

**Déclaration de conformité**  
**21 CFR Partie 11**  
**SIMATIC WinCC flexible 2007**

SIEMENS AG

Industry Sector

Industry Automation

D-76181 Karlsruhe, République fédérale d'Allemagne

Email : [pharma.aud@siemens.com](mailto:pharma.aud@siemens.com)

Fax : +49 (721) 595 6390

Janvier 2008



# Contenu

<b>Contenu</b>	<b>3</b>
<b>Introduction</b>	<b>5</b>
<b>1 Les exigences du FDA 21 CFR Part 11 en bref</b>	<b>7</b>
<b>2 La réponse de SIMATIC WinCC flexible 2007 au 21 CFR Part 11</b>	<b>9</b>
2.1 Solution technologique pour la protection d'accès .....	9
2.2 Solution technologique pour les Audit Trails .....	13
2.3 Solution technologique pour l'archivage et pour la relecture des données archivées .....	15
2.4 Solution technologique pour les signatures électroniques .....	16
<b>3 Liste d'évaluation pour SIMATIC WinCC flexible 2007</b>	<b>17</b>
3.1 Méthodes et mesures pour les systèmes fermés .....	17
3.2 Instructions procédurales complémentaires et mesures pour systèmes ouverts.....	21
3.3 Enregistrements électroniques signés.....	22
3.4 Signatures électroniques (généralités).....	23
3.4.1 Signatures électroniques (non biométriques).....	23
3.4.2 Signatures électroniques (biométriques).....	24
3.5 Contrôles des codes ID et des mots de passe.....	25
<b>Abréviations utilisées</b>	<b>26</b>



# Introduction

Le 20 août 1997 est entrée en vigueur la réglementation 21 CFR Part 11 de l'administration américaine de sécurité alimentaire et pharmaceutique FDA (Food and Drug Administration) sur les "enregistrements électroniques et signatures électroniques". 21 CFR Partie 11 (abrégé : Part 11) définit les critères d'acceptance de la FDA quant à l'utilisation d'enregistrements électroniques et de signatures électroniques au lieu d'enregistrements sous forme de papier et de signatures manuscrites sur papier. Les enregistrements et signatures électroniques doivent être aussi dignes de confiance et fiables que les enregistrements traditionnels et leur être équivalents.

L'application de cette réglementation est impérativement nécessaire en cas d'utilisation d'enregistrements et de signatures électroniques. Cependant, la Part 11 ne vaut que pour les enregistrements qui doivent être gérés conformément aux directives de la FDA (comme le stipulent les "predicate rules") ou qui seront soumis à la FDA sous forme électronique. Il existe quant à cette thématique différentes interprétations et recommandations par la FDA ainsi que par l'ISPE et la PDA. Il est possible, outre l'utilisation d'enregistrements et de signatures électroniques, de continuer à utiliser des documents traditionnels sur papier et des signatures manuscrites ou une combinaison des deux.

Afin d'aider ses clients, Siemens, en tant que fournisseur de SIMATIC WinCC flexible, a évalué son système conformément à ces exigences. Nous publions dans ce document les résultats de l'évaluation du logiciel IHM "SIMATIC WinCC flexible 2007".

**SIMATIC WinCC flexible 2007 répond en totalité aux exigences fonctionnelles de la norme 21 CFR Part 11.** L'utilisation conforme à la réglementation est assurée en liaison avec les mesures organisationnelles et les instructions méthodologiques à établir par le client.

Les recommandations de Siemens quant à l'architecture du système, la conception et la configuration aideront le client à mettre leurs applications en conformité. Vous trouverez des informations et de l'aide dans le "Manuel GMP Engineering : SIMATIC WinCC flexible Guidelines for Implementing automation projects in a GMP environment".

Les directives de la FDA, utilisées initialement dans l'industrie pharmaceutique, sont appliquées de plus en plus dans d'autres domaines des sciences de la vie (Life Sciences), tels que l'industrie agro-alimentaire, les cosmétiques et les produits d'entretien.

Les exigences de la réglementation Part 11 sont sujettes à interprétation. Ce document s'appuie sur l'interprétation actuelle reconnue dans le monde entier de l'ISPE CoP GAMP et de la PDA. Si l'interprétation d'une exigence diffère de la règle indiquée ici dans une entreprise, veuillez vous adresser au Competence Center Pharma de Siemens AG, Industry Sector, Industry Automation division à Karlsruhe pour des informations détaillées.

Ce document est constitué de trois parties. La première partie présente une vue d'ensemble des exigences de la Partie 11, la deuxième présente les fonctionnalités de SIMATIC WinCC flexible 2007 dans le contexte de ces exigences et la troisième partie comprend une évaluation détaillée du système selon ISPE / PDA<sup>1</sup>.

---

<sup>1</sup> *Good Practice and Compliance for Electronic Records and Signatures ; Partie 2 "Complying with 21 CFR Part 11, Electronic Records and Electronic Signatures" ; ISPE et PDA 2001/2002*

# 1 Les exigences du FDA 21 CFR Part 11 en bref

Le 21 CFR Part 11 tient compte de l'évidence que le risque de contrefaçon, de fausses interprétations et de modifications non traçables est plus élevé avec les enregistrements et signatures électroniques qu'avec les enregistrements traditionnels sur papier et les signatures manuscrites et qu'il est donc plus difficile à détecter. Des mesures supplémentaires sont requises pour cette raison.

"Les termes "enregistrement électronique" / "document électronique" désignent toute combinaison de texte, graphique, données, informations numériques sous forme auditive, figurative ou autre qui sont créés, modifiés, maintenus, archivés, récupérés ou transmis avec un système informatique".<sup>2</sup>

"Le terme "signature électronique" désigne la conversion en données informatiques de tout symbole ou série de symboles qui est exécuté, accepté ou autorisé par une personne en tant qu'équivalent juridique d'une signature manuscrite".<sup>1</sup>

Exigence	Description
Validation	Tous les systèmes automatisés importants pour le GMP doivent être validés afin de garantir une préparation précise, fiable et cohérente des données en conformité avec les directives.
Audit Trails	Toutes les interventions opérateur qui créent, modifient ou effacent un enregistrement électronique doivent être consignées dans un Audit Trail informatisé, sécurisé et horodaté.
Conservation, protection, reproductibilité et disponibilité	Les systèmes doivent être en mesure d'archiver les enregistrements, de les protéger et de les fournir sur demande, ceci pendant la durée de conservation paramétrable. Les systèmes doivent être capables de reproduire des enregistrements électroniques sous forme lisible aussi bien qu'électronique.
Gestion de la documentation	La documentation relative à l'exploitation et la maintenance du système doit être contrôlée quant à son accès, sa révision, sa diffusion et son utilisation.
Protection d'accès	L'accès aux enregistrements électroniques doit être exclusivement limité aux personnes autorisées et qualifiées. Au sein de systèmes ouverts, des mesures de sécurité supplémentaires doivent être implémentées pour que ceci soit garanti (voir également 21 CFR 11.30).

