

Déclaration de conformité
21 CFR Part 11
SIMATIC WinCC V6.2

SIEMENS AG

Groupe Automatisation et Entraînements

Competence Center Pharmaceuticals

D-76181 Karlsruhe, République Fédérale d'Allemagne

Email: pharma.aud@siemens.com

Fax: +49 (721) 595 6390

Aout 2007

TABLE DES MATIERES

TABLE DES MATIERES	3
INTRODUCTION	5
1 Les exigences de la norme 21 CFR Part 11 en bref	7
2 Déclaration de conformité de SIMATIC WinCC V6.2 à la norme 21 CFR Part 11	9
2.1 Solution technologique pour la sécurité d'accès	9
2.2 Solution technologique pour les Audit Trails	11
2.3 Solution technologique pour l'archivage et la récupération	13
2.4 Solution technologique pour les signatures électroniques	14
3 Liste d'évaluation pour SIMATIC WinCC V6.2	15
3.1 Procédures et contrôles pour les systèmes fermés.....	15
3.2 Procédures et contrôles supplémentaires pour les systèmes ouverts	18
3.3 Enregistrements électroniques signés	19
3.4 Signatures électroniques (généralités)	19
3.4.1 Signatures électroniques (non biométriques)	20
3.4.2 Signatures électroniques (biométriques)	20
3.5 Contrôles des identifiants utilisateur et des mots de passe	21
Liste des abréviations	22

INTRODUCTION

Le 20 août 1997, la réglementation 21 CFR Part 11 "Enregistrements électroniques ; Signatures électroniques" a été mise en place par la Food and Drug Administration (FDA), autorité de contrôle américaine. La réglementation 21 CFR Part 11 (également appelée Part 11) définit les critères d'acceptation de la FDA concernant l'utilisation des enregistrements/signatures électroniques qui remplacent les enregistrements/signatures manuscrites sous forme papier. Il faut pouvoir accorder la même confiance à ces enregistrements/signatures électroniques. Pour ce faire, ils doivent être aussi fiables que les enregistrements classiques et leur être équivalents.

La mise en oeuvre de cette réglementation est obligatoire si des enregistrements électroniques/signatures électroniques sont appliqués. Toutefois, Part 11 ne vaut que pour les enregistrements effectués en conformité avec les directives de la FDA (comme défini dans ce qu'on appelle les "Predicate Rules") ou soumis sous forme électronique à la FDA. Il existe à ce sujet diverses interprétations et recommandations, tant émises par la FDA que par l'ISPE et la PDA. De plus, les signatures manuscrites et les documents papier traditionnels, ou un mélange des deux, peuvent continuer à être utilisés.

Afin d'aider ses clients, Siemens, en tant que fournisseur de SIMATIC WinCC, a évalué le système dans la version 6.2 conformément à cette réglementation. Ce document publie les résultats de l'évaluation du système SCADA SIMATIC WinCC V6.2.

SIMATIC WinCC V6.2 est conforme aux exigences fonctionnelles de la norme 21 CFR Partie 11. Son fonctionnement conforme à la réglementation est assuré en combinaison avec des mécanismes de contrôle et des instructions procédurales dont la définition incombe au client.

Les recommandations de Siemens en matière d'architecture du système, de conception et de configuration permettront au client de mettre leurs applications en conformité. Pour plus d'informations et d'aides, référez-vous au "GMP Engineering Manual: SIMATIC WinCC - Guidelines for Implementing automation projects in a GMP environment".

Les spécifications FDA, en plus d'être destinées au secteur pharmaceutique, sont en outre de plus en plus appliquées dans d'autres sciences de la vie (comme par exemple dans la technologie alimentaire, la cosmétologie et les produits d'entretien).

Les exigences de la 21 CFR Part 11 sont sujettes à interprétation. Ce document s'appuie donc sur l'interprétation GAMP CoP de l'ISPE et de la PDA actuellement acceptée dans le monde entier. Si l'interprétation d'une exigence mise en oeuvre par une entreprise diffère de celle spécifiée ici, veuillez contacter le Competence Center Pharmaceuticals à Karlsruhe (SIEMENS AG A&D CC P) afin d'obtenir des informations supplémentaires (données relatives au contact ci-dessus).

Ce document comprend trois parties : la première présente un résumé des exigences de la Partie 11, la deuxième décrit les solutions apportées par SIMATIC WinCC V6.2 aux diverses exigences et la troisième comporte une évaluation détaillée du système conformément à l'ISPE / à la PDA¹.

¹ *Good Practice and Compliance for Electronic Records and Signatures; Part2 "Complying with 21 CFR Part 11, Electronic Records and Electronic Signatures"; ISPE and PDA 2001/2002*

1 Les exigences de la norme 21 CFR Part 11 en bref

La norme 21 CFR Part 11 établit que le risque de manipulation, de mauvaise interprétation et de modification sans consignation de justification est plus important et que ces cas sont plus difficilement détectables avec les enregistrements/signatures électroniques qu'avec les enregistrements papier/signatures manuscrites traditionnels. Des mesures supplémentaires de contrôle s'avèrent par conséquent nécessaires.

