JUMO GmbH & Co. KG

Enregistreur sans papier LOGOSCREEN *es*

Déclaration de conformité 21 CFR Part 11

Livre blanc (*White Paper*)

Sommaire

Sommaire

1 Généralités

1.1 Introduction

Dans les industries pharmaceutique, alimentaire et dans les branches apparentées, les protocoles d'enregistrement des données de fabrication sont obligatoires.

Traditionnellement, l'enregistrement des données de process se faisait avec des enregistreurs à bande de papier. Les bandes enregistrées étaient archivées plusieurs dizaines d'années, de façon à assurer un suivi ininterrompu de la production et la traçabilité en cas d'écarts.

L'arrivée des enregistreurs sans papier a déplacé l'enregistrement du papier vers l'écran.

Le service de santé américain

« Food & Drug Administration (FDA) »

a édicté en 1997 le r**èglement 21 CFR Part 11** (*Code of Federal Regulations*) pour régir l'enregistrement normalisé et la traçabilité sans ambiguïté des données électroniques de process.

Ce règlement définit les exigences des **Electronic Records & Electronic Signature**, c'est-à-dire l'enregistrement sans papier des flux de production et une signature électronique qui correspond à la signature manuelle.

Le respect des critères du règlement 21 CFR Part 11 est devenu depuis ce temps dans le monde entier la base de l'acceptation des produits des industries pharmaceutique et alimentaire.

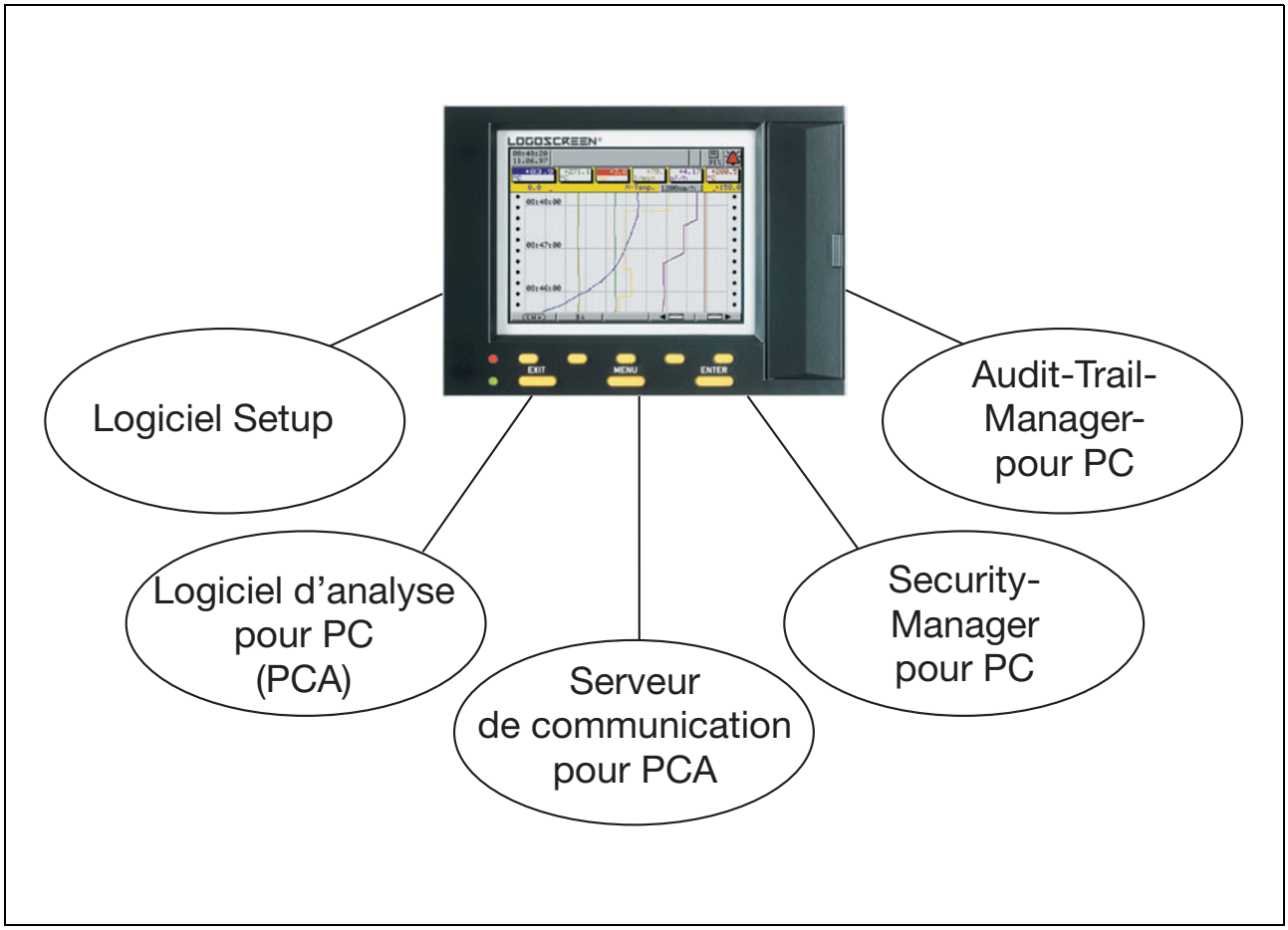
Le chapitre 3 de ce « Livre blanc » donne à l'utilisateur pour chaque section du règlement une indication de la réponse aux exigences.

