

La 21 CFR Part 11 - Enregistrements et signatures électroniques

Nouvelle évolution vers un assouplissement

Impact de la mise en œuvre de cette réglementation pour un monitoring de salle propre

Depuis sa publication en 1997, il existe une littérature abondante sur l'interprétation de cette réglementation, la 21 CFR Part 11. Nous rappelons ici quelques références sur Internet : le site de la FDA, www.fda.gov ; le site spécialisé sur ce thème www.21cfrpart11.com et le site de l'ISPE qui propose des guides d'application www.ispe.org. Nous citerons aussi le site de la Sfstp, www.sfstp.org, pour ses commissions et ses séminaires sur ce thème.

Cette réglementation a été soumise à de nombreuses interprétations et de luttes au sein de l'industrie pharmaceutique pour déterminer comment interpréter et implémenter les exigences de cette réglementation.

Entre autres, l'industrie pharmaceutique s'est beaucoup inquiétée des investissements énormes requis pour la mise en conformité de leur systèmes à la Part 11.

La FDA a été sensible à ces inquiétudes et dans le cadre d'une démarche globale, "cGMPs pour le XXI^e siècle", basée sur une approche analyse de risques de la validation des systèmes, a édité un guide Part 11 en août 2003 actant d'une nouvelle interprétation assouplie de la norme.

Dans ce dossier, nous avons l'ambition de décliner de manière pratique cette nouvelle interprétation de la 21 CFR Part 11 en l'illustrant d'un exemple de "Monitoring de salles propres".

La nouvelle interprétation de la 21 CFR Part 11

- Le texte réglementaire n'est pas modifié, cela prendra certainement du temps avant qu'il le soit. La nouvelle interprétation de la Part 11 par la FDA est décrite au niveau du guide FDA : "Guidance for Industry Part 11, Electronic Records; Electronic Signatures - Scope and Application. August 2003".
- La FDA reconnaît que certaines applications trop strictes de la réglementation par certains inspecteurs ont pu faire croire à une rigidité du texte réglementaire. Dorénavant, la FDA annonce qu'elle s'attachera plutôt à l'esprit de la réglementation et pas forcément à la lettre dans la mesure où les firmes peuvent prouver un risque réduit et des moyens appropriés (pas forcément technologiques) pour protéger l'intégrité des données. Attention, cela ne veut absolument pas dire que le texte n'est plus en vigueur comme certains se sont empressés de penser.
- La FDA a l'intention d'avoir une interprétation plus étroite du scope de la Part 11 : un nombre plus restreint d'enregistrements, les plus critiques, seront soumis à une compliance totale à la réglementation. Cela ne doit pas être interprété comme le fait que la FDA ne se préoccupe pas des données, hors scope, manipulées et stockées par un système mais plutôt comme la volonté de la FDA de se contenter de preuves apportées à l'intégrité

des données même si elles ne sont pas 100 % compliantes avec la réglementation. Cet assouplissement concerne notamment les systèmes mis en service avant le texte réglementaire le 20 août 1997.

- Les enregistrements électroniques (et signatures associées) qui ne doivent pas être stockés avec des **règles pré-définies** mais qui sont néanmoins stockés sous format électronique ne sont pas forcément considérés comme des enregistrements Part 11. Cela veut dire que les enregistrements électroniques non critiques pour la FDA n'ont pas forcément à se conformer à la 21 CFR Part 11. Ceci met notamment fin à la large interprétation qui prévalait jusqu'ici et qui considérait que tous les enregistrements et signatures électroniques d'un système soumis à la Part 11 devaient se conformer à la Part 11. La nouvelle interprétation se concentre donc plus sur les enregistrements et leur criticité que sur les systèmes eux-mêmes.

