartes, qui portent ou génèrent des codes d'identification ou des mots de passe, afin de s'assurer de leur bon fonctionnement et de détecter toute altération non autorisée.	**11** – Les systèmes informatisés doivent être évalués périodiquement afin de confirmer qu'ils demeurent dans un état validé et qu'ils sont conformes aux BPF. Ces évaluations doivent inclure, le cas échéant, les aspects liés à la sécurité.	☐ Yes ☐ No ☒ N/A	Getinge n'utilise pas de jetons, de cartes ou d'autres dispositifs portant ou générant des informations de code d'identification ou de mot de passe.
N/A (aucun équivalent direct dans le 21 CFR Part 11).	**13** - Tous les incidents, et pas uniquement les défaillances du système et les erreurs de données, doivent être signalés et évalués. La cause racine d'un incident critique doit être identifiée et servir de base aux actions correctives et préventives.	☐ Yes ☐ No ☒ N/A	Le signalement des incidents système est hors du périmètre de responsabilité de Getinge.
N/A (aucun équivalent direct dans le 21 CFR Part 11).	**15** - Lorsqu'un système informatisé est utilisé pour l'enregistrement de la certification et la libération des lots, le système doit permettre uniquement aux personnes qualifiées de certifier la libération des lots et doit identifier clairement et enregistrer la personne procédant à la libération ou à la certification des lots. Cette opération doit être réalisée au moyen d'une signature électronique.	☐ Yes ☐ No ☒ N/A	La fonctionnalité de libération de lot est hors du périmètre de Getinge.

Exigences 21 CFR Part 11	Annexe 11	Conformité	Notes d'application
N/A (aucun équivalent direct dans le 21 CFR Part 11).	**16** - Pour la disponibilité des systèmes informatisés supportant des processus critiques, des dispositions doivent être prises afin d'assurer la continuité du support de ces processus en cas de défaillance du système (par exemple, via un système manuel ou alternatif). Le délai de mise en œuvre de ces solutions alternatives doit être défini sur la base d'une analyse de risques et être adapté au système concerné ainsi qu'au processus métier qu'il supporte. Ces dispositions doivent être correctement documentées et testées.	☒ Yes ☐ No ☐ N/A	Après la réalisation de la SAT, les problèmes liés à l'équipement sont pris en charge par l'équipe de service locale.

Annexe 1

Piste d'audit SIMATIC WinCC Unified

Introduction

La fonctionnalité de piste d'audit dans SIMATIC WinCC Unified V20 est un composant essentiel pour garantir la conformité aux réglementations relatives aux enregistrements électroniques et signatures électroniques (ERES). Elle répond à l'exigence d'un système sécurisé, fiable et traçable permettant d'enregistrer les actions des opérateurs dans les processus pertinents au regard des BPF.
Il n'est pas possible pour l'utilisateur de désactiver la fonctionnalité de piste d'audit.

Fonctionnalité de piste d'audit

La piste d'audit enregistre toutes les modifications et saisies effectuées par l'opérateur lors du fonctionnement du système. Ces enregistrements incluent des informations essentielles telles que :

- Qui : identification de l'opérateur ayant effectué les modifications.
- Quoi : description de l'action réalisée.
- Quand : horodatage indiquant le moment où l'action a été effectuée
- Pourquoi : raison facultative de la modification.

Sécurité du système

Les modifications de la configuration du système sont gérées séparément et soumises à une procédure de gestion des changements. Ce processus comprend la planification, l'évaluation des impacts, la documentation et les tests de bonne mise en œuvre.
Le système garantit que toutes les informations enregistrées restent sécurisées et ne peuvent pas être modifiées ni supprimées par l'opérateur.

Enregistrements opérationnels

Le système distingue les enregistrements générés automatiquement, qui ne nécessitent pas de piste d'audit, et les enregistrements générés par l'opérateur, qui sont soumis aux exigences de piste d'audit.
Le package optionnel SIMATIC WinCC Unified Audit permet de configurer les variables pertinentes au regard des BPF afin qu'elles soient suivies dans la piste d'audit.