"Un enregistrement électronique correspond à toute combinaison de textes, de graphiques, de données, d'éléments audio, d'images ou d'autres informations sous forme numérique qui est créée, modifiée, mise à jour, archivée, récupérée ou distribuée par un système informatique."¹

"Une signature électronique correspond à une compilation de données par un ordinateur incluant tout symbole ou toute série de symboles exécuté(e), adopté(e) ou autorisé(e) par un individu pour avoir le même caractère obligatoire que la signature manuscrite dudit individu."¹

Exigence	Description
Validation	Tous les systèmes automatisés GMP doivent être validés en vue de garantir un traitement précis, fiable et cohérent conformément à la performance prévue.
Audit Trails	Les systèmes doivent fournir des Audit Trails sûrs, générés par ordinateur et horodatés pour enregistrer les actions de création, de modification ou de suppression des enregistrements électroniques.
Rétention, protection, reproductibilité et possibilité de récupération des enregistrements	Les systèmes doivent être capables de conserver, protéger et récupérer rapidement les enregistrements pendant toute la période de rétention des données définie. Ils doivent être en mesure de reproduire les enregistrements électroniques sous une forme électronique et lisible.
Contrôle des documents	Des contrôles doivent exister pour l'accès à la documentation sur l'exécution et la maintenance du système, sa révision, sa distribution et son utilisation.
Sécurité d'accès	Les systèmes doivent limiter l'accès au personnel qualifié et autorisé uniquement. Au sein des systèmes ouverts, des mesures de sécurité supplémentaires doivent permettre de garantir la sécurité d'accès (cf. également norme 21 CFR Part 11.30).

¹ Good Practice and Compliance for Electronic Records and Signatures; Part2 "Complying with 21 CFR Part 11, Electronic Records and Electronic Signatures"; ISPE and PDA 2001/2002

Exigence	Description
Signature électronique	Les systèmes doivent fournir des mesures visant à s'assurer que l'utilisation est limitée aux titulaires d'origine uniquement et que toute tentative d'utilisation par des tiers est détectée et rapidement signalée. Les systèmes non biométriques doivent utiliser deux mécanismes d'identification distincts (identifiant utilisateur/mot de passe). L'identifiant utilisateur et le mot de passe doivent être saisis avant une session de signature et au moins le mot de passe doit être saisi lors de chaque signature suivante effectuée au cours de la même session. Les signatures électroniques ne doivent pas être réutilisées ou réaffectées. Le but d'une signature électronique doit être clairement indiqué. Enfin, les systèmes doivent inclure des mesures visant à empêcher toute falsification des signatures électroniques par des outils standards. Des procédures écrites tenant les personnes concernées pour responsables des actions effectuées sous le couvert de leur signature électronique doivent être en place.
Certificat pour la FDA	Une certification écrite définissant que toutes les signatures électroniques utilisées ont le même caractère obligatoire que les signatures manuscrites traditionnelles, doit être fournie au bureau FDA régional.

2 Déclaration de conformité de SIMATIC WinCC V6.2 à la norme 21 CFR Part 11

Les exigences pouvant être satisfaites par des solutions technologiques peuvent se résumer **en quatre thèmes** :

- Sécurité d'accès
- Audit Trail
- Archivage et récupération
- Signature électronique

2.1 Solution technologique pour la sécurité d'accès

Le pack logiciel SIMATIC Logon offre une gestion des utilisateurs basée sur la sécurité MS Windows :

- Sur la base des groupes d'utilisateurs, les autorisations et les niveaux d'autorisation sont définis dans la gestion des utilisateurs de WinCC.
- Les différents utilisateurs ainsi que leur affectation aux groupes d'utilisateurs Windows sont définis dans la gestion des utilisateurs de Windows.
- SIMATIC Logon établit la connexion entre les groupes d'utilisateurs Windows et ceux de WinCC.

Les exigences suivantes concernant la sécurité d'accès sont ainsi satisfaites :

- Gestion centralisée des utilisateurs (création, désactivation, blocage, déblocage, affectation aux groupes) effectuée par l'administrateur
- Combinaison univoque identifiant utilisateur/mot de passe
- Définition de droits d'accès pour les groupes et les utilisateurs
- Accès dépendant de la zone du site et des niveaux d'autorisation
- Gestion de la durée de validité des mots de passe : l'utilisateur est obligé de changer son mot de passe à l'issue d'une période définissable et le mot de passe ne peut être réutilisé qu'après n générations
- Le système peut contraindre l'utilisateur à définir un nouveau mot de passe lors de sa première connexion (mot de passe initial)
- L'utilisateur est automatiquement bloqué après un nombre définissable de tentatives de connexion erronées et ne peut être débloqué que par l'administrateur
- Déconnexion automatique à l'issue d'une période définissable au cours de laquelle aucune action n'est entreprise sur le clavier ou la souris

