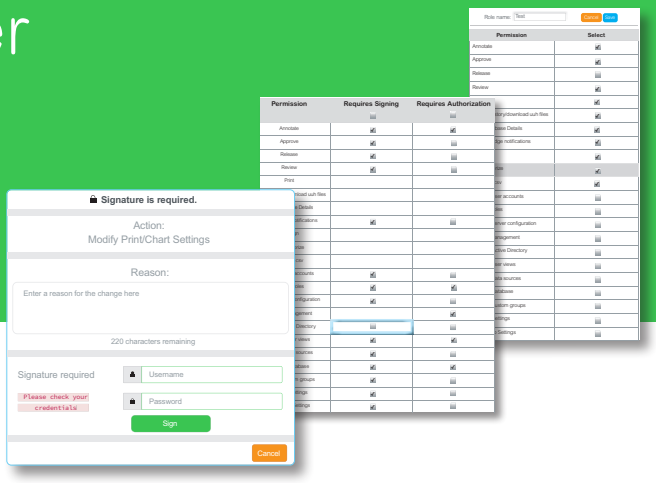
Eurotherm Data Reviewer & FDA 21 CFR Part 11

(Option Auditor)



Eurotherm®

Expertise en systèmes & solutions, services & support

Optimisez l'efficacité opérationnelle avec des solutions de gestion de données avancées

Conformité réglementaire

Dans le cadre d'un engagement continu pour aider à se conformer au code américain des réglementations fédérales de la FDA (Food & Drug Administration) et spécifiquement aux exigences FDA 21 CFR Part 11, ce document démontre comment l'expertise d'Eurotherm aide les clients à répondre aux différentes exigences de la FDA 21 CFR Part 11.

Chaque sous-section considérée est répertoriée dans l'en-tête des tableaux ci-dessous et les déclarations de chaque tableau sont accompagnées d'un commentaire démontrant comment la solution Eurotherm facilite la mise en conformité.

Sous-partie B - Enregistrements électroniques

11.10 Contrôle des systèmes fermés	
a) Validation des systèmes pour garantir la précision, la fiabilité et l'uniformité des performances prévues, et la capacité à discerner les enregistrements altérés ou invalides.	Eurotherm® propose une assistance pour la validation des produits selon les Bonnes Pratiques de Fabrication (BPF). Les données originales sont enregistrées dans des fichiers qui sont dans un format propriétaire, binaire, compressé et à somme de contrôle (checksum). Les détails ne sont pas publiés. L'outil de visualisation rejette les enregistrements invalides/modifiés (c'est-à-dire incorrectement vérifiés). Des tests approfondis sont effectués par Eurotherm (Certification ISO 9001). La validation (et la maintenance de l'état validé) est également supportée par l'incrémentation automatique des numéros de version de configuration/sécurité à chaque fois qu'une modification est enregistrée. Ces numéros sont stockés dans l'audit trail.
(b) La capacité de générer des copies exactes et complètes des enregistrements sous forme lisible par l'homme et sous forme électronique, pouvant être inspectées, examinées et copiées par l'agence. Les personnes doivent contacter l'agence en cas de questions concernant la capacité de l'agence à effectuer une telle revue et copie des enregistrements électroniques.	Des copies vraies, précises et complètes à l'écran ou sur papier sont disponibles en utilisant Eurotherm Data Reviewer. Des copies électroniques vraies, précises et complètes sont disponibles en copiant les fichiers de données brutes ou en configurant une 'imprimante PDF' (nécessite Adobe Acrobat ou similaire) afin d'exporter des graphiques au format PDF.
(c) Protection des enregistrements pour permettre leur récupération précise et rapide tout au long de la période de conservation des enregistrements.	Les données peuvent également être extraites périodiquement du produit à l'aide d'Eurotherm Data Reviewer. Une fois que les données ont quitté l'enregistreur, la stratégie de sécurité et de sauvegarde des données reste la responsabilité de l'utilisateur.
(d) Limiter l'accès au système aux personnes autorisées.	Comptes utilisateurs individuels protégés par mot de passe.
(e) Utilisation d'audit trails sécurisés, générés par ordinateur et horodatés pour enregistrer indépendamment la date et l'heure des entrées de l'opérateur et des actions qui créent, modifient ou suppriment des enregistrements électroniques. Les modifications d'enregistrement ne doivent pas masquer les informations enregistrées précédemment. Une telle documentation sur l'audit trail doit être conservée pendant une période au moins aussi longue que celle requise pour les enregistrements électroniques en question et doit être disponible pour examen et copie par l'agence.	Audit trail inaltérable (intégré dans un fichier d'historique binaire), généré par ordinateur et horodaté, des accusés de réception des notifications, des connexions, des détails des signatures et des changements de configuration.