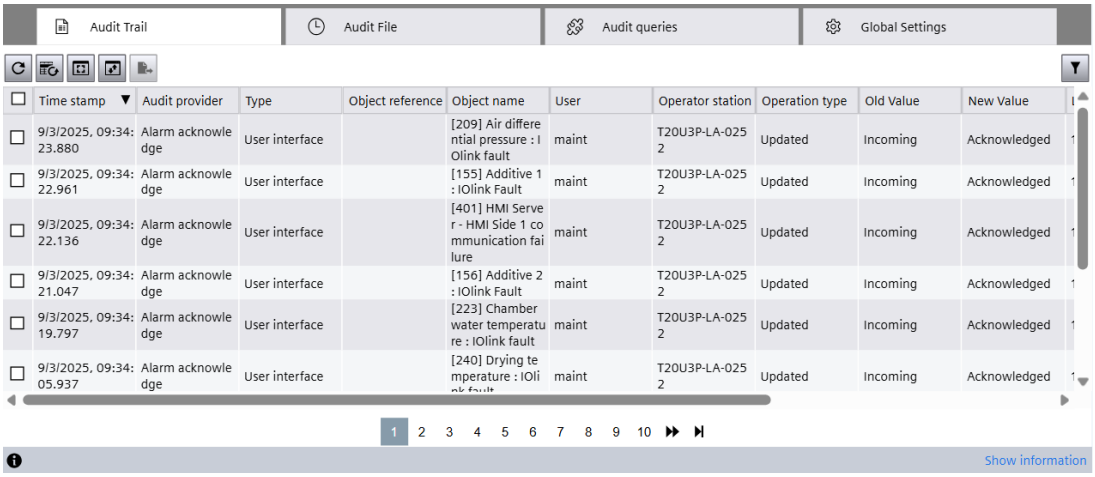

Figure 1 :
Certains des champs disponibles dans la piste d'audit

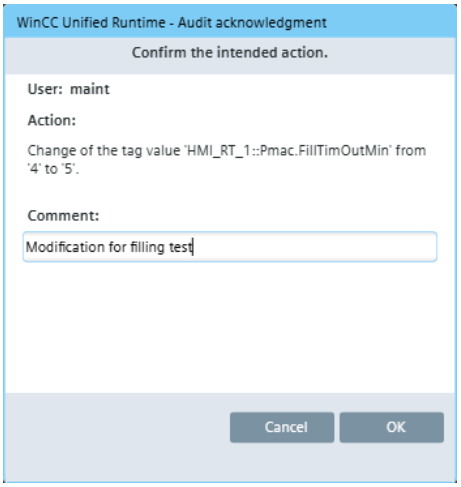

Figure 2 :
Saisie d'un commentaire lors de la réalisation d'une modification sur un paramètre BPF

Visualiseur d'audit

Le visualiseur d'audit dans WinCC Unified affiche les données de la piste d'audit en mode Runtime, permettant aux opérateurs et aux autorités de consulter les actions enregistrées.

Chaque entrée de la piste d'audit est sécurisée par une somme de contrôle intégrée (checksum). Le visualiseur d'audit est capable de détecter toute manipulation et d'indiquer quelle entrée de la piste d'audit a été modifiée.

Contrôle des paramètres

SIMATIC WinCC Unified prend également en charge l'enregistrement des actions via le contrôle des paramètres (PaCo).
Les actions de l'opérateur, telles que le téléchargement de jeux de paramètres et la modification de paramètres individuels, sont enregistrées en conséquence.

Conformité et documentation

La fonctionnalité de piste d'audit répond aux exigences du 21 CFR Part 11 ainsi qu'à l'annexe 11 des lignes directrices EU-GMP. Elle garantit que les enregistrements électroniques et les signatures électroniques sont aussi fiables et dignes de confiance que leurs équivalents papier, en fournissant un système sécurisé et traçable pour la conformité réglementaire.

Conclusion

La piste d'audit dans WinCC Unified constitue une solution complète pour garantir l'intégrité des données et la traçabilité des processus pertinents au regard des BPF. En enregistrant les actions des opérateurs et les modifications de configuration du système, elle fournit un environnement sécurisé et conforme pour les enregistrements et signatures électroniques.