Fonctions de journalisation pour les actions relatives à la sécurité d'accès telles que la connexion, la déconnexion (manuelle et automatique), l'identifiant incorrect, le mot de passe incorrect, l'utilisateur bloqué après un nombre prédéfini de tentatives consécutives de connexion avec un mot de passe erroné, le changement du mot de passe par l'utilisateur

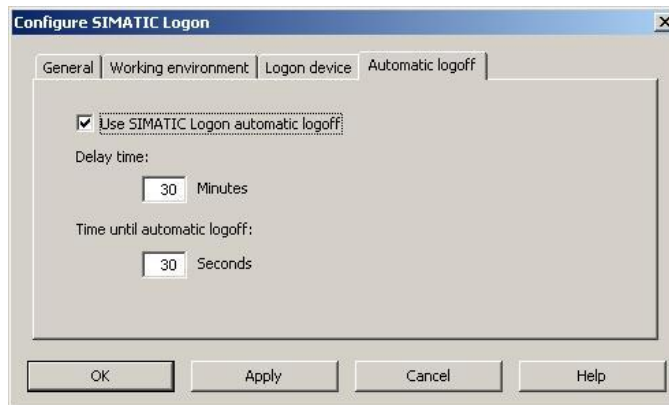


Fig. 1 : Configuration de SIMATIC Logon

SIMATIC Logon satisfait aux exigences de la norme 21 CFR Partie 11 en ce qui concerne la sécurité d'accès en combinaison avec d'autres procédures, comme par exemple la "Clarification de la responsabilité et de l'accès des utilisateurs du système".

Il faut en outre empêcher les accès non autorisés aux structures de répertoires des différents programmes du système via l'affectation des droits du système d'exploitation Windows et exclure ainsi les manipulations non souhaitées.

Si l'accès au système n'est pas contrôlé par les personnes qui sont responsables du contenu des enregistrements électroniques, le système est alors défini comme étant "ouvert". En cas de "chemin ouvert", celui-ci peut être sécurisé à l'aide d'outils standard.

2.2 Solution technologique pour les Audit Trails

Les Audit Trails sont particulièrement importants lorsque les utilisateurs créent, modifient ou suppriment des données dans le cadre de leurs opérations habituelles.

Lorsque les enregistrements électroniques sont générés automatiquement sans pouvoir être modifiés ou supprimés par l'utilisateur, aucun Audit Trail n'est alors nécessaire. Ces enregistrements sont en effet sécurisés par le système WinCC lui-même (ex. : sécurité d'accès).

La section suivante décrit la manière dont le système SIMATIC WinCC prend en charge la mise en pratique des exigences de la norme 21 CFR Part 11 en ce qui concerne l'Audit Trail lors des opérations d'exécution. Cette section présente également les outils que le système met à la disposition de l'utilisateur pour tracer les modifications dans le système d'ingénierie.

Lors des opérations d'exécution

Données de processus

Les données de processus (ex : valeurs de processus, alarmes de processus ou messages de conduite) sont sauvegardées sans que l'utilisateur puisse procéder à des modifications.

Modifications lors des opérations d'exécution

L'option Audit permet d'enregistrer dans un Audit Trail les modifications pertinentes que l'utilisateur a effectuées au cours de ses opérations d'exécution dans le système de visualisation des processus.

