ANNEE 2013 NUMERO 4

LA QUALITE EST L'AFFAIRE DE TOUS

Lettre Trimestrielle

Date: 10/03/2013

Dans ce numéro

Prochaine parution : 10/06/2013

Message de l'auteur

Cette lettre trimestrielle a pour but de donner des informations spécifiques à un public ciblé.

Elle est réservée à celles ou à ceux qui se sont inscrit volontairement sur le site www.demarcheiso17025.com afin de mieux s'informer sur l'accréditation et de développer une connaissance plus riche de la norme et des référentiels associés.

J'espère que PAPA NOEL ne vous a pas oublié et que ce début d'année qui s'annonce morose pour beaucoup de secteurs d'activités démarre pour vous avec de l'optimisme et de l'entrain.

Les difficultés étant plus importantes, autant ne pas relâcher ses efforts car aujourd'hui, on change de prestataire plus facilement qu'un forfait téléphonique et un client perdu, c'est toujours très difficile à reconquérir.

J'ai rajouté une petite note d'humour en fin de lettre que je poursuivrai dans les prochaines parutions.

Vous souhaitant bonne lecture de ce quatrième numéro.

Eric Laffineur

Les systèmes informatiques et la 17025.

Cette personne doit s'assurer qu'ils sont vérifiés avant mise en service

Les ordinateurs et les logiciels associés peuvent évidemment avoir une incidence sur la validité des données et doivent donc être correctement gérés et contrôlés, que ce soit sur une partie de l'instrumentation ou des systèmes simplement utilisés pour stocker et traiter les données.

Ceci s'applique à tous les matériels et logiciels et en particulier à un logiciel élaboré en interne ou les applications développées sur des feuilles de calcul, par exemple. Il devrait y avoir un registre des contrôles utilisés pour assurer un fonctionnement correct.

Vérifications des logiciels

Il doit y avoir une personne définie qui est chargé d'autoriser les logiciels pouvant être utilisés dans le laboratoire. Cette personne doit s'assurer qu'ils sont vérifiés pour démontrer qu'ils ne puissent pas corrompre les données ou autres informations avant qu'ils ne soient mis en service. Cette exigence doit s'appliquer non seulement aux nouveaux logiciels, mais aussi à toutes les mises à jour ou les modifications. La personne responsable doit être le responsable du laboratoire ou une personne qui a une responsabilité déléguée par le responsable du laboratoire.

Il n'y a aucune raison pour que le personnel ne puisse pas mettre en place des feuilles de calcul, par exemple pour effectuer des calculs de routine ou du traitement de données, mais elles doivent avoir été vérifiées et autorisées avant utilisation.

Il n'est pas acceptable d'avoir du personnel qui met en place des applications ad hoc et qui les utilisent sans aval de la direction du laboratoire.

Les feuilles de calcul doivent être protégées

Chaque fois que possible, les feuilles de calcul doivent être protégées contre toute modification à l'aide de mots de passe réservés à la gestion. Lorsque cela n'est pas possible, un ensemble de données entrée-sortie doit être disponible, qui peut être chargé dans le tableur et utilisé pour vérifier que les valeurs calculées sont déterminées correctement.

Tout nouveau logiciel ou toutes modifications aux logiciels existants, y compris les nouvelles versions des logiciels commerciaux, doivent être enregistrés dans un tableau de gestion des logiciels avec la date à laquelle ils sont entrés en application. Il est alors possible de déterminer la version du logiciel qui a été utilisé à un moment donné, si une erreur doit être tracée. Il doit y avoir des vérifications régulières des logiciels installés et tout logiciel non autorisé doit être supprimé.

Il est doit également être possible de réinstallés les versions précédentes de n'importe quel logiciel dans le cas d'une erreur ou si une requête se présente afin de déterminer si le logiciel était responsable. Le plus simple pour fournir cette preuve consiste à veiller à ce que, à chaque mise à jour, une copie de la version précédente soit conservée sur un support amovible tel qu'un disque dur ou sur serveur.

Les réseaux informatiques

De plus en plus, les laboratoires utilisent des réseaux informatiques locaux, surtout s'ils fonctionnent avec des LIMS : *Laboratory Information Management System*. Un tel réseau peut rendre le contrôle plus facile des logiciels avec des zones de travail qui peuvent être établies avec un accès restreint et différents niveaux d'accès. Ces réseaux doivent être exploités pour contrôler, par exemple, qui peut écrire de nouveaux fichiers sur le réseau du serveur.