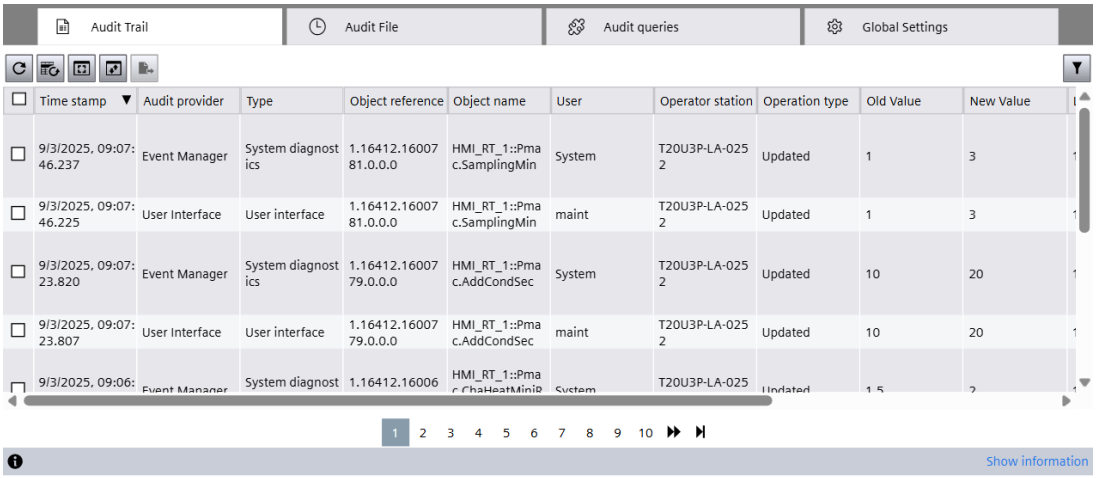

Figure 3 :
Visualiseur d'audit dans le système WinCC Unified

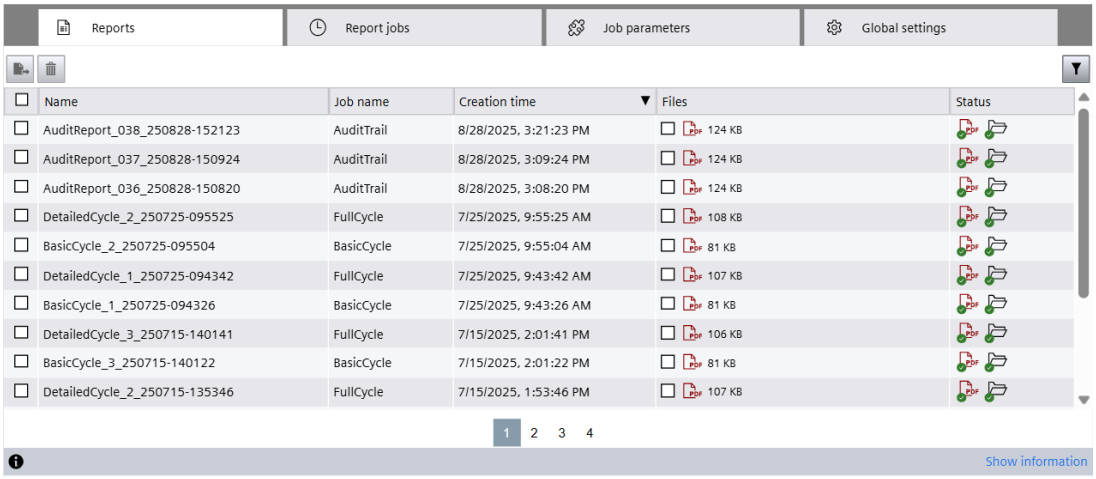

Figure 4 :
Gestion des rapports dans WinCC Unified

Annexe 2

Signature électronique SIMATIC WinCC Unified

Introduction

Dans le domaine des enregistrements électroniques et des signatures électroniques (ERES), SIMATIC WinCC Unified V20 propose des solutions robustes adaptées aux exigences réglementaires. La fonctionnalité de signature électronique de WinCC Unified garantit que les enregistrements électroniques sont aussi fiables et dignes de confiance que les enregistrements papier et les signatures manuscrites apposées sur papier.