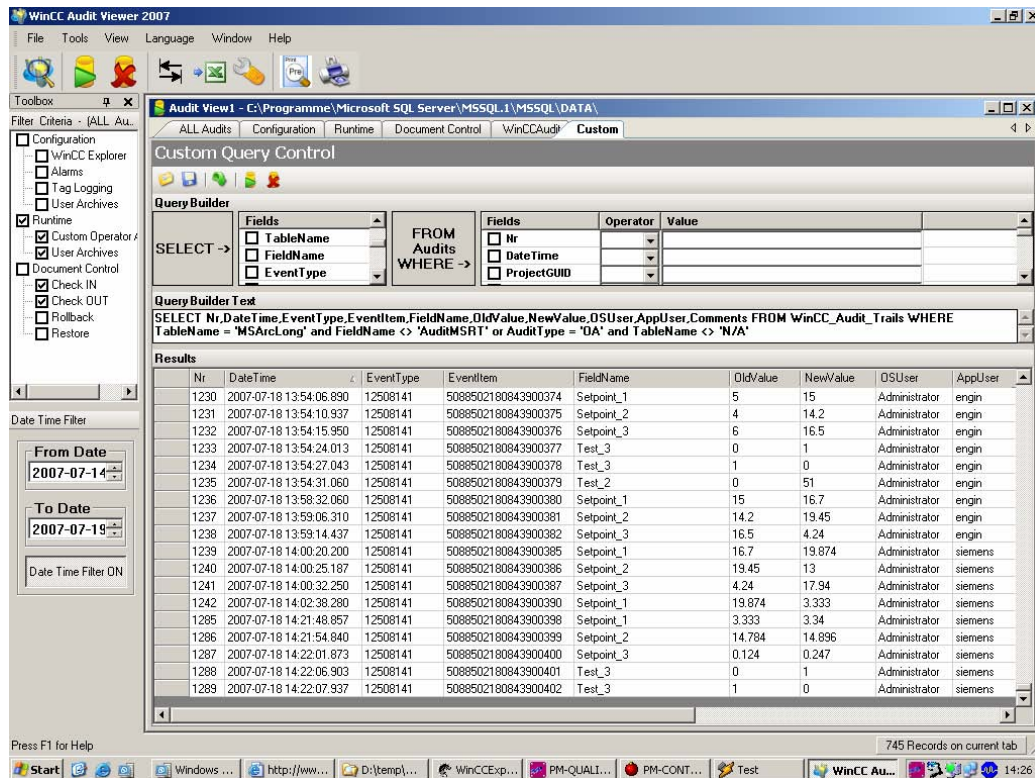


Fig. 2 : Affichage des Audit Trails via WinCC Audit

Les modifications peuvent également être présentées dans l'archive des messages WinCC sous la forme d'un Audit Trail.

Lors de la configuration

Configuration

Dans le cadre de la prise en charge d'une procédure formelle de contrôle des modifications, l'option WinCC/Audit permet d'enregistrer les modifications dans les projets WinCC (comme par exemple les archives, les graphiques, le paramétrage des droits des utilisateurs). La fonction de contrôle des documents de WinCC/Audit permet un contrôle complet à l'entrée, à la sortie, l'effacement, le rollback et la restauration de documents d'application et de documents utilisateur. Des copies de tous les états de configuration d'un document sont archivées dans une base de données sécurisée.

Modifications dans la gestion des utilisateurs

Les modifications apportées dans le cadre de la gestion des utilisateurs (comme par exemple la définition de nouveaux utilisateurs, le blocage d'utilisateurs, etc.) sont enregistrées par l'Audit Trail de Windows. C'est à cette fin que le journal des événements Windows doit être configuré en conséquence.

2.3 Solution technologique pour l'archivage et la récupération

Archivage continu

SIMATIC WinCC offre un concept d'archivage configurable et adaptable. Dans les archives WinCC locales, des messages et des valeurs de mesure sont continuellement sauvegardés. Ces données sauvegardées localement peuvent être automatiquement transférées dans l'archive longue durée. La création d'un checksum empêche de manipuler les données archivées. Les données archivées peuvent être récupérées durant toute la durée de la période de rétention définie. La récupération dans WinCC est possible via les fonctions standard, les interfaces standard ou les packs optionnels (ex : DataMonitor, Connectivity Pack).

