

ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DE COMPTEURS DE PARTICULES AU SEIN DE LA PHARMACIE CENTRALE DES ARMEES (P.C.A)

SOMMAIRE :

1. OBJET ET CONTEXTE DU MARCHE	2
1.1. OBJET.....	2
1.2. CONTEXTE.....	2
2. ABREVIATIONS.....	2
3. GLOSSAIRE	3
4. REFERENTIELS.....	4
5. ORGANISATION DU FOURNISSEUR.....	4
5.1. DOCUMENTATION.....	4
5.2. HYGIENE ET SECURITE.....	4
5.3. COMPETENCES.....	4
5.4. LIEU D'EXECUTION	4
5.5. DEVELOPPEMENT DURABLE	5
6. DESCRIPTIF DU BESOIN	5
6.1. LOTS 1 A 4 : VERIFICATION METROLOGIQUE ET MAINTENANCE DE COMPTEURS DE PARTICULES FIXES ET MOBILES AU SEIN DE LA PCA.....	5
6.2. LOT 5 : ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DE NOUVEAUX COMPTEURS DE PARTICULES DANS L'AIR	9
6.3. LOT 6 : ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DE NOUVEAUX COMPTEURS DE PARTICULES EN MILIEU LIQUIDE :	26
7. ANNEXES	42
7.1. ANNEXE 1	42
7.2. ANNEXE 2.....	42

PCA Production	Cahier des charges	Page 2 / 43
ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DES COMPTEURS DE PARTICULES FIXES ET MOBILES AU SEIN DE LA PHARMACIE CENTRALE DES ARMEES (P.C.A)		

1. OBJET ET CONTEXTE DU MARCHE

1.1. OBJET

Le but de ce document est de préciser les modalités pour l'acquisition, la mise en route, la qualification, la maintenance et la métrologie des compteurs de particules fixes et mobiles utilisés en production et au laboratoire de contrôle qualité au profit de la Pharmacie Centrale des Armées.

La prestation se déroulera en 6 lots séparés en 2 types de prestations :

- 4 lots correspondant aux prestations de vérification métrologique, maintenance et dépannage des appareils actuels de la PCA
- Un lot correspondant à une prestation d'acquisition, d'installation, de mise en route et de qualification des appareils de comptage particulaire dans l'air, ainsi que la vérification métrologique et la maintenance
- Un lot correspondant à une prestation d'acquisition, d'installation, de mise en route et de qualification des appareils de comptage particulaire en milieu liquide, ainsi que la vérification métrologique et la maintenance

Les prestations ont lieu à l'adresse suivante :

Pharmacie Centrale des armées
Camp d'Orléans Chateau
45404 Fleury les Aubrais cedex

1.2. CONTEXTE

La Pharmacie centrale des armées est un établissement possédant un ensemble de zones à atmosphère contrôlées de classe A, B, C et D (selon les bonnes pratiques de fabrication (BPF)).

Ces zones obéissent au référentiel BPF qui imposent la vérification, l'étalonnage ainsi que le maintien en l'état des équipements de contrôles.

A titre informatif, au moment de la notification du marché, l'ensemble des installations comprend 23 compteurs de particules fixes et mobiles (Annexe 1), qui sont répartis de la manière suivante :

• AEROTRACK :

- o Aerotrack 6510 : 8 compteurs
- o Aerotrack 7510 : 2 compteurs

• AIRNET

- o AIRNET II : 11 compteurs

• LASAIR

- o LASAIR II 310,350 550 : 1 compteur

• APSS

- o APSS-200 USP : 1 compteur

2. ABREVIATIONS

AQ Assurance qualité

PCA Production	Cahier des charges	Page 3 / 43
ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DES COMPTEURS DE PARTICULES FIXES ET MOBILES AU SEIN DE LA PHARMACIE CENTRALE DES ARMEES (P.C.A)		

BPF	Bonnes Pratiques de Fabrication
FDA	Food and Drug Administration
USP	Pharmacopée américaine
PE	Pharmacopée Européenne
COFRAC	COMité FRANçais d'ACcréditation
PCA	Pharmacie Centrale des Armées
PCA/AQ	service d'assurance de la qualité de la Pharmacie Centrale des Armées
PCA/PROD	service de production de la Pharmacie Centrale des Armées
PCA/MAINT	service de maintenance de la Pharmacie Centrale des Armées
PMAQ	Plan de Management d'Assurance Qualité
QC	Qualification de conception
QI	Qualification d'installation
QO	Qualification opérationnelle
QP	Qualification de performance
SAT	Site Acceptance Tests (= TAS)
SSA	Service de Santé des Armées
TAS	Tests d'acceptation sur site (= SAT)
VHP	Procédé de bio-décontamination au peroxyde d'hydrogène vaporisé

3. GLOSSAIRE

Maintenance préventive: Intervention permettant le remplacement systématique de certains composants d'usure courante, de vérification de l'état du matériel et son bon fonctionnement, mécanique, électrique et automatisme.

Analyse de Risque Fonctionnelle (ARF): Document permettant de minimiser les risques pour garantir que les produits pharmaceutiques sont sûrs, efficaces et conformes aux exigences réglementaires.

Tests d'acceptation sur site (TAS) ou Site acceptance tests (SAT): Il s'agit de tests d'ingénierie réalisés sur site qui vont permettre au donneur d'ordre de s'assurer que l'équipement est conforme au cahier des charges et que les différentes fonctions donnent satisfaction afin de valider l'acceptation ou non de l'équipement. Il est accepté du côté donneur d'ordre de capitaliser sur ces tests pour la qualification pharmaceutique de l'équipement. Ces tests devront être réalisés en amont des tests de QI et de QO.

Les TAS / SAT sont considérés acceptés si aucune non-conformité critique n'est observée.

En cas de conformité critique, le donneur d'ordre se réserve le droit de réaliser de nouveau cette phase.

Qualification de conception (QC): Vérification documentée attestant que la conception proposée pour les installations, les systèmes et les équipements convient pour l'objectif visé.

Qualification d'installation (QI): Vérification documentée attestant que les installations, les systèmes et les équipements, tels qu'ils sont installés ou modifiés, sont conformes à la conception approuvée et aux recommandations du fabricant. Elle comporte au moins les éléments suivants :

1. Vérification de l'installation correcte des composants, de l'instrumentation, des équipements, des canalisations et des utilités par rapport aux schémas techniques et aux spécifications.
2. Vérification de la conformité de l'installation par rapport aux critères prédéfinis.
3. Collecte et rassemblement des instructions de fonctionnement, de mise en œuvre et des exigences en matière de maintenance du fournisseur.
4. Exigences en matière d'étalonnage.
5. Vérification des matériaux de construction, certificats matière.

Qualification opérationnelle (QO): Vérification documentée attestant que les installations, les systèmes et les équipements, tels qu'ils sont installés ou modifiés, fonctionnent comme prévu dans les gammes de fonctionnement escomptées. Elle comporte au moins les éléments suivants :

1. Essais développés à partir de la connaissance des procédés, systèmes et équipements.
2. Essais visant à inclure une condition ou un ensemble de conditions englobant les limites d'exploitation supérieures et inférieures, parfois qualifiées de conditions représentatives du « pire cas ».

PCA Production	Cahier des charges	Page 4 / 43
ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DES COMPTEURS DE PARTICULES FIXES ET MOBILES AU SEIN DE LA PHARMACIE CENTRALE DES ARMEES (P.C.A)		

3. Tests de sauvegarde et de restauration de l'applicatif.

Change Control (CC): le Change Control est une réponse aux exigences réglementaires par laquelle des représentants qualifiés des disciplines concernées évaluent les changements proposés susceptibles d'affecter le statut de validation des équipements, des locaux, des utilités, des systèmes informatisés (SI) et des procédés. L'objectif est de déterminer les mesures pouvant s'avérer nécessaires pour garantir et démontrer le maintien de l'état validé de l'élément concerné. L'évaluation doit permettre de définir la nécessité ou non de réaliser des qualifications/validations.

4. REFERENTIELS

- Code du travail
- Code de la santé publique
- Code de l'environnement
- Bonnes Pratiques de Fabrication (BPF)
- 21CFR Part 11 (Norme Américaine relative à la traçabilité informatique des systèmes et équipements)
- Norme ISO 21501-4
- Norme ISO 14644
- USP 788
- Directive N°39 PORTANT SUR LA SÉCURITÉ NUMÉRIQUE DES SYSTÈMES INDUSTRIELS (DIR-SNSI).

5. ORGANISATION DU FOURNISSEUR

5.1.DOCUMENTATION

Tous les documents liés à l'exécution de ce marché sont référencés, datés et signés. Une traçabilité documentaire est réalisée par le titulaire, comprenant à minima une identification des documents et gestion des modifications.

5.2. HYGIENE ET SECURITE

La PCA étant un établissement pharmaceutique, le prestataire doit se soumettre aux règles d'hygiène et aux conditions et contraintes d'accès aux différents locaux. Un plan annuel de prévention est également établi avant toute première intervention.

5.3. COMPETENCES

Le prestataire doit démontrer la compétence de son organisation dans le domaine métrologique et informatique requis.

L'ensemble des prestations doit être conforme aux prescriptions des décrets, arrêtés, règlements, normes, règles de l'art et à celles de tous les textes subséquents, en vigueur au premier jour du mois d'exécution des prestations et pendant toute la durée du marché.

Le titulaire est réputé connaître et maîtriser les technologies des divers matériels et installations dont il a la charge au titre du présent marché. Il ne peut, en tout état de cause, prétendre à bénéficier d'une quelconque formation.

Pendant toute la durée du marché, le titulaire est responsable des dommages qui peuvent être causés de son fait, soit aux personnes, soit aux biens, soit aux installations dont il assure l'exploitation.

Le titulaire prend à sa charge les risques de toute nature et, notamment, ceux de responsabilité civile (accidents, incendies, explosions, vols, dégâts des eaux) découlant du marché. Il s'assure en conséquence.

5.4. LIEU D'EXECUTION

Les prestations sont principalement exécutées sur le site concerné. Les modalités d'accès et d'exécution seront définies d'un commun accord entre le responsable du bureau métrologie de l'établissement détenteur du matériel et le titulaire.

PCA Production	Cahier des charges	Page 5 / 43
ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DES COMPTEURS DE PARTICULES FIXES ET MOBILES AU SEIN DE LA PHARMACIE CENTRALE DES ARMEES (P.C.A)		

Le titulaire a pour obligation :

- D'apporter la preuve que les moyens de mesure employés pour l'étalonnage sont régulièrement étalonnés dans des laboratoires accrédités (COFRAC (COmité FRançais d'ACcréditation) ou autres accréditation équivalent) assurant ainsi la traçabilité jusqu'aux étalons nationaux ;
- En fonction des prestations, de se conformer aux normes NF EN ISO/CEI 17025, ISO 21501-4, ou toutes normes abrogeant celles-ci ;
- De disposer d'une expertise significative dans les domaines concernés par les prestations ;
- De réaliser sa propre veille réglementaire relative à l'évolution des recommandations et méthodes de référence ;
- De fournir les attestations de formations et habilitations individuelles des personnels intervenants.

Dans le cadre de l'exécution du présent accord-cadre, le titulaire n'est pas autorisé à :

- Communiquer les renseignements, documents ou objets dont il a pris connaissance dans le cadre de l'exécution de la prestation, ou de sa présence sur le site ;
- Se prévaloir dans l'exercice du marché d'une quelconque ignorance du cadre réglementaire d'une manière générale, de tout texte et de toute réglementation intéressant son activité pour l'exécution du présent marché.

Si le cas se présente, le titulaire, ainsi que l'ensemble de ses sous-traitants sont soumis à ces obligations.

5.5. DEVELOPPEMENT DURABLE

Le titulaire doit décrire dans son offre technique les actions mises en place pour le traitement et le recyclage des déchets, la diminution des émissions polluantes et les économies d'énergie.

6. DESCRIPTIF DU BESOIN

6.1.LOTS 1 A 4 : VERIFICATION METROLOGIQUE ET MAINTENANCE DE COMPTEURS DE PARTICULES FIXES ET MOBILES AU SEIN DE LA PCA

6.1.1. DESCRIPTION DES LOTS :

Les prestations de Vérifications métrologiques, étalonnage, maintenances préventive et corrective sont découpées en 4 lots :

- Lot 1 : Vérification métrologique, étalonnage, maintenances préventive et corrective pour les compteurs de marque AEROTRACK.
- Lot 2 : Vérification métrologique, étalonnage, maintenances préventive et corrective pour les compteurs de marque AIRNET.
- Lot 3 : Vérification métrologique, étalonnage, maintenances préventive et corrective pour les compteurs de marque LASAIR.
- Lot 4 : Vérification métrologique, étalonnage, maintenances préventive et corrective pour les compteurs de type APSS.

Le détail des compteurs et leurs numéros de série sont présents en Annexe 1 de ce document.

6.1.2. GENERALITES

Les prestations sur site doivent être réalisées obligatoirement du lundi au jeudi de 8h00 à 17h00 et le vendredi de 8h00 à 12h00.

PCA Production	Cahier des charges	Page 6 / 43
ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DES COMPTEURS DE PARTICULES FIXES ET MOBILES AU SEIN DE LA PHARMACIE CENTRALE DES ARMEES (P.C.A)		

Le personnel intervenant doit se présenter à chaque entrée et sortie du site. Il doit être qualifié et détenir une expérience dans le domaine concerné par les prestations du présent marché. Il est accompagné tout au long de son intervention.

Un système de protection du personnel isolé (équipements de protection individuelle (EPI)) est également mis à la disposition du titulaire pour tous les personnels sur site étant amenés à travailler seul.

Aucune installation ne peut être mise à l'arrêt par un technicien du titulaire sans en avoir, au préalable, prévenu le pharmacien responsable (Annexe 1).

L'obligation de résultat impose au titulaire :

- La planification des visites d'étalonnage et de vérification métrologique des capteurs de la PCA, en fonction de la taille du parc et dans le respect des délais imposés par la durée de validité des certificats, constats et rapports de test ; les dates d'intervention doivent être proposées au plus tard deux (2) mois avant les prestations, la PCA procède à une validation des dates d'interventions qui peuvent être modifiées en fonction des plannings de production. Aucune modification desdites dates n'est possible dans les 15 jours précédents une intervention.
- Le respect de cette planification.

6.1.3. ÉTALONNAGE ET VERIFICATION DES COMPTEURS DE PARTICULES FIXES ET MOBILES DE LA PCA.

Il est demandé au prestataire de réaliser l'ensemble des opérations d'étalonnage et de vérification des compteurs de particules fixes et mobiles sur site. En cas d'impossibilité d'une intervention sur site l'opération est réalisée dans les locaux du prestataire avec prise en charge des frais de conditionnement et de transport aller/retour depuis et vers la PCA.