---

<sup>2</sup> *Good Practice and Compliance for Electronic Records and Signatures ; Partie 2 "Complying with 21 CFR Part 11, Electronic Records and Electronic Signatures" ; ISPE et PDA 2001/2002*

<b>Exigence</b>	<b>Description</b>
Signature électronique	Les systèmes doivent offrir des mesures garantissant que l'usage de la signature électronique est limité aux seuls propriétaires authentiques et qu'une tentative d'utilisation par un tiers est immédiatement découverte et consignée. Les systèmes non biométriques doivent employer deux mécanismes d'identification distincts (nom d'utilisateur / mot de passe). Il faut saisir le nom d'utilisateur et le mot de passe avant d'apposer sa signature et au moins le mot de passe avant chaque signature suivante au cours de la même session. Il n'est pas permis de réutiliser la signature électronique ou de la transmettre. Le but de la signature électronique doit être indiqué clairement. Pour finir, le système doit contenir des fonctions qui empêchent la contrefaçon de la signature électronique au moyen d'outils classiques. Des dispositions écrites doivent permettre d'engager la responsabilité des personnes pour les actions effectuées sous couvert de leur signature électronique.
Attestation pour la FDA	Une attestation écrite doit être remise au bureau régional de la FDA pour confirmer que les signatures électroniques correspondent bien aux signatures manuscrites traditionnelles et qu'elles sont donc juridiquement équivalentes.

## **2 La réponse de SIMATIC WinCC flexible 2007 au 21 CFR Part 11**

Les exigences auxquelles les propriétés des systèmes doivent satisfaire peuvent être regroupées en quatre thèmes :

- Protection d'accès
- Audit Trail
- Archivage et disponibilité des enregistrements
- Signature électronique

### **2.1 Solution technologique pour la protection d'accès**

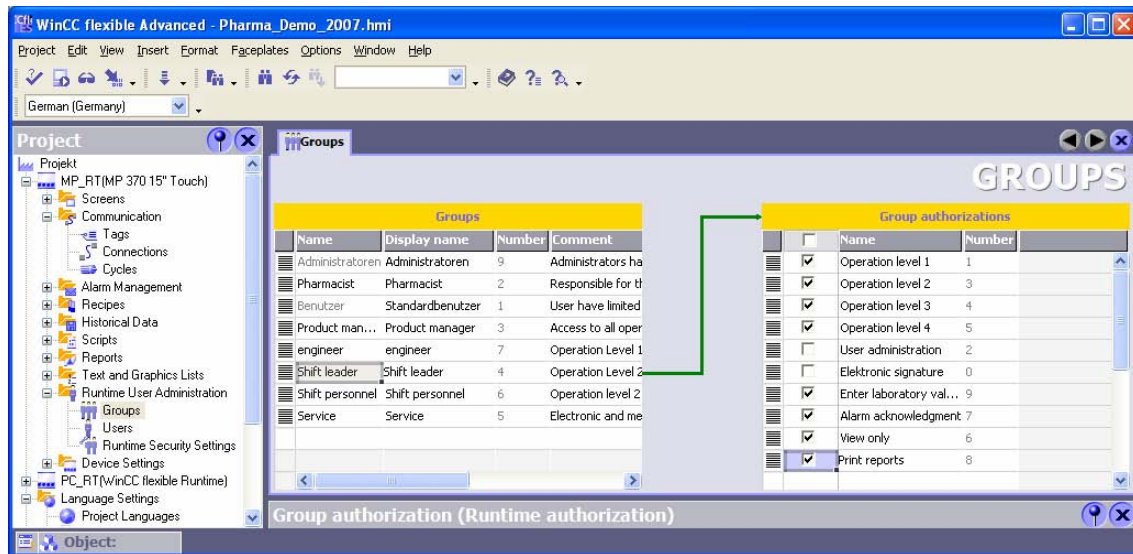
La gestion des utilisateurs est configurée pour chaque application dans un système d'ingénierie central, puis chargée dans l'appareil IHM concerné (PC ou pupitre).

Pour assurer la sécurité des enregistrements électroniques, WinCC flexible 2007 permet une gestion des utilisateurs locale et centrale.

#### **Gestion locale des utilisateurs**

Dans la gestion des utilisateurs locale, les différents utilisateurs et leur affectation à des groupes d'utilisateurs ne sont connus que localement.