1.2 Application du règlement 21 CFR Part 11

JUMO répond aux exigences du règlement 21 CFR Part 11 de la FDA, en ce qui concerne les enregistrements et la signature électroniques (Electronic Records, Electronic Signature), avec le nouvel enregistreur sans papier LOGOSCREEN *es* et les logiciels pour PC associés (logiciel Setup, logiciel d'analyse pour PC (PCA), serveur de communication pour PCA, assistant de sécurité (Security-Manager) et assistant de vérification (Audit-Trail-Manager)).

1.3 Composants du système LOGOSCREEN *es*

L'enregistreur **LOGOSCREEN *es***, avec ses composants système, représente un système fermé au sens du règlement 21CFR Part 11.



1.4 Composants logiciels pour PC

1.4.1 Logiciel Setup (pour la configuration de l'enregistreur)

- logiciel interactif de configuration de l'enregistreur
- les données de configuration peuvent être archivées sur un support de données et sorties sur imprimante.

1.4.2 Logiciel d'analyse sur PC pour le traitement des données de process (PCA)

- supervision, archivage et analyse des données enregistrées.

1.4.3 Serveur de communication pour PCA (permet la lecture des données)

- il permet la lecture des données par l'interface sérielle,
- la lecture peut être manuelle ou automatique, par exemple chaque jour à 23 heures 00,
- la lecture peut aussi s'effectuer à distance par modem.

1.4.4 Assistant de sécurité pour PC (Security-Manager, contrôle de l'accès au système)

- administre la liste d'utilisateurs du PC et de l'enregistreur,
- contrôle l'accès des utilisateurs aux logiciels PC et autorise ou interdit l'accès au système,
- assure l'authenticité des signatures électroniques.

1.4.5 Assistant de sécurité pour l'enregistreur (Recorder-Security-Manager, contrôle de l'accès à l'enregistreur)

- stocke la liste des utilisateurs dans l'enregistreur,
- contrôle l'accès à l'enregistreur et l'autorise ou l'interdit,
- assure l'authenticité des signatures électroniques.

1.4.6 Assistant de vérification sur PC (Audit-Trail-Manager, saisit et mémorise toutes les opérations)

- adjoint aux requêtes l'horodatage, le nom de l'utilisateur, les détails et la raison de la modification,
- mémorise et vérifie toutes les opérations effectuées par l'utilisateur.

2 Évaluation des exigences

Les développements qui suivent supposent que le lecteur possède une connaissance de base des exigences du règlement 21 CFR Part 11.

Section	Exigences : *Subpart B: Electronic Records* (Partie B : documents électroniques)
§ 11.10 *Controls for closed systems* (Contrôles de systèmes fermés)	
(a)	*Validation of systems to ensure accuracy, reliability, consistend intended performance, and the ability to discern invalid or altered records.* Validation de systèmes pour assurer l'exactitude, la fiabilité et la cohérence du fonctionnement et la capacité de détecter des enregistrements invalides ou altérés. Exigence satisfaite ! ✔ Le système, constitué d'un enregistreur sans papier (désigné par enregistreur dans la suite) et des logiciels PC associés, est validé de façon à garantir les performances annoncées en termes d'exactitude, fiabilité et continuité. ✔ Il est garanti que les enregistrements invalides ou altérés (par exemple par des tentatives de manipulation) sont reconnus, repérés dans l'assistant de vérification (Audit-Trail) et ne sont pas rendus disponibles pour l'analyse.
(b)	*The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.* Aptitude à produire des copies exactes et complètes des enregistrements, à la fois sous forme lisible pour l'homme et sous forme électronique pour l'inspection, la vérification et la copie par l'administration. On consultera l'administration s'il existe un doute sur la possibilité d'effectuer ces contrôles et de copier les documents électroniques. Exigence satisfaite ! ✔ Toutes les données sont mémorisées dans un format binaire propriétaire, non publié, sécurisé par des algorithmes de somme de contrôle. ✔ Les données de process sont lisibles sur l'enregistreur et sur PC. ✔ Le logiciel d'analyse pour PC de JUMO est disponible pour la représentation des données sur PC. Il permet de visualiser, copier et imprimer toutes les données mémorisées.