L'ensemble des prestations d'étalonnage et de vérification des compteurs de particules fixes et mobiles s'exécutent conformément à la norme ISO 21501-4 en vigueur ou toute autre norme abrogeant celle-ci, au minimum une fois par an.

Pour les lot 1 et 2, les chaînes de mesures sont étalonnées du compteur jusqu'à la supervision du logiciel FMS5 et VALIDAIR qui doit être vérifiée. La mise à jour du numéro du certificat d'étalonnage est incluse dans la prestation.

6.1.4. TRAÇABILITE

Dans les 24 heures suivant l'intervention pour les lots 1, 2, 3 et 4, et le repositionnement des compteurs de particules, un rapport d'intervention est remis au responsable du suivi des prestations par mail au format PDF (Annexe 1), et doit mentionner au minimum :

- L'ensemble des prestations exécutées pendant l'intervention (et dans les locaux du titulaire pour tous les lots), clairement décrites ;
- Les matériels concernés par la prestation ;
- La date, le nom, fonction et signature de l'intervenant.

6.1.5. ÉTIQUETAGE

Après chaque intervention et/ou lors du remontage, il est procédé à un étiquetage des matériels étalonnés et/ou vérifiés. Une étiquette est positionnée sur le matériel afin d'être immédiatement visible par tous les utilisateurs potentiels, elle renseigne au minimum sur la période de validité de la conformité métrologique :

- Date du dernier étalonnage ou vérification ;
- Numéro du certificat ou constat de vérification en cours de validité, localisation ;
- Date du prochain étalonnage ou vérification.

6.1.6. PARTICULARITES

En cas d'impossibilité d'étalonner ou d'avarie majeure ou de non-conformité d'un des compteurs, le titulaire propose une date d'intervention de maintenance afin de proposer une réparation. Dans le cas où aucune réparation n'est possible un devis doit être proposée pour procéder au remplacement de celui-ci ainsi que

PCA Production	Cahier des charges	Page 7 / 43
ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DES COMPTEURS DE PARTICULES FIXES ET MOBILES AU SEIN DE LA PHARMACIE CENTRALE DES ARMEES (P.C.A)		

son raccordement au logiciel FMS5 édité par TSI de la PCA. Ce devis doit être conforme à l'annexe financière et être accepté par l'établissement et se traduit par l'émission d'un bon de commande.

6.1.7. DEROULE DES INTERVENTIONS

Pour les lots 1 et 2, le prestataire doit procéder au démontage des compteurs de particules fixes et raccordés au logiciel FMS5-FMS (Factory monitoring system), de ce fait, il est demandé au titulaire de disposer de l'outillage nécessaire afin de réaliser cette opération.

Le technicien intervenant est obligatoirement accompagné par un personnel de la PCA, afin de réaliser les prestations situées dans les zones stériles, à cet effet le technicien dispose d'EPI mis à disposition par la PCA (à noter que certains compteurs sont situés dans des espaces étroits et obligent à un travail au sol).

Le titulaire effectue sur site une vérification métrologique des compteurs avec ajustage puis un test de conformité, conformément à la norme 21501-4 en vigueur ou toute autre norme abrogeant celle-ci.

La norme décrit en détail les paramètres à vérifier et leurs limites acceptables.

Les paramètres pris en considération sont :

- Débit de prélèvement ;
- Efficacité de comptage ;
- Vérification de la précision du positionnement en taille ;
- Résolution sur la taille ;
- Faux comptages sur absence totale de particules ;
- Rapidité de la réponse ;
- Temps d'échantillonnage ;
- Concentration maximale acceptable ;
- Étalonnage en taille (à ne pas confondre avec « la précision du positionnement en taille »).

Une prestation d'étalonnage donne lieu à un étiquetage du matériel étalonné et à l'émission d'un certificat d'étalonnage.

Lorsqu'un compteur à étalonner a été ajusté ou réparé, les résultats d'étalonnage avant et après l'ajustage ou la réparation doivent être rapportés dans le rapport d'intervention.

Une fois l'ensemble des opérations nécessaires effectuées, le prestataire procède au repositionnement des compteurs de particules fixes, conformément à leurs emplacements initiaux.

6.1.8. RAPPORT DE TEST ET CERTIFICAT D'ETALONNAGE

Après chaque intervention, le titulaire doit établir un rapport de test et un certificat d'étalonnage mentionnant dans les deux cas, les informations minimales suivantes doivent être consignées dans un rapport de test :

- Date de l'essai / étalonnage ;
- Particules d'essai / d'étalonnage utilisées ;
- Résultats pour les paramètres :
 - 1) Erreur de réglage de la taille ;
 - 2) Efficacité de comptage ;
 - 3) Erreur de débit d'échantillonnage ;
 - 4) Résolution en taille (avec la taille de particule utilisée) ;
 - 5) Faux compte ;
- Les valeurs de tension de seuil ou les canaux du PHA intégrés correspondant aux réglages de taille ;
- Une déclaration de la méthode d'essai / d'étalonnage utilisée (par exemple, ISO 21501-4 en vigueur) ;
- L'identification du rapport / certificat, le lieu de l'essai / de l'étalonnage, le titre et l'identification de l'essai / l'étalonnage fournisseur avec signature et date ;

PCA Production	Cahier des charges	Page 8 / 43
ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DES COMPTEURS DE PARTICULES FIXES ET MOBILES AU SEIN DE LA PHARMACIE CENTRALE DES ARMEES (P.C.A)		

- Identification du client et du dispositif testé, y compris comment la sortie a été obtenue pour le comptage efficacité (par exemple analogique, affichage ou sortie numérique).

Un certificat d'étalonnage doit en outre comprendre :

- Identification et déclaration de traçabilité métrologique de tout le matériel de référence et les particules d'étalonnage utilisées ;
- Les conditions environnementales pertinentes (température, pression atmosphérique et humidité, par exemple) dans lesquelles l'étalonnage a été effectué ;
- Une incertitude déclarée pour chaque résultat pour les paramètres 1 à 4 (voir ci-dessus) en référence au calcul méthode (p. ex. Guide ISO / CEI 98-3) – voir Annexe E de la norme ISO 21501-4 qui contient des procédures pour évaluer l'incertitude des résultats des tests de performance recommandés dans ce document pour les paramètres 1 et 2 (voir ci-dessus) ;
- Un faux compte déclaré à une limite de confiance de 95% (voir Annexe C de la norme ISO 21501-4).

Les certificats d'étalonnage et rapports de test doivent être envoyés dans le mois suivant les interventions à la personne responsable du suivi des prestations ((Annexe 1) en format PDF).

Après chaque intervention, le titulaire doit établir un rapport de test et un certificat d'étalonnage mentionnant dans les deux cas, les informations minimales suivantes doivent être consignées dans un rapport de test :

- Date de l'essai / étalonnage ;
- Particules d'essai / d'étalonnage utilisées ;
- Résultats pour les paramètres :
 - 1) Erreur de réglage de la taille ;
 - 2) Efficacité de comptage ;
 - 3) Erreur de débit d'échantillonnage ;
 - 4) Résolution en taille (avec la taille de particule utilisée) ;
 - 5) Faux compte ;
- Les valeurs de tension de seuil ou les canaux du PHA intégrés correspondant aux réglages de taille ;
- Une déclaration de la méthode d'essai / d'étalonnage utilisée (par exemple, ISO 21501-4 en vigueur) ;
- L'identification du rapport / certificat, le lieu de l'essai / de l'étalonnage, le titre et l'identification de l'essai / l'étalonnage fournisseur avec signature et date ;
- Identification du client et du dispositif testé, y compris comment la sortie a été obtenue pour le comptage efficacité (par exemple analogique, affichage ou sortie numérique).

Un certificat d'étalonnage doit en outre comprendre :

- Identification et déclaration de traçabilité métrologique de tout le matériel de référence et les particules d'étalonnage utilisées ;
- Les conditions environnementales pertinentes (température, pression atmosphérique et humidité, par exemple) dans lesquelles l'étalonnage a été effectué ;
- Une incertitude déclarée pour chaque résultat pour les paramètres 1 à 4 (voir ci-dessus) en référence au calcul méthode (p. ex. Guide ISO / CEI 98-3) – voir Annexe E de la norme ISO 21501-4 qui contient des procédures pour évaluer l'incertitude des résultats des tests de performance recommandés dans ce document pour les paramètres 1 et 2 (voir ci-dessus) ;
- Un faux compte déclaré à une limite de confiance de 95% (voir Annexe C de la norme ISO 21501-4).

Les certificats d'étalonnage et rapports de test doivent être envoyés dans le mois suivant les interventions à la personne responsable du suivi des prestations ((Annexe 1) en format PDF).

PCA Production	Cahier des charges	Page 9 / 43
ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DES COMPTEURS DE PARTICULES FIXES ET MOBILES AU SEIN DE LA PHARMACIE CENTRALE DES ARMEES (P.C.A)		

6.1.9. MODALITES D'EXECUTION

Des bons de commandes sont émis par l'administration selon les besoins du service avec facturation à l'issue de la réception de la prestation.

Les interventions s'effectuent conformément à la validation de la planification des visites (cf. article 6.1.2 du CCTP) pour les opérations d'étalonnage et de vérification. Le bon de commande est transmis au titulaire au plus tard dans les 7 jours précédents une intervention.

Le prestataire doit respecter le délai planifié pour réaliser les prestations de démontage, étalonnage et/ou vérification et remontage des compteurs dans les locaux de la PCA.

Dans le cadre d'une demande de remplacement d'un élément des compteurs (pompe, compteur, pièce détachée etc.) le titulaire dispose d'un délai de 15 jours pour proposer un devis, à compter de l'émission du bon de commande. Le titulaire dispose ensuite d'un délai de 8 semaines à compter de la pour procéder à la livraison.

En cas de non-respect des délais, des pénalités seront appliquées.

6.1.10. LIVRABLES

A l'issue de chaque intervention, le titulaire remettra un rapport d'intervention conformément à l'article 6.1.4 du présent CCTP et procédera à un étiquetage des capteurs étalonnés et vérifiés comme décrit à l'article 6.1.5 du CCTP.

En fonction du type de prestation, le titulaire établira un certificat d'étalonnage et un rapport de test comme décrit à l'article 6.1.8 du présent CCTP, ou un bon de livraison dans le cas d'un remplacement de compteur ou de pompe.

La facturation ne peut être établie qu'à l'issue de la transmission du certificat ou rapport de test ou bon de livraison.

6.2. LOT 5 : ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DE NOUVEAUX COMPTEURS DE PARTICULES DANS L'AIR

Ce lot concerne l'acquisition de compteurs à particules dans l'air destinés à compléter et/ou remplacer le parc actuel en fonction des besoins.

Les équipements concernés et leurs modalités d'approvisionnement doivent respecter les exigences ci-après.

Leur acquisition fait l'objet de bons de commandes sur la base des stipulations figurant dans l'annexe financière à l'acte d'engagement relative au présent lot.

6.2.1. PHASAGE ET LIVRABLES ATTENDUS

Etape		F	PCA/PROD	PCA/MAINT PCA/INFRA PCA/INFO	PCA/AQ
Conception des appareils Livrables :		R	V	V	A
N°	Livrables				
L1.1	Documents de conception				
L1.2	Spécifications techniques des équipements				
Installation, mise en route des appareils, nettoyage et calibration initial Livrables :		R		V	A
N°	Livrables				
L2.1	Installation des appareils aux endroits indiqués en ZAC.				
L2.2	Rapport de mise en route des appareils et de calibration				
Branchement des équipements aux utilités et au logiciel FMS 5 et mise en route. Livrables :		R		V	
N°	Livrables				
L3.1	Comptes rendus				
Qualification des éléments installés.		R	V	V	A
N°	Livrables				
L4.1	Analyse des risques fonctionnelle				
L4.2	Qualification de conception				
L4.3	Protocole de QI				
L4.4	Exécution de la QI				
L4.5	Rapport de QI				
L4.6	Protocole de QO				
L4.7	Exécution de la QO				
L4.8	Rapport de QO				
Fourniture des documents demandés (DOE). Livrables :		R	V	V	A
N°	Livrables				
L5.1	Un manuel d'utilisation en français				
L5.2	Certificat CE.				
L5.3	Les schémas électriques et pneumatiques.				
L5.4	Le programme d'installation				
L5.5	Un plan de maintenance décrivant notamment les procédures et fréquences des maintenances préventives et éléments d'usure à remplacer.				
L5.6	Les certificats d'étalonnage de l'instrumentation en place et de celle utilisée pour la mise en service				
L5.7	Les certificats matières				
L5.8	Support informatique comprenant tous les documents				

R = réalise ; V = vérifie ; A = approuve

6.2.2. EXIGENCES

6.2.2.1. REGLEMENTAIRES

N°	Objet	Tolérance	Exigence
E1.01	Code du travail	Obligatoire	• Equipements conformes aux règles techniques.
E1.02	BPF Européennes	Obligatoire	• Equipements conformes aux BPF européennes.
E1.03	Certificat CE	Obligatoire	• Equipements avec certificat CE.
E1.04	directive N°39 PORTANT SUR LA SÉCURITÉ NUMÉRIQUE DES SYSTÈMES INDUSTRIELS (DIR-SNSI)	Obligatoire	• Conformité des systèmes industriels à la directive 39 pour une classe 2 .
E1.05	Norme ISO 21501-4	Obligatoire	• Equipement conforme à la norme ISO 21501-4

PCA Production	Cahier des charges	Page 11 / 43
ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DES COMPTEURS DE PARTICULES FIXES ET MOBILES AU SEIN DE LA PHARMACIE CENTRALE DES ARMEES (P.C.A)		