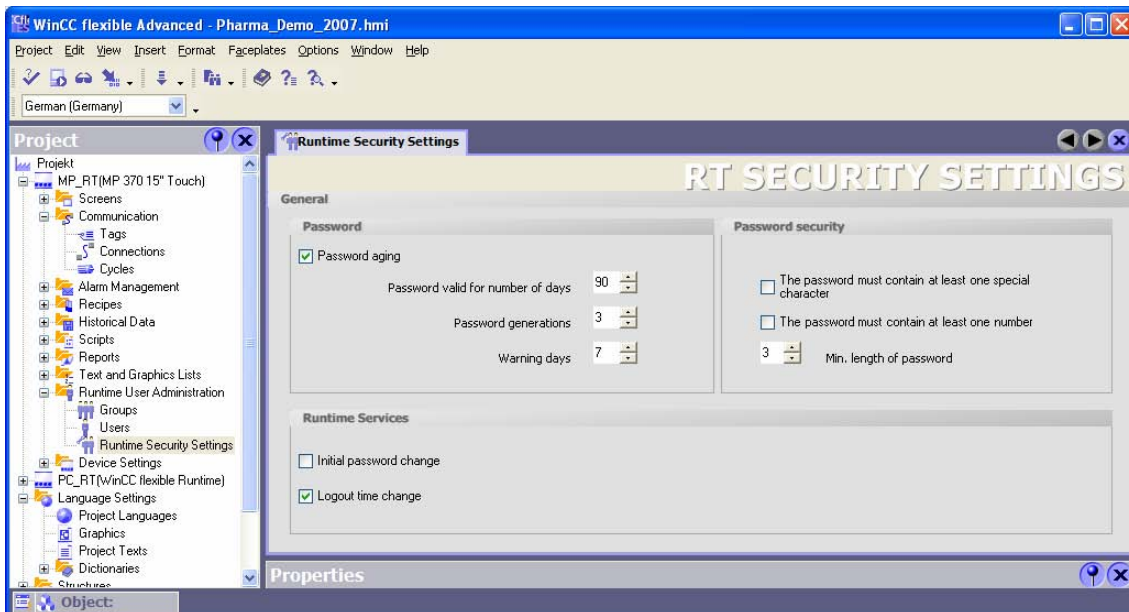
- Chaque utilisateur et son affectation à des groupes d'utilisateurs est défini dans la configuration WinCC flexible.
- Les autorisations sont définies avec des niveaux d'autorisation dans la gestion des utilisateurs de WinCC flexible sur la base des groupes d'utilisateurs.



La figure 1 montre l'affectation de droits de groupe à des groupes d'utilisateurs.

De cette manière, les exigences suivantes sur la protection d'accès sont satisfaites :

- Les utilisateurs ne peuvent se connecter à l'appareil IHM qu'au moyen d'une combinaison unique du nom d'utilisateur et du mot de passe.
- L'utilisateur peut modifier son mot de passe localement et en toute indépendance sur l'appareil IHM.
- Les paramètres de sécurité du mot de passe suivants sont possibles :
  - Le mot de passe doit comporter au moins un caractère spécial
  - Le mot de passe doit comporter au moins un chiffre
  - La longueur minimum du mot de passe peut être choisie entre 3 et 24 caractères
- Le vieillissement des mots de passe est pris en charge, la durée de validité d'un mot de passe et le nombre de générations étant paramétrables.
- Le système est en mesure de contraindre l'utilisateur à changer le mot de passe initial qui lui a été attribué pour sa première connexion.
- L'utilisateur est automatiquement bloqué après trois échecs de tentative de connexion et peut être débloqué par un administrateur.
- En l'absence d'activité, l'utilisateur connecté est déconnecté automatiquement par le système au terme d'un délai paramétrable.
- Fonctions de consignation des actions ayant rapport avec la protection d'accès comme par ex. la connexion, la déconnexion manuelle et automatique, la saisie d'un nom d'utilisateur ou d'un mot de passe erroné, le blocage d'un utilisateur après plusieurs saisies erronées du mot de passe, modification du mot de passe par l'utilisateur.



La figure 2 montre les paramètres de sécurité de la gestion des utilisateurs□□

### Gestion centrale des utilisateurs

La gestion centrale des utilisateurs est réalisée avec le logiciel SIMATIC Logon<sup>3</sup>. Pour cela, SIMATIC Logon est installé sur un ordinateur central avec un système d'exploitation MS-Windows (la liste des systèmes d'exploitation pris en charge se trouve dans les ReleaseNotes de SIMATIC Logon). Une gestion des utilisateurs basée sur des mécanismes de sécurité MS-Windows peut y être créée. Les appareils IHM sont connectés à l'ordinateur via Ethernet.

- Chaque utilisateur et son affectation à des groupes d'utilisateurs Windows sont définis dans la gestion des utilisateurs de Windows.
- Les autorisations sont définies avec des niveaux d'autorisation dans la gestion des utilisateurs de WinCC flexible sur la base des groupe d'utilisateurs.
- SIMATIC Logon établit la liaison entre les groupes d'utilisateurs Windows et les groupes d'utilisateurs WinCC flexible.
- Si la connexion réseau est interrompue, les utilisateurs créés localement peuvent être utilisés pour le maintien du fonctionnement. Les utilisateurs (utilisateurs centraux) SIMATIC Logon déjà connectés restent actifs jusqu'à la déconnexion.

<sup>3</sup> A partir de SIMATIC Logon V1.4.1 (V1.4 SP1)

SIMATIC Logon répond aux exigences de 21 CFR Part 11 en ce qui concerne la protection d'accès en combinaison avec des instructions procédurales, comme par ex. la définition de la compétence et de l'autorisation d'accès des utilisateurs système.

De plus, les accès non autorisés aux différentes structures de répertoire des différents programmes sont évités par l'affectation de droits du système d'exploitation et les manipulations indésirables exclues. Quand l'accès au système n'est pas contrôlé par des personnes responsables du contenu des enregistrements électroniques, on parle de système "ouvert". S'il existe un "chemin ouvert", il peut être protégé à l'aide de moyens standard.

## 2.2 Solution technologique pour les Audit Trails

Les Audit Trails sont particulièrement importants dans les cas où l'utilisateur peut générer, modifier et supprimer, durant le fonctionnement normal, les données destinées à la documentation normalisée du processus sous forme électronique. WinCC flexible 2007 répond à l'exigence d'une consignation traçable des actions opérateur jouant un rôle pour le GMP en enregistrant ces actions dans un fichier-journal Audit Trail. C'est le client qui définit les données importantes pour le GMP selon les directives légales le concernant.

Nous distinguons entre modifications effectuées durant la phase de production du système (runtime) et celles effectuées durant la phase de configuration (hors ligne).

### Phase de runtime

Vous pouvez déterminer, dans le système d'ingénierie, les données qui seront consignées dans l'Audit Trail durant l'exécution. Les informations requises sont mémorisées pour les différents enregistrements, par ex. le nom d'objet, l'ancienne valeur, la nouvelle valeur, l'horodatage, le nom d'utilisateur et un commentaire facultatif de la modification.