2 Évaluation des exigences

Section	Exigences : *Subpart B: Electronic Records* (Partie B : documents électroniques)
§ 11.10 *Controls for closed systems* (Contrôles de systèmes fermés)	
(c)	*Protection of records to enable their accurate and ready retrieval throughout the records retention period.* Protection des documents de façon à permettre une consultation exacte et immédiate tout au long de la période de rétention des enregistrements. Exigence satisfaite ! ✔ Les données sont mémorisées dans la mémoire interne de l'ordinateur. ✔ La mémoire interne de l'enregistreur ne contribue pas au transport des données. ✔ Les données archivées dans la mémoire interne peuvent être lues et archivées dans le PC par une personne autorisée, au moyen d'une liaison sérielle ou d'une carte Compact Flash. ✔ L'accès à la liaison sérielle est protégé par un nom d'utilisateur et un mot de passe ; l'accès à la carte Compact Flash est protégé par un verrouillage mécanique et une surveillance électronique. ✔ La sécurité de la manipulation des données est garantie par un format binaire propriétaire, non publié, sécurisé par des algorithmes de somme de contrôle. ✔ Les données recopiées sur la carte Compact Flash sont mémorisées dans un système PC pour l'archivage et l'analyse.
(d)	*Limiting system access to authorized individuals.* Accès au système réservé aux personnes autorisées. Exigence satisfaite ! ✔ L'accès au système est réservé aux personnes autorisées par l'attribution de différentes autorisations. ✔ Chaque utilisateur doit se connecter au système avec son nom d'utilisateur et son mot de passe. ✔ Les autorisations sont attribuées par l'administrateur et vérifiées lors de chaque accès par l'assistant de sécurité (Security-Manager). ✔ Seul l'administrateur peut modifier les droits des utilisateurs. ✔ Les données déjà collectées et archivées restent inchangées même en cas de changement des droits.

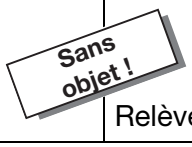
2 Évaluation des exigences

Section	Exigences : *Subpart B: Electronic Records* (Partie B : documents électroniques)
§ 11.10 *Controls for closed systems* (Contrôles de systèmes fermés)	
(e)	*Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.* Utilisation de traces de contrôle (Audit Trails) automatiques sécurisées, horodatées pour l'enregistrement indépendant des dates et heures des interventions, des saisies et actions de l'opérateur qui créent, modifient ou effacent des enregistrements électroniques. La modification d'enregistrements ne doit pas masquer une information enregistrée précédemment. Cette trace de contrôle sera conservée et sera disponible pour le contrôle et la copie par l'administration pendant un temps au moins égal au temps de conservation requis pour les enregistrements électroniques visés. Exigence satisfaite ! ✔ L'assistant de vérification (Audit-Trail) fait partie du logiciel de l'appareil et du logiciel pour PC (Audit-Trail distincts). La trace de contrôle est produite automatiquement et ne peut être ni modifiée ni désactivée par la configuration. ✔ Il est garanti que toutes les actions déclenchées par le personnel exploitant sont automatiquement captées et archivées avec la date et l'heure. ✔ Les traces de contrôle dans l'appareil ne peuvent être ni modifiées ni effacées. ✔ L'adjonction de textes / commentaires est possible par les personnes dûment autorisées après saisie de leur identification et de leur mot de passe. ✔ Toutes les données mémorisées dans la trace de contrôle de l'enregistreur sont prises en charge avec les données du process par le logiciel d'analyse pour PC de JUMO et restent disponibles pour l'exploitation. ✔ Les données de la trace de contrôle peuvent être rendues accessibles à tout moment par le logiciel d'analyse pour PC pour vérification.
(f)	*Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.* Utilisation de tests fonctionnels du système pour exécuter, le cas échéant, les séquences autorisées d'étapes et d'événements. Exigence satisfaite ! ✔ La séquence des étapes, comme par exemple le rapport de production d'un lot, est définie. ✔ Ainsi on peut déterminer par la configuration si une signature électronique doit être produite ou non pour le rapport de production d'un lot. Dans le cas où elle est nécessaire, elle peut par exemple ne pas être autorisée pour un rapport de production de lot en cours (par opposition à un rapport terminé). ✔ Autre cas : l'enregistreur peut être configuré pour demander à l'utilisateur, lors de la déconnexion, une signature électronique pour la plage de temps enregistrée.