(f) Utilisation de vérifications opérationnelles du système pour appliquer le séquencement autorisé des étapes et des événements, selon les cas.	Si nécessaire, une deuxième signature d'autorisation peut être appliquée, qui est également enregistrée dans l'audit trail.
(g) Recours à des contrôles d'autorisation pour s'assurer que seules les personnes autorisées peuvent utiliser le système, signer électroniquement un enregistrement, accéder au fonctionnement ou au dispositif d'entrée ou de sortie du système informatique, enregistrer ou effectuer l'opération concernée.	Comptes utilisateurs individuels protégés par mot de passe. Chaque utilisateur peut avoir son propre ensemble d'autorisations ou de privilèges d'accès pour personnaliser ce qu'il peut faire dans l'application.
(h) Utilisation de vérifications de l'appareil (par exemple, terminal) pour déterminer, le cas échéant, la validité de la source de données ou les instructions opérationnelles.	Les événements sont enregistrés. L'accès à la configuration de Data Reviewer est contrôlé et les modifications apportées sont enregistrées dans l'audit trail.
(i) Détermination que les personnes qui développent, entretiennent ou utilisent des systèmes d'enregistrement électronique / de signature électronique ont les connaissances, la formation et l'expérience nécessaires pour accomplir les tâches qui leur sont assignées.	Suivant procédure.
(j) L'établissement et le respect de politiques écrites qui maintiennent les individus responsables des actions initiées sous leurs signatures électroniques, afin de détecter les falsifications de dossiers et de signatures.	Suivant procédure. Cependant, Microsoft® Active Directory peut être utilisé pour gérer les procédures de connexions et de mots de passe. vous pouvez également définir votre procédure de connexion / de mot de passe dans Data Reviewer.
(k) Utilisation de contrôles appropriés sur la documentation des systèmes comprenant: (1) Contrôles adéquats sur la distribution, l'accès et l'utilisation de documentation pour le fonctionnement et la maintenance du système. (2) Procédures de contrôle de révision et de changement pour maintenir un audit trail qui documente le développement chronologique et les modifications de la documentation des systèmes.	Selon procédure conformément aux directives et au dossier ISPE Gamp © 5 et à la gestion de la somme de contrôle (checksum) de la configuration du fichier lors du contrôle des modifications.

11.30 Contrôles pour systèmes ouverts	
Les personnes qui utilisent des systèmes ouverts pour créer, modifier, conserver ou transmettre des enregistrements électroniques doivent utiliser des procédures et des contrôles conçus pour garantir l'authenticité, l'intégrité et, selon les cas, la confidentialité des enregistrements électroniques du point de leur création jusqu'au moment de leur réception. Ces procédures et contrôles doivent inclure ceux identifiés dans la Sec. 11.10, selon les cas, et des mesures supplémentaires telles que le cryptage des documents et l'utilisation de normes de signatures numériques appropriées pour garantir, si nécessaire selon les circonstances, l'enregistrement de l'authenticité, de l'intégrité et de la confidentialité.	L'application est destinée à être utilisée dans des systèmes fermés. Avec des systèmes/procédures externes appropriés, l'application peut être utilisée dans un système ouvert.