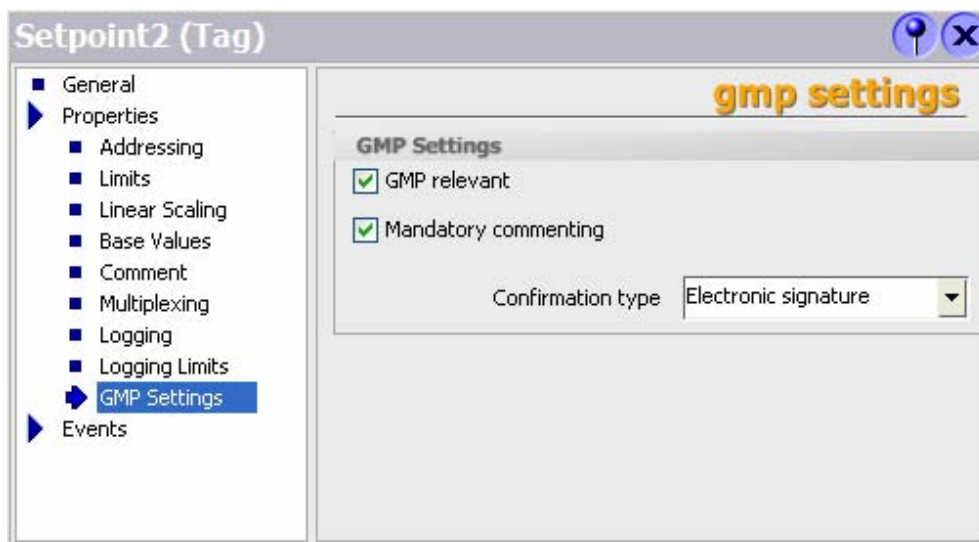


Fig. 3 : Une variable est définie comme importante pour le GMP afin qu'une entrée soit générée dans l'Audit Trail chaque fois que l'opérateur modifiera sa valeur.

L'Audit Trail est mémorisé sous forme de fichier CSV. Un algorithme intégré calcule automatiquement un total de contrôle par enregistrement et permet de reconnaître les modifications manuelles des enregistrements. Il est possible de mémoriser les données sur des ressources externes de réseau, ce qui assure une gestion simple de la sauvegarde et de l'archivage.

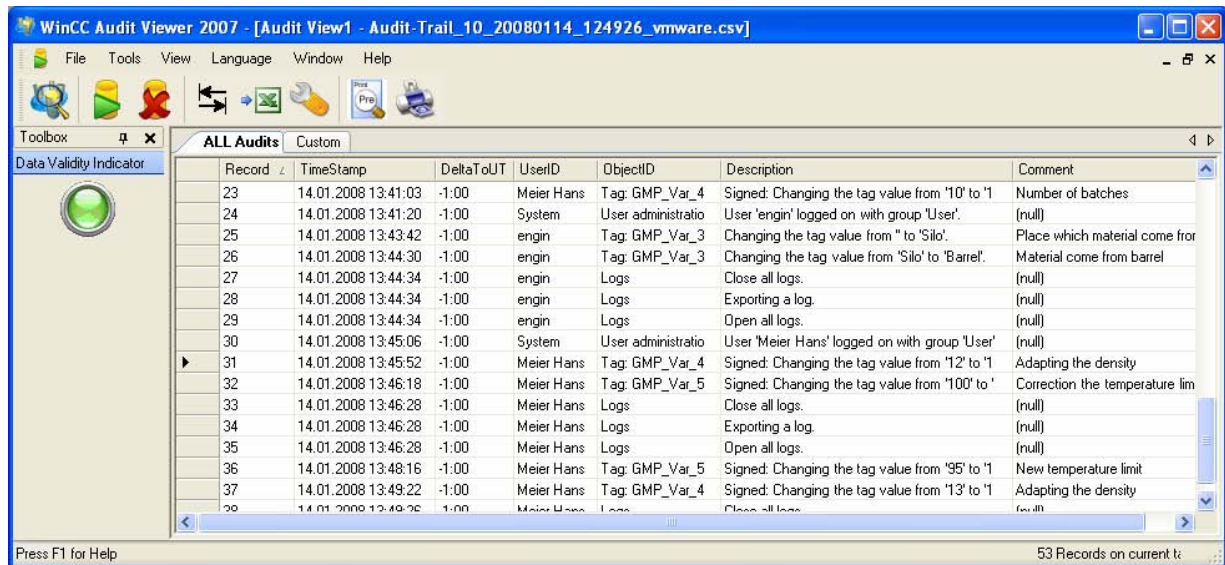
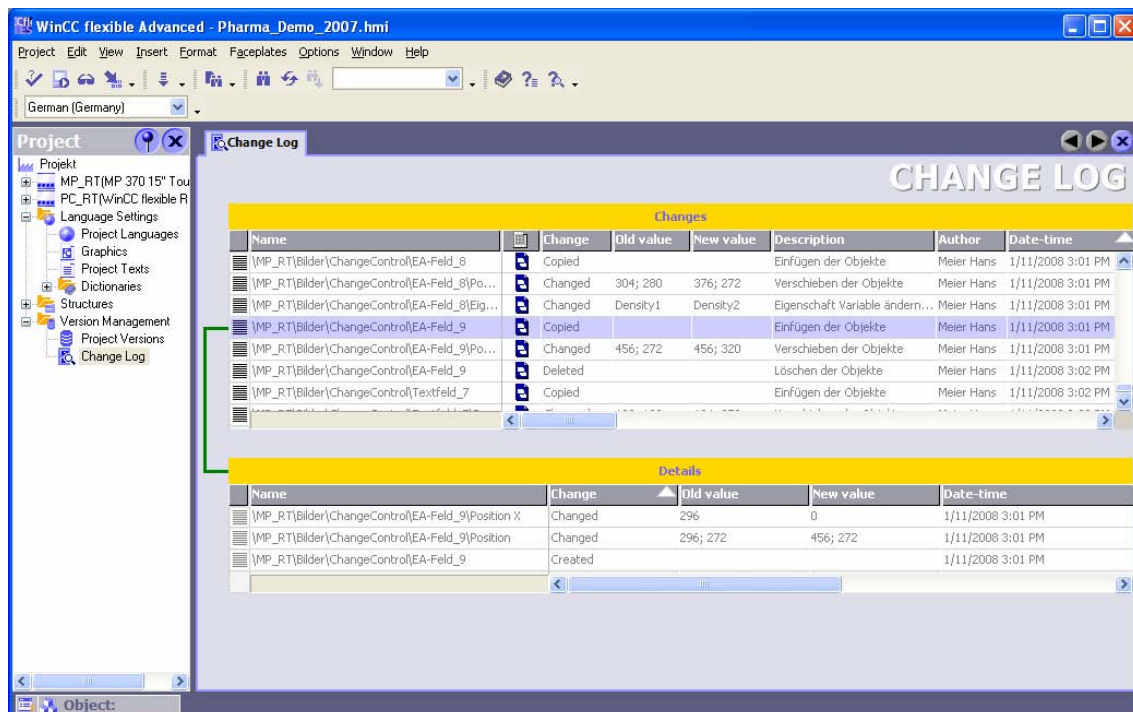


Fig. 4 : L'Audit Viewer affiche l'Audit Trail et confirme par le témoin vert qu'il n'a pas été manipulé.

