PcVue Solutions
21CFR part 11 FR

Dernière mise à jour :	6-oct.-20
Révision :	1.0
Contenu :	Description
Confidentialité :	Publique

Contenu

1 PcVue et la norme 21CFR Part 11

21 CFR Part 11 est un document de référence de la FDA (Food and Drug Administration aux Etats-Unis) qui définit les exigences à respecter afin que les enregistrements et les signatures électroniques soient considérés comme dignes de confiance au même titre que les documents papier signés manuellement.

PcVue intègre un certain nombre de fonctionnalités répondant à une interprétation des exigences de la réglementation 21CFRpart11 pour les sous-parties suivantes :

Sous-partie B - Enregistrements Electroniques. Décrit les contrôles pour les systèmes fermés et ouverts. Le Superviseur est considéré comme un système fermé.
Sous-partie C - Signatures Electroniques. Décrit l'implémentation et l'utilisation des signatures électroniques. Dans le Superviseur, une signature électronique correspond à un compte utilisateur.

Il est important de noter que la plupart de ces fonctionnalités sont intégrées nativement dans PcVue disponibles gratuitement dans toutes les versions PcVue.

Elles sont largement décrites dans l'aide en ligne de PcVue.

Le développeur d'application doit être conscient que l'utilisation de ces fonctionnalités n'est pas une garantie de conformité car le logiciel seul ne peut pas fournir de conformité.
La plupart des exigences sont respectées par des procédures, la conformité vis-à-vis des autres pouvant être résolue par une restriction d'accès au PC d'un point de vue physique et électronique.

Il faut également tenir compte du fait que la 21 CFR Part 11 est un document concernant les enregistrements et les signatures électroniques - il n'est pas spécifique à l'utilisation des PC et des applications telles que les SCADA. De ce fait, il est ouvert à l'interprétation et son application doit tenir compte des documents de conseils qui sont régulièrement délivrés par la FDA.

Ce document décrit les conformités entre la réglementation 21CFR Part 11 « Fichiers et signatures électroniques » et le logiciel **PcVue** , développé par ARC Informatique.
Les réponses aux demandes de la norme peuvent être applicatives, ou intégrées depuis la version 7.20 du produit.

1.1 Définitions utilisées dans ce document

Les termes suivants sont utilisés dans ce document :

Projet	Configuration de **PcVue** en vue de l'adapter à une utilisation applicative particulière.
Utilisateur	Personne utilisant **PcVue** une fois celui-ci adapté à une utilisation applicative particulière.

1.2 Paragraphe A – Clauses Générales

Section	Réglementation	CONFORMITE
11.1	Portée. Définit l'étendue de la réglementation.	ARC Informatique accepte les intentions de la réglementation.
11.2	Mise en œuvre : Les fichiers peuvent être conservés sous format informatique et soumis à la FDA, sous réserve que les règles de la norme 21CFR soient respectées	Ce point de la réglementation s'applique aux utilisateurs système pour une application. ARC Informatique ne soumet pas directement de documents à la FDA.
11.3	Définitions. Définit les termes utilisés dans la correspondance avec la FDA. Ceci est principalement un lexique.	Sans commentaire.

