# *ATTENTION à la SENSIBILITE des données du Moyen Industriel*

# *Stockage, export, maintenance chez l’industriel => des clauses sont à ajouter selon le contexte*

# Documents applicables

1. CAHIER DES CLAUSES SIMPLIFIEES DE CYBERSECURITE, Arrêté du 18 septembre 2018 portant approbation du cahier des clauses simplifiées de cyber sécurité
2. Fiche FiSSII issue de l’INSTRUCTION N°500398/DEF/EMAA/SCPA/GALSIC/NP DU 29/01/2016

Contrôle de la cyber sécurité des interventions industrielles sur les systèmes d’information de l’Armée de l’air - Version 1.0 du 1er Février 2016

1. Fiche d’inventaire matériel et logiciel AIA BR
2. Norme NF EN 60529 Degrés de protection procurés par les enveloppes (Code IP)

# Terminologie

|  |
| --- |
| BIOS : Basic Input Output System – système d’opérations élémentaires d’un ordinateur |
| FiSSII : Fiche SSI (Sécurité des Systèmes d’Information) d’Intervention |
| MI : Moyen Industriel, désigne le système complet objet du contrat |
| MINARM : Ministère des Armées |
| MCO/S : Maintien en Condition Opérationnelle et de Sécurité |

# Cas du Moyen Industriel NP avec poste(s) isolé(s)

EXIGENCES

1. A la livraison, aucun des systèmes d’exploitations, micrologiciels (‘*firmware*s’), logiciels et leurs composants (modules, librairies, …) ne doit faire l’objet de vulnérabilité connue ni d’obsolescence ; à ce titre, ils doivent être à jour des derniers correctifs de sécurité disponibles.
2. A la livraison, aucun matériel ne doit faire l’objet d’une obsolescence technique connue (avérée ou à moyen terme).
3. Tout échange de données d’un support appartenant au titulaire avec le MI doit obligatoirement être réalisé via une station blanche antivirale du client par transfert sur un support du client.
4. En cas d’absolue nécessité de connecter un poste informatique du titulaire à des fins d’investigation ou de dépannage sur le MI du client, des garanties doivent être apportées par le titulaire, quant au niveau de sécurité du poste et de son innocuité virale (cf. FiSSII en [DA2] ). L’intervention est soumise à l’approbation du client.

### Postes informatiques

1. Les postes informatiques permettant le pilotage, la configuration et la supervision du MI doivent être équipés d’un système d’exploitation soutenu et pouvant être mis à jour des correctifs de sécurité pendant toute la durée légale de garantie, plus 3 ans (5 ans au total). MICROSOFT Windows 11 est le système à privilégier ; tout empêchement doit être explicité et justifié.
2. Les postes informatiques doivent disposer d’une solution antivirale conforme à la politique du MINARM : TREND MICRO APEX ONE AGENT en mode isolé. En cas d’incompatibilité, le titulaire doit apporter des justifications techniques et demander une dérogation au client.
3. Les mises à jour du système d’exploitation et de l’antivirus doivent pouvoir être faites par le client en s’appuyant sur les serveurs de dépôt du MINARM.
4. Les applicatifs installés sur les postes informatiques doivent fonctionner sur un compte utilisateur restreint aux droits d’un utilisateur standard.
5. Les postes informatiques doivent être isolés de tout réseau MINARM ; aucun accès externe type internet n’est autorisé.
6. Si l’environnement physique est insalubre (poussières, liquides, produits chimiques, brouillard), des ordinateurs type industriels équipés de filtres doivent être mis en place. Ils doivent être conformes au degré de protection IP50 ( [DA4] ).

### Configuration des matériels informatiques et programmables

1. Le BIOS doit être configuré à l’état de l’art, et en particulier :

* Configuration d’un mot de passe d’accès aux paramétrages du BIOS ;
* Paramétrage de boot exclusif sur le disque dur principal ;
* Désactivation des périphériques inutiles : USB, CD/DVD-ROM, cartes réseau, lecteurs divers, micro, caméra, Wifi, Bluetooth… ; à défaut, les périphériques non autorisés doivent être bloqués physiquement (bloqueur de port USB / Ethernet …).
* La configuration des systèmes d’exploitation, logiciels métier et équipements doit être durcie conformément à l’état de l’art, et en particulier :
* Suppression des logiciels/services non indispensables à la fonction ; à défaut les désactiver ;
* Désactivation des services à accès externes type envoi de rapport d’erreur, accès distant,
* Désactivation de la fonction de scan automatique de l’antivirus, ainsi que la mise en quarantaine et la suppression automatique ;
* Utilisation des protocoles de communication dans leur version sécurisée ;
* Désactivation ou destruction des comptes inutiles et en particulier ceux à privilèges qui ne sont pas indispensables ;
* Modification des mots de passe par défaut et utilisation de mots de passe robustes ;
* Configuration des comptes nominatifs requis pour l’utilisation et l’administration selon le principe du moindre privilège ;
* Activation des journaux systèmes et de sécurité permettant la traçabilité et l’imputabilité des actions sur le système (en particulier redémarrages, échecs d’authentification, problèmes d’intégrité, rejets de flux non autorisés, alertes virales, mises à jour système/ applicatives/ base virale) ; fonctionnement des journaux sur rotation avec alerte préalable à la rotation ; ces traces doivent être sauvegardées régulièrement et archivées afin d’être conservées 1 an (durée réglementaire).

