

FDA 21 CFR Part 11 et INDUSCREEN Series

Introduction

L'administration américaine, au travers de la *Food and Drug Administration* (FDA), a édicté un ensemble de règles conditionnant l'acceptation d'enregistrements électroniques (*electronic records*) et de signatures électroniques (*electronic signatures*). Ce document 21 CFR Part 11 (noté [11] dans la suite) est un document essentiel en ce sens qu'il reconnaît, sous le respect des règles données, la validité de documents électroniques en tant que documents de référence sans exiger leur existence sous une forme traditionnelle « papier ».

Ces règles sont essentielles pour les industries pharmaceutiques et médicales, d'une part parce qu'elles sont d'importantes utilisatrices des enregistrements électroniques et d'autre part par la responsabilité de santé publique engagée. Mais leur application engage l'ensemble des industries agroalimentaires, la chimie, les cosmétiques, ...etc, et leur pertinence peut même s'étendre au delà.

L'impact de la [11] sur les systèmes informatisés et en particulier les logiciels commerciaux sur lesquels ils s'appuient est évident, bien que la conformité d'une installation à la [11] ne dépende pas uniquement de ceux-ci. Bon nombre de règles sont en effet liées à l'exécution stricte de procédures qui vont garantir la conformité.

Le but de ce « papier blanc » est l'étude, au travers des points clés de la [11], de la conformité d'une application réalisée avec la gamme INDUSCREEN Series.

Note importante : Volontairement, nous n'avons pas redéfini les termes employés par la [11] et reformulé l'énoncé des règles. Le choix précis de ces termes, évidemment en anglais, ayant fait l'objet de nombreux commentaires (*wording*), il est de loin préférable de se tourner vers le document source de la FDA pour éviter toute interprétation erronée. Les termes anglais employés dans la [11] sont indiqués en italiques.

Enregistrements électroniques (*Electronic Records*)

Les logiciels INDUSCREEN Series disposent de trois mécanismes standard permettant de réaliser des enregistrements :

- les enregistreurs (recorders)
- le journal d'événements (logger)
- les recettes (recipes)

Grâce aux scripts compatibles Visual Basic intégrés, le développeur peut également créer d'autres formes d'enregistrements (requêtes SQL via ODBC par exemple). En regard de la [11], ces autres formes sont à considérer comme des développements spécifiques et ne seront pas étudiées dans ce document. S'il y a lieu, une étude sera néanmoins nécessaire pour assurer la conformité de l'application.

Disposition générales

- La capacité à garantir la précision, la fiabilité, et la performance d'enregistrement des données, ainsi que le discernement d'enregistrements invalides ou altérés [11.10(a)] repose à la fois sur les qualités du système d'exploitation (l'emploi de Windows NT et d'un système de gestion de fichiers avancé comme NTFS est préférable), et sur les qualités intrinsèques d'INDUSCREEN (organisation multi-tâche, contrôle préliminaire des bases enregistrées à chaque lancement, ...).
- Pour assurer les meilleures performances en vitesse et en compacité, les enregistrements des mécanismes standard d'INDUSCREEN s'effectuent en format binaire. La possibilité d'obtenir des copies « lisibles » de ces enregistrements pour inspection [11.10(b)] est fournie par les actions « export au format tableur » qui transforment les enregistrements en fichiers ASCII délimités standard.

- La protection des enregistrements durant leur période de rétention [11.10(c)] dépend essentiellement du support choisi pour leur stockage (disque dur, bandes, ...) et des procédures mises en œuvre à cet effet.
- Pour limiter l'accès du système au personnel autorisé [11.10(d)], INDUSCREEN Series dispose de 10 niveaux d'accès hiérarchisés permettant le contrôle individuel de tous les actions effectuées au travers du système. L'identification du personnel autorisé au travers d'INDUSCREEN Series sera étudié plus loin dans le chapitre traitant des signatures électroniques.
- Si nécessaire, le contrôle strict d'une séquence d'actions [11.10(f)] peut être mis en place facilement au travers de variables d'état (script d'automate d'états finis).
- La validité des données d'entrées (API ou E/S déportées) [11.10(h)] dépend à la fois des programmes automates et des contrôles de communication. Les protocoles de communication INDUSCREEN Series implémentent systématiquement des variables d'erreur qui peuvent être utilisées pour invalider l'enregistrement de données susceptibles d'être erronées.
- Les autres règles de la partie [11.10] relèvent des procédures mises en place pour garantir la formation du personnel, leur respect des procédures et leur acception de responsabilité quant aux formes d'identification retenues.

Piste pour audit (Audit Trail)

La [11] impose l'utilisation d'une trace d'audit pour tracer toutes les créations, modifications et suppressions d'enregistrements électroniques [11.10(e)]. Elle exige également un contrôle au travers d'une signature électronique et sa trace pour toute intervention autorisée sur les enregistrements [11.10(g)].

