



Annexe de cybersécurité

système CONFORT USAGERS de classe 1



1.	HOMOLOGATION DU SYSTÈME.....	2
2.	CONTRATS.....	2
3.	TRANSFERT EN EXPLOITATION.....	2
4.	EXPLOITATION	2
5.	CONNAISSANCE DU SYSTÈME.....	3
6.	GESTION DES INTERVENANTS ET DES INTERVENTIONS	4
7.	MCO/MCS	6
8.	ARCHITECTURE DU SYSTÈME.....	6
9.	RESEAUX SUPPORT DU SYSTÈME.....	7
10.	SECURITE PHYSIQUE ET ENVIRONNEMENTALE	7



Annexe de cybersécurité système CONFORT USAGER de classe 1

1. HOMOLOGATION DU SYSTÈME

REF	LIBELLE
76	Un système industriel doit être homologué. La démarche d'homologation à suivre est SOMMAIRE.
301	La durée de validité de l'homologation doit être inférieure ou égale à 7 ans.
324	Le titulaire doit fournir les procédures d'exploitation de la sécurité (PES) qui peuvent être incluses dans un dossier d'utilisation et d'administration (DAU) ou un dossier d'exploitation et de maintenance (DEM).

2. CONTRATS

REF	LIBELLE
43	<p>Le titulaire doit désigner un point de contact pour la cybersécurité du projet. Celui-ci doit être chargé de :</p> <ul style="list-style-type: none">— la liaison avec la chaîne de responsabilité de l'entité responsable ;— la garantie du respect de la politique de cybersécurité ;— la communication sur les divergences par rapport aux exigences et les autres non-conformités.

3. TRANSFERT EN EXPLOITATION

REF	LIBELLE
75	<p>Avant de mettre en exploitation une installation il faut :</p> <ul style="list-style-type: none">— établir un état des lieux exhaustif du niveau de cybersécurité de l'installation ;— s'assurer des moyens disponibles pour le maintenir à un niveau acceptable.

4. EXPLOITATION

REF	LIBELLE
209	<p>Sur les équipements, on doit désactiver :</p> <ul style="list-style-type: none">— les comptes par défaut ;— les ports physiques non inutilisés ;— les supports amovibles, s'ils ne sont pas utilisés ;— les services non indispensables (service web par exemple).



Annexe de cybersécurité

système CONFORT USAGER de classe 1

REF	LIBELLE
214	Les préconisations de durcissement des systèmes d'exploitation doivent être appliquées pour chaque équipement. Lorsque des guides de configuration rédigés ou recommandés par DGA-MI ou l'ANSSI existent, ils doivent être appliqués.
215	Les applications doivent s'exécuter avec les privilèges strictement nécessaires à leur fonctionnement.
257	Les stations d'ingénierie doivent respecter les règles suivantes : <ul style="list-style-type: none">— être dédiées aux activités d'ingénierie ;— ne pas être connectées à Internet ;— être installées dans des locaux maîtrisés (sous contrôle d'accès) ;— se voir appliquer les règles de durcissement des stations de travail ;— être éteintes lorsqu'elles ne sont pas utilisées.
258	Les consoles de programmation doivent : <ul style="list-style-type: none">— être dédiées aux activités de maintenance et d'exploitation ;— ne pas être connectées à Internet ;— ne pas être connectées à d'autres installations que le système industriel ;— appliquer les règles pour les terminaux mobiles ;— appliquer les règles de durcissement de configuration et de renforcement des protections ;— être stockées dans un local sécurisé ;— être facilement identifiables (marquage visuel par exemple).
259	Les postes d'administration doivent : <ul style="list-style-type: none">— être dédiés à l'administration des équipements d'infrastructure ;— ne pas être connectés à Internet ;— appliquer les règles de durcissement de configuration et de renforcement des protections ;— être installés dans des locaux maîtrisés (sous contrôle d'accès) ;— être éteints lorsqu'ils ne sont pas utilisés.

5. CONNAISSANCE DU SYSTÈME

REF	LIBELLE
-----	---------



Annexe de cybersécurité système CONFORT USAGER de classe 1

REF	LIBELLE
8	Il est nécessaire d'établir/mettre à jour une cartographie : — physique du système industriel ; — logique du système industriel ; — des applications (flux) ; — de l'administration du système (si elle existe).
19	La documentation relative au dossier d'homologation du système industriel fait l'objet d'une mention de protection au minimum Diffusion Restreinte. Les documents doivent être traités en conséquence.
20	L'ensemble des documents relatifs à la conception, à la configuration ou au fonctionnement du système industriel doit faire l'objet d'une mention de protection au minimum sensible.
21	Les documents doivent être stockés dans un système d'information dont le niveau de sensibilité est adapté. Les exigences de l'instruction interministérielle 901 (II 901) doivent être appliquées en fonction du niveau de sensibilité des informations à stocker.
22	La confidentialité de la documentation doit être garantie.

6. GESTION DES INTERVENANTS ET DES INTERVENTIONS

REF	LIBELLE
29	Les intervenants doivent être habilités et formés à la cybersécurité.
30	Une charte de bonne conduite doit être mise en place et tous les intervenants doivent la signer lors de leur arrivée.
32	La formation des intervenants est obligatoire AVANT toute intervention sur le système industriel.
34	Les séances de formation et sensibilisation à la cybersécurité des systèmes industriels doivent être dispensées en fonction de la spécificité de la formation administrative ou de l'établissement.
40	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. Une telle situation ne doit arriver qu'en cas d'absolue nécessité et doit rester exceptionnelle.
41	L'utilisation d'outils particuliers hors d'un cadre prévu par la politique de sécurité du système industriel est interdite.