6.2.2.2. SYSTEME INDUSTRIEL (DIRECTIVE 39 – Classe 2)

N°	Nature	Intitulé	SI	C2	Remarque	Responsable
Maîtriser l'organisation de la sécurité numérique						
ORG2	ORG	Dans un cadre contractuel, demander au prestataire de mettre en place une chaîne de responsabilité en matière de sécurité numérique pour les besoins de ses prestations.		O	Le point de contact peut être chargé de : - la liaison avec la chaîne de responsabilité de l'entité responsable - la garantie du respect de la politique de cyber sécurité ; - la communication sur les divergences par rapport aux exigences et les autres non-conformités.	SSA / F
ORG3	ORG	Le prestataire doit désigner en son sein un point de contact en matière de sécurité numérique qui est en charge de la liaison avec la chaîne de responsabilité SSI du ministère durant les phases amont (aider le RSSI-P dans le cadre de l'homologation) et aval du projet (aider le RSSI-A dans le cadre du maintien en condition de sécurité (MCS)). Ce point de contact est soit formé, soit accompagné d'un expert en sécurité.	O			F
Maîtriser les intervenants						
PERS1	ORG	Sensibiliser toute personne amenée à intervenir sur un système industriel aux risques numériques propres aux systèmes industriels. La sensibilisation est adaptée à leurs spécificités, à leur fonction et à leur environnement. Un point d'attention est à porter sur les administrateurs techniques et fonctionnels ainsi que sur les opérateurs.	O		La règle est aussi valable pour ceux qui interviennent dans la maintenance du système. Les séances de formation et de sensibilisation à la cyber sécurité des systèmes industriels peuvent être dispensées en même temps que les formations de sûreté et de sécurité du site.	SSA / F
PERS2	ORG	Former à la sécurité numérique le personnel amené à intervenir sur les systèmes industriels. La formation doit être adaptée à sa fonction, à son profil ou encore à ses droits d'accès dans le système. Un point d'attention est à porter sur : - les administrateurs techniques et fonctionnels ainsi que sur les opérateurs ; - les RSSI (RSSI-A, RSSI-P) s'ils ne sont pas accompagnés de spécialistes en sécurité numérique des systèmes industriels.	O			SSA / F
Intégrer la sécurité numérique dans le projet						
ISSIP2	ORG	Définir des procédures et des moyens techniques pour permettre des opérations de maintenance préventive et curative et ainsi maintenir le niveau de sécurité dans la durée.	O		Des modes dégradés peuvent être prévus pour réaliser des mises à jour. On peut configurer les sorties d'un automate pour qu'elles restent sur leurs derniers états, pendant la mise à jour de son firmware.	SSA / F
ISSIP4	ORG	Exiger que les opérations non indispensables à la conduite du système industriel soient effectuées sur un autre système d'information. Les équipements et logiciels associés ne doivent pas être présents sur le système industriel. À titre d'exemple, des postes bureautiques non connectés au système industriel doivent être prévus pour permettre la consultation de la documentation, le remplissage de feuilles de suivi, etc.	R			F
ISSIP14	TECH	En cas de développement réalisé au titre du système, appliquer les règles de bonnes pratiques, notamment la directive 40 (portant sur le développement des applications informatiques et des logiciels robustes du ministère).		O	Voir Directive DGNUM n°40 sur le développement robuste	F

PCA Production		Cahier des charges			Page 12 / 43	
ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DES COMPTEURS DE PARTICULES FIXES ET MOBILES AU SEIN DE LA PHARMACIE CENTRALE DES ARMEES (P.C.A)						
N°	Nature	Intitulé	SI	C2	Remarque	Responsable
ISSIP15	TECH	Dédier un environnement de développement aux opérations de développement du système industriel. Cet environnement ne peut être utilisé pour d'autres activités.		O		F
ISSIP16	TECH	Séparer l'environnement de développement de l'environnement de production.	O			F
ISSIP17	TECH	Protéger l'environnement de développement de manière à satisfaire aux mêmes besoins de sécurité du système industriel en matière de disponibilité, d'intégrité et de confidentialité. Il doit satisfaire aux mêmes exigences de sécurité auxquelles s'ajoutent des exigences de sécurité en matière de développement. En cas de prestation externe, fournir un plan d'assurance sécurité (PAS).	O			F
ISSIP18	ORG	Vérifier le niveau de sécurité de l'environnement de développement.		R		F
Protéger physiquement le système et les contrôles d'accès aux locaux, aux équipements et aux câblages						
PHY1	ORG	Appliquer les mesures de protection physique définies dans l'IGI 1300 et l'IM 900 si le système industriel traite de données classifiées ou portant une mention de protection Diffusion Restreinte.	O			F
PHY2	ORG TECH	Mettre en place des mécanismes de contrôle d'accès adaptés aux enjeux de sécurité du système industriel ou conformes aux réglementations selon la nature du système ou son niveau de confidentialité.	O			SSA / F
PHY7	ORG	Déployer les serveurs et les postes d'exploitation dans des locaux différents.		O		F
PHY11	TECH	Mettre en place un dispositif de détection d'ouverture avec remontée d'alarme sur les armoires des équipements sensibles. A minima, sur les coffrets extérieurs contenant des composants sensibles, un moyen de contrôle visuel, comme la pose de scellés par exemple, doit être installé. Le retrait de ces moyens visuels doit suivre une procédure bien définie et être soumis à autorisation préalable.		R		SSA / F
Maîtriser les zones de sécurité au sein du système industriel						
RSO2	TECH	Mettre en place un cloisonnement entre les zones de sécurité. Le cloisonnement est physique entre les zones de classe 3 et les zones de classe inférieure. L'utilisation de cloisonnement logique est alors interdite. Pour les autres niveaux de classe, privilégier autant que possible un cloisonnement physique entre les zones de sécurité.	O			F
RSO3	ORG	Lorsque la séparation physique n'est pas possible entre des zones de sécurité de classes différentes, mettre en place une solution de tunnel VPN labellisée.		O		F
RSO4	ORG	Lorsque la séparation de tunnel VPN n'est pas possible entre des zones de sécurité de classes différentes, mettre en place un cloisonnement logique de type VLAN.		O		F

N°	Nature	Intitulé	SI	C2	Remarque	Responsable
RSO5	TECH	Mettre en place une politique de filtrages entre les zones de sécurité. Les flux sont limités au strict besoin.	O		Pour définir une politique de filtrage, on peut notamment se reporter au guide de l'ANSSI. Pour les flux utilisant le protocole IP, on en rappelle néanmoins ici quelques grands principes : - un flux est identifié par l'adresse IP source, l'adresse IP destination, le protocole de transport (par exemple UDP ou TCP) et, le cas échéant, les numéros de port source et destination ; - tous les flux entrants ou sortants du système industriel doivent être journalisés. Les moyens assurant le filtrage peuvent être physiques et/ou dédiés selon les risques à couvrir et dans la mesure du possible. - les flux sont refusés par défaut ; - seuls les flux nécessaires au fonctionnement du système industriel sont autorisés ; - les flux rejetés doivent être journalisés et analysés ;	F
RSO6	TECH	Lorsque des flux non-IP doivent transiter entre deux zones distinctes, effectuer un filtrage sur les identifiants source et destination, ou un filtrage sur les protocoles autorisés.		O	Dans le cas d'Ethernet, on peut effectuer le filtrage* sur les adresses MAC source et destination.	F
RSO7	TECH	Mettre en place des flux unidirectionnels entre deux zones de classes différentes afin de n'autoriser les flux que de la zone de classe la plus élevée vers la zone de classe la moins élevée. Dans le cas de zones de classe 3, l'unidirectionnalité est assurée par une diode labellisée.	R		L'unidirectionnalité des flux peut être assurée par un pare-feu.	F
RSO8	TECH	Former au moins une zone de sécurité à part entière pour le réseau d'administration.		O		F
RSO9	TECH	Cloisonner le réseau d'administration des équipements des autres réseaux de manière physique.		R	Le périmètre porte sur les équipements d'informatique classique comme les commutateurs, passerelles, routeurs, pare-feu, etc.	F
RSO10	TECH	Protéger le système industriel du système d'information de gestion (niveau 4) par un dispositif de filtrage (pare-feu). Les flux sont limités au strict minimum.		O		F
RSO11	TECH	Proscrire l'usage de protocoles non sécurisés (telnet, http, ftp, etc.) en leur privilégiant des protocoles garantissant confidentialité, intégrité, authenticité des points communicants (https, ssh, sftp, bacnets-c). Si l'usage de protocoles non sécurisés est nécessaire pour des raisons techniques et opérationnelles, mettre en place des mesures compensatoires comme : - mettre en place des protections paramétriques (pare-feu) ; - encapsuler les flux dans un VPN pour en assurer l'authenticité et l'intégrité.	O			F
Maîtriser l'accès au réseau						
RSO13	TECH	Désactiver les points d'accès réseau non utilisés (commutateurs, automates, baies de brassage, prise de maintenance sur les bus de terrain, etc.).	O			F
RSO14	TECH	En cas de liens sans protection physique, déployer des passerelles VPN aux extrémités des liaisons pour protéger l'intégralité du trafic. L'équipement doit être positionné derrière un pare-feu ne laissant passer que les flux strictement indispensables. En particulier, le trafic externe au VPN doit être bloqué.		O		F

PCA Production	Cahier des charges	Page 14 / 43
ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DES COMPTEURS DE PARTICULES FIXES ET MOBILES AU SEIN DE LA PHARMACIE CENTRALE DES ARMEES (P.C.A)		

N°	Nature	Intitulé	SI	C2	Remarque	Responsable
RSO15	ORG	Protéger l'accessibilité des points d'accès réseau. Ils ne doivent être accessibles que dans des locaux, armoires ou coffrets à accès maîtrisés.		O		F
RSO16	TECH	Remonter une alerte en cas de tentative de connexion et de déconnexion sur les ports réseau, et la traiter.		O		F
Maîtriser les interconnexions						
RSO17	TECH	Assurer un cloisonnement entre le système industriel et d'autres systèmes (industriels ou d'information).	O			F
RSO18	TECH	Limiter strictement les flux d'informations entre le système industriel et d'autres systèmes, uniquement lorsqu'ils sont fonctionnellement requis, et durant la plage horaire autorisée, et au bénéfice du système industriel, sous réserve : - d'en maîtriser la nature, le sens et le chemin suivi (les flux unidirectionnels devront être privilégiés) ; - d'authentifier les interfaces participant aux échanges ; - d'en préserver l'intégrité des échanges, voire leur confidentialité ; - de détecter les intrusions éventuelles ; - d'assurer la traçabilité des échanges. Dans tous les autres cas, ces flux d'informations sont interdits.		O		F
RSO19	TECH	Protéger les interconnexions entre des systèmes répartis sur des localisations différentes pour garantir la confidentialité, l'intégrité, la disponibilité, et l'authenticité des communications.		O	On peut utiliser un VPN IPsec par exemple.	F
RSO20	TECH	Dans le cadre d'interconnexions entre des systèmes répartis sur des localisations différentes, mettre en place un dispositif de filtrage (pare-feu).		O		F
RSO21	TECH	Configurer les passerelles d'interconnexion selon le guide de l'ANSSI relatif à l'interconnexion d'un système d'information à Internet.		O	Guide ANSSI relatif à l'interconnexion d'un SI à Internet.	F
RSO22	TECH	Interdire l'interconnexion d'un système industriel avec Internet de manière permanente sauf en cas de besoins dûment justifiés et sur autorisation de l'autorité d'homologation (AH).	O			F
RSO23	TECH	Ne pas autoriser une interconnexion directe entre un système industriel de classe 3 (ou zones de classe 3) et Internet.	O			F
RSO24	TECH	En cas d'interconnexion autorisée entre un système industriel de classe 1 ou 2 (ou zones de classe 1 et 2) avec Internet, limiter les accès au strict nécessaire vers Internet depuis le système industriel.	O			F
RSO25	TECH	Réciproquement, limiter les accès depuis Internet vers le système industriel au strict nécessaire.	O			F
RSO26	TECH	Pour l'interconnexion, utiliser des équipements labellisés.		R		F
Maîtriser l'usage de la technologie sans fil						
RSO27	TECH	Limiter l'usage de la technologie sans fil au strict nécessaire ; En cas d'usage de la technologie sans fil, limiter sa période d'activation au strict nécessaire.	O			SSA/ F
RSO28	TECH	Si la technologie sans fil est utilisée, appliquer la directive 23 (DGNUM) portant sur les technologies sans fil.	O		Directive 23 du 2 février 2021 portant sur la sécurité de technologies sans fil.	SSA/ F

N°	Nature	Intitulé	SI	C2	Remarque	Responsable
RSO29	TECH	Constituer une zone de sécurité contenant le réseau sans-fil.	O		Les communications sans fil doivent être cloisonnées au maximum en isolant les périphériques sans fil dans un réseau physique ou logique séparé.	SSA/ F
RSO30	TECH	Les points d'accès sans fil doivent mettre en place les mécanismes suivants : - l'authentification du point d'accès et du dispositif qui se connecte à l'infrastructure ; - les fonctionnalités de contrôle d'accès réseau (ex : EAP) ; - la journalisation des connexions.		O		SSA/ F
RSO31	ORG	Lorsque les événements de sécurité ne sont pas supervisés par un dispositif centralisé, examiner régulièrement les événements générés par les équipements sans fil.		O		SSA/ F
Maîtriser les équipements						
EXP1	TECH	Durcir la configuration des équipements en désactivant ou supprimant : - les comptes par défaut ou non utilisés ; - les ports physiques inutilisés (ports de maintenance inclus) ; - les supports amovibles, s'ils ne sont pas utilisés ; - les services non indispensables (service Web par exemple) ; - les logiciels non indispensables.		O		F
EXP2	TECH	Restreindre la connexion d'équipement en désactivant ou bloquant les ports physiques (ports USB, port maintenance) lorsque leur utilisation n'est pas nécessaire.		O	Mesures possibles : Par exemple, on peut envisager les mesures suivantes : - blocage des ports USB à l'aide de mécanismes de sécurité physiques ou logiques, comme les verrous USB physiques (avec clés) ou par un logiciel - de sécurité capable de bloquer l'utilisation de clés USB et autres périphériques ; - le retrait ou la déconnexion des lecteurs de médias amovibles.	F
EXP3	TECH	Sur les postes et serveurs, - désactiver l'ensemble des programmes non indispensables ; - supprimer les données de tests ainsi que les comptes créés lors des tests, désormais inutiles.		O		F
EXP4	TECH	Supprimer les données de tests, toutes les fonctions de développement, les outils temporaires liés aux tests et aux évolutions (débugueur, script de configuration, ...) ou fonctions locales de maintenance non utiles à la production sur les équipements (automates, postes SCADA, postes maintenance, serveurs, etc.) d'un système en production.		R		F
EXP5	TECH	Sur les automates et les applications SCADA, ne pas charger dans les équipements les mnémoniques et commentaires		O		F
EXP6	ORG	Privilégier les équipements labellisés.		R		F
EXP7	TECH	Pour sécuriser les systèmes d'exploitation des équipements, appliquer les guides de configuration rédigés ou recommandés par le ministère ou l'ANSSI s'ils existent.	O		Voir référentiels Guide et configuration et Référentiel ANSSI	F
EXP8	TECH	Appliquer sur les paramètres de durcissement de configuration une étude d'impacts fonctionnels pour ne pas remettre en cause la sûreté de fonctionnement du système industriel.	O			F
EXP9	TECH	Appliquer le principe du moindre privilège sur les applications. Elles doivent		O		F