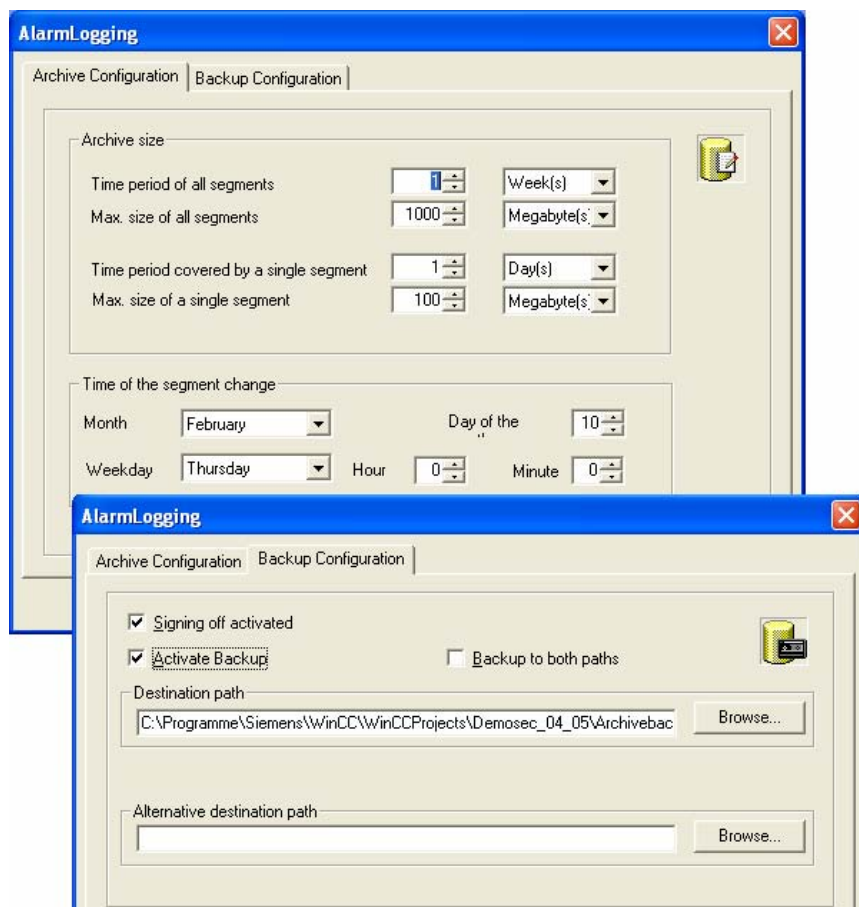


Fig. 3 : Configuration des archives

Archivage par lots

Le Premium Add-on WinCC PM Quality est utilisé pour effectuer un archivage par lots. PM Quality gère de manière autonome les archives locales et de longue durée. Pour pouvoir accéder aux données WinCC, PM Quality utilise les interfaces standards de WinCC. Ces dernières permettent d'accéder à d'autres outils d'archivage (Siemens ou tiers).

2.4 Solution technologique pour les signatures électroniques

SIMATIC Logon met à disposition une interface (API) de configuration des signatures électroniques dans WinCC.

La signature électronique s'effectue dans le dialogue de SIMATIC Logon. L'identifiant utilisateur et le mot de passe sont demandés et vérifiés à des fins d'identification.

3 Liste d'évaluation pour SIMATIC WinCC V6.2

La liste de contrôle suivante pour l'évaluation de SIMATIC WinCC est extraite d'un document de consultation du "GAMP Special Interest Group"¹.

Cette liste de contrôle servant à l'évaluation des systèmes comprend toutes les exigences, et pas uniquement celles pouvant être satisfaites par des solutions technologiques. L'utilisateur doit introduire des procédures de contrôle dans son entreprise pour satisfaire à certaines exigences de la réglementation 21 CFR Part 11. Les spécifications de 21 CFR Part 11 se rapportent toujours à l'application client réalisée avec WinCC. C'est pourquoi les solutions spécifiées ne sont valables qu'en jonction avec les procédures de contrôle spécifiques et les mesures organisationnelles.

3.1 Procédures et contrôles pour les systèmes fermés

Si l'accès au système est contrôlé par les personnes qui sont responsables du contenu des enregistrements électroniques, alors le système est considéré comme "fermé" et il doit être évalué par rapport aux exigences définies dans ce chapitre.

Paragraphe / Point	Question / Exigence	Commentaires
11.10(a) Point 1	Le système est-il validé ?	<p>Le client est responsable de la validation des applications/du système. La validation doit suivre une méthodologie de cycle de vie système (SLC) établie, par ex. comme décrit dans GAMP 4².</p> <p>WinCC a été développé selon le système de gestion qualité Siemens (certification ISO 9001:2000). Siemens peut apporter son aide pour la validation de l'application lors des projets.</p>
11.10(a) Point 2	Est-il possible de détecter les enregistrements non valides ou modifiés ?	<p>Oui.</p> <p>Un Audit Trail peut être généré lors de toute commande opérateur (par ex. lorsque l'opérateur change les consignes/les limites d'alarme/le mode de surveillance, etc. ou acquitte les alarmes). Toutes les modifications significatives sont enregistrées y compris l'horodatage, l'identifiant utilisateur, l'ancienne valeur/la nouvelle valeur et le commentaire. Les modifications non autorisées sont empêchées par le système via la fonction de sécurité d'accès.</p> <p>Les enregistrements archivés sont sécurisés via un mécanisme de checksum permettant de détecter les modifications non autorisées.</p> <p>Les modifications de configuration de WinCC peuvent être détectées par l'outil WinCC/Audit.</p>