2 Évaluation des exigences

Section	Exigences : *Subpart B: Electronic Records* (Partie B : documents électroniques)
§ 11.10 *Controls for closed systems* (Contrôles de systèmes fermés)	
(g)	*Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.* Contrôle d'autorisation pour vérifier que seules des personnes autorisées peuvent utiliser le système, apposer une signature électronique sur un enregistrement, accéder aux organes d'entrée ou de sortie de l'ordinateur ou de l'appareil, modifier un enregistrement ou effectuer une opération manuelle. Exigence satisfaite ! ✔ Les droits d'accès au système sont attribués par l'administrateur. ✔ Ces droits d'accès sont vérifiés et administrés par l'assistant de sécurité (Security-Manager) dans l'enregistreur ou dans le PC. ✔ Seules les personnes titulaires des droits administrateur peuvent créer ou effacer des listes d'utilisateurs. ✔ L'accès d'un utilisateur au système est toujours conditionné par la connexion avec une identification unique (identité et mot de passe). ✔ La validité d'un mot de passe peut être limitée dans le temps par l'administrateur. Après ce délai, l'utilisateur doit fournir un nouveau mot de passe, sans quoi il perd ses droits d'accès.
(h)	*Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.* Utilisation d'appareils (par exemple terminaux) pour déterminer, le cas échéant, la validité de la source des données d'entrée ou des instructions de fonctionnement. Exigence satisfaite ! ✔ L'enregistreur ne peut être configuré ou utilisé que par la personne habilitée à cet effet. C'est valable aussi pour le raccordement des lignes de capteurs ou câbles d'interface sur la face arrière protégée de l'enregistreur. ✔ Les données mémorisées dans l'enregistreur sont accompagnées automatiquement par un numéro d'identification de l'appareil (numéro de série) unique et définitif.
(i)	*Determination that persons who develop, maintain, or use electronic record / electronic signature systems have the education, training, and experience to perform their assigned tasks.* Assurance que les personnes qui développent, entretiennent ou utilisent des systèmes d'enregistrement et de signature électroniques ont le niveau d'instruction, la formation et l'expérience requis pour accomplir les tâches qui leur sont assignées. Exigence satisfaite ! ✔ Toutes les personnes impliquées dans le développement du LOGOSCREEN *es* ont reçu une formation relative au contenu et aux exigences du règlement 21 CFR Part 11. ✔ Des formations correspondantes sont également proposées aux utilisateurs du LOGOSCREEN *es*.

2 Évaluation des exigences

Section	Exigences : *Subpart B: Electronic Records* (Partie B : documents électroniques)
§ 11.10 *Controls for closed systems* (Contrôles de systèmes fermés)	
(j)	*The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.* Instauration et acceptation d'engagements écrits qui rendent les personnes responsables des actions effectuées sous leur signature électronique, comme dissuasion contre la falsification des enregistrements et signatures.  Relève de la responsabilité de l'utilisateur.
(k)	*Use of appropriate controls over systems documentation including:* *(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.* *(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.* Exécution des contrôles appropriés sur la documentation du système, y compris : (1) Contrôle adéquat sur la distribution, l'accessibilité et l'utilisation de la documentation relative à l'exploitation et à la maintenance du système. (2) Procédures de révision et de modification pour tenir à jour une trace datée du développement et des modifications de la documentation.  Relève de la responsabilité de l'utilisateur.

2 Évaluation des exigences

Section	Exigence : *Subpart B: Electronic Records* (Partie B : documents électroniques)
§ 11.30 *Controls for open systems* (Contrôles de systèmes ouverts)	
	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. Si des systèmes ouverts sont utilisés pour créer, modifier, mettre à jour ou transmettre des documents électroniques, les procédures et contrôles mis en œuvre seront conçus de façon à assurer l'authenticité, l'intégrité et le cas échéant la confidentialité, depuis le moment de la création des documents électroniques jusqu'à leur réception. Ces procédures et contrôles incluront celles du paragraphe 11.10 quand elles s'appliquent, et des mesures additionnelles telles que le cryptage et les normes de signature numérique en vue de garantir, en fonction des circonstances et des nécessités, l'authenticité, l'intégrité et la confidentialité des enregistrements. Sans objet ! Le LOGOSCREEN *es* et les logiciels PC associés constituent un système fermé.