Le gestionnaire du réseau doit accepter de consulter la direction du Laboratoire

Systèmes informatiques gérés par un autre service

Il arrive souvent que le laboratoire n'ait pas de contrôle direct sur le serveur du réseau. Celui-ci fait partie du réseau général de l'entreprise (c'est le cas pour moi). La direction du laboratoire devra démontrer aux évaluateurs qu'il sait ce qui est fait sur le réseau en son nom et qu'il est informé des mises à jour logicielles afin qu'il puisse procéder à des vérifications.

La façon la plus convaincante pour le laboratoire de démontrer sa volonté est d'avoir un accord écrit entre le laboratoire et le gestionnaire de réseau qui spécifie la répartition des responsabilités.

Cela devrait couvrir au moins les points suivants:

Le gestionnaire du réseau doit accepter de consulter la direction du laboratoire et obtenir son accord pour installer un nouveau logiciel accessible au personnel de laboratoire. Si nécessaire, la direction du laboratoire doit se réserver le droit de procéder à des vérifications sur le logiciel avant de l'accepter.

Le gestionnaire du réseau doit s'engager à informer le laboratoire, s'il entend mettre à jour ou modifier tout logiciel utilisé par le laboratoire. Il doit clairement être établi que le gestionnaire du réseau vérifiera que le laboratoire aura effectué ses contrôles avant que la révision du logiciel soit en application.

Le gestionnaire du réseau doit savoir qui est autorisé à demander des modifications

La clé est de définir clairement les responsabilités de chaque partie dans le but d'éviter des contrôles inadéquats lorsque les deux parties supposent que l'autre est responsable.

La responsabilité de fournir la possibilité de revenir en arrière à la version précédente du logiciel doit être clairement convenue.

En particulier, le gestionnaire de réseau doit savoir qui est autorisé à demander des modifications logicielles pour le compte du laboratoire et ne doivent pas répondre aux demandes des membres non autorisés du personnel de laboratoire.

Les dispositions relatives à la sauvegarde des données du laboratoire sur le réseau doivent être convenues.

L'intégrité des données sur les ordinateurs

Lorsqu'un laboratoire gère les données sur les ordinateurs, il y'a des précautions particulières, principalement sur la sécurité des données et le contrôle des modifications de ces données. Il se peut qu'il y'ait une nécessité pour des raisons parfaitement légitimes, pour un laboratoire, de modifier des données qui ont été enregistrée : par exemple, la répétition de mesures qui fournissent un résultat différent.

La première question que le laboratoire doit se poser est de définir si l'enregistrement informatique constitue des données brutes, c'est à dire les données enregistrées au moment de l'observation.

Cela ne sera pas le cas si les données sont enregistrées dans l'ordinateur directement à partir de l'instrument.

Si les données sont enregistrées dans un cahier de paillasse avant le transfert à l'ordinateur, alors ce document papier constitue les données brutes.

Les données brutes doivent être préservées dans le cadre de l'enregistrement du laboratoire. S'il y'a un transfert manuel à l'ordinateur, alors le laboratoire devra convaincre les évaluateurs qu'il existe des garanties adéquates pour vérifier que cela est fait correctement et que, une fois que le transfert est terminé et vérifié, toutes les modifications apportées aux données sont sous contrôle et en conformité avec les exigences de la norme.

La saisie manuelle des données dans les ordinateurs est clairement une source d'erreur potentielle. Idéalement, tous ces transferts devraient être vérifiés par une deuxième personne. Dans les cas critiques, la double saisie des données peut être pratiquée, où bien les données sont saisies deux fois pour créer deux fichiers qui peuvent ensuite être comparés par un logiciel approprié. Il incombera au laboratoire de démontrer aux évaluateurs qu'il prend des mesures raisonnables pour vérifier que les données sont correctement saisies. À minima, le laboratoire doit vérifier les données saisies et mettre en place des moyens pour éviter de commettre des erreurs.

Un problème plus fondamental se pose avec les ordinateurs quand il est possible de modifier les données sans laisser de trace sur la modification ou de l'enregistrement original. Cela contrevient aux exigences de base que toutes modifications doivent être traçables à la personne qui les exécutent et que cela doit être fait de telle sorte que la valeur d'origine est récupérable. Les logiciels dédiés aux applications de laboratoire intègrent généralement une piste d'audit qui enregistre les modifications et l'identité de la personne par son nom d'utilisateur. Ces logiciels normalement peuvent aussi conserver une trace de l'enregistrement original et peuvent même exiger la raison de la modification. Si la trace existe, le laboratoire répond aux exigences de la norme à condition qu'il y ait un enregistrement de la piste d'audit dans le cadre de la procédure de contrôle de la qualité.