**Phase de configuration**

Avec l'option Change Control de WinCC flexible 2007, vous pouvez consigner les modifications apportées aux projets WinCC flexible 2007, par ex. aux archives, aux vues des alarmes et aux graphiques, à la définition des droits d'accès, etc. Les versions du projet sont entièrement reproductibles et récupérables. En outre, la version en question peut être identifiée dans l'Audit Trail du runtime.



La figure 5 montre le journal qui consigne les modifications apportées à la configuration.

## 2.3 Solution technologique pour l'archivage et pour la relecture des données archivées

### Données de processus

A l'aide d'une commande manuelle ou bien déclenchée par horloge ou par le processus, les données de processus acquises (alarmes, valeurs de processus) peuvent être sauvegardées au format CSV dans une archive à long terme, sur des supports de données locaux ou via le réseau. Suivant la longueur de la période archivée, les données de processus peuvent être rangées dans des archives suite ou dans des archives circulaires, soit comme fichiers CSV, soit dans des bases de données ODBC (par ex. serveur MS SQL) pour les projets PC. Vous pouvez utiliser tous les supports de mémorisation à long terme pris en charge par Windows.

Les enregistrements de recette (paramètres) sont gérés par le système dans un format interne et peuvent être exportés et importés sur demande au format CSV.

Dans le cas de l'archivage à long terme local, les données de processus peuvent continuer à être affichées sur le pupitre. Pour l'archivage à long terme via le réseau, l'affichage des données est possible à l'aide d'un programme de tableur, ou elles peuvent être importées et affichées par le Premium Add-on PM-QUALITY.

### Audit Trail

Les interventions opérateur au runtime sont consignées dans l'Audit Trail en tant qu'archive sans fin. L'appareil IHM transfère ces données à un PC quelconque du réseau ou sur le support de stockage interne (carte CF) avec une commande par horloge ou par capacité. Depuis ce lieu, vous pouvez indiquer un chemin de votre choix pour le lieu de stockage du fichier d'Audit Trail afin de garantir la disponibilité de ces données. Il est possible de les sauvegarder du lieu de stockage sur d'autres supports de mémorisation, comme par ex. des CD. Les données Audit Trail peuvent être affichées et imprimées avec le WinCC Audit Viewer.

## 2.4 Solution technologique pour les signatures électroniques

WinCC flexible 2007 permet à l'utilisateur de signer électroniquement les actions qu'il effectue. Au cours de la phase de configuration, le concepteur détermine pour quelles variables il faudra confirmer une modification par une signature électronique. L'utilisateur peut apposer sa signature électronique en confirmant son intention d'agir par son mot de passe. De cette façon, la signature électronique est mémorisée dans l'Audit Trail avec l'utilisateur, l'action effectuée et un commentaire complémentaire. Ce commentaire peut être défini comme facultatif ou obligatoire.

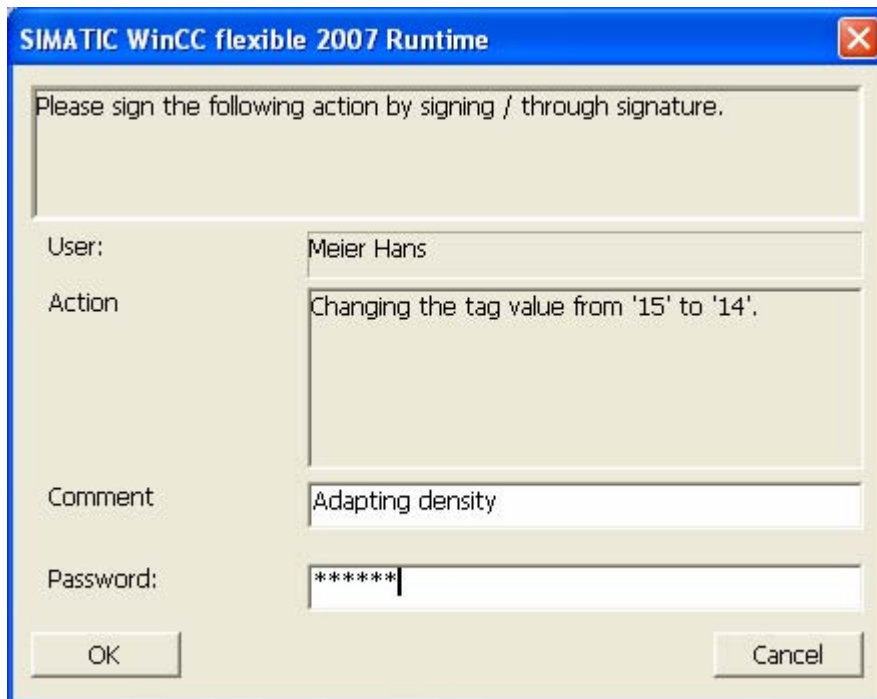


Fig. 6 : La modification de la valeur d'une variable est à confirmer par une signature électronique, compte tenu du commentaire obligatoire.

### 3 Liste d'évaluation pour SIMATIC WinCC flexible 2007

Les questions ou exigences de la liste de contrôle suivante pour l'évaluation de la conformité Part 11 de SIMATIC WinCC flexible 2007 proviennent du Good Practice Guide de l'ISPE et la PDA<sup>4</sup>.

Pour répondre à certaines exigences de la réglementation 21 CFR Part 11, le client devra introduire des instructions méthodologiques appropriées dans son entreprise. Les directives du 21 CFR Part 11 se réfèrent toujours à l'application spécifique au client qui a été réalisée avec WinCC flexible 2007. C'est pourquoi les solutions indiquées ci-après ne sont valables que combinées aux instructions méthodologiques spécifiques correspondantes citées et à des mesures organisationnelles.