1. La configuration des automates et de leurs logiciels de gestion (configuration, diagnostic, supervision) doit être durcie conformément à l’état de l’art, et en particulier :

* Modification des mots de passe par défaut, usage de mots de passe robustes et suppression des comptes par défaut ;
* Désactivation des services non utilisés ;
* Désactivation des fonctions de débogage ;
* Désactivation de la programmation à distance ;
* Activation des fonctions de sécurité quand elles existent : contrôle d’accès des usagers et des flux autorisés, protection mémoire, protection du mode d’exécution, contrôle d’intégrité, communication sécurisée, journaux d’activité et d’erreurs, …

1. La configuration de l’automate ainsi que les mises à jour du micrologiciel doivent être effectuées en point à point hors réseau.
2. Le logiciel de configuration de l’automate doit être déconnecté en fonctionnement normal.
3. Les automates et équipements réseau doivent être placés dans des boitiers sécurisés ou dans des armoires fortes fermées à clés.

### Documentation

1. En complément aux exigences techniques précisées dans le CCTP, les livrables documentaires doivent être conformes à une nomenclature stable et pour la durée du contrat, du type : AAMMJJ\_NOM LIVRABLE\_sujet\_version

*Par exemple :*

*20250614\_MAN\_exploitation\_v3*

*20250810\_MAN\_référence automate\_v1*

*Les noms des livrables à utiliser sont indiqués entre crochets [NOM LIVRABLE] dans les exigences.*

1. La documentation technique et de maintenance est livrée sur support informatique au format bureautique standard ; en sus, 2 exemplaires papier des livrables notés (P) dans l’exigence suivante doivent être fournis.
2. La documentation technique et de maintenance doit contenir :

* [ARCHI] L’architecture fonctionnelle et technique de l’ensemble des composants du MI : schémas technico-opérationnels, description du fonctionnement de la solution et des fonctions/services de chaque composant (y compris ceux de maintenance, configuration, supervision, diagnostic). Les protocoles de communication, interfaces, flux de données et de service doivent y être décrits. Les mesures de sécurisation doivent être explicitées.
* [INV] L’inventaire de la configuration matérielle et logicielle du MI (systèmes d’exploitation, logiciels, composants logiciels, librairies, micrologiciels, …) des matériels informatiques et programmables (postes informatiques, périphériques, automates, cartes, équipements, …) à la livraison, et à chaque mise à jour, conforme au [DA3] .

La traçabilité des mises à jour et des correctifs des logiciels et micrologiciels effectuées sur le MI doit être incluse dans l’inventaire, ainsi que la liste des sources publiques utilisées pour les logiciels/micrologiciels.

* [CONF] Les méthodes, rôles et moyens d’accès aux matériels informatiques et programmables, aux applications ;

La description des programmes, des configurations et paramétrages appliqués à tous les composants du MI ; la description de l’arborescence des dossiers des systèmes ;

Les guides de durcissement utilisés et les mesures de sécurisation appliquées.

* [INST] La procédure d’installation et de paramétrage permettant la réinstallation du système complet ; les configurations à appliquer (paramètres, politique, …).
* [ADMIN] (P) Les manuels d’administration (configuration/paramétrage, tâches de maintenance préventive [périodicité, durée] et d’exploitation de niveau administrateur) de tous les composants du MI ;

Les tâches de mise à jour, la procédure de sauvegarde et de restauration de chacun des composants numériques du MI (étapes, durées, outils et niveau d’expertise requis, spécificités liées au composant) ;

La supervision du MI, l’archivage, l’analyse des journaux, …

Le mode opératoire de contrôle des signatures numériques des logiciels/micrologiciels ;

Les procédures de diagnostic, dépannage d’urgence et de remise en service ;

Les manuels de programmation le cas échéant.

* [MAN] (P) Les manuels d’utilisation de tous les composants du MI avec les tâches de maintenance préventive et d’exploitation de niveau utilisateur [périodicité, durée] ;

Les manuels de référence des constructeurs ;

* [MDP] L’inventaire des comptes et des mots de passe du MI.
* [EVOL] L’analyse annuelle des évolutions logiciel/micrologiciel.