N°	Nature	Intitulé	SI	C2	Remarque	Responsable
		s'exécuter avec des privilèges strictement nécessaires à leur fonctionnement.				
EXP10	TECH	Pour les automates, lorsque les équipements le permettent, activer les mécanismes suivants : - protection d'accès à la CPU et/ou au programme ; - restriction des adresses IP pouvant se connecter (liste blanche) ; - désactivation du mode de programmation à distance.		R		F
EXP11	TECH	Mettre en place, dans le processus de livraison, un mécanisme de vérification de contrôle d'intégrité des équipements et programmes applicatifs, et d'authenticité de l'émetteur des composants du système industriel (signature), notamment dans le processus de livraison. La vérification doit s'effectuer au chargement du composant et de manière périodique par mesure de contrôle.		R	Éléments concernés : firmwares, systèmes d'exploitation et logiciels standards, progiciels SCADA, programmes d'automates et de SCADA, fichier de configuration des équipements réseau, etc.	F
EXP12	TECH	Vérifier l'intégrité des équipements et logiciels au chargement du composant et de manière périodique par mesure de contrôle. Cette vérification concerne : - les systèmes d'application et firmware ; - les logiciels et progiciels SCADA ; - les paramètres de configuration durcis.		O		F
EXP13	TECH	Ne pas installer d'outils de développement sur les machines de production. Seuls les environnements de production (runtime) doivent être installés sur les serveurs et stations SCADA par exemple. En cas d'impossibilité, mettre en place des mesures palliatives pour réduire la surface d'attaque.		O		F
EXP14	TECH	Dédier les consoles de programmation, les stations d'ingénierie, les postes d'administration et les stations de maintenance, fixes ou nomades, à leur seul usage.	O			F
Maîtriser les postes sensibles du système (consoles de programmation, stations d'ingénierie, poste de maintenance, poste d'administration)						
EXP15	TECH	Durcir la configuration des consoles de programmation, des stations d'ingénierie, des postes d'administration et des stations de maintenance	O			F
EXP16	TECH	Appliquer les règles suivantes aux stations d'ingénierie : - ne pas les connecter à Internet ; - les installer dans des locaux maîtrisés (sous contrôle d'accès) ; - les éteindre lorsqu'elles ne sont pas utilisées. Activer la veille avec verrouillage de session si la station et l'activité le permettent	O			F
EXP17	TECH	Appliquer les règles suivantes aux consoles de programmation : - ne pas les connecter à Internet ; - ne pas les connecter à d'autres systèmes que le système industriel ; Appliquer les règles pour les terminaux mobiles ; - les stocker dans un local sécurisé ; - les rendre facilement identifiables (marquage visuel par exemple) ; Activer la veille avec verrouillage de session si la station et l'activité le permettent	O			F

N°	Nature	Intitulé	SI	C2	Remarque	Responsable
EXP18	TECH	Appliquer les règles suivantes aux postes d'administration : - ne pas les connecter à Internet ; - ne pas les connecter à un réseau de gestion ; - les installer dans des locaux maîtrisés (sous contrôle d'accès) ; - les éteindre lorsqu'ils ne sont pas utilisés ; Activer la veille avec verrouillage de session si la station et l'activité le permettent	O			F
Maîtriser la gestion des accès et des comptes						
EXP19	ORG	Définir et gérer les droits d'accès aux ressources selon les principes du besoin d'en connaître et du moindre privilège.	O			SSA/F
EXP20	ORG	Décrire dans la documentation du système les processus d'affectation, de révision et de suppression des droits d'accès applicables aux utilisateurs et administrateurs.	O			F
EXP21	ORG	Définir et maintenir la liste des utilisateurs autorisés à accéder au système industriel, notamment aux postes sensibles (stations d'ingénierie, consoles de programmation, postes d'administration).	O			SSA / F
EXP24	ORG	Créer des comptes selon le principe de moindre privilège. Porter une attention particulière sur les comptes de privilèges élevés.	O		Exemples de comptes de privilèges élevés : - « administrateur système » permettant l'administration informatique des équipements (serveurs, stations et équipements réseau par exemple) et des systèmes d'exploitation ; - « ingénieur de procédé » permettant d'accéder à des fonctions de configuration ou de programmation des applications SCADA et automates par exemple.	F
EXP25	ORG	Affecter des comptes de manière individuelle. Chaque compte doit être attribué à une seule personne bien identifiée, via un compte nominatif dans la mesure du possible. En cas de compte non nominatif, le faire prendre en compte à son détenteur.		O		F
EXP26	TECH	Interdire les comptes génériques disposant de privilèges comme les comptes administrateurs.	O			F
EXP27	TECH	Pour les comptes ne disposant pas de privilèges, ne pas employer de compte générique ou fonctionnel sauf besoins dûment justifiés.		O		F
EXP28	ORG	Si les comptes génériques ou fonctionnels doivent être utilisés en raison de besoins dûment justifiés : - limiter son usage au strict nécessaire (fonctionnel, temporel) ; - désactiver le compte en dehors des périodes autorisées d'utilisation ; - mettre en place des mesures permettant de tracer les accès ; - documenter l'usage des comptes.		O		F
EXP29	TECH	Protéger les comptes, et plus particulièrement les comptes à privilège (comptes administrateur, comptes de service), par un mécanisme d'authentification.	O			F
EXP30	TECH	Séparer strictement les comptes utilisateurs et administrateurs.	O			F
EXP31	TECH	Mettre en place un audit des événements liés à l'utilisation des comptes.	O			F

PCA Production	Cahier des charges	Page 18 / 43
ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DES COMPTEURS DE PARTICULES FIXES ET MOBILES AU SEIN DE LA PHARMACIE CENTRALE DES ARMEES (P.C.A)		

N°	Nature	Intitulé	SI	C2	Remarque	Responsable
EXP32	ORG	Valider l'usage de comptes à privilèges par le responsable hiérarchique de l'utilisateur.	R			F
EXP33	TECH	Lorsque cela est possible, configurer un accès en lecture seule pour les interventions de maintenance de premier niveau.	R			F
EXP34	TECH	Si la gestion des comptes est centralisée, contrôler régulièrement, au moins une fois par an, la configuration de l'annuaire centralisé.	O			F
Maîtriser l'accès au système						
EXP35	ORG	Lorsque le système n'offre pas de mécanisme d'identification, mettre en place des mesures organisationnelles permettant d'identifier l'auteur des actions associées. Contrôler leur application au moins une fois par an.	O			SSA/F
EXP36	TECH	Mettre en place une authentification forte (carte à puce, OTP) ou multi facteur pour accéder, et lorsque cela est possible : - à des comptes à privilège sur les postes, les serveurs ; - aux équipements de terrain (automates, entrées/sorties, déportés, etc.) ; - aux équipements exposés (ordinateurs portables, consoles de programmation, pare-feu, VPN, etc.).		R		F
EXP37	TECH	Mettre en place une authentification pour accéder aux différents composants (équipements et logiciels) lorsque cela est techniquement possible. Elle s'appuie sur des identifiants personnels afin de permettre une imputabilité individuelle des accès et des actions.	O			F
EXP38	ORG TECH	En cas d'impossibilité d'authentification forte, renforcer le paramétrage de mots de passe et appliquer des mesures compensatoires. Celles-ci sont définies dans les procédures d'exploitation de sécurité (PES).		O	À titre d'exemple : - contrôle d'accès physique ; - limitation des fonctionnalités accessibles (consultation sans modification, par exemple) ; - mise en place d'une authentification par carte à puce sans code ; - cloisonnement de l'équipement plus fort ; - etc.	F
EXP39	TECH	Configurer les paramètres des mots de passe de manière à les rendre robustes (durée de validité minimale et maximale, nombre de mots de passe non réutilisable, ...) en tenant compte des risques et des dérives possibles des pratiques des utilisateurs en cas de règles trop contraignantes (changement trop fréquent de mots de passe).	O			F
EXP40	TECH	Modifier les mots de passe par défaut si cela est réalisable. Identifier ceux qui ne peuvent être modifiés afin d'y appliquer une surveillance particulière.	O			F
EXP41	TECH	Privilégier une temporisation d'inhibition par rapport au blocage en cas d'échec d'authentification.	R			F
EXP42	TECH	Protéger les mots de passe (ou leur empreinte) en confidentialité et en intégrité, en particulier lorsqu'ils sont transmis en réseau ou stockés dans un fichier.	O			F
EXP43	ORG	Définir une procédure garantissant la sécurité pour la réinitialisation des mots de passe en cas de perte ou d'oubli.	R			F

N°	Nature	Intitulé	SI	C2	Remarque	Responsable
EXP44	TECH	Enregistrer les échecs d'authentification et les authentification réussies des comptes à privilèges.		○		F
Journaliser et surveiller						
EXP45	ORG	Définir une politique de journalisation. Elle doit permettre : - de définir les responsabilités ; - de déterminer les événements pertinents à journaliser ; - d'organiser le stockage et l'archivage des données journalisées (volumétrie, durée, conservation, protection, etc.) ; - de définir les conditions d'analyse (en préventif, post-incident, etc.) - de définir les événements qui devront déclencher des alertes.		○	Voir la liste d'événements possibles en annexe B du guide ANSSI sur les mesures détaillées à appliquer sur les systèmes industriels.	SSA/F
EXP46	TECH	Activer les fonctions de traçabilité sur les équipements et logiciels s'ils le permettent (Syslog, Windows Event, etc.).		○		F
EXP47	TECH	Mettre en place un système de gestion centralisée et sécurisée des journaux d'événements. Les besoins de sauvegarde, de confidentialité, d'intégrité et de disponibilités doivent être évalués et garantis.		○		F
EXP48	TECH	Journaliser les modifications de paramètres des capteurs, actionneurs, fonctions d'asservissement et de régulation.		○		F
Maîtriser l'usage des supports amovibles						
EXP51	ORG	Identifier les supports amovibles (clé USB, disquette, carte (micro-)SD, disque dur, etc.) nécessaires au système industriel et limiter leur usage au strict nécessaire.	○			SSA / F
EXP53	ORG	Dédier les supports amovibles au système industriel. Sont interdites : - la connexion de tout autre support sur le système ; - leur connexion sur un autre système non maîtrisé par le ministère ; - leur utilisation pour tout autre usage. Les supports dédiés sont mis à disposition des personnes intervenant sur le système industriel.	○			SSA / F
Maîtriser l'usage des équipements mobiles						
EXP56	ORG	Faire prendre en compte les équipements mobiles (supports amovibles, poste de maintenance, nomadisme, etc.).	○			SSA / F
EXP57	ORG	Identifier les équipements mobiles nécessaires au système industriel et limiter leur usage au strict nécessaire.	○			SSA / F
EXP58	ORG	Définir l'emploi des équipements mobiles autorisés à se connecter sur le système en s'assurant de leur traçabilité.	○			SSA / F
EXP59	ORG	Dédier les équipements mobiles autorisés à se connecter sur le système industriel, y compris ceux utilisés par des prestataires extérieurs.		○		SSA / F
EXP60	ORG	Proscrire la connexion ou le raccordement d'équipements personnels sur le système industriel.	○			SSA / F
Maîtriser la maintenance						
MAINT4	ORG	Pour les cas particuliers où l'intervenant apporte ses propres outils (des outils de diagnostic propres à l'équipementier par exemple), une procédure, même succincte, doit être mise en place pour vérifier que les équipements de l'intervenant ont un niveau de sécurité		○		SSA/ F

[illegible]

N°	Nature	Intitulé	SI	C2	Remarque	Responsable
MCS13	ORG TECH	Tracer les mises à jour et modifications apportées au système industriel.	○			SSA / F
MCS16	TECH	Faire évaluer et valider les modifications ou évolutions dans un environnement de test préalable avant leur déploiement.		R		SSA / F
MCS18	TECH	Mettre en œuvre un environnement de test représentatif du système en production afin de s'assurer de sa non-régression après l'application des correctifs.		R		SSA / F
Garantir une gestion des vulnérabilités						
MCS19	ORG	Mettre en place un processus de veille sur les menaces, en particulier sur l'évolution des techniques d'attaque, et vulnérabilités pour les éléments préalablement définis dans une stratégie de maintien en condition de sécurité (MCS). Le processus commence dès la phase de réalisation.		○		SSA / F
MCS20	ORG	Contractualiser la diffusion par les fournisseurs des bulletins de vulnérabilité pour l'ensemble des équipements, matériels et logiciels utilisés dans le système industriel.		R		SSA / F
MCS21	ORG	Un processus de gestion des vulnérabilités doit être mis en œuvre pour : - identifier les composants du système sensibles qui doivent faire l'objet d'une veille de vulnérabilité ; - identifier les vulnérabilités connues et mesurer leurs impacts sur les systèmes ; - rechercher les correctifs disponibles pour corriger ces vulnérabilités ; - déployer les correctifs de manière cohérente, en conformité avec le plan de maintenance ; - recenser les vulnérabilités qui n'ont pas pu être corrigées ; - mettre en place des mesures palliatives pour diminuer l'exposition aux risques. Il est possible de s'appuyer sur la Directive 47 portant sur le MCS. Parmi les composants du système industriel sensibles à identifier : équipements en interconnexion, équipements les plus exposés (postes de travail, postes nomades, consoles de programmes, postes de maintenance, équipement de sécurité (pare-feu, VPN), etc.).		○	Voir Directive 47 portant sur le MCS	SSA / F
MCS23	ORG TECH	Vérifier et valider les correctifs de sécurité avant leur déploiement.		○	Les correctifs doivent être validés par les fournisseurs pour les équipements qui relèvent de leur responsabilité. Les correctifs de sécurité doivent être appliqués en priorité sur les équipements les plus exposés (postes de travail, PC portables, stations d'ingénierie*, consoles de programmation*, pare-feu, VPN, etc.).	SSA / F
MCS23	ORG	Mettre en place un suivi des déploiements des correctifs.	○			SSA / F
Maîtriser l'obsolescence						
MCS24	ORG	Intégrer dans les contrats avec les fournisseurs des clauses relatives à la gestion de l'obsolescence.	○		Par exemple, indiquer la date à laquelle les équipements ne seront plus pris en charge.	SSA / F
MCS25	ORG	Identifier les dates auxquelles un équipement n'est plus maintenu. Insérer cette exigence dans les clauses relatives à la gestion de l'obsolescence.	○			SSA / F
MCS26	ORG	Mettre en place un plan de gestion de l'obsolescence pour remplacer les équipements et applications obsolètes.	○			SSA / F

N°	Nature	Intitulé	SI	C2	Remarque	Responsable
MCS27	ORG TECH	Mettre en place des mesures palliatives, techniques ou organisationnelles, pour réduire les risques que pose l'obsolescence d'équipements toujours en exploitation. Ces équipements font l'objet d'une plus grande surveillance.	O			SSA / F
Assurer la continuité de l'activité et sa reprise						
CONT1	ORG	Mettre en place un plan de maintien de la production avec possibilité de fournir des compteurs mobiles ou identiques à ceux présents dans le cas d'une panne des compteurs du site.		O		SSA / F
Mettre en place des moyens de détection et de réaction						
INC1	TECH	Mettre en place des moyens de détection d'intrusion en périphérie des systèmes et sur les points identifiés comme critiques qui comprennent notamment : - les interconnexions entre des systèmes distants ; - les interconnexions des systèmes de télégestion ; - les interconnexions entre le SI de gestion et le SI industriel ; - les points de connexion spécifiques vers l'extérieur (Wifi industriel par exemple) ; - le réseau fédérateur de postes de supervision industriel (SCADA) ; - les réseaux d'automates jugés sensibles.		R		SSA / F
INC2	ORG	Utiliser des moyens de détection labellisés.		R		SSA / F
INC3	TECH	Mettre en place une solution de SIEM ainsi que les ressources (RH, matérielles, etc.) pour garantir son efficacité.		C	Une solution de SIEM n'est efficace que si elle dispose de ressources humaines et matérielles suffisantes. Elle peut notamment être liée à un SOC (centre opérationnel de sécurité).	SSA / F
INC4	ORG	Dans le cas d'une mise en place d'une supervision de sécurité, prendre en compte le guide de détection pour les systèmes industriels publiés par l'ANSSI.		R	Voir Doctrine de détection pour les systèmes industriels, ANSSI, 3 décembre 2020.	SSA / F
INC5	ORG	Déterminer en cas d'incident : - que faire lors de la détection d'un incident ; - qui alerter ; - qui doit coordonner les actions en cas de crise ; - quelles sont les premières mesures à appliquer.	O			SSA / F

6.2.2.3. MATERIAUX

N°	Objet	Tolérance	Exigence
E2.01	Eléments non en contact avec le produit	Obligatoire	- Les parties inox du boîtier devront être à minima en acier inoxydable AISI 304. - Les parties en inox de la sonde (cône de prélèvement) devront être à minima en acier inoxydable 316L - Les surfaces externes des équipements devront pouvoir résister au nettoyage avec les produits de nettoyage suivants : - Alcool isopropylique 70% v/v - ANIOS SURFA'SAFE Premium - Peroxyde d'hydrogène vaporisé (VHP)

6.2.2.4. EXIGENCES TECHNIQUES

N°	Objet	Tolérance	Exigence
E3.01	Mesure	Obligatoire	- Débit d'aspiration de 1 pied cube par minute soit 28.3 L/min. - Gamme de mesure de particules de 0.5 µm à 5 µm Minimum. - Pompe intégrée au compteur de particules.
E3.02	Connexions	Obligatoire	Les compteurs doivent avoir une prise type RJ45 en façade pour communication avec le logiciel FMS5.