11.50 Démonstrations signature	
(a) Les enregistrements électroniques signés contiennent des informations avec la signature qui indique clairement tout ce qui suit : (1) Le nom imprimé du signataire; (2) la date et l'heure de la signature ; (3) La signification (telle que révision, approbation, responsabilité ou auteur) associée à la signature.	Les enregistrements signés, contenant le nom imprimé (ID utilisateur), la date, l'heure et la signification sont attribuables à un individu. La signification inclut signé/autorisé ensemble avec un type généré automatiquement (par exemple, "config" pour un changement de configuration), ainsi qu'une note entrée par l'opérateur (désignée comme : annotation, approbation, révision, publication).
(b) Les éléments identifiés aux alinéas (a) (1), (a) (2) et (a) (3) du présent article sont soumis aux mêmes contrôles que pour les enregistrements électroniques et doivent être inclus dans toute forme lisible par l'homme de l'enregistrement électronique (comme l'affichage électronique ou l'impression).	Le nom (ID utilisateur), l'horodatage et la signification sont tous intégrés dans le fichier d'historique au format binaire.

11.70 Lien signature/enregistrement	
Les signatures électroniques et les signatures manuscrites exécutées sur des enregistrements électroniques doivent être liées à leurs enregistrements électroniques respectifs afin de garantir que les signatures ne peuvent pas être excisées, copiées ou bien transférées pour falsifier un enregistrement électronique par des moyens ordinaires.	La démonstation de la signature est intégrée dans le fichier d'historique au format binaire. Pour les systèmes hybrides, les impressions créées via Eurotherm Data Reviewer pour les signatures manuscrites contiendront toujours les détails d'horodatage qui permettent la recréation à partir des données d'origine.

Sous-partie C - Enregistrements électroniques

11.100 Exigences générales	
(a) Chaque signature électronique doit être unique à une personne et ne doit pas être réutilisée ou réaffectée à quelqu'un d'autre. (b) Avant qu'une organisation ne crée, attribue, certifie ou bien sanctionne la signature électronique d'un individu ou tout élément de signature électronique, l'organisation vérifie l'identité de la personne.	Eurotherm Data Reviewer satisfait à cette exigence, car les comptes utilisateurs ne peuvent pas avoir le même nom d'utilisateur. Les comptes arrivés à expiration restent dans le système et sont définis comme 'retirés'. Le nombre de comptes utilisateurs n'est pas limité dans le logiciel. Suivant procédure.
(c) Les personnes utilisant des signatures électroniques doivent, avant ou au moment de cette utilisation, certifier à l'agence que les signatures électroniques dans leur système, utilisées le 20 août 1997 ou après, sont destinées à être l'équivalent juridiquement contraignant des signatures manuscrites. (1) L'attestation doit être soumise sur papier et signée avec une signature manuscrite traditionnelle, au Bureau des opérations régionales (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. (2) Les personnes utilisant des signatures électroniques doivent, sur demande de l'agence, fournir une certification ou un témoignage supplémentaire qu'une signature est l'équivalent juridiquement contraignant de la signature manuscrite du signataire.	Suivant procédure.