Nous allons examiner le traitement de cette règle dans le cas des mécanismes standard d'enregistrement d'INDUSCREEN Series.

Enregistreurs (*recorders*)

Dès leur conception, les enregistreurs INDUSCREEN ont été considérés comme des dispositifs critiques et disposent des capacités suivantes :

- Horodatage (time-stamp) : la résolution de cet horodatage est la milliseconde. Il est systématiquement inclus à chaque enregistrement et peut être fourni directement par la source si nécessaire.
- Les seules opérations standard modifiant le contenu d'un enregistreur sont l'ajout d'un nouvel enregistrement et l'effacement complet de l'enregistreur. L'altération partielle de son contenu et sa modification ne sont pas possibles par des actions standard, ce qui limite considérablement le risque de falsification. Dans l'examen complet d'une application, il faut néanmoins vérifier qu'une telle altération n'est pas rendue possible par des scripts spécifiques ou par un programme externe.

Nous préconisons pour la trace des accès en modification aux enregistreurs l'utilisation d'un enregistreur en enregistrement « à la demande » uniquement (pas de périodicité) que l'on pourra baptiser « AUDIT » et qui contiendra les champs suivants :

- Date-heure : inséré automatiquement
- Nom : nom de l'enregistreur concerné
- Type de l'opération effectuée (texte ou code) = AJOUT, RAZ, EXPORT, ...
- Code d'identification de l'opérateur (Variable interne Identity)
- Password de l'opérateur (Variable interne Password)

Une action d'ajout d'enregistrement dans « AUDIT » sera insérée dans toutes les touches entraînant une modification.

Notes :

- a) si l'ajout est automatique (mécanisme d'enregistrement périodique ou sur bande morte), il vaut mieux ne pas tracer les ajouts qui n'apportent rien par rapport à l'enregistreur principal.
- b) La gestion de la signature électronique à deux composantes (Identity/password) sera étudiée plus loin.

Journal d'événements (*logger*)

Dès sa conception, le journal d'événements INDUSCREEN a été considéré comme un dispositif critique et dispose des capacités suivantes :

- Horodatage (time-stamp) : la résolution de cet horodatage est la milliseconde. Il est systématiquement inclus à chaque enregistrement et peut être fourni directement par la source si nécessaire.
- Les seules opérations standard modifiant le contenu du journal sont l'ajout d'un nouvel enregistrement et l'effacement complet. L'altération partielle de son contenu et sa modification ne sont pas possibles par des actions standard, ce qui limite considérablement le risque de falsification. Dans l'examen complet d'une application, il faut néanmoins vérifier qu'une telle altération n'est pas rendu possible par des scripts spécifiques ou par un programme externe.

On pourra utiliser l'enregistreur « AUDIT » défini précédemment pour tracer les RAZ éventuelles du journal, en donnant par extension le nom « LOGGER » comme nom. Là encore, une action d'ajout d'enregistrement dans « AUDIT » sera insérée dans toutes les touches entraînant une modification.

Recettes (*recipes*)

Le mécanisme des recettes n'est pas systématiquement utilisé pour la réalisation de documents susceptibles d'être inspectés par la FDA . Mais si tel est le cas, les actions permises en standard par les logiciels de la gamme INDUSCREEN Series sont plus nombreuses et nécessitent une protection appropriée. INDUSCREEN permet en effet :

- la création d'une nouvelle fiche de recette
- la modification d'une fiche de recette existante
- la suppression d'une fiche de recette
- l'effacement de la totalité d'un classeur de recettes.

Pour être conforme à la [11], toutes ces actions peuvent être tracées sur l'enregistreur « AUDIT » dont le format a été évoqué précédemment. On indiquera le nom du classeur de recettes dans le champ précédemment utilisé comme « nom de l'enregistreur ».

Contrôles supplémentaires pour les systèmes ouverts (*open systems*)

Les règles précédentes considèrent le cas des applications industrielles qui sont des systèmes fermés (*closed systems*), c'est à dire des systèmes monopostes, multipostes en réseau local ou Intranet, auxquels n'ont accès que des personnes responsables, en tant que collaborateurs, de l'intégrité des enregistrements.

Dans le cas de systèmes ouverts (*open systems*), la [11] exige de garantir depuis leur création jusqu'à leur utilisation l'authenticité et l'intégrité des documents [11.30]. Des procédés tels que le cryptage de données des enregistrements, disponible dans la version 4.51 d'INDUSCREEN, permettent de satisfaire cette exigence.

Signatures électroniques (*Electronic Signatures*)

Selon la règle [11], les signatures (électroniques ou traditionnelles) doivent être utilisées dans les circonstances suivantes :

- Contrôle de l'accès au système par le personnel autorisé
- Validation d'enregistrements électroniques destinés à être inspectés
- Equivalence d'une signature traditionnelle dans un document électronique spécifique (fiche de validation, certificat de conformité, ..etc.)