2 Évaluation des exigences

Section	Exigences : *Subpart B: Electronic Records* (Partie B : documents électroniques)
§ 11.50 *Signature manifestations* (Formes de signatures)	
(a)	*Signed electronic records shall contain information associated with the signing that clearly indicates of the following:* *(1) The printed name of the signer;* *(2) The date and time when the signature was executed; and* *(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.* Les documents électroniques signés doivent contenir des informations liées à la signature qui indiqueront clairement : (1) Le nom du signataire en lettres capitales. (2) La date et l'heure d'apposition de la signature. (3) La signification de la signature (par exemple vérification, agrément, responsabilité ou création). Exigence satisfaite ! ✔ La signature électronique attachée aux enregistrements est représentée en clair sur l'enregistreur ou par l'intermédiaire du logiciel d'analyse pour PC. La signature électronique comporte dans tous les cas le nom du signataire en capitales, la date et l'heure, à la seconde près, de l'apposition de la signature, de même que sa signification. Des lots, intervalles de temps ou commentaires peuvent être associés à des signatures électroniques. Les manipulations sont impossibles puisque l'enregistreur et les logiciels PC utilisent leur propre horodateur. Une modification de l'heure de l'enregistreur suppose que l'utilisateur est habilité. Chaque modification est enregistrée de façon indélébile dans la trace de contrôle.

2 Évaluation des exigences

Section	Exigences : *Subpart B: Electronic Records* (Partie B : documents électroniques)
§ 11.50 *Signature manifestations* (Formes de signatures)	
(b)	*The items identified in paragraphs (a)(1), (a)(2) and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).* Les points spécifiés dans les alinéas (a)(1), (a)(2) et (a)(3) de ce paragraphe seront soumis aux mêmes contrôles que les documents électroniques et fournis sous une forme lisible par l'homme (affichage ou impression). Exigence satisfaite ! ✔ La signature électronique fait partie intégrante des données brutes de l'enregistreur. ✔ Les données brutes de l'enregistreur sont constituées par l'enregistrement électronique, la signature électronique, les données de la trace de contrôle et la somme de contrôle. Le format est créé dans l'enregistreur et il est utilisé sans altération possible pour le transfert et le stockage des données sur le PC. ✔ Les données brutes de l'enregistreur, signature électronique comprise, sont enregistrées dans un format binaire propriétaire, non publié et vérifié par des algorithmes de somme de contrôle. Les données brutes de l'enregistreur, avec la signature électronique indélébile, sont à l'abri de la manipulation. ✔ La signature électronique est ajoutée à la version lisible – dérivée des données brutes — du document électronique (affichage ou impression). ✔ L'impression papier et l'édition électronique (format PDF) indiquent qu'il s'agit d'une représentation dérivée des données brutes de l'enregistreur.

2 Évaluation des exigences

Section	Exigence : *Subpart B: Electronic Records* (Partie B : documents électroniques)
§ 11.70 *Signature/record linking* (liaison signature/document)	
	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means. Les signatures électroniques et manuelles des documents électroniques doivent être liées aux documents correspondants de façon à garantir qu'elles ne peuvent pas être retirées, copiées ou transférées pour falsifier un document électronique par des moyens ordinaires. Exigence satisfaite ! ✔ Les données brutes de l'enregistreur, y compris la signature électronique, sont enregistrées dans un format binaire propriétaire, non publié et vérifié par des algorithmes de somme de contrôle. ✔ Les données brutes de l'enregistreur, avec la signature électronique indélébile, sont à l'abri de la manipulation. ✔ L'enregistreur et les logiciels associés sur PC comportent des fonctions de l'assistant de sécurité (Security-Manager) avec les tâches obligatoires suivantes : Assistant de sécurité (Security-Manager) sur le PC - crée et administre la liste des utilisateurs du PC et de l'enregistreur - vérifie l'accès aux logiciels du PC et délivre les autorisations - assure l'authentification de la signature électronique Assistant de sécurité (Security-Manager) sur l'enregistreur - stocke la liste d'utilisateurs dans l'enregistreur - vérifie l'accès à l'enregistreur et délivre les autorisations - assure l'authentification de la signature électronique ✔ La restriction, par l'assistant de sécurité (Security-Manager), de l'accès à l'enregistreur et aux logiciels sur PC associés exclut la falsification et la copie d'une signature électronique par une personne isolée. ✔ L'enregistreur et les logiciels PC associés n'autorisent pas la modification ou la suppression d'une signature électronique. L'enregistreur et les logiciels PC associés détectent et affichent les tentatives de falsification ou de suppression d'une signature électronique. ✔ L'événement est enregistré dans la trace de contrôle et ne peut pas être effacé.