11.200 Composants et contrôle de la signature électronique	
(1) Employer au moins deux éléments d'identification distincts tels qu'un code d'identification et un mot de passe. **(i)** Lorsqu'un individu exécute une série de signatures au cours d'une seule période continue d'accès contrôlé au système, la première signature doit être exécutée à l'aide de tous les composants de signature électronique; les signatures ultérieures doivent être exécutées à l'aide d'au moins un composant de signature électronique qui n'est exécutable que par et conçu pour être utilisé uniquement par la personne. **(ii)** Lorsqu'un individu exécute une ou plusieurs signatures non effectuées pendant une seule période continue d'accès contrôlé au système, chaque signature doit être exécutée à l'aide de tous les composants de la signature électronique.	Nécessite une nouvelle saisie de l'ID utilisateur et du mot de passe lors d'une signature. Les deux composants seront requis pour toutes les signatures.
(2) N'être utilisé que par leurs véritables propriétaires.	Les utilisateurs peuvent uniquement modifier leurs propres mots de passe et aucun accès en lecture aux autres mots de passe des utilisateurs n'est fourni. Il est également possible que les connexions expirent après une période d'inactivité définie, pour limiter le nombre de tentatives de connexion avant qu'un compte ne soit désactivé, pour définir une longueur minimale pour les mots de passe, et pour forcer l'expiration du mot de passe après un nombre de jours défini , empêcher la réutilisation du mot de passe et forcer l'utilisation de caractères non alphanumériques. Eurotherm Data Reviewer peut également utiliser Microsoft Active Directory pour gérer l'authentification des utilisateurs.
(3) Être administré et exécuté pour garantir que toute tentative d'utilisation de la signature électronique d'une personne par une autre personne que son véritable propriétaire nécessite la collaboration de deux personnes ou plus.	Les utilisateurs peuvent uniquement modifier leurs propres mots de passe et aucun accès en lecture aux autres mots de passe des utilisateurs n'est fourni. À moins qu'un utilisateur n'ait partagé son mot de passe, une piste d'audit complète sera laissée. Avec l'option Auditor activée, il est en outre possible de forcer les changements d'administrateur système pour que les comptes utilisateurs soient autorisés par une deuxième personne.

11.300 Contrôles pour les codes d'identification/mots de passe	
Les personnes qui utilisent des signatures électroniques basées sur l'utilisation de codes d'identification en combinaison avec des mots de passe doivent utiliser des contrôles pour garantir leur sécurité et leur intégrité. Ces contrôles comprennent :	
(a) Maintenir l'unicité de chaque code d'identification et mot de passe combinés, de sorte que deux personnes n'aient pas la même combinaison de code d'identification et de mot de passe.	Les comptes utilisateurs sont retirés. Tous les noms d'utilisateurs sont forcés pour être uniques.
(b) Veiller à ce que les codes d'identification et les mots de passe soient vérifiés, rappelés ou révisés périodiquement (par exemple pour couvrir des événements tels que l'expiration du mot de passe).	Il est possible de forcer l'expiration du mot de passe après un nombre de jours défini. Si un utilisateur quitte l'entreprise, son compte peut être marqué comme retiré.
(c) Suivre les procédures de gestion des pertes pour annuler l'autorisation électronique des jetons, cartes et autres appareils perdus, volés, manquants ou potentiellement compromis qui portent ou génèrent des informations de code d'identification ou de mot de passe, et pour émettre des remplacements temporaires ou permanents à l'aide de contrôles appropriés et rigoureux.	Suivant procédure. Les comptes compromis peuvent être désactivés. Concernant la perte du mot de passe, l'administrateur peut en définir un nouveau pour le compte d'un utilisateur qui doit ensuite immédiatement le remplacer par un mot de passe qui lui est propre.
(d) Utilisation de garanties de transaction pour empêcher l'utilisation non autorisée de mots de passe et/ou de codes d'identification, et pour détecter et 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 gestion de l'organisation.	Il est possible que les connexions expirent après une période d'inactivité définie; pour limiter le nombre de tentatives de connexion avant qu'un compte ne soit désactivé; pour définir une longueur minimale pour les mots de passe; et pour forcer l'expiration du mot de passe après un nombre de jours défini. Les connexions infructueuses qui désactivent les comptes sont détaillées dans l'audit trail dans Eurotherm Data Reviewer.

Life Is On | Schneider Electric

Eurotherm Automation SAS

6 chemin des Joncs, CS20214
69574 Dardilly cedex
France
T. +33 (0)4 78 66 45 00

www.eurotherm.com

Publié en Décembre 2020

Document Réf. HA033530FRA indice 1