Les logiciels n'étant pas conçus spécifiquement pour les laboratoires n'offrent généralement pas cette piste d'audit. L'option la plus simple est de définir une règle qui déclare que toutes les modifications doivent être enregistrées dans un journal papier. On doit stipuler l'identité de la personne effectuant la modification, la date de cette modification, le motif du changement et les anciennes et nouvelles valeurs. Un tel système, bien que simple, n'est pas garant comme étant conforme à la norme car il est, dans la plupart des situations non auditable. Si quelqu'un fait une modification de données brutes dans un ordinateur et ne parvient pas à remplir le journal, alors il ne peut pas être détecté. D'autre part, si les données brutes existent sur une feuille de travail, il y aura un écart entre la feuille de travail et l'enregistrement informatique. Dans ce cas, le système est vérifiable et acceptable. Notez ici le besoin d'être clair sur ce qui constitue les données brutes.

Les données de l'ordinateur peuvent être protégées par le logiciel contre toute altération, par exemple en se voyant accorder le statut de lecture seule lorsque l'information est entrée. Le laboratoire doit établir des règles claires sur qui est autorisé à apporter des modifications aux données.

Le laboratoire doit établir des règles claires sur qui est autorisé à apporter des modifications aux données

Si l'autorisation de modification des données est à un niveau suffisamment élevé, les évaluateurs sont susceptibles d'être satisfaits. Un niveau approprié serait au moins le personnel technique de haut niveau.

Il y aurait une non-conformité critique si l'enregistrement du laboratoire ne reflète pas le contenu du rapport. Des procédures spécifiques doivent être suivies lorsque des rapports doivent être modifiés, et les données originales et modifiées doivent toutes deux être disponibles. Il doit également être possible de générer une nouvelle version du rapport original avec les données modifiées en étant conforme aux exigences de la norme. La nécessité de modifier le rapport exige également un enregistrement d'une non-conformité et des mesures correctives.

Si les données ont été modifiées sur un ordinateur, mais pas sur la feuille de travail correspondante, il existe un risque critique, car il est impossible de dire quelles sont les données qui sont valides. Une modification paraphée sur la feuille de travail pour la mettre en conformité avec la valeur de l'ordinateur peut palier à ce problème.

Les PC intégrés à l'instrumentation

Les PC qui commandent et recueillent des données à partir de l'instrumentation doivent être traités comme une partie de l'instrument et être vérifiés avec l'ensemble du système.

Les mises à niveau doivent être traitées de la même manière que toute autre modification à l'instrument, et doivent être vérifiées avant leur mise en utilisation.

Un soin particulier doit être pris lorsque les instruments sont installés par le fournisseur puisqu'il n'est pas rare pour les ingénieurs de charger des correctifs logiciels et des modifications. La direction du laboratoire doit être informée de toutes les modifications apportées au logiciel afin qu'elles puissent être vérifiées et enregistrées dans la fiche de vie.

Les PC intégrés aux instruments peuvent fournir un excellent moyen de conserver les données brutes dans un format compact « propriétaire ». Par exemple, les données de chromatographie peuvent être un problème pour mettre les données sur papier mais on peut les archiver sur CD. Cependant, une sauvegarde sécurisée sur serveur est préférable pour s'assurer de récupérer les données.

Des outils informatiques « passerelles » sont parfois également nécessaires pour pouvoir lire les données sur un autre appareil, par exemple, votre chromatographie tombe en panne et n'est pas réparable (modèle très ancien, pièces critiques plus fabriquées et épuisées), le laboratoire avait anticipé cet état de fait et a déjà investi dans un autre équipement.

Réclamations client suite à des contre-essais et vos résultats provenaient de votre ancien équipement, impossible de vérifier s'il s'agit d'une erreur matérielle ou d'une mauvaise configuration par l'opérateur, les données ne sont pas lisibles par le nouvel équipement.

Les LIMS

L'utilisation des LIMS est de plus en plus fréquente et peut contribuer grandement à l'exploitation d'un système de management de la qualité. Il est même possible d'obtenir des systèmes qui intègrent les intervalles d'étalonnage, ce qui permettra d'éviter l'entrée de données générées sur des instruments ayant leur date d'étalonnage en retard.

Les LIMS peuvent parfois introduire des anomalies et peuvent ne pas fournir exactement ce que la direction du laboratoire désire.

Lorsqu'un opérateur est connecté, il faut que le système puisse se déconnecter seul au bout d'une certaine période d'inactivité pour éviter qu'un autre opérateur non habilité puisse intervenir dans le système.