2 Évaluation des exigences

Section	Exigences : *Subpart B: Electronic Records* (Partie B : documents électroniques)
§ 11.100 *General requirements* (Prescriptions générales)	
(a)	*Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.* Chaque signature électronique doit être unique, attribuée à une personne, ne doit être ni réutilisée, ni attribuée à une autre personne. Exigence satisfaite ! ✔ L'assistant de sécurité (Security-Manager) pour PC permet à l'administrateur de définir les droits des utilisateurs sur l'enregistreur, leur mot de passe initial et les restrictions de leur mot de passe, de les rassembler, de les verrouiller dans une liste d'utilisateurs et de transférer cette liste dans l'enregistreur. ✔ L'assistant de sécurité pour PC garantit le caractère unique et univoque de la combinaison d'un nom d'utilisateur avec un mot de passe pour chaque utilisateur figurant dans la liste. ✔ L'administrateur peut retirer des droits aux utilisateurs mais pas les retirer de la liste. ✔ L'assistant de sécurité (Security-Manager) de l'enregistreur s'appuie sur la liste d'utilisateurs pour vérifier l'authenticité de la signature électronique.
(b)	*Before an organization establishes, assigns, certifies, or otherwise sanctions an in individual's electronic signature or any element of such signature, the organization shall verify the identify of the individual.* Avant d'établir, attribuer, certifier ou sanctionner de quelque façon la signature électronique d'une personne, un organisme doit vérifier l'identité de cette personne. Sans objet ! Relève de la responsabilité du propriétaire du système.
(c)	*Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.* Les personnes qui utilisent une signature électronique devront, avant cette utilisation ou au début, certifier à l'administration que les signatures électroniques de leur système, utilisées à partir du 20 août 1997, sont les équivalents légaux des signatures manuscrites traditionnelles. Sans objet ! Relève de la responsabilité du propriétaire du système.

2 Évaluation des exigences

Section	Exigences : *Subpart B: Electronic Records* (Partie B : documents électroniques)
§ 11.100 *General requirements* (Prescriptions générales)	
(1)	*The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.* La certification doit être présentée sur papier, avec une signature manuscrite traditionnelle, à l'Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. Sans objet ! Relève de la responsabilité du propriétaire du système.
(2)	*Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.* Les personnes qui utilisent des signatures électroniques devront, sur demande de l'administration, fournir un certificat ou une déclaration attestant qu'une signature électronique définie est l'équivalent légal de la signature manuscrite du signataire. Sans objet ! Relève de la responsabilité du propriétaire du système.

2 Évaluation des exigences

Section	Exigences : *Subpart B: Electronic Records* (Partie B : documents électroniques)
§ 11.200 *Electronic signature components and controls* **(Composants et contrôles de la signature électronique)**	
(a) (1)	*Electronic signatures that are not based upon biometrics shall:* *Employ at least two distinct identification components such as an identification code and password.* Les signatures électroniques qui ne sont pas basées sur la biométrie devront utiliser au moins deux éléments d'identification distincts, comme un code d'identification et un mot de passe. Exigence satisfaite ! ✔ La signature électronique ne peut être apposée que par un utilisateur habilité par l'administrateur, reconnu par le contrôle d'accès de l'enregistreur ou du PC (assistant de sécurité (Security-Manager)) au moyen de son identification et de son mot de passe.
(i)	*When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be excecuted using all electronic components; subsequent signings shall be excecuted using at least one electronic signature component that is only excecutable by, and designed to be used only by, the individual.* Quand une personne appose une série de signatures pendant une période unique et ininterrompue d'accès contrôlé au système, la première signature comportera tous les composants ; les signatures suivantes comporteront au moins un des composants, exécutable seulement par le signataire et conçu pour n'être utilisé que par lui. Exigence satisfaite ! ✔ Un seul utilisateur peut, à un instant donné, être autorisé par l'assistant de sécurité (Security-Manager) du PC ou de l'enregistreur à user des droits qui lui sont attribués. ✔ L'apposition d'une signature électronique n'est possible que par l'utilisateur connecté à l'enregistreur ou aux logiciels PC. Elle requiert, autant pour la première signature que pour toutes les suivantes, l'authentification complète par l'assistant de sécurité (Security-Manager) avec l'identification (nom d'utilisateur) et le mot de passe. ✔ Avant l'apposition d'une signature électronique, l'utilisateur est avisé par un texte de la suite des opérations : « Votre signature vous engage légalement comme l'équivalent de votre signature manuscrite ! ».