PCA Production	Cahier des charges	Page 23 / 43
ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DES COMPTEURS DE PARTICULES FIXES ET MOBILES AU SEIN DE LA PHARMACIE CENTRALE DES ARMEES (P.C.A)		

N°	Objet	Tolérance	Exigence
E3.04	Interface logiciel	Obligatoire	- Les compteurs doivent être compatibles avec le logiciel de gestion déjà en place au sein de la PCA. Ce logiciel est le logiciel FMS5 édité par TSI. L'intégration au sein du logiciel doit être prise en compte. - Les compteurs doivent être compatibles avec les systèmes de verrines colorées présentes en zone ou être proposés avec un système de verrines de remplacement.
E3.05	Stockage des données	Obligatoire	- Les compteurs doivent être en mesure de stocker au minimum 100 000 mesures en local. - Ces mesures doivent être accessibles par connexion directe au compteur par la prise RJ45 et extractibles sous format CSV. - Les données stockées localement sur les appareils doivent s'écarter uniquement au fur et à mesure des enregistrements supplémentaires.
E3.06	Audit trail	Obligatoire	- Un audit trail horodaté conforme aux exigences 21CFR PART11 et de l'annexe 11 des BPF doit permettre de tracer la modification et la suppression de toutes les données BPF et les actions critiques réalisées sur le système. Les données devront être libellées de façon claire et en français. - Lors de l'enregistrement d'une modification, l'audit trail doit faire figurer la valeur avant et après modification. - Cet audit trail doit pouvoir être consultable facilement par un responsable. Il doit pouvoir être imprimable et exportable et ne doit pas être falsifiable et non supprimable. Il doit pouvoir être enregistrable sur clé et directement exploitable (pas besoin de convertir avec un logiciel par exemple). Il doit être possible de filtrer les événements afin de pouvoir les revoir. - L'audit trail doit aussi tracer les créations, modifications, annulation des accès.
E3.07	Sauvegarde et restauration	Obligatoire	- Le système doit disposer d'un système de sauvegarde restaure : - Pour le système d'exploitation - Pour le logiciel - Pour les données (données de base et recettes). - Ces sauvegardes devront être restaurées au moins une fois en fin du processus de SAT pour vérification documentée.

6.2.2.5. EQUIPEMENTS

N°	Objet	Tolérance	Exigence
E4.01	Conception générale	Obligatoire	Le système doit permettre le comptage particulaire conformément aux BPF et selon la norme ISO 21501-4 en vigueur
E4.02	Tube de prélèvement	Obligatoire	- L'équipement doit être équipé d'un tube de prélèvement selon les caractéristiques suivantes : - La longueur ne peut excéder 1m et sans présence d'angles serrés. - Le diamètre intérieur doit être adapté au débit pour éviter la création d'un flux turbulent et les pertes. La norme veut que ce débit soit supérieur ou égal à 4mm. Tout autre diamètre doit être argumenté. - L'embout de prélèvement doit être droit, pas d'angle serrés et en position vertical. - Le matériau du tube doit être inerte et ne pas absorber ou relarguer de particules (ex : Acier inoxydable).
E4.03	Conception interne	Obligatoire	- Le chemin optique doit être conçu pour réduire la diffusion multiple de lumière. - Le couple prélèvement/optique ne doit pas engendrer de pertes significatives (<10%). - Le débit doit être précis à $\pm 5\%$ de la valeur nominale. - L'erreur maximale sur la taille de particule détectée doit être inférieure ou égale à 10%. - L'appareil doit avoir un système d'arrêt automatique en cas de sonde de prélèvement bouchée
E4.04	Résistance aux désinfectants	Obligatoire	L'intégralité de l'équipement doit être résistant au procédé de bio-décontamination par voie aérienne avec de l'H₂O₂ (VHP)

6.2.2.6. DOCUMENTATION

c	Objet	Tolérance	Exigence
E5.01	Documents à fournir pour chacun des équipements	Obligatoire	- DOE incluant au moins : ➢ Certificat CE ➢ La liste de tous les composants de l'installation avec leur référence fournisseur, et la documentation technique associée. ➢ Un manuel d'utilisation détaillé incluant pour chaque équipement : démarrage, arrêt, réglages, interventions maintenance. ➢ Un plan de maintenance décrivant notamment les procédures et fréquences des maintenances préventives et éléments d'usure à remplacer. ➢ Les certificats d'étalonnage de l'instrumentation en place et de celle utilisée pour la mise en service - Ces documents seront datés et référencés. - Conformément à la norme NFX 60.200 les notices d'utilisation et de maintenance technique seront obligatoirement en français. - Seront fournis au moins : ➢ 1 exemplaire papier complet sous forme de classeurs ➢ 1 support informatique de type USB

6.2.2.7. LIVRAISON ET MISE EN SERVICE

N°	Objet	Tolérance	Exigence
E6.01	Livraison et mise en place	Obligatoire	Le fournisseur est responsable du transport des équipements depuis les différents sites de fabrication vers le quai de livraison de la PCA.
E6.02	Mise en service	Obligatoire	- Le fournisseur aura la charge du branchement des différents éléments aux utilités avant mise en service. - Mise en service : toutes opérations nécessaires pour permettre aux matériels de fonctionner de manière normale et satisfaisante. - Tests de bon fonctionnement

« Avant l'installation des équipements un protocole de chargement/déchargement et un plan de prévention seront établis entre le titulaire et la Pharmacie centrale des armées. Le titulaire s'engagera à respecter l'ensemble des prescriptions relatives à l'hygiène et à la

PCA Production	Cahier des charges	Page 25 / 43
ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DES COMPTEURS DE PARTICULES FIXES ET MOBILES AU SEIN DE LA PHARMACIE CENTRALE DES ARMEES (P.C.A.)		

sécurité du travail et plus particulièrement celles relatives au travail en hauteur¹ (interdiction d'emploi d'échelle comme poste de travail, etc.) et aux interventions sur les installations électriques² (présentation des titres d'habilitation électriques, etc.). »

6.2.2.8. QUALIFICATION DES EQUIPEMENTS

N°	Objet	Tolérance	Exigence
E7.01	Qualification complète	Obligatoire	- Chaque équipement doit bénéficier d'une qualification complète par le titulaire. - La QP n'est pas incluse et est à la charge exclusive de la PCA après validation de la mise en production.
E7.02	Documents de qualification	Obligatoire	- Les documents suivants sont requis : - Rapport de conception (QC) avant mise en production de l'équipement : cette étape permet de démontrer et de documenter la conformité des aux BPF et au cahier des charges. - Protocole de QI - Rapport de QI - Protocole de QO. - Rapport de QO - Tous les documents proposés devront être conformes aux procédures et chartes graphiques internes à la PCA et aux BPF en vigueur. - Les documents devront être fournis à la PCA pour relecture et approbation avant d'être mis en œuvre par le fournisseur. Ces documents restent la propriété de la PCA.
E7.03	Exécution des tests	Obligatoire	- Devront être inclus les exécutions des protocoles et l'enregistrement des données en présence d'un personnel de la PCA pour les protocoles suivants : - QI - QO - Tout test non conforme fera l'objet de l'ouverture d'une fiche d'anomalie signée entre le prestataire et un représentant du donneur d'ordres. Cette fiche doit préciser au minimum : - Date de l'anomalie - La référence du test - La description de l'anomalie - Une pondération de l'anomalie : mineure, majeure, critique - Une proposition de correction de l'anomalie - Un plan d'action (action, responsable, dead line)
E7.04	Modifications en cours de projet	Obligatoire	- Chaque modification apportée au cours du projet doit être tracée de manière documentée. - La traçabilité de chaque changement doit contenir à minima : - Une description de la modification - Une proposition de correction - Une étude d'impact de la correction - Une approbation client - Plan d'action afin de vérifier le bon fonctionnement de la correction et la non régression des autres fonctionnalités. - Clôture
E9.05	Métrologie	Obligatoire	- Liste exhaustive des composants sous métrologie. - Fourniture des certificats d'étalonnage usine. - Etalonnage de la chaîne de mesure complète. - Les certificats d'étalonnage devront être conformes au moins jusqu'à l'installation des compteurs

6.2.3. VERIFICATION METROLOGIQUE ET MAINTENANCE

Les équipements acquis au titre du présent lot bénéficient de prestations de vérification métrologique et de maintenance (préventive et corrective) selon les modalités définies par le titulaire dans son offre et dans l'annexe financière à l'acte d'engagement. Ces modalités doivent être conformes aux stipulations des articles 5 et 6.1.2 à 6.1.10 du présent cahier.

¹ Décret 2004-924 du 1^{er} septembre relatif à l'utilisation des équipements de travail mis à disposition pour les travaux temporaires en hauteur et modifiant le code du travail et le décret n° 65-48 du 8 janvier 1965

² Décret n° 88-1056 du 14 novembre 1988 pris pour l'exécution des dispositions du livre II du Code du travail en ce qui concerne la protection des travailleurs dans les établissements qui mettent en œuvre des courants électriques

6.3. LOT 6 : ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DE NOUVEAUX COMPTEURS DE PARTICULES EN MILIEU LIQUIDE :

Ce lot concerne l'acquisition de compteurs à particules en milieu liquide destinés à compléter et/ou remplacer le parc actuel en fonction des besoins.

Les équipements concernés et leurs modalités d'approvisionnement doivent respecter les exigences ci-après.

Leur acquisition fait l'objet de bons de commandes sur la base des stipulations figurant dans l'annexe financière à l'acte d'engagement relative au présent lot.

6.3.1. PHASAGE ET LIVRABLES ATTENDUS

Etape		F	PCA/PROD	PCA/MAINT PCA/INFRA PCA/INFO	PCA/AQ
Conception des appareils Livrables :					
N°	Livrables	R	V	V	A
L1.1	Documents de conception				
L1.2	Spécifications techniques des équipements				
Installation, mise en route des appareils, nettoyage et calibration initial Livrables :					
N°	Livrables	R		V	A
L2.1	Installation des appareils aux endroits indiqués.				
L2.2	Rapport de mise en route des appareils et de calibration				
Branchement et installation des équipements. Livrables :					
N°	Livrables	R		V	
L3.1	Comptes rendus				
Qualification des éléments installés.					
N°	Livrables	R	V	V	A
L4.1	Analyse des risques fonctionnelle				
L4.2	Qualification de conception				
L4.3	Protocole de QI				
L4.4	Exécution de la QI				
L4.5	Rapport de QI				
L4.6	Protocole de QO				
L4.7	Exécution de la QO				
L4.8	Rapport de QO				
Fourniture des documents demandés (DOE). Livrables :					
N°	Livrables	R	V	V	A
L5.1	Un manuel d'utilisation en français				
L5.2	Certificat CE.				
L5.3	Le programme d'installation				
L5.4	Un plan de maintenance décrivant notamment les procédures et fréquences des maintenances préventives et éléments d'usure à remplacer.				
L5.5	Les certificats d'étalonnage de l'instrumentation en place et de celle utilisée pour la mise en service				
L5.6	Les certificats matières				
L5.7	Support informatique comprenant tous les documents				

6.3.2. EXIGENCES

6.3.2.1. REGLEMENTAIRES

N°	Objet	Tolérance	Exigence
E1.01	Code du travail	Obligatoire	• Equipements conformes aux règles techniques.
E1.02	21 CFR Part 11	Obligatoire	• Equipements conformes au règlement 21 CFR Part 11
E1.03	Certificat CE	Obligatoire	• Equipements avec certificat CE.