Fonctionnalité de signature électronique

Signature électronique simple
La configuration d'une signature électronique est disponible avec l'option WinCC Unified Audit (Basique ou Améliorée).
La signature électronique est exécutée dans une boîte de dialogue où les utilisateurs confirment l'action prévue en saisissant leur mot de passe. Les variables nécessitant une signature électronique en cas de modification sont définies lors de la phase de configuration.
Les utilisateurs peuvent signer électroniquement en confirmant l'action prévue, et la signature électronique est enregistrée dans la piste d'audit avec le nom de l'utilisateur, l'horodatage et l'action effectuée. La saisie obligatoire d'un commentaire peut être activée.

Signature électronique multiple
Avec la variante WinCC Unified Audit Améliorée, une double signature électronique peut également être configurée, assurant un niveau supplémentaire de validation et de sécurité.

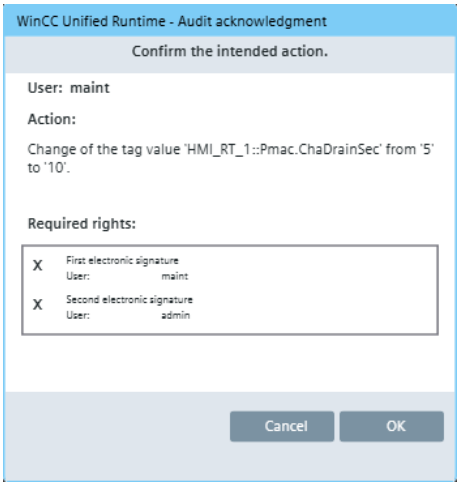

Figure 5 :
Écran de double signature dans WinCC Unified

Garantie de l'unicité et de l'intégrité
La signature électronique dans WinCC Unified est conçue pour être unique à chaque individu, empêchant la réutilisation ou la réattribution des signatures. Elle est liée à l'enregistrement électronique correspondant afin de garantir qu'elle ne puisse être extraite, copiée ou autrement transférée par des moyens ordinaires dans le but de falsifier l'enregistrement électronique.

Conformité règlementaire
La fonctionnalité de signature électronique répond aux exigences du 21 CFR Part 11 ainsi que de l'annexe 11 des lignes directrices EU-GMP.
Cette conformité réglementaire garantit que les signatures électroniques sont juridiquement contraignantes et équivalentes aux signatures manuscrites apposées sur papier.
Le système prend également en charge la génération de copies exactes et complètes des enregistrements électroniques, incluant les détails des signatures électroniques, sous forme lisible par l'homme et sous forme électronique.

Conclusion

La fonctionnalité de signature électronique dans WinCC Unified fournit un environnement sécurisé et conforme pour l'enregistrement et la vérification des signatures électroniques dans les processus pertinents au regard des BPF. Elle garantit l'intégrité, l'authenticité et la traçabilité des données, ce qui en fait un élément essentiel pour la conformité réglementaire dans l'industrie des sciences de la vie.

GETINGE

Convaincu que tout le monde devrait pouvoir bénéficier des meilleurs soins possibles, Getinge propose aux établissements de santé et de sciences de la vie, des solutions visant à améliorer les résultats cliniques et à optimiser les flux de travail. La gamme de produits est destinée aux soins intensifs, aux procédures cardiovasculaires, aux blocs opératoires ainsi qu'aux services de stérilisation centrale et des sciences de la vie. Avec plus de 12 000 employés dans le monde, les solutions Getinge sont commercialisées dans plus de 135 pays.

Fabricant · Ekebergsvägen 26 · Box 69 · SE-305 05 Getinge · Sweden

Getinge France, société par actions simplifiées au capital de 8.793.677,10 euros, dont le siège social est situé à MASSY (91300) – Carnot Plaza, 14/16 Avenue Carnot - immatriculée sous le numéro 562 096 297 RCS EVRY · 02 38 25 88 88 · operation-ventes.projet.fr@getinge.com

www.getinge.fr

DMS-0013383-PUB-2026-0195-A, version de juin 2026-livre-blanc-laveurs-stérilisateurs-getinge-utilisant-winccunified. Tous droits réservés. Le contenu peut être sujet à des modifications.