2 Évaluation des exigences

Section	Exigences : *Subpart B: Electronic Records* (Partie B : documents électroniques)
§ 11.200 *Electronic signature components and controls* **(Composants et contrôles de la signature électronique)**	
(ii)	*When an individual excecutes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be excecuted using all of the electronic signature components.* Quand une personne appose une ou plusieurs signatures électroniques en-dehors d'une période ininterrompue d'accès au système, chaque signature comportera tous les composants de la signature électronique. Exigence satisfaite ! ✔ L'apposition d'une signature électronique n'est possible que par l'utilisateur connecté à l'enregistreur ou aux logiciels PC. Elle requiert, autant pour la première signature que pour toutes les suivantes, l'authentification complète par l'assistant de sécurité (Security-Manager) avec l'identification (nom d'utilisateur) et le mot de passe.
(2) (3)	*Be used only by their genuine owners; and be adminstered and excecuted to ensure that attempted use of an individual's electronic signature by anyone other than it's genuine owner requires collaboration of two or more individuals.* Les signatures électroniques qui ne sont pas basées sur la biométrie ne pourront être utilisées que par leur véritable propriétaire ; elles seront administrées et exécutées de telle façon que l'utilisation par quiconque autre que le véritable propriétaire requière la collaboration de deux personnes ou plus. Exigence satisfaite ! ✔ Ceci est assuré par la façon, déjà décrite, de créer et d'administrer la liste d'utilisateurs, laquelle sert de base à l'authentification et à l'autorisation d'un utilisateur. ✔ Un utilisateur seul n'est pas en mesure d'utiliser une signature électronique autre que la sienne propre. ✔ Toute tentative est enregistrée dans la trace de contrôle et ne peut pas être effacée. ✔ Chaque utilisateur utilise un mot de passe fixé en fonction des restrictions prévues. Ce mot de passe n'est connu que de l'utilisateur. Personne ne peut lire les mots de passe dans l'enregistreur ni à l'aide des logiciel du PC.
(b)	*Electronic signatures based upon biometrics shall be designed to ensure that the cannot be used by anyone other than their genuine owners.* Les signatures électroniques basées sur la biométrie doivent être créées de façon à ne pouvoir être utilisées par personne d'autre que l'utilisateur lui-même. Sans objet ! Les signatures électroniques basées sur la biométrie ne sont pas prévues.

2 Évaluation des exigences

Section	Exigences : *Subpart B: Electronic Records* (Partie B : documents électroniques)
§ 11.300 *Controls for identification codes/passwords* **(Contrôle des codes d'identification/mots de passe)**	
(a)	*Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:* *Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.* Les personnes qui utilisent des signatures électroniques basées sur des codes d'identification combinés à des mots de passe exerceront un contrôle pour garantir leur sécurité et leur intégrité. Ces contrôles peuvent comprendre : gestion de l'unicité de chaque combinaison code d'identification-mot de passe, de telle façon que deux individus ne puissent pas avoir la même combinaison d'identifiant et de mot de passe. Exigence satisfaite ! ✔ L'assistant de sécurité (Security-Manager) pour PC permet à l'administrateur de définir les droits des utilisateurs sur l'enregistreur, leur mot de passe initial et les restrictions de leur mot de passe, de les rassembler, de les verrouiller dans une liste d'utilisateurs et de transférer cette liste dans l'enregistreur. ✔ L'affectation de toutes les données à un enregistreur est garantie par un numéro d'identification unique (numéro de série) pour chaque appareil. ✔ L'assistant de sécurité (Security-Manager) pour PC garantit l'unicité de la combinaison d'un nom d'utilisateur avec un mot de passe.
(b)	*Ensuring that identification code and password issurances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).* Garantie que les saisies d'identifiants et de mots de passe sont vérifiées régulièrement ou que les identifiants et mots de passe sont changés ou vérifiés (par exemple pour parer au vieillissement des mots de passe). Exigence satisfaite ! ✔ Les critères de sécurité élevée appliqués à la liste d'utilisateurs qui sert de base au contrôle d'accès à l'enregistreur et au PC sont les mêmes que ceux qui s'appliquent aux enregistrements électroniques. ✔ Une manipulation de la liste d'utilisateurs est détectée. Dans ce cas, l'utilisation de la liste est bloquée et cet événement est enregistré dans la trace de contrôle, sans possibilité d'effacement. ✔ Les assistants de sécurité (Security-Manager) de l'enregistreur et du PC garantissent une vérification des restrictions instaurées par l'administrateur, parmi lesquelles la péremption des mots de passe, lors de chaque modification de la liste d'utilisateurs, de même qu'à chaque vérification du contrôle d'accès. ✔ L'utilisateur dont le mot de passe est périmé est bloqué et l'événement est enregistré dans la trace de contrôle, sans possibilité d'effacement. Seul l'administrateur peut redonner une autorisation à cet utilisateur.