Si un second opérateur est habilité à utiliser le système pour intervenir sur des données, ce second opérateur doit pouvoir s'identifier de manière formelle dans le système lors de son intervention.

Sauvegarde des données sur des ordinateurs

De manière générale, un laboratoire a l'obligation de veiller à ce qu'il protège toutes les données qu'il détient : données brutes ou une partie essentielle de la traçabilité. Lorsqu'un laboratoire a données brutes sur l'ordinateur, le système de sauvegarde doit être extrêmement rigoureux.

La politique de sauvegarde doit être telle que, en cas de défaillance du système où les données non encore sauvegardées seraient irrémédiablement perdues, le laboratoire serait en mesure de les récupérer, soit à partir des feuilles de calcul ou en répétant les essais. Dans le cas extrême où un laboratoire effectue des travaux qui ne peuvent pas être répétés et où la seule copie des données est sur l'ordinateur, la sauvegarde doit être très fréquente. Une stratégie courante consiste pour les laboratoires d'avoir deux disques durs : ordinateur principal et sur serveur réseau.

Ce stockage doit être séparé de la zone du laboratoire par un coupe-feu et, idéalement, être muni d'un coffre-fort ignifugé conçu pour le stockage de données.

Coffres ignifugés conçus pour les documents qui ne sont pas adaptés : destruction à une température trop élevée.

Si les données doivent être conservées dans le laboratoire, un coffre-fort est essentiel et son utilisation doit être rigoureusement sous-contrôle.

Il existe aujourd'hui des serveurs sécurisés non situés dans l'entreprise sur lesquels le système télécharge de manière quotidienne et de façon automatique, l'ensemble des données de la journée.

L'avantage de ce principe est la restitution garantie sous 24 heures des données du laboratoire : mieux vaut prévenir que guérir !!

Les outils de l'amélioration continue : Méthode 6-SIGMA.

Méthode rigoureuse, applicable à tous types de processus (Production, Achats, Ressources Humaines…) et basée sur les statistiques : technique de Management qui permet d'introduire ordre et rigueur dans l'Entreprise.

Aujourd'hui, elle est surtout basée sur la satisfaction client contrairement à son origine dans les années 80 ou elle s'appliquait à l'amélioration de la qualité.

Elle contribue à :

- une diminution des rebuts, retouches, et plus généralement des coûts de non-qualité ;
- une amélioration de la disponibilité des machines et de leurs rendements,
- de meilleures parts de marché consécutives à l'amélioration de la qualité des produits/Analyses/essais.

Un des principes de base de Six Sigma est la réduction de la variabilité : l'insatisfaction d'un client résulte toujours d'un écart entre une situation attendue et une situation réelle.

Elle vise donc à obtenir un Z = 6 qui correspond à 3,4 DPMO ou PPM (Défauts Par Million d'Opportunités).

Il s'agit d'un pourcentage de non-conformes dans une situation donnée basé sur une loi normale décentrée de 1,5 sigma.

La démarche DMAICS (Définir, Mesurer, Analyser, Innover/Améliorer, Contrôler, Standardiser):

C'est le moteur de la démarche et elle repose sur ces 6 étapes.

Définir : cette étape a pour but d'identifier les points critiques de la qualité en se mettant à l'écoute du client, bien définir le problème, les limites de remise en cause, l'équipe de travail.

Résultats : Charte du projet - Cartographie générale du processus

Planning et affectation des ressources

Outils : Diagramme CTQ (Critical To Quality) ; QQOQCP ; QFD (Quality Function Development) ; Diagramme de Kano ; Benchmarking ; Cartographie ; SIPOC (Supplier Input Process Output Customer).

Mesurer le niveau de qualité :

Trouver un moyen de mesure de la qualité, vérifier sa capabilité, récolter des faits et déterminer le z du processus.

On voit toute la limite de cette méthode avec les laboratoires.

Par exemple, sur 3000 analyses que mon labo traite par an, j'ai enregistré 53 non-conformités qui correspondent à 4 opportunités significatives, je vais calculer le DPMO.

Il suffit de diviser 53/3000 et de multiplier par 1 million/nombre d'opportunités de générer des NC soit un DPMO de 4416.

Les tables statistiques ou la formule suivante permet de calculer le Z :

$$Z = 0{,}8406 + \sqrt{29{,}37 - 2{,}221.\ln(DPMO)}$$

Pour notre laboratoire : Z = 4,1 et à l'inverse pour tendre vers un Z = 6, il faudrait que mes non-conformités tendent vers « 0 » : atteinte de l'objectif difficile à obtenir ou bien traiter plus de 45 Millions d'analyses par an avec toujours 53 NC, (on voit toute la limite de cette méthode pour les labos), mais la démarche peut tout de même contribuer à une amélioration du système.