² GAMP Guide for Validation of Automated Systems

Paragraphe / Point	Question / Exigence	Commentaires
11.10(b) Point 1	Est-ce que le système est capable de produire sur papier des copies précises et complètes des enregistrements numériques ?	Oui. WinCC fournit des imprimés de données de processus, de messages et d'Audit Trails.
11.10(b) Point 2	Est-ce que le système est capable de produire des copies précises et complètes des enregistrements sous forme électronique pour inspection, contrôle et copie par la FDA ?	Oui. Les valeurs de processus, les messages et les Audit Trails peuvent être exportés au format électronique et être affichés via WinCC ou l'option DataMonitor. L'option WinCC/Audit permet d'exporter les Audits Trail au format Microsoft Excel, PDF ou CSV.
11.10(c)	Est-ce que les enregistrements peuvent-être lus pendant la période de rétention ?	Oui. Les enregistrements peuvent être archivés dans un format lisible, par ex. sur CD/DVD. Nous partons du principe que ces périphériques et formats resteront lisibles à l'avenir. Les enregistrements archivés peuvent être visualisés via l'option DataMonitor ou être de nouveau lus dans WinCC. De plus, le client doit spécifier les périodes de rétention et définir les processus d'archivage, de sauvegarde et de récupération de ses enregistrements électroniques.
11.10(d)	Est-ce que l'accès au système est limité aux personnes autorisées ?	Oui. Par le biais du SIMATIC Logon, il est permis d'utiliser l'ensemble des possibilités offertes par la gestion des utilisateurs de Windows (cf. chapitre 2, Solution technologique pour la sécurité d'accès). Le client doit s'assurer que seules les personnes qui ont un besoin professionnel légitime d'utiliser le système peuvent avoir un accès physique au système (par ex. serveur, console systèmes). Comme cette exigence est presque identique à l'exigence [11.10(g)], elles sont généralement interprétées comme faisant référence, respectivement, à l'accès physique et logique.
11.10(e) Point 1	Existe-t-il un Audit Trail horodaté, généré par ordinateur et sécurisé qui enregistre la date et l'heure des entrées effectuées par l'utilisateur et de ses actions visant à créer, modifier ou supprimer des enregistrements électroniques ?	Oui. L'audit Trail est sécurisé au sein du système et ne peut être modifié par un utilisateur. Les modifications apportées en phase de production sont ajoutées à l'Audit Trail par le système lui-même et incluent les informations d'horodatage, l'identifiant utilisateur, l'ancienne et la nouvelle valeur ainsi que le commentaire.
1.10(e) point 2	Une fois modifié un enregistrement électronique, est-ce que les informations précédemment enregistrées restent disponibles (ne sont-elles par exemple pas masquées par la modification) ?	Oui. Les informations enregistrées sont toujours disponibles dans la base de données.

Paragraphe / Point	Question / Exigence	Commentaires
0(e) Point 3	Est-ce que l'Audit Trail d'un enregistrement électronique est disponible durant la période de rétention de l'enregistrement ?	Oui. L'Audit Trail est disponible pendant toute la période de rétention (cf. 11.10(c)).
11.10(e) Point 4	Est-ce que l'Audit Trail est disponible pour vérification et copie par la FDA ?	Oui. L'option WinCC/Audit permet d'exporter l'Audit Trail au format Microsoft Excel, PDF ou CSV. Si l'Audit Trail a été enregistré dans le système des messages, il peut être exporté au format PDF ou CSV.
11.10(f)	Lorsqu'une séquence d'événements ou d'étapes du système est importante, est-elle imposée par le système (comme c'est le cas par exemple dans un système de conduite de processus) ?	Oui. Une séquence donnée de commandes opérateur peut être prise en compte par une configuration correspondante de l'application.
11.10(g)	Est-ce que le système s'assure que seules des personnes autorisées peuvent utiliser le système, signer électroniquement des enregistrements, accéder à la commande ou aux périphériques d'entrée ou de sortie, modifier un enregistrement ou effectuer une autre opération ?	Oui. Le pack logiciel SIMATIC Logon se base sur le système de sécurité MS Windows. Un identifiant utilisateur et un mot de passe sont utilisés. Une gestion centralisée des utilisateurs est utilisée pour gérer les utilisateurs et les groupes d'utilisateurs. De plus, le client doit définir de quelle manière l'accès est limité aux personnes autorisées uniquement (par ex. qui a accès à quel objet ou quelle fonction dans WinCC Runtime), y compris les droits spéciaux pour les administrateurs.
11.10(h)	Si le système exige que les commandes ou données de saisie ne puissent venir que de certains périphériques d'entrée (par ex. des terminaux), est-ce que le système contrôle la validité de la source de toute donnée ou commande entrante ? (Remarque : cela s'applique lorsque des données ou commandes peuvent provenir de plusieurs périphériques, et que donc le système doit vérifier l'intégrité de la source, comme pour une balance ou des terminaux distants à commande radio).	Oui. Les stations de travail WinCC peuvent être conçues de manière à ce que toute entrée particulière de données / commandes ne puisse être effectuée que depuis une station de travail dédiée ou depuis un groupe de stations de travail dédiées. Toutes les autres stations disposent tout au plus de droits de lecture. Le système effectue des contrôles de validité parce que la connexion des stations s'opère avec le système.

Paragraphe / Point	Question / Exigence	Commentaires
11.10(i)	Existe-t-il une documentation sur les formations, y compris les formations des utilisateurs système, des développeurs, des techniciens du support technique ?	Oui. Siemens propose non seulement des sessions de formation standard mais également des sessions de formation spécifiques aux projets du client qui doivent être prévues et exécutées au cas par cas. La définition du besoin en formation et l'organisation des sessions de formation nécessaires incombent au client.
11.10(j)	Existe-t-il des règles écrites selon lesquelles les personnes sont entièrement responsables des actions effectuées sous leur signature électronique ?	Il incombe au client de fournir ces procédures.
11.10(k) Point 1	Est-ce que la distribution de la documentation sur la maintenance et le fonctionnement du système ainsi que l'accès à cette documentation et son utilisation sont contrôlés ?	
11.10(k) Point 2	Existe-t-il une procédure de contrôle des modifications formelle pour la documentation du système qui garantit un Audit Trail chronologique pour les modifications apportées par l'entreprise pharmaceutique ?	