1.3 Paragraphe B – Fichiers Informatiques

Section	Réglementation	CONFORMITE
11.10	Décrit le contrôle sur les systèmes fermés. Un système fermé est un système dont l'accès est réservé aux dirigeants. Les mesures qui doivent être prises, afin de prouver le contrôle sont :	**PcVue** peut être configuré comme système propriétaire, dans ce cas-là, toutes les fonctions de **PcVue** et du système d'exploitation sont réservées aux utilisateurs autorisés. Toutes les informations collectées par **PcVue** font partie du projet et peuvent être uniquement générées par **PcVue** sauf export explicite.
	a. Validation du système	**PcVue** utilise une base de données de variables temps réel propriétaire et des fichiers historiques binaires, ASCII ou au format base de données SQL server **PcVue** stocke, au format choisi lors de la configuration, les évolutions des mesures, changement d'état des bits et alarmes. Dans le cas d'un Projet configuré en tant que système propriétaire, les fichiers de données peuvent être accessibles uniquement depuis **PcVue**.
	b. Génération de copies papier à partir de fichiers informatiques.	Les enregistrements sont maintenus dans des fichiers d'archives et peuvent être aisément récupérés. **PcVue** offre la possibilité d'extraction, à une date précise du nombre d'enregistrements souhaités, soit directement dans l'application, soit à l'aide d'un outil d'extraction complémentaire des données.
	c. Protection des fichiers pour permettre une récupération facile et précise pendant toute la	Les fichiers peuvent être sauvegardés sur le disque dur de l'ordinateur, dans la structure du projet, sur un disque réseau ou dans un espace de stockage (cloud privé).

	période de rétention de ceux-ci.	Le projet peut être configuré afin de garantir l'accès uniquement aux personnes autorisées. Les fichiers peuvent être protégés en lecture. Des mécanismes permettent l'archivage des données de manière automatique ou manuelle sur un autre support par un utilisateur autorisé. Pour activer cette fonction, il n'est pas nécessaire de passer par le système d'exploitation. Le client utilisateur doit établir applicativement les modalités et procédures pour s'assurer de la conservation des données pendant la durée appropriée.
	d. Limites de l'accès au système pour les Utilisateurs autorisés.	Le projet peut être configuré de sorte que seuls les utilisateurs correspondant à un profil configuré puissent y accéder. Un « Nom d'utilisateur » et « Mot de passe » sont requis pour accéder au système.
	e. Horodatage et traces informatique	Les actions de l'utilisateur, connexion, déconnexion, acquittement d'alarmes et changement de consignes, peuvent toutes être enregistrées dans des fichiers de consignation. Le fichier d'évènements est protégé des modifications intentionnelles. Un mécanisme complémentaire permettant d'enregistrer d'autres actions de l'utilisateur (générer un rapport, ouvrir un synoptique, etc.) peut être réalisé applicativement. Le traçage des actions opérateur telles que modification d'une consigne (ancienne et nouvelle valeur) est possible. Tous les évènements système peuvent être sauvegardés dans les fichiers de consignation.

	f. Test pour prouver le contrôle	Ceci relève du développement applicatif.
	g. Système limité aux Utilisateurs autorisés.	Toutes opérations de modifications, d'accès au système d'exploitation sont limitées aux exploitants appropriés. Un historique d'attribution et d'évolution des droits d'accès doit être crée. Il est également possible de s'appuyer sur un annuaire utilisateur Windows (Active Directory) pour contrôler l'accès à l'application de supervision.
	h. Validation de la source de données.	Afin de valider l'origine de la source d'entrée de données, le concepteur du système doit tenir compte de l'architecture producteur/consommateur de **PcVue** afin de limiter le stockage des données à des postes dédiés (serveur d'archive) pour que la génération soit unique.
	i. Formation des Utilisateurs système.	ARC Informatique propose des formations relatives à la configuration de **PcVue**. Une formation sur un projet spécifique est en principe réalisée par les personnes en charge du développement du projet. Les utilisateurs d'une application impliquée dans un système réglementé doivent posséder la formation et l'expérience nécessaire pour accomplir leurs tâches.
	j. L'application de signatures électroniques est légalement reconnue comme un engagement.	Le client utilisateur est responsable du développement des modalités et procédures permettant l'utilisation d'une application dans un environnement réglementé.
	k.(1) Contrôle approprié sur les documents. Distribution	ARC Informatique fournit des manuels d'utilisation à ses clients à