Résultats : Cartographie détaillée du processus

Capabilité des moyens de mesure

Capabilité du processus

Outils : Analyse processus, logigramme

Répétabilité et reproductibilité

Analyse des 5M (Matrice Causes/Effets)

Feuille de relevés et maîtrise statistique des procédés (SPC)

Analyser :

Examiner, analyser les données, prouver statistiquement les facteurs influents.

Résultats : Établissement de la preuve statistique

Compréhension du processus

Outils : Statistique descriptive

Statistique inférentielle (méthode de Monte Carlo par ex)

Plans d'expériences

Innover :

Expérimenter, modifier, améliorer, optimiser, prouver statistiquement que les améliorations sont efficaces.

Résultats : Processus pilote

Amélioration du z

Détermination des caractéristiques à mettre sous contrôle

Outils : Méthode de créativité

Vote pondéré

Plans d'expériences

AMDEC

Contrôler :

Appliquer la solution, la formaliser et la mettre sous contrôle.

Résultats : Rédaction de modes opératoires

Cartes de contrôle

Outils : Maîtrise statistique des procédés (SPC)

Standardiser :

Pérenniser la solution, déployer les bonnes pratiques et clore le projet.

Résultats : Indicateurs de performance

Tableau de bord

Plan d'audit

Bilan de fin de projet

Outils : Audit ; Benchmarking ; Bonnes pratiques.

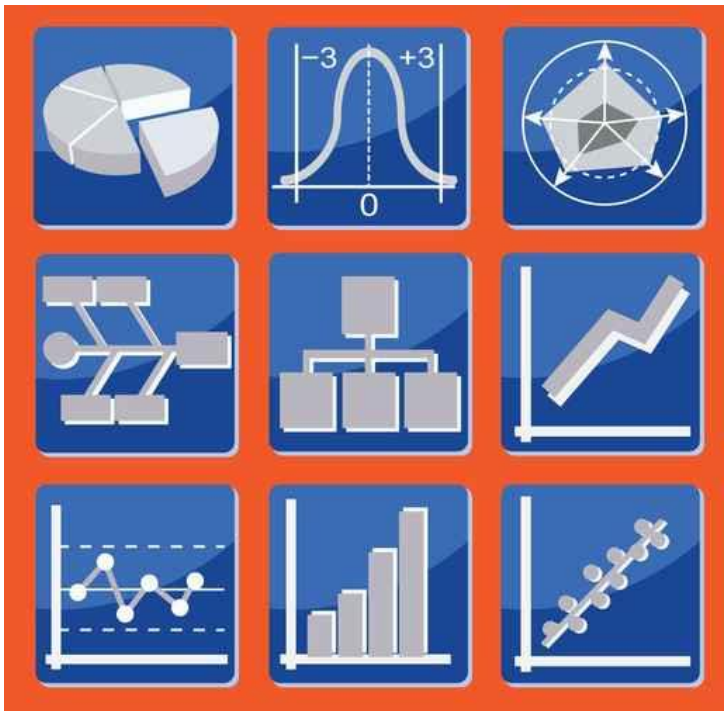
Il va s'en dire qu'une telle démarche ne se fait pas sans formation et un accompagnement par du personnel aguerri à la méthode et à l'ensemble des outils statistiques utilisés.

Chaque responsable de Labo utilise de manière chirurgicale une partie de cette méthode (Cartes de contrôle, analyse des retours de satisfaction client, réduction des non conformités, Analyse des processus, AMDEC..).

Cette méthode est tout de même plus adaptée aux entreprises qui réalisent des productions de grandes séries ou une dérive de quelques PPM entraine une perte financière significative (rappel véhicules chez les concessionnaires par ex).

Le facteur temps est également un handicap dans nos labos ou le personnel réalise souvent plusieurs fonctions, comment se dégager du temps pour mener à bien un tel projet ?

Ci-dessous, une cartographie qui résume bien la démarche 6 Sigma.



News sur la documentation

ILAC-P10:01/2013 Policy on the Traceability of Measurement Results vient de paraître

ILAC-P14:01/2013 Policy for Uncertainty in Calibration vient de paraître.

ISO 13528-2013 que vous pouvez consulter ou commenter en version DRAFT sur le site de l'AFNOR.

Note d'humour