#### 3.1 Méthodes et mesures pour les systèmes fermés

Si l'accès au système est contrôlé par des personnes responsables du contenu des enregistrements électroniques, on dit que le système est "fermé" et il faut l'évaluer en fonction des exigences énoncées dans ce paragraphe.

Paragraphe / Point	Questions / Exigences	Commentaires
11.10(a) Point 1	Le système est-il validé ?	La validation des applications/du système incombe au client. La validation doit suivre un modèle de cycle de vie du système (System Life Cycle) établi par ex. comme décrit dans GAMP 4 <sup>5</sup> . SIMATIC WinCC flexible 2007 a été développé conformément au système de gestion de qualité de Siemens (certifié ISO 9001:2000). Siemens peut apporter son aide pour la validation de l'application lors des projets.

---

<sup>4</sup> *Good Practice and Compliance for Electronic Records and Signatures ; Partie 2 "Complying with 21 CFR Part 11, Electronic Records and Electronic Signatures" ; ISPE et PDA 2001/2002*

<sup>5</sup> *GAMP 4 Guide for Validation of Automated Systems, ISPE 2001*

Paragraphe / Point	Questions / Exigences	Commentaires
11.10(a) Point 2	Est-il possible de reconnaître des enregistrements non valables ou modifiés ?	<p>Oui.</p> <p>En consignnant les interventions de l'opérateur dans un Audit Trail. L'Audit Trail Viewer permet d'afficher les enregistrements contenus. Les données à consigner dans l'Audit Trail sont repérées lors de la configuration par l'activation du drapeau "Important pour le GMP". Pour chaque enregistrement, un total de contrôle est calculé et intégré à l'Audit Trail. De cette manière, les manipulations éventuelles sont identifiables dans l'Audit Trail. Les informations requises sont mémorisées pour les différents enregistrements, par ex. le nom d'objet, l'ancienne valeur, la nouvelle valeur, l'horodatage, le nom d'utilisateur et un commentaire facultatif de la modification.</p> <p>L'option Change Control permet de tracer les modifications dans la configuration de WinCC flexible.</p>
11.10(b) Point 1	Le système est-il en mesure d'établir sur papier des copies exactes et complètes d'enregistrements électroniques ?	<p>Oui.</p> <p>Les données de processus (valeurs de processus, alarmes et messages) peuvent être transférées sur une ressource réseau et sont ainsi disponibles pour impression par d'autres applications.</p> <p>L'Audit Trail peut être affiché et imprimé avec le WinCC Audit Viewer.</p>
11.10(b) Point 2	Le système est-il en mesure d'établir des copies exactes et complètes d'enregistrements sous forme électronique pour vérification, contrôle et copie par la FDA ?	<p>Oui.</p> <p>Les données de processus comme les enregistrements de l'Audit Trail sont générés en tant que fichiers CSV et peuvent être sauvegardés sur une ressource de réseau.</p>
11.10(c)	Les enregistrements sont-ils immédiatement disponibles durant leur durée de conservation ?	<p>Oui.</p> <p>Le système utilise des ressources accessibles via un réseau pour stocker durablement les données.</p> <p>Les enregistrements peuvent être enregistrés à partir de ces ressources par ex. sur CD ou DVD. Nous supposons que les appareils de sortie et les formats seront encore lisibles à l'avenir.</p> <p>En outre, le client doit déterminer les durées de conservation et définir des procédés pour l'archivage, la sauvegarde et la relecture d'enregistrements électroniques.</p>

Paragraphe / Point	Questions / Exigences	Commentaires
11.10(d)	L'accès au système est-il limité aux personnes autorisées ?	Oui. En cas d'utilisation de la gestion centrale des utilisateurs avec SIMATIC Logon, vous avez recours à toutes les possibilités de gestion des utilisateurs de Windows. Pour la gestion locale des utilisateurs, la connexion au système n'est possible que pour des personnes habilitées, au moyen d'un nom d'utilisateur et d'un mot de passe. Dans ce cas, les paramètres de sécurité Runtime locaux sont utilisés (voir Chapitre 2, Solution technologique pour la protection d'accès). Le client doit garantir que seules des personnes pouvant justifier d'une habilitation au système (par ex. pupitres opérateur, système d'ingénierie) y ont accès physique. Comme l'exigence est pratiquement la même que 11.10(g), elle est conçue de manière générale de sorte à s'appliquer aussi bien à l'entrée physique qu'à l'accès logique.
11.10(e) Point 1	Existe-t-il un Audit Trail sécurisé, informatisé et muni d'un horodatage qui consigne le jour et l'heure des entrées opérateur et des actions créant, modifiant ou effaçant un enregistrement électronique ?	Oui. L'Audit Trail est sécurisé au sein du système et ne peut pas être modifié par un utilisateur. Les modifications pendant la production sont tracées par le système lui-même et contiennent les informations avec horodatage, nom d'utilisateur, ancienne et nouvelle valeur et commentaire.
11.10(e) Point 2	En cas de modification de données électroniques, les informations enregistrées auparavant restent-elles disponibles ? (ou sont-elles écrasées par la modification, par exemple ?)	Oui. En cas de modifications des valeurs de paramètres à l'aide de l'interface graphique, l'ancienne valeur et la nouvelle sont consignées dans l'Audit Trail. L'utilisateur ne peut pas modifier via l'interface graphique des données de processus enregistrées électroniquement.
11.10(e) Point 3	Les Audit Trails des enregistrements électroniques sont-ils disponibles pendant toute la durée de conservation des enregistrements ?	Oui. L'Audit Trail est disponible pendant toute la durée de conservation. (voir 11.10 (c))
11.10(e) Point 4	L'Audit Trail est-il à la disposition de la FDA à des fins de vérification et de copie ?	Oui. Cette disponibilité est assurée par la consignation dans un fichier CSV séparé.
11.10(f)	Quand la séquence des étapes système ou des événements a son importance, est-elle prise en considération par le système (comme c'est le cas dans un système de contrôle du processus, par exemple) ?	Oui. Il est possible de réaliser une suite déterminée de commandes opérateur en configurant l'application de manière appropriée.