3.2 Procédures et contrôles supplémentaires pour les systèmes ouverts

Si l'accès au système n'est PAS contrôlé par les personnes responsables du contenu des enregistrements électroniques, alors le système est considéré comme "ouvert" et doit être évalué selon les exigences de ce chapitre. SIMATIC WinCC peut être utilisé tant dans un environnement fermé que dans un environnement ouvert. Des exigences supplémentaires doivent être satisfaites lors d'une mise en œuvre dans des systèmes ouverts.

Paragraphe / Point	Question / Exigence	Commentaires
11.30 Point 1	Les données sont-elles cryptées?	Dans le cas des systèmes ouverts, il existe sur le marché des outils standard pour crypter le transfert de données et sécuriser davantage le "chemin ouvert".
11.30 Point 2	Des signatures électroniques sont-elles utilisées ?	WinCC ne fournit pas de fonctionnalité de signature électronique. Il existe des outils stand sur le marché autorisant une signature électronique des enregistrements (par exemple dans le cas des fichiers PDF).

3.3 Enregistrements électroniques signés

Paragraphe / Point	Question / Exigence	Commentaires
11.50 Point 1	Est-ce que les enregistrements électroniques signés contiennent les informations connexes suivantes ? Le nom imprimé du signataire La date et l'heure de la signature La signification de la signature (par ex. approbation, révision, responsabilité)	Oui. Les enregistrements électroniques signés contiennent, en plus d'autres informations : le nom imprimé ou l'identifiant utilisateur du signataire la date et l'heure de la signature la signification de la signature
11.50 Point 2	Est-ce que les informations ci-dessus sont indiquées sur les copies affichées à l'écran et sur les copies imprimées de l'enregistrement électronique ?	Oui. Les informations mentionnées ci-dessus peuvent être imprimées et affichées comme composant de l'enregistrement électronique.
11.70	Est-ce que les signatures sont associées aux enregistrements électroniques respectifs de manière à garantir qu'elles ne peuvent pas, via des moyens ordinaires, être coupées/copiées ou transférées d'une autre manière à des fins de falsification ?	Oui Une fois qu'un enregistrement électronique a été signé, il peut être archivé dans la base de données de WinCC. Cet enregistrement ne peut être coupé, copié, modifié ou supprimé. L'accès externe à la base de données est protégé par un mot de passe. Il est en outre recommandé d'appliquer des restrictions d'accès fichiers à la base de données à l'aide des fonctions de sécurité Windows.

3.4 Signatures électroniques (généralités)

Paragraphe / Point	Question / Exigence	Commentaires
11.100(a) Point 1	Est-ce que les signatures électroniques sont attribuées de manière univoque ?	Oui. La signature électronique utilise l'identifiant utilisateur et le mot de passe de l'utilisateur. Le caractère univoque de l'identifiant est garanti par la fonction de sécurité de MS Windows. Il n'est pas possible de définir plusieurs utilisateurs avec le même identifiant dans le même groupe de travail/domaine. De plus, le client doit garantir que chaque signature électronique correspond à une seule personne (caractère univoque).
11.100(a) Point 2	Est-ce que les signatures électroniques sont réutilisées par d'autres personnes ou réaffectées à d'autres utilisateurs ?	Le client doit s'assurer et est responsable de l'affectation systématique d'un identifiant utilisateur à une seule et unique personne.
11.100(b)	Est-ce que l'identité de la personne est vérifiée avant qu'une signature électronique ne lui soit affectée ?	C'est du ressort du client. Il doit prendre les mesures nécessaires.

3.4.1 Signatures électroniques (non biométriques)

Paragraphe / Point	Question / Exigence	Commentaires
11.200 (a)(1)(i)	Est-ce que la signature est constituée d'au moins deux composants, comme un identifiant utilisateur et un mot de passe, ou une carte d'identification et un mot de passe ?	Oui. SIMATIC Logon identifie la personne via deux composants distincts : un identifiant utilisateur et un mot de passe.
11.200 (a)(1)(ii)	Lorsque plusieurs signatures sont effectuées au cours d'une session continue, est-ce que le mot de passe est entré pour chaque signature ? (Remarque : les deux composants doivent être exécutés au début de la session)	Oui. Chaque signature nécessite au moins deux composants (identifiant utilisateur et mot de passe).
11.200 (a)(1)(iii)	Si les signatures ne sont pas effectuées au cours d'une session continue, est-ce que les deux composants de la signature électronique sont exécutés pour chaque signature ?	Oui. Chaque signature nécessite au moins deux composants (identifiant utilisateur et mot de passe).
11.200 (a)(2)	Est-ce que les signatures non biométriques sont utilisées uniquement par leur véritable titulaire ?	Oui. Le client est responsable de la mise à disposition de procédures visant à interdire la divulgation des mots de passe.
11.200 (a)(3)	Est-ce qu'une tentative de falsification d'une signature électronique nécessiterait la collaboration d'au moins deux personnes ?	Oui. Il n'est pas possible de falsifier une signature électronique lors de la signature et une fois que le système l'a écrite dans un enregistrement. L'administrateur ne peut pas utiliser de manière incorrecte la signature, bien qu'il configure l'identifiant et le mot de passe, car l'utilisateur est obligé de modifier son mot de passe lors de sa première tentative de connexion. Toute utilisation non autorisée des identifiants/mots de passe (échec de tentatives de connexion) est immédiatement détectée et signalée. De plus, le client doit mettre en place des procédures pour que les utilisateurs ne divulguent pas leur signature électronique.