Annexe de cybersécurité

système CONFORT USAGER de classe 1

REF	LIBELLE
123	Chaque utilisateur doit être identifié de manière unique.
124	Tous les comptes disposant de privilèges importants comme les comptes administrateurs doivent être protégés par un mécanisme d'authentification comme un mot de passe par exemple. Les comptes utilisateurs et administrateurs doivent être strictement séparés.
125	Les comptes génériques, en particulier ceux disposant de privilèges importants sont déconseillés. Lorsqu'ils sont indispensables, leur utilisation devra être limitée à des usages très précis et être documentée.
126	Des rôles doivent être définis, documentés et implémentés pour que les comptes des utilisateurs aient des privilèges correspondant exactement à leurs missions.
136	Les différents composants (équipements et logiciels) ne doivent être accessibles qu'après une authentification avec identifiant et mot de passe. Lorsque cela est possible, la politique de mots de passe doit répondre à minima à l'exigence suivante : — les mots de passe par défaut doivent être changés ; — les mots de passe peuvent être éventuellement robustes.
233	Une politique d'utilisation des médias amovibles (clé USB, disquette, disque dur, etc.) doit être définie.
234	L'emploi des médias amovibles doit être limité au strict minimum.
235	Une station de décontamination doit être installée afin d'analyser et décontaminer tous les périphériques amovibles avant de les utiliser sur le système industriel.
236	La connexion des périphériques amovibles qui n'ont pas été vérifiés par la station de décontamination doit être interdite.
237	Des médias amovibles dédiés aux systèmes industriels doivent être mis à disposition des intervenants. L'utilisation de ces médias pour tout autre usage doit être interdite. Réciproquement, l'utilisation de tout autre média doit être interdite.
239	Les ports de médias amovibles doivent être désactivés lorsque leur utilisation n'est pas nécessaire. Si le blocage physique n'est pas possible, le port doit être désactivé logiquement. Par exemple, on pourrait envisager les mesures suivantes : — le 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.
241	Un SAS doit être mis en place pour échanger des données avec les systèmes industriels. Il doit être placé dans une zone maîtrisée. Cet échange de données est une action ponctuelle qui doit être encadrée par une procédure.
315	Le SAS doit être placé dans une zone maîtrisée. Un SAS doit respecter les règles d'hygiène informatique.



Annexe de cybersécurité

système CONFORT USAGER de classe 1

REF	LIBELLE
248	L'usage des périphériques personnels quels qu'ils soient (ordiphones, tablettes, clés USB, appareils photos, etc.) doit être interdit.
249	Une charte d'utilisation des terminaux nomades et une signalétique pour rappeler cette exigence doivent être mises en place.
250	Les équipements autorisés à se connecter aux installations doivent être clairement identifiés et validés.
252	Un processus d'attribution des terminaux mobiles doit être mis en place. Il doit permettre, à minima : <ul style="list-style-type: none">— de valider l'attribution du terminal par le responsable hiérarchique ;— d'assurer la traçabilité entre le terminal et ses utilisateurs ;— de sensibiliser l'utilisateur aux règles d'usage en vigueur.
254	Les équipements utilisés doivent être dédiés au système industriel, y compris ceux utilisés par des prestataires extérieurs.
255	Ces équipements ne doivent pas quitter le site.

7. MCO/MCS

REF	LIBELLE
111	Un plan de sauvegarde des données sensibles doit être mis en place afin de pouvoir reconstruire l'installation après sinistre.
15	Un plan de sauvegarde des données importantes doit être mis en place afin de permettre leur restauration en cas d'incident.
17	<p>Le processus de restauration des sauvegardes doit être testé régulièrement. Il pourrait être testé sur un échantillon limité mais représentatif du système industriel dans son ensemble.</p> <p>Les données concernées sont toutes les données nécessaires à la reconstruction de l'installation après un sinistre : les programmes, les fichiers de configuration, les firmwares, les paramètres de procédé (réglages d'asservissement par exemple), etc. Cela peut également concerner des données ayant un aspect réglementaire comme des exigences de traçabilité.</p>

8. ARCHITECTURE DU SYSTÈME

REF	LIBELLE
154	Les postes d'administration ne doivent pas avoir d'autre usage. Ils ne doivent pas être connectés à Internet ni à un réseau de gestion.



Annexe de cybersécurité système CONFORT USAGER de classe 1

9. RESEAUX SUPPORT DU SYSTÈME

REF	LIBELLE
318	Protéger physiquement les points d'accès.
206	Les protocoles non sécurisés (http, telnet, ftp, etc.) doivent être désactivés au profit des protocoles sécurisés (https, ssh, sftp, etc.) pour assurer l'intégrité, la confidentialité, l'authenticité et l'absence de rejeu des flux.

10. SECURITE PHYSIQUE ET ENVIRONNEMENTALE

REF	LIBELLE
94	Une politique de contrôle d'accès physique doit être définie. Cette politique doit notamment prévoir de : — récupérer les clés ou badges d'un employé à son départ ; — changer régulièrement les codes de l'alarme de l'entreprise ; — ne jamais donner de clé ou de code d'alarme à des prestataires extérieurs sauf s'il est possible de tracer les accès et de les restreindre à des plages horaires données.
99	L'accès aux équipements doit être strictement réservé aux personnes habilitées.
102	Les serveurs doivent être installés dans des locaux fermés sous contrôle d'accès (si possible dans des salles informatiques).
103	Les unités centrales des stations, les équipements réseaux industriels et les automates doivent être placés dans des armoires fermées à clé.
104	Des prises d'accès au système industriel ne doivent pas être accessibles dans les endroits ouverts au public.