	de documents, révision et changement des contrôles	l'achat du logiciel. Ces manuels sont fournis sur CD-ROM en lecture seule et ne doivent pas être modifiés par le client. Il est de la responsabilité du client utilisateur de maintenir le contrôle sur la destination, l'accès et l'utilisation de cette documentation.
	k.(2)Traçabilité des modifications des versions logicielles. - Historique des versions.	La liste des principales modifications apportées à **PcVue** est consignée sur un document « lisezmoi.txt » installé avec la release logicielle. Des additifs décrivant l'implémentation des nouvelles fonctionnalités sont fournis dans la documentation électronique. Une liste exhaustive et détaillée des nouveautés et corrections existe sur un document ARC Informatique. Pour la traçabilité des modifications applicatives, **PcVue** dispose d'une fonction « Gestion des Versions » permettant de tracer les évolutions apportées au projet et de restituer en cas de besoin la version d'origine, et d'un fichier traçant les modifications apportées aux variables.
11.30	Cryptage de données pour les systèmes ouverts. Un système ouvert a un contrôle limité ou non quant aux interfaces utilisateurs.	**PcVue** peut être configuré comme système propriétaire, dans ce cas là, toutes les fonctions de **PcVue** et du système d'exploitation sont réservées aux Utilisateurs autorisés. Toutes les informations collectées font partie du Projet et peuvent être générées uniquement par **PcVue** sauf export explicite.
11.50(a)	Les signatures électroniques contiennent les informations suivantes	
11.50(a)(1)	Nom du signataire	Le « Login » utilisateur est actuellement tracé lors de la connexion ou déconnexion de cet utilisateur.

11.50(a)(2)	Horodate de la signature électronique	Toute connexion ou déconnexion d'un utilisateur est horodatée dans les évènements de PcVue.
11.50(a)(3)	La signification de la signature (approbation, niveau de responsabilité)	La boite de dialogue de définition d'un utilisateur contiendra à terme les champs Nom, Prénom et Qualité.
11.50(b)	Les éléments de signature ci-dessus doivent être apparents dans toute lecture, extraction ou impressions d'enregistrements ou rapports	
11.70	Les signatures électroniques ne doivent pas pouvoir être falsifiées. L'enregistrement et la signature sont liés. - La signature est protégée pour empêcher son transfert vers un autre enregistrement. Celui-ci est protégé contre toute modification de signature. - Toute modification de signature doit être consignée.	Le nom de l'opérateur (Login) figure dans chaque enregistrement. Il est très difficile, voire impossible de transférer une signature d'un enregistrement vers un autre dans des archives PcVue définies au format binaire. Le fichier user.dat peut être crypté selon un codage ARC Informatique. La nature BINAIRE du fichier d'enregistrement interdit toute tentative de falsification.

1.4 Paragraphe C – Signatures Electroniques

Section	Réglementation	CONFORMITE
11.100	a. Les signatures électroniques doivent être uniques pour chaque individu.	Un "Nom d'utilisateur" ainsi qu'un "Mot de passe" uniques sont délivrés à chaque utilisateur ayant un profil configuré. Les anciens « Mot de passe » sont mémorisés et ne sont plus réutilisables, pour les « Login » la modification est en cours.
	b. Les signatures électroniques doivent être comparées à la signature authentique.	Le client utilisateur d'une application dans un environnement réglementé par la FDA doit prendre en charge la vérification de l'identité des personnes susceptibles d'utiliser des signatures électroniques.
	c. Les signatures électroniques doivent être reconnues légalement comme un engagement.	Le client utilisateur d'une application dans un environnement réglementé par la FDA doit être en mesure de certifier que les signatures électroniques de son système sont destinées à être utilisées comme l'équivalent légal de signatures manuscrites traditionnelles.
11.200	Les signatures électroniques doivent comporter les 2 éléments suivants : - Nom d'utilisateur et mot de passe. - doivent être utilisées par leur véritable propriétaire.	Un nom d'utilisateur ainsi qu'un mot de passe unique sont délivrés à chaque utilisateur ayant un profil configuré. Il est de la responsabilité de l'utilisateur de fournir la meilleure sécurité afin de prévenir contre une utilisation frauduleuse des mots de passe.
	a.(1)(i)) Signature nom – mot de passe pour une période d'accès continue au système.	PcVue oblige l'utilisateur à ressaisir son nom et mot de passe lorsqu'il se connecte au système. Il est également possible de contraindre l'utilisateur à ressaisir son mot de passe avant toute action critique.