3.4.2 Signatures électroniques (biométriques)

Paragraphe / Point	Question / Exigence	Commentaires
11.200(b)	Est-ce qu'il est prouvé que les signatures électroniques biométriques ne peuvent être utilisées que par leur véritable titulaire ?	L'utilisation d'outils standards de fournisseurs tiers permet de générer des signatures électroniques biométriques. L'intégrité d'une telle solution doit être évaluée au cas par cas.

3.5 Contrôles des identifiants utilisateur et des mots de passe

Si des jetons, des cartes ou d'autres dispositifs portant ou générant un identifiant utilisateur ou des informations de mot de passe sont utilisés sur un système d'automatisation pour les signatures électroniques, le système en question doit alors être évalué par rapport aux exigences indiquées dans ce chapitre.

Paragraphe/ Point	Question / Exigence	Commentaires
11.300(a)	Est-ce que des contrôles sont en place afin de maintenir le caractère unique de chaque combinaison identifiant utilisateur/mot de passe, de manière à ce qu'aucune autre personne ne puisse avoir la même combinaison identifiant utilisateur/mot de passe ?	Voir 11.100(a).
11.300(b) Point 1	Existe-t-il des procédures permettant de s'assurer que la validité de l'identifiant utilisateur est contrôlée à intervalles réguliers ?	Il incombe au client de fournir ces procédures.
11.300(b) Point 2	Est-ce que les mots de passe expirent de manière régulière et doivent-ils être contrôlés à intervalles réguliers ?	Oui. Le mot de passe expire après un nombre de jours donné et ne peut alors plus être réutilisé pendant un nombre de générations défini, conformément aux paramètres des politiques de sécurité de MS Windows. La gestion de la durée de validité des mots de passe n'a aucune influence sur l'utilisation antérieure (enregistrements, signatures).
11.300(b) Point 3	Existe-t-il une procédure de révocation des mots de passe et identifiants utilisateur si une personne quitte l'entreprise ou est mutée ?	Il incombe au client de fournir cette procédure. Les fonctions de sécurité de MS Windows permettent de désactiver les comptes utilisateurs.
11.300(c)	Existe-t-il une procédure de désactivation électronique d'un mot de passe ou identifiant utilisateur s'il s'avère qu'il peut être compromis, ou en cas de perte ?	Il incombe au client de fournir cette procédure. Les fonctions de sécurité de MS Windows permettent de modifier les comptes utilisateurs. Chaque utilisateur peut à tout moment modifier son mot de passe dans SIMATIC Logon.
11.300(d) Point 1	Existe-t-il une procédure de détection des tentatives d'utilisation non autorisée ainsi qu'un système d'information du service de sécurité ?	Les tentatives d'utilisation non autorisées sont enregistrées dans le journal de sécurité MS Windows. Le compte utilisateur est bloqué après un nombre donné de tentatives non autorisées. De plus, il incombe au client de fournir les procédures organisationnelles correspondantes.

Paragraphe/ Point	Question / Exigence	Commentaires
11.300(d) Point 2	Existe-t-il une procédure de génération de rapports à destination de la direction sur les tentatives sérieuses ou répétées d'utilisation non autorisée ?	Il incombe au client de fournir les procédures organisationnelles correspondantes.
11.300(e) Point 1	Existe-t-il un contrôle à l'entrée ainsi que des vérifications régulières des jetons et des cartes ?	
11.300(e) Point 2	Est-ce que ce test vérifie aussi qu'aucune modification non autorisée ne s'est produite ?	

Liste des abréviations

API : Application Programming Interface
 CD : Compact Disk
 CFR : Code of Federal Regulations
 CoP : Community of Practice
 CSV : Comma Separated Values
 DVD : Digital Versatile Disc
 FDA : Food and Drug Administration
 GAMP : Good Automated Manufacturing Practice
 GMP : Good Manufacturing Practice
 ID : Identification
 ISPE : International Society for Pharmaceutical Engineering
 ISO : International Standards Organization
 PDA : Parenteral Drug Association
 SCADA : Supervisory Control and Data Acquisition
 SLC : System Life Cycle