Application sur un système de monitoring

Un monitoring de salles propres est composé de deux systèmes :

- le "Système informatique" le poste informatique qui contrôle l'ensemble du système et les données
- le système "d'Acquisition", essentiellement des capteurs (température, hygrométrie, poussières...) et quelques actionneurs (voyant, klaxon). Ces acquisitions de mesures passent par des systèmes comme les "cartes d'acquisition", directement implantés dans l'ordinateur, et/ou des automates programmables raccordés à l'ordinateur par des "bus" ou des "réseaux".

Pour généraliser, "le système d'acquisition" peut être remplacé par "un système de contrôle commande" avec ses capteurs et ses actionneurs qui pilote les équipements : process industriels, équipements de laboratoire, machines...

La constitution de ce système est décrit figure 1.

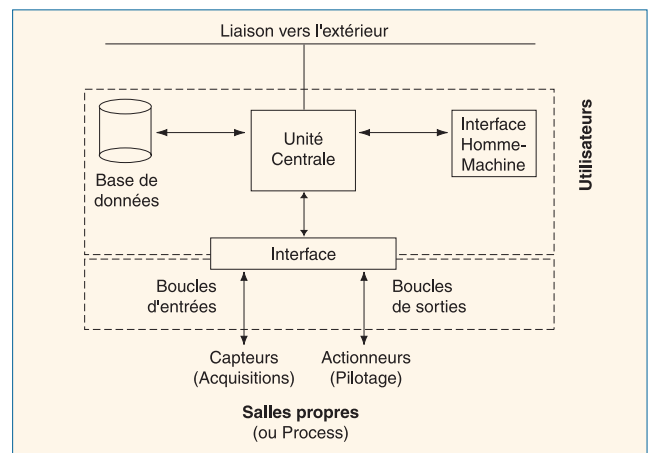


Figure 1 : Système d'acquisition

Validation du système

L'application de la réglementation 21 CFR Part 11 ne peut s'appliquer que sur un système "validé".

Il est donc impératif de commencer par cette tâche. Sur la base de la spécification, conception du système, de ses fonctionnalités et des risques, notamment pour le produit final, il est nécessaire de procéder à des qualifications d'installation, opérationnelle et de performance.

Les items de la mise en conformité

Gestion des sécurités

La gestion des sécurités intègre l'ensemble des accès et des modifications possibles sur le système. Cette gestion est générique à tous les systèmes informatiques : système de monitoring de salles propres et autres.

Cela se décompose :

- Verrouillage du poste (ou de l'application) "bas niveau", afin :
 - d'empêcher de changer l'heure du poste (qui tromperait les enregistrements sécurisés)
 - d'empêcher de prendre la main par des séquences de touches de type "Ctrl + Alt + Del" ou "Alt + Tab"
 - ou d'accéder à la gestion des droits, à l'application et autres.
- Pérennité des comptes utilisateurs :
 - basée sur un identifiant, géré par l'administrateur, et un mot de passe connu uniquement par le propriétaire du compte ; il est possible d'utiliser des systèmes avec badge + mot de passe ou un système "biométrique" comme la reconnaissance d'une empreinte digitale, mais dans le cas d'un monitoring de salles propres, ces types de contrôle d'accès ne s'imposent pas
 - identifiant unique : les mots de passe peuvent être accidentellement identiques, cela ne créera pas de confusions car le couple "identifiant + mot de passe" sera toujours unique
 - changement de mot de passe obligatoire au bout d'une période paramétrable (en mois)
 - impossibilité d'utiliser des mots de passe génériques (toto, nom de l'entreprise) et de réutiliser les précédents mots de passe (paramétrable)
 - déconnexion automatique du poste au bout d'un certain temps paramétrable (en minutes) d'inactivité sur la souris ou sur le clavier
 - déconnexion manuelle de l'utilisateur de son compte
 - audit trail des comptes (voir chapitre sur ce thème)
 - identification de tentative d'intrusion avec blocage immédiat du compte
 - définition de plusieurs niveaux d'accès avec des droits spécifiques pour chaque "groupe".

Gestion des données

La gestion des données peut-être généralisée à tous les systèmes informatiques.