	a.(1)(ii)) signature d'un ou plusieurs documents dans des périodes discontinues	PcVue intègre un paramètre « temps d'inactivité » pour chaque utilisateur. L'expiration de ce délai provoque le « Delog » automatique et nécessite que chaque utilisateur accédant au système ressaisisse son nom et mot de passe.
	a.(3)) Tentative d'utilisation de la signature électronique d'un individu par quiconque d'autre que son propriétaire	Pour permettre à un utilisateur non habilité d'intervenir occasionnellement sur l'application, il est possible d'utiliser l'option « Double Signature » intégrée dans **PcVue**. Cette fonction nécessite les « Login » et « Mot de Passe » d'au moins deux utilisateurs distincts.
11.300	Les signatures électroniques qui sont conformes à la section 11.200 et qui sont composées de 2 éléments doivent également :	
	a. être uniques	Toute combinaison « Login » et « mot de passe » est unique. Il est impossible de définir deux utilisateurs possédant le même « Login ». un mot de passe n'est pas réutilisable plusieurs fois.
	b. être périodiquement demandées ou revalidées (expiration nom et mot de passe utilisateur)	La configuration de **PcVue** oblige l 'utilisateur à modifier son mot de passe, tous les n jours (n'étant paramétrable de 1 jour à 12 mois).
	c. être générées de telle sorte que le risque de perte ou de compromis sur les mots de passe soit minimisé	Ceci relève d'une procédure interne à la charge du client. Après le premier changement du mot de passe sur l'initiative de l'utilisateur, celui-ci est le seul à le détenir.
	d. résister, de façon prouvée, à toute utilisation frauduleuse.	Une solution intégrée générant à l'issue de 3 tentatives infructueuses une alarme tracée dans les archives est proposée dans **PcVue**.

		Il est possible de notifier l'administrateur système par email ou SMS de la tentative d'accès frauduleuse à l'application.
	e. un système de cartes coup de poing doit être opérationnel, de façon prouvée, pour cet utilisateur discret.	Il appartient au constructeur de système de lecteur de badges de garantir l'inviolabilité de sa fourniture et d'assurer l'interfaçage de celui-ci avec le système informatique.

ARC Informatique
Siège social
2 avenue de la Cristallerie
92310 Sèvres - France

tel + 33 1 41 14 36 00
fax + 33 1 46 23 86 02
hotline +33 1 41 14 36 25
arcnews@arcinfo.com
www.pcvuesolutions.com

Aix-en-provence
Le Galice Mirabeau - Bât C
11, rue Louise Colet
13090 AIX EN PROVENCE
Tel: + 33 4 42 52 36 83
Fax: + 33 4 42 29 74 55
email: arcaix@arcinfo.com

Grenoble
120, chemin de l'étoile
38330 Montbonnot Saint-Martin – France
Tel: + 33 4 76 1873 01
Fax: + 33 4 76 41 06 71
email: arcgrenoble@arcinfo.com

Lyon
Les Jardins d'Eole
1, allée des Séquoias «Le Shamal»
69760 LIMONEST - France
Tel: + 33 4 78 35 93 93
Fax: + 33 4 78 35 35 92
email: arclyon@arcinfo.com

Strasbourg
Immeuble le Véga
5 rue de Dublin
67300 Schiltigheim - France
Tel: +33 3 88 210 210
Fax: +33 3 88 210 211
email:arcstrasbourg@arcinfo.com

ARC Informatique
Société Anonyme au capital de
1 250 000 € - RCS Nanterre B 320
695 356- APE 5829C - SIREN 320
695 356- VAT N° FR 19 320 695 356

PcVue Solutions
21CFR part 11 FR

Certifiée ISO 9001 et ISO 14001