2 Évaluation des exigences

Section	Exigences : *Subpart B: Electronic Records* (Partie B : documents électroniques)
§ 11.300 *Controls for identification codes/passwords* (Contrôle des codes d'identification/mots de passe)	
(c)	*Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.* Procédures de gestion des pertes en vue d'invalider électroniquement, en cas de perte, de disparition ou de vol, les cartes ou autres objets qui portent ou produisent des informations de code d'identification ou de mot de passe, et en vue de délivrer des moyens de contrôle de remplacement, rigoureux, temporaires ou définitifs et utilisables immédiatement. **Exigence satisfaite !** ✔ Les logiciels de l'enregistreur et ceux du PC ne fournissent ni jeton ni pointeur. La sécurité est assurée par les restrictions des droits d'accès du mot de passe délivrés par l'administrateur. Ainsi par exemple l'administrateur délivre un mot de passe initial que l'utilisateur doit changer dès son premier accès, afin qu'il soit connu de lui seul. De plus, le mot de passe peut être assorti d'une durée de validité limitée. ✔ Le défaut de respect des restrictions conduit au retrait des droits de l'utilisateur. ✔ Cet événement est enregistré dans la trace de contrôle, sans possibilité d'effacement.
(d)	*Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.* Utilisation de garde-fous des transactions de façon à empêcher l'utilisation abusive de codes d'identification ou de mots de passe, et à détecter et rapporter immédiatement et en urgence, au système de sécurité et éventuellement à la direction de l'organisme, toute tentative d'utilisation non autorisée. **Exigence satisfaite !** ✔ Les assistants de sécurité (Security-Manager) du PC et de l'enregistreur empêchent l'accès non autorisé. Toute tentative est détectée et enregistrée dans la trace de contrôle du PC, sans possibilité d'effacement.
(e)	*Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.* Test initial et périodique des appareils comme les jetons ou cartes qui portent ou produisent des informations de code d'identification ou de mot de passe, pour vérifier qu'ils fonctionnent correctement et n'ont pas subi de modification non autorisée. **Sans objet !** L'enregistreur et les logiciels associés du PC n'utilisent ni ne produisent aucun jeton ni marque porteur d'une information d'identification ou de mot de passe.

3 Bibliographie

[1] Mass & Peither GMP Verlag
21 CFR 210/211 cGMP FOR FINISHED PHARMACEUTICALS
(Bonnes pratiques de fabrication pour les produits pharmaceutiques)
y compris *21 CFR 11 electr. Records/electr. Signature*
(documents électroniques/signatures électroniques)
avec traduction en allemand et index

JUMO GmbH & Co. KG

Adresse :
Moltkestraße 13 - 31
36039 Fulda, Allemagne
Adresse de livraison :
Mackenrodtstraße 14
36039 Fulda, Allemagne
Adresse postale :
36035 Fulda, Allemagne
Téléphone : +49 661 6003-0
Télécopieur : +49 661 6003-607
E-Mail : mail@jumo.net
Internet : www.jumo.net

JUMO Régulation S.A.

Actipôle Borny
7 rue des Drapiers
B.P. 45200
57075 Metz - Cedex 3, France
Téléphone : +33 3 87 37 53 00
Télécopieur : +33 3 87 37 89 00
E-Mail : info@jumo.net
Internet : www.jumo.fr

JUMO AUTOMATION S.P.R.L. / P.G.M.B.H. / B.V.B.A

Industriestraße 18
4700 Eupen, Belgique
Téléphone : +32 87 59 53 00
Télécopieur : +32 87 74 02 03
E-Mail : info@jumo.be
Internet : www.jumo.be

09.02/00422527