Paragraphe / Point	Questions / Exigences	Commentaires
11.10(g)	Le système donne-t-il la garantie que seules des personnes autorisées peuvent l'utiliser et apposer leur signature électronique, avoir accès à la commande ou aux appareils d'entrée et de sortie du système informatique, modifier un enregistrement ou effectuer toute autre opération ?	Oui. WinCC flexible 2007 propose une gestion des utilisateurs avec groupes d'utilisateurs, autorisations et utilisateurs. Ceci règle de manière satisfaisante non seulement la gestion de l'accès au système, mais également celle des différentes autorisations. Pour apposer une signature électronique, il faut saisir un mot de passe. SIMATIC Logon permet de réaliser une gestion centrale des utilisateurs (voir 11.10 (d)).
11.10(h)	Quand une condition du système stipule que les données d'entrée ou les instructions ne doivent provenir que de certains appareils d'entrée (par ex. des terminaux), le système vérifie-t-il la validité de la source des données ou instructions reçues ?  (Remarque : ceci s'applique lorsque les données ou les instructions peuvent provenir de plus d'un appareil et que le système doit par conséquent vérifier l'intégrité de leur source, comme le réseau de balances de dosage ou de terminaux télécommandés ou radiocommandés.)	Oui. Les pupitres opérateur WinCC flexible sont configurables pour que des données de saisie / des commandes ne puissent être exécutées que par un utilisateur unique dédié ou un groupe de pupitres opérateurs dédiés. Tous les autres pupitres opérateurs disposent au plus de droits d'accès en lecture.
11.10(i)	Des cours de formation sont-ils proposés, y compris sur les applications, aux utilisateurs du système, développeurs, personnel du support technique IT ?	Oui. Siemens offre des cours de formation standard mais également des cours de formation spécifiques aux projets clients qui sont planifiés et se tiennent séparément. La responsabilité de planifier ces cours et d'y participer revient au client.
11.10(j)	Existe-t-il des dispositions écrites établissant l'entière responsabilité d'une personne pour les actes accomplis sous sa signature électronique ?	La mise en place d'instructions procédurales incombe au client.
11.10(k) Point 1	La diffusion des documents d'exploitation et de maintenance, leur accès et leur utilisation font-ils l'objet d'un contrôle pour le système ?	La mise en place d'instructions procédurales incombe au client.
11.10(k) Point 2	Existe-t-il un procédé de contrôle formel pour les modifications de la documentation du système établissant un Audit Trail chronologique des modifications de l'entreprise pharmaceutique ?	La mise en place d'instructions procédurales incombe au client.

### 3.2 Instructions procédurales complémentaires et mesures pour systèmes ouverts

Quand l'accès au système **N'EST PAS** contrôlé par des personnes responsables du contenu des enregistrements électroniques, on dit que le système est "ouvert" et il faut l'évaluer en fonction des exigences énoncées dans ce paragraphe. Nous supposons que WinCC flexible 2007 est mis en œuvre comme système fermé.

Paragraphe / Point	Questions / Exigences	Commentaires
11.30 Point 1	Les données sont-elles codées ?	WinCC flexible est conçu pour une utilisation dans des systèmes fermés. En cas d'utilisation de systèmes ouverts, le "chemin ouvert" du transfert de données à l'aide d'outils standard
11.30 Point 2	Des signatures électroniques sont-elles utilisées ?	WinCC flexible est conçu pour une utilisation dans des systèmes fermés. En cas d'utilisation de systèmes ouverts, le "chemin ouvert" du transfert de données à l'aide d'outils standard

### 3.3 Enregistrements électroniques signés

Voir le Chapitre 2 (Solution technologiques pour les signatures électroniques)

Paragraphe / Point	Questions / Exigences	Commentaires
11.50 Point 1	<p>Les enregistrements électroniques signés contiennent-ils les informations suivantes ?</p> <p>Nom imprimé du signataire</p> <p>Date et l'heure de l'apposition de la signature</p> <p>Signification de la signature (par ex. approbation, vérification, compétence)</p>	<p>Les enregistrements électroniques signés contiennent outre d'autres informations les indications suivantes :</p> <p>a) Nom d'utilisateur du signataire</p> <p>b) Date et horodatage de l'apposition de la signature</p> <p>c) Signification de la signature</p>
11.50 Point 2	<p>Les informations citées ci-dessus figurent-elles sur les copies affichées et imprimées de l'enregistrement électronique ?</p>	<p>Oui.</p> <p>Les informations citées ci-dessus font partie de l'Audit Trail et peuvent être imprimées et affichées.</p>
11.70	<p>La signature électronique est-elle liée à l'enregistrement électronique auquel elle s'applique, afin de garantir qu'elle ne pourra pas être séparée, copiée ni appliquée d'autre manière à d'autres enregistrements par intention frauduleuse ?</p>	<p>Oui.</p> <p>Au sein de l'Audit Trail, la signature électronique est un élément de l'enregistrement signé. Le total de contrôle intégré protège contre toute modification.</p>

### 3.4 Signatures électroniques (généralités)

Paragraphe / Point	Questions / Exigences	Commentaires
11.100(a) Point 1	Les signatures électroniques sont-elles associées sans équivoque à une seule personne ?	Oui. La signature électronique utilise le nom et le mot de passe de l'utilisateur. L'univocité du nom d'utilisateur est garantie en cas d'utilisation de SIMATIC Logon par le système de sécurité MS-Windows. Il est impossible de définir un utilisateur avec le même nom d'utilisateur au sein d'un groupe de travail / d'un domaine. En cas d'utilisation de la gestion locale des utilisateurs, l'univocité du nom d'utilisateur et la combinaison du nom d'utilisateur et du mot de passe est garantie avec WinCC flexible. Le client doit en outre garantir l'univocité de la signature électronique de la personne.
11.100(a) Point 2	Les signatures électroniques sont-elles réutilisées ultérieurement par une autre personne ou attribuées à une autre ?	Le client doit s'assurer qu'un nom d'utilisateur n'est jamais attribué à plusieurs personnes et en est responsable.
11.100(b)	L'identité d'une personne est-elle vérifiée avant qu'une signature électronique ne lui soit attribuée ?	Cela relève de la responsabilité du client. Des mesures organisationnelles doivent être prises.