N°	Objet	Tolérance	Exigence
E1.04	directive N°39 PORTANT SUR LA SÉCURITÉ NUMÉRIQUE DES SYSTÈMES INDUSTRIELS (DIR-SNSI)	Obligatoire	• Conformité des systèmes industriels à la directive 39 pour une classe 2 .
E1.05	USP 788	Obligatoire	• Equipement conforme à l'USP 788
E1.06	Pharmacopée Européenne	Obligatoire	• Equipement conforme à la pharmacopée européenne (Chapitre 2.9.19)
E1.07	Bonnes Pratiques de Fabrication	Obligatoire	• Equipement conforme aux Bonnes Pratiques de Fabrication en vigueur

6.3.2.2. SYSTEME INDUSTRIEL (DIRECTIVE 39 – Classe 2)

N°	Nature	Intitulé	SI	C2	Remarque	Responsable
Maîtriser l'organisation de la sécurité numérique						
ORG2	ORG	Dans un cadre contractuel, demander au prestataire de mettre en place une chaîne de responsabilité en matière de sécurité numérique pour les besoins de ses prestations.		O	Le point de contact peut être chargé de : - la liaison avec la chaîne de responsabilité de l'entité responsable - la garantie du respect de la politique de cyber sécurité ; - la communication sur les divergences par rapport aux exigences et les autres non-conformités.	SSA / F
ORG3	ORG	Le prestataire doit désigner en son sein un point de contact en matière de sécurité numérique qui est en charge de la liaison avec la chaîne de responsabilité SSI du ministère durant les phases amont (aider le RSSI-P dans le cadre de l'homologation) et aval du projet (aider le RSSI-A dans le cadre du maintien en condition de sécurité (MCS)). Ce point de contact est soit formé, soit accompagné d'un expert en sécurité.	O			F
Maîtriser les intervenants						
PERS1	ORG	Sensibiliser toute personne amenée à intervenir sur un système industriel aux risques numériques propres aux systèmes industriels. La sensibilisation est adaptée à leurs spécificités, à leur fonction et à leur environnement. Un point d'attention est à porter sur les administrateurs techniques et fonctionnels ainsi que sur les opérateurs.	O		La règle est aussi valable pour ceux qui interviennent dans la maintenance du système. Les séances de formation et de sensibilisation à la cyber sécurité des systèmes industriels peuvent être dispensées en même temps que les formations de sûreté et de sécurité du site.	SSA / F
PERS2	ORG	Former à la sécurité numérique le personnel amené à intervenir sur les systèmes industriels. La formation doit être adaptée à sa fonction, à son profil ou encore à ses droits d'accès dans le système. Un point d'attention est à porter sur : - les administrateurs techniques et fonctionnels ainsi que sur les opérateurs ; - les RSSI (RSSI-A, RSSI-P) s'ils ne sont pas accompagnés de spécialistes en sécurité numérique des systèmes industriels.	O			SSA / F
Intégrer la sécurité numérique dans le projet						
ISSIP2	ORG	Définir des procédures et des moyens techniques pour permettre des opérations de maintenance préventive et curative et ainsi maintenir le niveau de sécurité dans la durée.	O		Des modes dégradés peuvent être prévus pour réaliser des mises à jour. On peut configurer les sorties d'un automate pour qu'elles restent sur leurs derniers états, pendant la mise à jour de son firmware.	SSA / F
ISSIP4	ORG	Exiger que les opérations non indispensables à la conduite du système industriel soient effectuées sur un autre système d'information. Les équipements et logiciels associés ne doivent pas être présents sur le système industriel. À titre d'exemple, des postes bureautiques non	R			F

PCA Production	Cahier des charges	Page 28 / 43
ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DES COMPTEURS DE PARTICULES FIXES ET MOBILES AU SEIN DE LA PHARMACIE CENTRALE DES ARMEES (P.C.A)		

N°	Nature	Intitulé	SI	C2	Remarque	Responsable
		connectés au système industriel doivent être prévus pour permettre la consultation de la documentation, le remplissage de feuilles de suivi, etc.				
ISSIP14	TECH	En cas de développement réalisé au titre du système, appliquer les règles de bonnes pratiques, notamment la directive 40 (portant sur le développement des applications informatiques et des logiciels robustes du ministère).		O	Voir Directive DGNUM n°40 sur le développement robuste	F
ISSIP15	TECH	Dédier un environnement de développement aux opérations de développement du système industriel. Cet environnement ne peut être utilisé pour d'autres activités.		O		F
ISSIP16	TECH	Séparer l'environnement de développement de l'environnement de production.	O			F
ISSIP17	TECH	Protéger l'environnement de développement de manière à satisfaire aux mêmes besoins de sécurité du système industriel en matière de disponibilité, d'intégrité et de confidentialité. Il doit satisfaire aux mêmes exigences de sécurité auxquelles s'ajoutent des exigences de sécurité en matière de développement. En cas de prestation externe, fournir un plan d'assurance sécurité (PAS).	O			F
ISSIP18	ORG	Vérifier le niveau de sécurité de l'environnement de développement.		R		F
Protéger physiquement le système et les contrôles d'accès aux locaux, aux équipements et aux câblages						
PHY1	ORG	Appliquer les mesures de protection physique définies dans l'IGI 1300 et l'IM 900 si le système industriel traite de données classifiées ou portant une mention de protection Diffusion Restreinte.	O			F
PHY2	ORG TECH	Mettre en place des mécanismes de contrôle d'accès adaptés aux enjeux de sécurité du système industriel ou conformes aux réglementations selon la nature du système ou son niveau de confidentialité.	O			SSA / F
PHY7	ORG	Déployer les serveurs et les postes d'exploitation dans des locaux différents.		O		F
PHY11	TECH	Mettre en place un dispositif de détection d'ouverture avec remontée d'alarme sur les armoires des équipements sensibles. A minima, sur les coffrets extérieurs contenant des composants sensibles, un moyen de contrôle visuel, comme la pose de scellés par exemple, doit être installé. Le retrait de ces moyens visuels doit suivre une procédure bien définie et être soumis à autorisation préalable.		R		SSA / F
Maîtriser les zones de sécurité au sein du système industriel						
RSO2	TECH	Mettre en place un cloisonnement entre les zones de sécurité. Le cloisonnement est physique entre les zones de classe 3 et les zones de classe inférieure. L'utilisation de cloisonnement logique est alors interdite. Pour les autres niveaux de classe, privilégier autant que possible un cloisonnement physique entre les zones de sécurité.	O			F

N°	Nature	Intitulé	SI	C2	Remarque	Responsable
RSO3	ORG	Lorsque la séparation physique n'est pas possible entre des zones de sécurité de classes différentes, mettre en place une solution de tunnel VPN labellisée.		O		F
RSO4	ORG	Lorsque la séparation de tunnel VPN n'est pas possible entre des zones de sécurité de classes différentes, mettre en place un cloisonnement logique de type VLAN.		O		F
RSO5	TECH	Mettre en place une politique de filtrages entre les zones de sécurité. Les flux sont limités au strict besoin.	O		Pour définir une politique de filtrage, on peut notamment se reporter au guide de l'ANSSI. Pour les flux utilisant le protocole IP, on en rappelle néanmoins ici quelques grands principes : - un flux est identifié par l'adresse IP source, l'adresse IP destination, le protocole de transport (par exemple UDP ou TCP) et, le cas échéant, les numéros de port source et destination ; - tous les flux entrants ou sortants du système industriel doivent être journalisés. Les moyens assurant le filtrage peuvent être physiques et/ou dédiés selon les risques à couvrir et dans la mesure du possible. - les flux sont refusés par défaut ; - seuls les flux nécessaires au fonctionnement du système industriel sont autorisés ; - les flux rejetés doivent être journalisés et analysés ;	F
RSO6	TECH	Lorsque des flux non-IP doivent transiter entre deux zones distinctes, effectuer un filtrage sur les identifiants source et destination, ou un filtrage sur les protocoles autorisés.		O	Dans le cas d'Ethernet, on peut effectuer le filtrage* sur les adresses MAC source et destination.	F
RSO7	TECH	Mettre en place des flux unidirectionnels entre deux zones de classes différentes afin de n'autoriser les flux que de la zone de classe la plus élevée vers la zone de classe la moins élevée. Dans le cas de zones de classe 3, l'unidirectionnalité est assurée par une diode labellisée.	R		L'unidirectionnalité des flux peut être assurée par un pare-feu.	F
RSO8	TECH	Former au moins une zone de sécurité à part entière pour le réseau d'administration.		O		F
RSO9	TECH	Cloisonner le réseau d'administration des équipements des autres réseaux de manière physique.		R	Le périmètre porte sur les équipements d'informatique classique comme les commutateurs, passerelles, routeurs, pare-feu, etc.	F
RSO10	TECH	Protéger le système industriel du système d'information de gestion (niveau 4) par un dispositif de filtrage (pare-feu). Les flux sont limités au strict minimum.		O		F
RSO11	TECH	Proscrire l'usage de protocoles non sécurisés (telnet, http, ftp, etc.) en leur privilégiant des protocoles garantissant confidentialité, intégrité, authenticité des points communicants (https, ssh, sftp, bacnets-c). Si l'usage de protocoles non sécurisés est nécessaire pour des raisons techniques et opérationnelles, mettre en place des mesures compensatoires comme : - mettre en place des protections paramétriques (pare-feu) ; - encapsuler les flux dans un VPN pour en assurer l'authenticité et l'intégrité.	O			F
Maîtriser l'accès au réseau						
RSO13	TECH	Désactiver les points d'accès réseau non utilisés (commutateurs, automates, baies de brassage, prise de maintenance sur les bus de terrain, etc.).	O			F

N°	Nature	Intitulé	SI	C2	Remarque	Responsable
RSO14	TECH	En cas de liens sans protection physique, déployer des passerelles VPN aux extrémités des liaisons pour protéger l'intégralité du trafic. L'équipement doit être positionné derrière un pare-feu ne laissant passer que les flux strictement indispensables. En particulier, le trafic externe au VPN doit être bloqué.		O		F
RSO15	ORG	Protéger l'accessibilité des points d'accès réseau. Ils ne doivent être accessibles que dans des locaux, armoires ou coffrets à accès maîtrisés.		O		F
RSO16	TECH	Remonter une alerte en cas de tentative de connexion et de déconnexion sur les ports réseau, et la traiter.		O		F
Maîtriser les interconnexions						
RSO17	TECH	Assurer un cloisonnement entre le système industriel et d'autres systèmes (industriels ou d'information).	O			F
RSO18	TECH	Limiter strictement les flux d'informations entre le système industriel et d'autres systèmes, uniquement lorsqu'ils sont fonctionnellement requis, et durant la plage horaire autorisée, et au bénéfice du système industriel, sous réserve : - d'en maîtriser la nature, le sens et le chemin suivi (les flux unidirectionnels devront être privilégiés) ; - d'authentifier les interfaces participant aux échanges ; - d'en préserver l'intégrité des échanges, voire leur confidentialité ; - de détecter les intrusions éventuelles ; - d'assurer la traçabilité des échanges. Dans tous les autres cas, ces flux d'informations sont interdits.		O		F
RSO19	TECH	Protéger les interconnexions entre des systèmes répartis sur des localisations différentes pour garantir la confidentialité, l'intégrité, la disponibilité, et l'authenticité des communications.		O	On peut utiliser un VPN IPsec par exemple.	F
RSO20	TECH	Dans le cadre d'interconnexions entre des systèmes répartis sur des localisations différentes, mettre en place un dispositif de filtrage (pare-feu).		O		F
RSO21	TECH	Configurer les passerelles d'interconnexion selon le guide de l'ANSSI relatif à l'interconnexion d'un système d'information à Internet.		O	Guide ANSSI relatif à l'interconnexion d'un SI à Internet.	F
RSO22	TECH	Interdire l'interconnexion d'un système industriel avec Internet de manière permanente sauf en cas de besoins dûment justifiés et sur autorisation de l'autorité d'homologation (AH).	O			F
RSO23	TECH	Ne pas autoriser une interconnexion directe entre un système industriel de classe 3 (ou zones de classe 3) et Internet.	O			F
RSO24	TECH	En cas d'interconnexion autorisée entre un système industriel de classe 1 ou 2 (ou zones de classe 1 et 2) avec Internet, limiter les accès au strict nécessaire vers Internet depuis le système industriel.	O			F
RSO25	TECH	Réciproquement, limiter les accès depuis Internet vers le système industriel au strict nécessaire.	O			F
RSO26	TECH	Pour l'interconnexion, utiliser des équipements labellisés.		R		F
Maîtriser l'usage de la technologie sans fil						
RSO27	TECH	Limiter l'usage de la technologie sans fil au strict nécessaire ;	O			SSA/ F

N°	Nature	Intitulé	SI	C2	Remarque	Responsable
		En cas d'usage de la technologie sans fil, limiter sa période d'activation au strict nécessaire.				
RSO28	TECH	Si la technologie sans fil est utilisée, appliquer la directive 23 (DGNUM) portant sur les technologies sans fil.	O		Directive 23 du 2 février 2021 portant sur la sécurité de technologies sans fil.	SSA/ F
RSO29	TECH	Constituer une zone de sécurité contenant le réseau sans-fil.	O		Les communications sans fil doivent être cloisonnées au maximum en isolant les périphériques sans fil dans un réseau physique ou logique séparé.	SSA/ F
RSO30	TECH	Les points d'accès sans fil doivent mettre en place les mécanismes suivants : - l'authentification du point d'accès et du dispositif qui se connecte à l'infrastructure ; - les fonctionnalités de contrôle d'accès réseau (ex : EAP) ; - la journalisation des connexions.		O		SSA/ F
RSO31	ORG	Lorsque les événements de sécurité ne sont pas supervisés par un dispositif centralisé, examiner régulièrement les événements générés par les équipements sans fil.		O		SSA/ F
Maîtriser les équipements						
EXP1	TECH	Durcir la configuration des équipements en désactivant ou supprimant : - les comptes par défaut ou non utilisés ; - les ports physiques inutilisés (ports de maintenance inclus) ; - les supports amovibles, s'ils ne sont pas utilisés ; - les services non indispensables (service Web par exemple) ; - les logiciels non indispensables.		O		F
EXP2	TECH	Restreindre la connexion d'équipement en désactivant ou bloquant les ports physiques (ports USB, port maintenance) lorsque leur utilisation n'est pas nécessaire.		O	Mesures possibles : Par exemple, on peut envisager les mesures suivantes : - blocage des ports USB à l'aide de mécanismes de sécurité physiques ou logiques, comme les verrous USB physiques (avec clés) ou par un logiciel - de sécurité capable de bloquer l'utilisation de clés USB et autres périphériques ; - le retrait ou la déconnexion des lecteurs de médias amovibles.	F
EXP3	TECH	Sur les postes et serveurs, - désactiver l'ensemble des programmes non indispensables ; - supprimer les données de tests ainsi que les comptes créés lors des tests, désormais inutiles.		O		F
EXP4	TECH	Supprimer les données de tests, toutes les fonctions de développement, les outils temporaires liés aux tests et aux évolutions (débugueur, script de configuration, ...) ou fonctions locales de maintenance non utiles à la production sur les équipements (automates, postes SCADA, postes maintenance, serveurs, etc.) d'un système en production.		R		F
EXP5	TECH	Sur les automates et les applications SCADA, ne pas charger dans les équipements les mnémoniques et commentaires		O		F
EXP6	ORG	Privilégier les équipements labellisés.		R		F
EXP7	TECH	Pour sécuriser les systèmes d'exploitation des équipements, appliquer les guides de configuration rédigés ou recommandés par le ministère ou l'ANSSI s'ils existent.	O		Voir référentiels Guide et configuration et Référentiel ANSSI	F