Les contraintes imposées par la règle [11] ne s'appliquent que si cette signature électronique est celle qui garantit l'authenticité du document. Les entreprises qui le souhaitent pouvant toujours utiliser les signatures traditionnelles (manuscrites) pour la validation des documents.

Hormis les signatures traditionnelles, la règle [11] identifie trois types de signatures :

- bio-métriques (biometrics) : empreintes digitales, rétine, ...
- dispositif électronique d'identification (electronic device) : badge ou carte, ...
- code d'identification et mot de passe

Les deux premiers types de signatures ne sont clairement pas du ressort des logiciels INDUSCREEN Series. Pour le troisième type de signature, les logiciels INDUSCREEN Series disposent d'un mécanisme de base permettant de gérer 10 niveaux d'accès hiérarchisés associés à des groupes d'utilisateurs. Utilisé seul, ce mécanisme n'est pas suffisant pour la conformité à la [11] pour les raisons suivantes :

- Un seul composant (mot de passe) est suffisant pour autoriser l'accès.
- L'ensemble identifiant/mot de passe ne caractérise pas un individu unique mais un groupe d'utilisateurs, et ne garantit donc pas une responsabilisation suffisante.

Ce mécanisme peut néanmoins être complété assez aisément pour la mise en conformité des applications. Pour cela, nous préconisons la création d'un nouveau fichier « classeur de recettes » nommé « IDENTITY » contenant les champs suivants :

- Identity : variable interne de login = clé de la recette, spécifique à chaque utilisateur
- Password : mot de passe associé
- N° de matricule ou nom complet
- Code : code correspondant au niveau d'accès souhaité dans le mécanisme de base d'INDUSCREEN

Lors de toute opération nécessitant une signature électronique, on appellera une vue de saisie des informations Identity et Password. Lors de la validation, un script effectuera les opérations suivantes :

- recherche de la fiche associée au code Identity (nécessairement unique car clé de la recette)
- contrôle de l'égalité entre le password saisi et celui inscrit dans la fiche.
- si tout est correct chargement du code niveau d'accès (mécanisme de base) avec le code indiqué dans la fiche.

Le champ N° de matricule ou nom complet servira à l'administrateur du système pour annuler les codes dans certaines circonstances spéciales : perte du code d'accès initial, démission ou licenciement, ...etc.

S'appuyant sur le mécanisme de fiches de recettes d'INDUSCREEN Series, ce mécanisme est facile à adapter à toute application particulière en terme d'ergonomie d'exploitation et d'administration. On devra néanmoins veiller, pour satisfaire la [11.200(a)], à ce que l'usurpation d'identité requière au moins l'intervention de deux individus (et non de l'administrateur seul par exemple), ce qui exige que certaines données ne soient pas à la disposition de l'administrateur (les mots de passe par exemple), tout en lui laissant la possibilité de les effacer. Noter également que la [11.100(a)] exige l'unicité et interdit la réassignation d'un code existant.

La règle [11] exige qu'une signature soit liée à un document électronique quelconque de manière à garantir que cette signature ne puisse être copiée ou falsifiée [11.70]. Nous préconisons à cet effet la réalisation conjointe de deux actions lors de la production d'un document validé :

- l'export (ASCII délimité) de ce document sous un nom encodé unique créé par le système (Date-heure, numérotation incrémentale,...)
- L'inscription du type d'opération (revue, validation définitive, ..) dans le champ type de la trace d'audit (*Audit trail*)
- l'inscription de ce nom encodé unique dans la trace d'audit (*Audit trail*) dans le champ « nom »

Ces opérations peuvent aisément être enchaînées en tant qu'actions INDUSCREEN lors de l'appui d'une touche de validation.

La règle [11] exige également la clôture automatique d'une session au bout d'un temps prédéfini. Cette disposition peut être mise en œuvre facilement par un script du type :

```
If Sys_code<>"" then
    Tempo=Tempo-1
    If tempo=0 then
        Sys_Code=""
    End if
End if
```

La variable Tempo et la périodicité du script étant à ajuster en fonction du temps de maintien souhaité. Notons que la règle [11] autorise [11.200(a)] l'utilisation d'un seul composant d'identification (le mot de passe par exemple) pour les validations au sein d'une même session. On pourra facilement mettre en place un tel dispositif sur la base de la fiche de recette « IDENTITY » en ne contrôlant volontairement qu'un seul champ.

Conclusion

Il apparaît clairement qu'il n'existe pas d'obstacle majeur à la mise en conformité d'une application réalisée avec la gamme logicielle INDUSCREEN Series en regard de la règle [11]. Chaque application doit néanmoins être examinée avec soin. N'hésitez pas à entrer en contact avec le support d'ORDINAL Technologies pour tout complément concernant votre application.