Il s'agit de la gestion des données elle-même. Ceci implique :

- Source de la donnée :
 - identification des données : il s'agit de sélectionner les informations à maîtriser selon l'activité, la réglementation et le risque pour la qualité du produit final ; dans le cas d'un monitoring de salles propres, on peut relever, en plus des résultats des mesures, les seuils d'alarmes, les temporisations de dépassement de ces seuils, certains événements critiques, l'acquiescement des alarmes, la maintenance effectuée sur les capteurs de mesure critiques, autres
 - qualification, étalonnage des systèmes qui produisent les données
 - vérification de la source de la donnée (réseau informatique)
 - gestion de l'heure : synchronisation de l'heure de tous les systèmes, changement d'heures été et hiver, utilisation de plusieurs fuseaux horaires.
- Maîtrise de la donnée :
 - création, modification, destruction
 - lisible par l'utilisateur
 - sauvegarde
 - archivage pérenne selon une période définie ; cet archivage pérenne concerne à la fois le support informatique mais aussi les logiciels de lecture qui doivent prendre en compte l'ensemble de l'information
 - exportation des données dans un format sécurisé.

Audit trail

Le but de l'audit trail est de retrouver les modifications qu'a subit une donnée critique, que cela soit volontaire ou involontaire.

L'audit trail comprend :

- Actions à tracer :
 - actions de modification de paramètres critiques lors de la conduite de l'opération
 - actions critiques des opérateurs et autres intervenants
 - actions sur les comptes d'accès des utilisateurs.
- Constitution de l'audit trail :
 - le jour, l'heure de l'action, enregistrée directement par le système informatique
 - l'identification de la personne qui fait l'action
 - l'enregistrement de commentaires sur les raisons ou le sens de l'action
 - la nouvelle valeur ne doit pas supprimer l'ancienne
 - la modification doit être visible pour ceux qui ont en charge d'utiliser les informations.

Signatures électroniques

Dans cette mise en œuvre, nous ne développerons pas toutes les possibilités de la signature électronique. Nous vous suggérons, dans le cadre de ce monitoring de salles propres, qui pourra être étendue à d'autres systèmes, la "signature électronique" de paramétrages sensibles.

Les réglages des seuils d'alarmes, temporisation, pourrait faire l'objet d'un suivi électronique au lieu d'être enregistré sur la fiche de poste papier.

Lors des actions sur le monitoring, quels que soient ses droits d'accès, une "confirmation électronique" sera demandée à l'opérateur.

Cette signature électronique prendra la forme suivante :

- une fenêtre (un pop up) apparaîtra spontanément lorsque le curseur sera dans le champ d'une donnée à confirmer
- le code d'identification et le mot de passe seront demandés
- après validation de l'identification, la nouvelle valeur et un commentaire seront demandés
- la confirmation de l'action sera à valider selon un résumé de la modification.

Des variantes peuvent être mises en œuvre :

- pour une série continue de modifications dans un court laps de temps (paramétrable), les confirmations pourront requérir uniquement le mot de passe, le code d'identification ayant été entré au début, pourra rester actif pendant toute la série
- le commentaire pourra être du texte libre ou pris dans une liste pré-définie : "Paramétrage de nuit", "Erreur de valeur d'entrée", autres...

Note importante :

Ces "signatures électroniques" seront vues comme des "enregistrements électroniques" avec les exigences d'intégrité des données et d'audit trail.

Conclusion

Le monitoring est un système informatisé qui se prête bien à l'application de la réglementation 21 CFR Part 11 - Enregistrements Electroniques - Signatures Electroniques.

Les fonctionnalités vues dans ce dossier sont proposées comme un minimum permettant de répondre à la fois aux exigences du législateur et comme une sécurité pour les entreprises. Ces fonctionnalités peuvent être bien sûr étendues.

Dossier réalisé pour
le Guide de l'Ultra-Propreté

Jérôme LARFI
EURILOGIC