#### 3.4.1 Signatures électroniques (non biométriques)

Paragraphe / Point	Questions / Exigences	Commentaires
11.200 (a)(1)(i)	Les signatures non biométriques se composent-elles au minimum de deux parties, telles que code ID et mot de passe ou carte ID et mot de passe ?	Oui. SIMATIC Logon ou WinCC flexible identifie la personne au moyen de deux composants différents : nom d'utilisateur et mot de passe.
11.200 (a)(1)(ii)	Quand l'opérateur appose plusieurs fois sa signature au cours d'une même session, doit-il saisir son mot de passe à chaque fois ? (Remarque : pour la première signature dans une session, les deux éléments doivent être exécutés.)	Pour l'apposition d'une signature, le nom d'utilisateur de l'opérateur connecté est toujours fourni par le système. Le mot de passe doit être saisi de nouveau pour chaque signature.
11.200 (a)(1)(iii)	Quand les signatures ne sont pas apposées dans une même session, faut-il exécuter les deux éléments de la signature électronique pour chaque signature ?	Le nom d'utilisateur est toujours fourni par le système et seul le mot de passe doit être saisi.

Paragraphe / Point	Questions / Exigences	Commentaires
11.200 (a)(2)	Les signatures non biométriques sont-elles utilisées uniquement par leurs propriétaires authentiques ?	Le client est responsable de la mise à disposition d'instructions méthodologiques qui interdisent la divulgation de mots de passe.
11.200 (a)(3)	Une tentative de contrefaçon de la signature électronique nécessite-t-elle la coopération de deux personnes au moins ?	Oui. Il n'est pas possible de contrefaire une signature électronique lors de la signature. L'administrateur ne peut pas utiliser abusivement la signature même s'il crée le nom d'utilisateur et le mot de passe initial car l'utilisateur est obligé de modifier le mot de passe à la première connexion. L'utilisation non autorisée de noms d'utilisateur / mots de passe (échecs de tentatives de connexion) est détectée immédiatement et consignée. Une tentative de contrefaçon par des administrateurs après la mémorisation provoquerait une modification du total de contrôle et serait donc remarquée. En outre, le client est responsable de la mise à disposition d'instructions méthodologiques qui interdisent la divulgation de mots de passe.

### 3.4.2 Signatures électroniques (biométriques)

Paragraphe / Point	Questions / Exigences	Commentaires
11.200(b)	Les signatures électroniques biométriques peuvent-elles être utilisées uniquement par leur propriétaire authentique ?	Actuellement, WinCC flexible ne prend pas en charge les procédés de signature biométrique.

### 3.5 Contrôles des codes ID et des mots de passe

Quand le système utilise des jetons, des cartes ou autres appareils pour signatures électroniques contenant ou générant un code ID ou des informations de mot de passe, il faut l'évaluer en fonction des exigences énoncées dans ce paragraphe.

Paragraphe / Point	Questions / Exigences	Commentaires
11.300(a)	Existe-t-il des contrôles pour défendre l'univocité de chaque combinaison code ID / mot de passe, de sorte que personne d'autre ne peut avoir la même combinaison code ID / mot de passe ?	Voir 11.100(a). La création d'instructions méthodologiques incombe au client.
11.300(b) Point 1	Existe-t-il des procédés pour garantir que la validité des codes ID est vérifiée régulièrement ?	La création d'instructions méthodologiques incombe au client.
11.300(b) Point 2	Les mots de passe sont-ils périmés à intervalles réguliers et font-ils l'objet d'une vérification ?	Oui. La validité d'un mot de passe expire après un nombre de jours paramétrable et ne peut plus être utilisé pour un nombre de générations paramétrable.
11.300(b) Point 3	Existe-t-il un procédé pour annuler codes ID et mots de passe quand un collaborateur quitte l'entreprise ou change de poste ?	Oui. Des comptes utilisateur peuvent être désactivés en cas d'utilisation de SIMATIC Logon pour la gestion centrale des utilisateurs en liaison avec le système de sécurité MS-Windows. Si la gestion des utilisateurs de WinCC flexible est utilisée, le verrouillage d'accès utilisateur n'est pas possible. Mais il est possible de créer un groupe d'utilisateurs sans autorisations actives et d'affecter un tel collaborateur à ce groupe. Ainsi, les données du collaborateur en question demeurent dans l'historique du système, mais il n'est plus en mesure d'exécuter dans le système des actions non autorisées. La création d'instructions méthodologiques incombe au client.
11.300(c)	Existe-t-il un procédé pour modifier un code ID ou un mot de passe quand il a éventuellement été divulgué ou qu'il a été perdu ?	Oui. L'opérateur peut modifier lui-même son mot de passe à tout moment quand il soupçonne qu'il n'est plus sûr. La modification (réinitialisation) par les administrateurs en cas d'oubli est possible à tout moment. La "désactivation" d'un nom d'utilisateur sera effectuée à l'aide des mesures de gestion, comme il est dit au paragraphe 11.300(b) article 3.

Paragraphe / Point	Questions / Exigences	Commentaires
11.300(d) Point 1	Existe-t-il un procédé pour détecter les tentatives d'accès non autorisées et en informer le système de sécurité ?	Oui. Les tentatives d'accès erronées sont consignées dans l'Audit Trail où elles peuvent être identifiées et tracées. Le compte utilisateur est verrouillé après un certain nombre de tentatives erronées. En outre, le client est responsable de la mise en place des mesures organisationnelles correspondantes.
11.300(d) Point 2	Existe-t-il un procédé pour signaler à l'administrateur les tentatives répétées ou graves d'utilisation non autorisée ?	Le client est responsable de la mise en place des mesures organisationnelles correspondantes.

### Abréviations utilisées

CF : Compact Flash

CFR : Code of Federal Regulations

CoP : Community of Practice

CSV : Comma Separated Values

FDA : Food and Drug Administration

GAMP : Good Automated Manufacturing Practice

GMP : Good Manufacturing Practice

HMI : Human Machine Interface

ID : Identification

ISO : International Organization for Standardization

ISPE : International Society for Pharmaceutical Engineering

IT : Information Technology

ODBC : Open Database Connectivity

PDA : Parenteral Drug Association (aujourd'hui "International Association for Pharmaceutical Science and Technology")

SQL : Structured Query Language