PCA Production		Cahier des charges			Page 32 / 43	
ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DES COMPTEURS DE PARTICULES FIXES ET MOBILES AU SEIN DE LA PHARMACIE CENTRALE DES ARMEES (P.C.A)						
N°	Nature	Intitulé	SI	C2	Remarque	Responsable
EXP8	TECH	Appliquer sur les paramètres de durcissement de configuration une étude d'impacts fonctionnels pour ne pas remettre en cause la sûreté de fonctionnement du système industriel.	O			F
EXP9	TECH	Appliquer le principe du moindre privilège sur les applications. Elles doivent s'exécuter avec des privilèges strictement nécessaires à leur fonctionnement.		O		F
EXP10	TECH	Pour les automates, lorsque les équipements le permettent, activer les mécanismes suivants : - protection d'accès à la CPU et/ou au programme ; - restriction des adresses IP pouvant se connecter (liste blanche) ; - désactivation du mode de programmation à distance.		R		F
EXP11	TECH	Mettre en place, dans le processus de livraison, un mécanisme de vérification de contrôle d'intégrité des équipements et programmes applicatifs, et d'authenticité de l'émetteur des composants du système industriel (signature), notamment dans le processus de livraison. La vérification doit s'effectuer au chargement du composant et de manière périodique par mesure de contrôle.		R	Éléments concernés : firmwares, systèmes d'exploitation et logiciels standards, progiciels SCADA, programmes d'automates et de SCADA, fichier de configuration des équipements réseau, etc.	F
EXP12	TECH	Vérifier l'intégrité des équipements et logiciels au chargement du composant et de manière périodique par mesure de contrôle. Cette vérification concerne : - les systèmes d'application et firmware ; - les logiciels et progiciels SCADA ; - les paramètres de configuration durcis.		O		F
EXP13	TECH	Ne pas installer d'outils de développement sur les machines de production. Seuls les environnements de production (runtime) doivent être installés sur les serveurs et stations SCADA par exemple. En cas d'impossibilité, mettre en place des mesures palliatives pour réduire la surface d'attaque.		O		F
EXP14	TECH	Dédier les consoles de programmation, les stations d'ingénierie, les postes d'administration et les stations de maintenance, fixes ou nomades, à leur seul usage.	O			F
Maîtriser les postes sensibles du système (consoles de programmation, stations d'ingénierie, poste de maintenance, poste d'administration)						
EXP15	TECH	Durcir la configuration des consoles de programmation, des stations d'ingénierie, des postes d'administration et des stations de maintenance	O			F
EXP16	TECH	Appliquer les règles suivantes aux stations d'ingénierie : - ne pas les connecter à Internet ; - les installer dans des locaux maîtrisés (sous contrôle d'accès) ; - les éteindre lorsqu'elles ne sont pas utilisées. Activer la veille avec verrouillage de session si la station et l'activité le permettent	O			F

N°	Nature	Intitulé	SI	C2	Remarque	Responsable
EXP17	TECH	Appliquer les règles suivantes aux consoles de programmation : - ne pas les connecter à Internet ; - ne pas les connecter à d'autres systèmes que le système industriel ; Appliquer les règles pour les terminaux mobiles ; - les stocker dans un local sécurisé ; - les rendre facilement identifiables (marquage visuel par exemple) ; Activer la veille avec verrouillage de session si la station et l'activité le permettent	O			F
EXP18	TECH	Appliquer les règles suivantes aux postes d'administration : - ne pas les connecter à Internet ; - ne pas les connecter à un réseau de gestion ; - les installer dans des locaux maîtrisés (sous contrôle d'accès) ; - les éteindre lorsqu'ils ne sont pas utilisés ; Activer la veille avec verrouillage de session si la station et l'activité le permettent	O			F
Maîtriser la gestion des accès et des comptes						
EXP19	ORG	Définir et gérer les droits d'accès aux ressources selon les principes du besoin d'en connaître et du moindre privilège.	O			SSA/F
EXP20	ORG	Décrire dans la documentation du système les processus d'affectation, de révision et de suppression des droits d'accès applicables aux utilisateurs et administrateurs.	O			F
EXP21	ORG	Définir et maintenir la liste des utilisateurs autorisés à accéder au système industriel, notamment aux postes sensibles (stations d'ingénierie, consoles de programmation, postes d'administration).	O			SSA / F
EXP24	ORG	Créer des comptes selon le principe de moindre privilège. Porter une attention particulière sur les comptes de privilèges élevés.	O		Exemples de comptes de privilèges élevés : - « administrateur système » permettant l'administration informatique des équipements (serveurs, stations et équipements réseau par exemple) et des systèmes d'exploitation ; - « ingénieur de procédé » permettant d'accéder à des fonctions de configuration ou de programmation des applications SCADA et automates par exemple.	F
EXP25	ORG	Affecter des comptes de manière individuelle. Chaque compte doit être attribué à une seule personne bien identifiée, via un compte nominatif dans la mesure du possible. En cas de compte non nominatif, le faire prendre en compte à son détenteur.		O		F
EXP26	TECH	Interdire les comptes génériques disposant de privilèges comme les comptes administrateurs .	O			F
EXP27	TECH	Pour les comptes ne disposant pas de privilèges, ne pas employer de compte générique ou fonctionnel sauf besoins dûment justifiés.		O		F
EXP28	ORG	Si les comptes génériques ou fonctionnels doivent être utilisés en raison de besoins dûment justifiés : - limiter son usage au strict nécessaire (fonctionnel, temporel) ; - désactiver le compte en dehors des périodes autorisées d'utilisation ; - mettre en place des mesures permettant de tracer les accès ;		O		F

N°	Nature	Intitulé	SI	C2	Remarque	Responsable
		- documenter l'usage des comptes.				
EXP29	TECH	Protéger les comptes, et plus particulièrement les comptes à privilège (comptes administrateur, comptes de service), par un mécanisme d'authentification.	O			F
EXP30	TECH	Séparer strictement les comptes utilisateurs et administrateurs.	O			F
EXP31	TECH	Mettre en place un audit des événements liés à l'utilisation des comptes.	O			F
EXP32	ORG	Valider l'usage de comptes à privilèges par le responsable hiérarchique de l'utilisateur.	R			F
EXP33	TECH	Lorsque cela est possible, configurer un accès en lecture seule pour les interventions de maintenance de premier niveau.	R			F
EXP34	TECH	Si la gestion des comptes est centralisée, contrôler régulièrement, au moins une fois par an, la configuration de l'annuaire centralisé.	O			F
Maîtriser l'accès au système						
EXP35	ORG	Lorsque le système n'offre pas de mécanisme d'identification, mettre en place des mesures organisationnelles permettant d'identifier l'auteur des actions associées. Contrôler leur application au moins une fois par an.	O			SSA/F
EXP36	TECH	Mettre en place une authentification forte (carte à puce, OTP) ou multi facteur pour accéder, et lorsque cela est possible : - à des comptes à privilège sur les postes, les serveurs ; - aux équipements de terrain (automates, entrées/sorties, déportés, etc.) ; - aux équipements exposés (ordinateurs portables, consoles de programmation, pare-feu, VPN, etc.).		R		F
EXP37	TECH	Mettre en place une authentification pour accéder aux différents composants (équipements et logiciels) lorsque cela est techniquement possible. Elle s'appuie sur des identifiants personnels afin de permettre une imputabilité individuelle des accès et des actions.	O			F
EXP38	ORG TECH	En cas d'impossibilité d'authentification forte, renforcer le paramétrage de mots de passe et appliquer des mesures compensatoires. Celles-ci sont définies dans les procédures d'exploitation de sécurité (PES).		O	À titre d'exemple : - contrôle d'accès physique ; - limitation des fonctionnalités accessibles (consultation sans modification, par exemple) ; - mise en place d'une authentification par carte à puce sans code ; - cloisonnement de l'équipement plus fort ; - etc.	F
EXP39	TECH	Configurer les paramètres des mots de passe de manière à les rendre robustes (durée de validité minimale et maximale, nombre de mots de passe non réutilisable, ...) en tenant compte des risques et des dérives possibles des pratiques des utilisateurs en cas de règles trop contraignantes (changement trop fréquent de mots de passe).	O			F

PCA Production	Cahier des charges	Page 35 / 43
ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DES COMPTEURS DE PARTICULES FIXES ET MOBILES AU SEIN DE LA PHARMACIE CENTRALE DES ARMEES (P.C.A)		

N°	Nature	Intitulé	SI	C2	Remarque	Responsable
EXP40	TECH	Modifier les mots de passe par défaut si cela est réalisable. Identifier ceux qui ne peuvent être modifiés afin d'y appliquer une surveillance particulière.	O			F
EXP41	TECH	Privilégier une temporisation d'inhibition par rapport au blocage en cas d'échec d'authentification.	R			F
EXP42	TECH	Protéger les mots de passe (ou leur empreinte) en confidentialité et en intégrité, en particulier lorsqu'ils sont transmis en réseau ou stockés dans un fichier.	O			F
EXP43	ORG	Définir une procédure garantissant la sécurité pour la réinitialisation des mots de passe en cas de perte ou d'oubli.	R			F
EXP44	TECH	Enregistrer les échecs d'authentification et les authentifications réussies des comptes à privilèges.		O		F
Journaliser et surveiller						
EXP45	ORG	Définir une politique de journalisation. Elle doit permettre : - de définir les responsabilités ; - de déterminer les événements pertinents à journaliser ; - d'organiser le stockage et l'archivage des données journalisées (volumétrie, durée, conservation, protection, etc.) ; - de définir les conditions d'analyse (en préventif, post-incident, etc.) - de définir les événements qui devront déclencher des alertes.		O	Voir la liste d'événements possibles en annexe B du guide ANSSI sur les mesures détaillées à appliquer sur les systèmes industriels.	SSA/F
EXP46	TECH	Activer les fonctions de traçabilité sur les équipements et logiciels s'ils le permettent (Syslog, Windows Event, etc.).		O		F
EXP47	TECH	Mettre en place un système de gestion centralisée et sécurisée des journaux d'événements. Les besoins de sauvegarde, de confidentialité, d'intégrité et de disponibilités doivent être évalués et garantis.		O		F
EXP48	TECH	Journaliser les modifications de paramètres des capteurs, actionneurs, fonctions d'asservissement et de régulation.		O		F
Maîtriser l'usage des supports amovibles						
EXP51	ORG	Identifier les supports amovibles (clé USB, disquette, carte (micro-)SD, disque dur, etc.) nécessaires au système industriel et limiter leur usage au strict nécessaire.	O			SSA / F
EXP53	ORG	Dédier les supports amovibles au système industriel. Sont interdites : - la connexion de tout autre support sur le système ; - leur connexion sur un autre système non maîtrisé par le ministère ; - leur utilisation pour tout autre usage. Les supports dédiés sont mis à disposition des personnes intervenant sur le système industriel.	O			SSA / F
Maîtriser l'usage des équipements mobiles						
EXP56	ORG	Faire prendre en compte les équipements mobiles (supports amovibles, poste de maintenance, nomadisme, etc.).	O			SSA / F
EXP57	ORG	Identifier les équipements mobiles nécessaires au système industriel et limiter leur usage au strict nécessaire.	O			SSA / F
EXP58	ORG	Définir l'emploi des équipements mobiles autorisés à se connecter sur le système en s'assurant de leur traçabilité.	O			SSA / F

PCA Production	Cahier des charges	Page 36 / 43
ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DES COMPTEURS DE PARTICULES FIXES ET MOBILES AU SEIN DE LA PHARMACIE CENTRALE DES ARMEES (P.C.A)		

N°	Nature	Intitulé	SI	C2	Remarque	Responsable
EXP59	ORG	Dédier les équipements mobiles autorisés à se connecter sur le système industriel, y compris ceux utilisés par des prestataires extérieurs.		O		SSA / F
EXP60	ORG	Proscrire la connexion ou le raccordement d'équipements personnels sur le système industriel.	O			SSA / F
Maîtriser la maintenance						
MAINT4	ORG	Pour les cas particuliers où l'intervenant apporte ses propres outils (des outils de diagnostic propres à l'équipementier par exemple), une procédure, même succincte, doit être mise en place pour vérifier que les équipements de l'intervenant ont un niveau de sécurité satisfaisant. Leur innocuité virale doit être garantie. L'intervenant doit alors fournir un certificat d'innocuité. Celui-ci présente le résultat d'une analyse antivirale et sa date, et précise l'éditeur du produit, la version du moteur, la date et la version de la base de signature.		O		SSA/ F
Maîtriser la télémaintenance						
MAINT13	TECH	Mettre en œuvre une authentification forte à deux facteurs pour opérer la Télémaintenance.		O		SSA/ F
MAINT15	TECH	Utiliser pour la télémaintenance un équipement de connexion labellisé.		R		SSA/ F
MAINT16	TECH	Interdire toute possibilité de modification non autorisée du cloisonnement, du filtrage, des mécanismes d'authentification et de la journalisation par le prestataire (depuis l'extérieur du système industriel).	O			SSA/ F
MAINT18	TECH	Si des opérations de télémaintenance sont impérativement nécessaires, les équipements distants et la liaison doivent être intégrés dans le périmètre et être inclus dans une zone de classe 3. L'ensemble des mesures de classe 3 doivent leur être appliquées.		R		SSA/ F
MAINT19	TECH	Mettre en place des solutions de télédiagnostic sous réserve d'appliquer les règles suivantes : - la connexion distante ne s'effectue que sur un serveur cloisonné ; - les données nécessaires au télédiagnostic sont poussées sur ce serveur au travers d'une diode labellisée.				SSA/ F
Garantir le maintien en condition de sécurité						
MCS1	ORG	Définir une stratégie de maintien en condition de sécurité (MCS) à partir de la directive 47 de la DGNUM ou d'une directive portant sur le MCS et émanant des EMDS.	O		Voir Directive 47 portant sur le MCS	SSA / F
MCS2	ORG	Assurer une continuité contractuelle dans le maintien en condition de sécurité (MCS) des systèmes industriels. Le cas échéant, les ruptures doivent être identifiés et donner lieu à une plus grande vigilance, voire à des mesures palliatives et défensives supplémentaires.	O			SSA / F

PCA Production	Cahier des charges	Page 37 / 43
ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DES COMPTEURS DE PARTICULES FIXES ET MOBILES AU SEIN DE LA PHARMACIE CENTRALE DES ARMEES (P.C.A)		

N°	Nature	Intitulé	SI	C2	Remarque	Responsable
Garantir la connaissance du système						
MCS3	ORG	Établir une cartographie physique et logique du système industriel. Le niveau de granularité des informations à fournir dépend des enjeux du système. La stratégie d'homologation définit les éléments de la cartographie.	O			SSA / F
MCS6	ORG	Mettre à jour la cartographie du système industriel à chaque évolution du système et avant le renouvellement d'homologation.	O			SSA / F
MCS7	ORG	Définir la liste de la documentation relative au système industriel.	R			SSA / F
MCS8	ORG	Réactualiser la documentation à intervalle régulier, au moins avant toute ré homologation, pour : - s'assurer que les documents nécessaires existent bien et répondent toujours aux besoins ; - éliminer ceux qui ne servent plus.	O			SSA / F
Garantir la configuration et son évolution						
MCS13	ORG TECH	Tracer les mises à jour et modifications apportées au système industriel.	O			SSA / F
MCS16	TECH	Faire évaluer et valider les modifications ou évolutions dans un environnement de test préalable avant leur déploiement.		R		SSA / F
MCS18	TECH	Mettre en œuvre un environnement de test représentatif du système en production afin de s'assurer de sa non-régression après l'application des correctifs.		R		SSA / F
Garantir une gestion des vulnérabilités						
MCS19	ORG	Mettre en place un processus de veille sur les menaces, en particulier sur l'évolution des techniques d'attaque, et vulnérabilités pour les éléments préalablement définis dans une stratégie de maintien en condition de sécurité (MCS). Le processus commence dès la phase de réalisation.		O		SSA / F
MCS20	ORG	Contractualiser la diffusion par les fournisseurs des bulletins de vulnérabilité pour l'ensemble des équipements, matériels et logiciels utilisés dans le système industriel.		R		SSA / F

PCA Production	Cahier des charges	Page 38 / 43
ACQUISITION, VERIFICATION METROLOGIQUE ET MAINTENANCE DES COMPTEURS DE PARTICULES FIXES ET MOBILES AU SEIN DE LA PHARMACIE CENTRALE DES ARMEES (P.C.A)		

N°	Nature	Intitulé	SI	C2	Remarque	Responsable
MCS21	ORG	Un processus de gestion des vulnérabilités doit être mis en œuvre pour : - identifier les composants du système sensibles qui doivent faire l'objet d'une veille de vulnérabilité ; - identifier les vulnérabilités connues et mesurer leurs impacts sur les systèmes ; - rechercher les correctifs disponibles pour corriger ces vulnérabilités ; - déployer les correctifs de manière cohérente, en conformité avec le plan de maintenance ; - recenser les vulnérabilités qui n'ont pas pu être corrigées ; - mettre en place des mesures palliatives pour diminuer l'exposition aux risques. Il est possible de s'appuyer sur la Directive 47 portant sur le MCS. Parmi les composants du système industriel sensibles à identifier : équipements en interconnexion, équipements les plus exposés (postes de travail, postes nomades, consoles de programmes, postes de maintenance, équipement de sécurité (pare-feu, VPN), etc.).		○	Voir Directive 47 portant sur le MCS	SSA / F
MCS23	ORG TECH	Vérifier et valider les correctifs de sécurité avant leur déploiement.		○	Les correctifs doivent être validés par les fournisseurs pour les équipements qui relèvent de leur responsabilité. Les correctifs de sécurité doivent être appliqués en priorité sur les équipements les plus exposés (postes de travail, PC portables, stations d'ingénierie*, consoles de programmation*, pare-feu, VPN, etc.).	SSA / F
MCS23	ORG	Mettre en place un suivi des déploiements des correctifs.	○			SSA / F
Maîtriser l'obsolescence						
MCS24	ORG	Intégrer dans les contrats avec les fournisseurs des clauses relatives à la gestion de l'obsolescence.	○		Par exemple, indiquer la date à laquelle les équipements ne seront plus pris en charge.	SSA / F
MCS25	ORG	Identifier les dates auxquelles un équipement n'est plus maintenu. Insérer cette exigence dans les clauses relatives à la gestion de l'obsolescence.	○			SSA / F
MCS26	ORG	Mettre en place un plan de gestion de l'obsolescence pour remplacer les équipements et applications obsolètes.	○			SSA / F
MCS27	ORG TECH	Mettre en place des mesures palliatives, techniques ou organisationnelles, pour réduire les risques que pose l'obsolescence d'équipements toujours en exploitation. Ces équipements font l'objet d'une plus grande surveillance.	○			SSA / F
Assurer la continuité de l'activité et sa reprise						
CONT1	ORG	Mettre en place un plan de maintien de la production avec possibilité de fournir des compteurs mobiles ou identiques à ceux présents dans le cas d'une panne des compteurs du site.		○		SSA / F

N°	Nature	Intitulé	SI	C2	Remarque	Responsable
Mettre en place des moyens de détection et de réaction						
INC1	TECH	Mettre en place des moyens de détection d'intrusion en périphérie des systèmes et sur les points identifiés comme critiques qui comprennent notamment : - les interconnexions entre des systèmes distants ; - les interconnexions des systèmes de télégestion ; - les interconnexions entre le SI de gestion et le SI industriel ; - les points de connexion spécifiques vers l'extérieur (Wifi industriel par exemple) ; - le réseau fédérateur de postes de supervision industriel (SCADA) ; - les réseaux d'automates jugés sensibles.		R		SSA / F
INC2	ORG	Utiliser des moyens de détection labellisés.		R		SSA / F
INC3	TECH	Mettre en place une solution de SIEM ainsi que les ressources (RH, matérielles, etc.) pour garantir son efficacité.		C	Une solution de SIEM n'est efficace que si elle dispose de ressources humaines et matérielles suffisantes. Elle peut notamment être liée à un SOC (centre opérationnel de sécurité).	SSA / F
INC4	ORG	Dans le cas d'une mise en place d'une supervision de sécurité, prendre en compte le guide de détection pour les systèmes industriels publiés par l'ANSSI.		R	Voir Doctrine de détection pour les systèmes industriels, ANSSI, 3 décembre 2020.	SSA / F
INC5	ORG	Déterminer en cas d'incident : - que faire lors de la détection d'un incident ; - qui alerter ; - qui doit coordonner les actions en cas de crise ; - quelles sont les premières mesures à appliquer.	O			SSA / F

6.3.2.3. Matériaux

N°	Objet	Tolérance	Exigence
E2.01	Eléments en contact avec le produit	Obligatoire	Les éléments en contact avec le produit (ex : tube de prélèvement, seringue...) doivent être inertes chimiquement

6.3.2.4. EXIGENCES TECHNIQUES

N°	Objet	Tolérance	Exigence
E3.01	Mesure	Obligatoire	- Débit d'aspiration d'environ 20mL/min - Seringue avec un volume de minimum de 5 mL - Gamme de mesure au minimum de 2 à 30µm (norme PE 2.9.19/USP788 particules supérieures à 10 et particules supérieures à 25µm) - Seringue et laser intégrés au compteur à particules (un seul bloc)
E3.02	Connexions	Obligatoire	- Connexion USB (ou RJ45 à défaut) entre le PC et l'appareil - Pilotage de l'appareil via logiciel sur PC
E3.03	Stockage des données	Obligatoire	- Les mesures acquises doivent être enregistrées sur PC - Les rapports doivent être configurables pour impression et exportation
E3.04	Gestion des accès	Obligatoire	- Les comptes utilisateurs doivent être classés selon les niveaux suivants : - Administrateur - Utilisateur

N°	Objet	Tolérance	Exigence
E3.06	Audit trail	Obligatoire	- Un audit trail horodaté conforme aux exigences 21CFR PART11 et de l'annexe 11 des BPF doit permettre de tracer la modification et la suppression de toutes les données BPF et les actions critiques réalisées sur le système. Les données devront être libellées de façon claire et en français. - Lors de l'enregistrement d'une modification, l'audit trail doit faire figurer la valeur avant et après modification. - Cet audit trail doit pouvoir être consultable facilement par un responsable. Il doit pouvoir être imprimable et exportable et ne doit pas être falsifiable et non supprimable. Il doit pouvoir être enregistrable sur clé et directement exploitable (pas besoin de convertir avec un logiciel par exemple). Il doit être possible de filtrer les événements afin de pouvoir les revoir. - L'audit trail doit aussi tracer les créations, modifications, annulation des accès.
E3.07	Sauvegarde et restauration	Obligatoire	- Le système doit disposer d'un système de sauvegarde restaure : - Pour le système d'exploitation - Pour le logiciel - Pour les données (données de base et recettes). - Ces sauvegardes devront être restaurées au moins une fois en fin du processus de SAT pour vérification documentée.

6.3.2.5. EQUIPEMENTS

N°	Objet	Tolérance	Exigence
E4.01	Conception générale	Obligatoire	Le système doit permettre le comptage selon les normes européennes 2.9.19/USP788 méthode n°1
E4.02	Tube de prélèvement	Obligatoire	- Le tube de prélèvement doit être inerte chimiquement, il est plongé directement dans l'échantillon pour être aspiré via la seringue - L'échantillon doit pouvoir être agité avec un agitateur magnétique
E4.03	Conception interne	Obligatoire	- Le débit doit être précis à +/-5% de la valeur nominale - La mesure est réalisée par un spectromètre à obscuration de la lumière

6.3.2.6. Documentation

c	Objet	Tolérance	Exigence
E5.01	Documents à fournir pour chacun des équipements	Obligatoire	- DOE incluant au moins : - Certificat CE - La liste de tous les composants de l'installation avec leur référence fournisseur, et la documentation technique associée. - Un manuel d'utilisation détaillé incluant pour chaque équipement : démarrage, arrêt, réglages, interventions maintenance. - Un plan de maintenance décrivant notamment les procédures et fréquences des maintenances préventives et éléments d'usure à remplacer. - Les certificats d'étalonnage de l'instrumentation en place et de celle utilisée pour la mise en service - Ces documents seront datés et référencés. - Conformément à la norme NFX 60.200 les notices d'utilisation et de maintenance technique seront obligatoirement en français. - Seront fournis au moins : 1 exemplaire papier complet sous forme de classeurs 1 support informatique de type USB

6.3.2.7. LIVRAISON ET MISE EN SERVICE

N°	Objet	Tolérance	Exigence
E6.01	Livraison et mise en place	Obligatoire	Le fournisseur est responsable du transport des équipements depuis les différents sites de fabrication vers le quai de livraison de la PCA.

N°	Objet	Tolérance	Exigence
E6.02	Mise en service	Obligatoire	- Le fournisseur aura la charge du branchement des différents éléments aux utilités avant mise en service. - Mise en service : toutes opérations nécessaires pour permettre aux matériels de fonctionner de manière normale et satisfaisante. - Tests de bon fonctionnement

6.3.2.8. QUALIFICATION DES EQUIPEMENTS

N°	Objet	Tolérance	Exigence
E7.01	Qualification complète	Obligatoire	- Chaque équipement doit bénéficier d'une qualification complète par le titulaire. - La QP n'est pas incluse et est à la charge exclusive de la PCA après validation de la mise en production.
E7.02	Documents de qualification	Obligatoire	- Les documents suivants sont requis : - Rapport de conception (QC) avant mise en production de l'équipement : cette étape permet de démontrer et de documenter la conformité des aux BPF et au cahier des charges. - Protocole de QI - Rapport de QI - Protocole de QO. - Rapport de QO - Tous les documents proposés devront être conformes aux procédures et chartes graphiques internes à la PCA et aux BPF en vigueur. - Les documents devront être fournis à la PCA pour relecture et approbation avant d'être mis en œuvre par le fournisseur. Ces documents restent la propriété de la PCA.
E7.03	Exécution des tests	Obligatoire	- Devront être inclus les exécutions des protocoles et l'enregistrement des données en présence d'un personnel de la PCA pour les protocoles suivants : - QI - QO - Tout test non conforme fera l'objet de l'ouverture d'une fiche d'anomalie signée entre le prestataire et un représentant du donneur d'ordres. Cette fiche doit préciser au minimum : - Date de l'anomalie - La référence du test - La description de l'anomalie - Une pondération de l'anomalie : mineure, majeure, critique - Une proposition de correction de l'anomalie - Un plan d'action (action, responsable, dead line)
E7.04	Modifications en cours de projet	Obligatoire	- Chaque modification apportée au cours du projet doit être tracée de manière documentée. - La traçabilité de chaque changement doit contenir à minima : - Une description de la modification - Une proposition de correction - Une étude d'impact de la correction - Une approbation client - Plan d'action afin de vérifier le bon fonctionnement de la correction et la non régression des autres fonctionnalités. - Clôture
E9.05	Métrologie	Obligatoire	- Liste exhaustive des composants sous métrologie. - Fourniture des certificats d'étalonnage usine. - Etalonnage de la chaîne de mesure complète. - Les certificats d'étalonnage devront être conformes au moins jusqu'à l'installation des compteurs

6.3.3. VERIFICATION METROLOGIQUE ET MAINTENANCE

Les équipements acquis au titre du présent lot bénéficient de prestations de vérification métrologique et de maintenance (préventive et corrective) selon les modalités définies par la titulaire dans son offre et dans l'annexe financière à l'acte d'engagement. Ces modalités doivent être conformes aux stipulations des articles 5 et 6.1.2 à 6.1.10 du présent cahier.

7. ANNEXES

7.1. ANNEXE 1

Description : L'annexe 1 a pour but définir les interlocuteurs du site de la PCA donnant les informations par la voie de ce tableau (Fiche de contact Site PCA) tel que (poste, nom, contact, etc....)

Fiche de contact - Site PCA			
Poste	Grade/Nom	Numéro de téléphone	Adresse mail
Pharmacien Responsable/Directrice d'établissement	PHCSCN MENDES Anne- Christine	0238607311	anne.mendes@intradef.gouv.fr
Pharmacien Assurance qualité	PH BADEY- BETTEMBOURG Louis	0238607591	louis.badey- bettembourg@intradef.gouv.fr
Pharmacien Production	PH DOUET Gwendolyne	/	gwendolyne.douet@intradef.gouv.fr
Pharmacien Production	PHC JARZUEL Florence	0238607305	florence.jarzuel@intradef.gouv.fr
Responsable Qualification/Validation/Métrologie	TAILLIERE Nicolas	0245403928	nicolas1.tailliere@intradef.gouv.fr
Technicien Métrologie	ROUTIER Stephane	0234085354	stephane.routier@intradef.gouv.fr
Responsable Maintenance	LE GALL Alain	0238607530	alain.legall@intradef.gouv.fr
Adjoint Maintenance	TONEGUTTI Cyrille	0238607475	cyrille.tonegutti@intradef.gouv.fr

7.2. ANNEXE 2

Description : L'annexe 2 a pour objectif de récapituler par l'intermédiaire ce tableau (Tableau de suivi des compteurs de particules – Site de la PCA) les 23 compteurs de particules qui sont soumis à la prestation.

Tableau de suivi des compteur de particules – Site de la PCA	
référence	N° série
AEROTRAK 6510-VHP	2027003
AEROTRAK 6510-VHP	2009001
AEROTRAK 6510-VHP	2008017
AEROTRAK 6510-VHP	2008015
AEROTRAK 6510-VHP	2008016
AEROTRAK 6510-VHP	2008017
AEROTRAK 6510-VHP	2008022
AEROTRAK 6510-VHP	2008006
AEROTRAK 7510-22050V	75102125002
AEROTRAK 7510-22050V	75102125003
AIRNET II	102806
AIRNET II	110722
AIRNET II	110715
AIRNET II	88417
AIRNET II	102807
AIRNET II	66034
AIRNET II	88415
AIRNET II	88416
AIRNET II	110714
AIRNET II	110716
AIRNET II	110721
APSS-200	62678/62652
LASAIR II	58479