### Formation

1. En complément aux exigences de formation précisées dans le CCTP, La formation au MI doit être réalisée sur site pour chaque profil d’utilisation (utilisateur / administrateur). Les tâches de maintenance et de diagnostic doivent être explicitées et expérimentées. Toutes les procédures de sauvegarde/restauration de chaque composant du MI (postes informatiques, automates, équipements réseau, …) doivent être déroulées.

PRESTATIONS

1. **INSTALLATION et PARAMETRAGE**

Le titulaire doit installer et configurer les matériels informatiques et programmables (postes informatiques, automates, équipements réseau, capteurs communicants, …), dans le respect de l’état de l’art, de façon à les sécuriser et à optimiser leurs ressources, et en particulier être conforme aux exigences du présent clausier.

Le titulaire doit :

* démontrer le bon fonctionnement du MI et de ses composants,
* effectuer les sauvegardes des systèmes et des configurations,
* effectuer les copies à l’identique sur les disques et mémoires de secours,
* produire la documentation technique et de maintenance adéquate,
* assurer la formation aux utilisateurs et administrateurs selon leur profil.

1. **MAINTIEN EN CONDITION OPERATIONNELLE ET DE SECURITE (MCO/S)**

Le titulaire s’engage à mettre en place des procédures et des moyens techniques dans le but de permettre les opérations de maintenance préventive et curative afin de maintenir son fonctionnement optimum et un niveau de cybersécurité à l’état de l’art sur toute la durée du contrat, conformément au [DA1] . Le titulaire décrit ces dispositions dans la documentation technique et de maintenance ; un soin particulier doit être apporté à la rédaction du livrable [ADMIN] pour tous les matériels informatiques et programmables du MI. A tout moment du contrat, le client peut exiger la mise en place de procédures et moyens complémentaires si les actions de MCO/S sont jugées insatisfaisantes.

### Evolution logicielle (hors correction de vulnérabilité cyber)

Tous les ans, le titulaire doit fournir au client une analyse décrivant les évolutions disponibles et pertinentes des logiciels/micrologiciels du MI ainsi que leurs composants et dépendances (modules, librairies) en précisant en particulier :

* la description fine des évolutions
* la description de résolution de dysfonctionnements connus
* les résultats des tests dans l’environnement du titulaire
* l’impact éventuel sur le fonctionnement ou l’utilisation du système
* la procédure de mise à jour et de paramétrage
* la possibilité de retour-arrière

Après accord du client, le titulaire procède aux sauvegardes nécessaires et aux mises à jour.

La validation du bon fonctionnement et de non-régression du MI doit être démontrée au client à chaque mise à jour. Le titulaire doit mettre à jour toute la documentation technique et de maintenance impactée (y compris l’inventaire logiciel) et effectuer les sauvegardes nécessaires avant et après intervention sur le disque externe (défini dans le §livrables). Le titulaire doit également procéder à la mise à jour des disques et cartes mémoire de secours (définis dans le §livrables). Le titulaire livre les supports numériques contenant les mises à jour et tous les fichiers nécessaires à l’installation et au paramétrage.

### Intégrité et authenticité des systèmes et des supports

Le titulaire doit mettre en place un processus de livraison de l’ensemble des logiciels, micrologiciels, programmes, configurations, correctifs qui garantit leur intégrité et leur authenticité.

Le titulaire doit permettre au client d’effectuer les contrôles des signatures numériques des logiciels et micrologiciel à chaque livraison/mise à jour (moyen, procédure).

Toute livraison de données du titulaire sur support informatique doit obligatoirement s’accompagner d’un certificat d’innocuité virale mentionnant la version du moteur, la version de la base de signatures et sa date de publication. Les fichiers d'exécution automatique des supports numériques ne sont pas autorisés. Les sources publiques utilisées pour ces fournitures doivent être réputées fiables et listées dans la documentation.

Le titulaire doit s’assurer de la validité des licences logicielles mises à disposition.

### Gestion des vulnérabilités/veille cyber

Le titulaire doit mettre en œuvre un processus de gestion des vulnérabilités logicielles & micrologiciels afin de :

* identifier les vulnérabilités connues et mesurer leurs impacts sur les installations,
* rechercher les correctifs disponibles pour corriger ces vulnérabilités (patchs, configurations, …) et s’assurer de leur innocuité virale ; les possibilités de retour-arrière doivent être identifiées ; des solutions de contournement peuvent également être proposées,
* tester les correctifs dans l’environnement du titulaire,
* sur accord du client, déployer les correctifs en commençant par les plus importants et s’assurer que le système ne présente aucune régression ni dysfonctionnement,
* recenser les vulnérabilités qui n’ont pas pu être corrigées (soit par manque de correctifs, soit parce que le correctif n’a pas pu être appliqué en raison de contraintes opérationnelles) et aviser le client des impacts potentiels.
* Procéder aux mises à jours documentaires et livraisons telles que définies au §1).

Le titulaire est tenu d’informer le client de toute faille de sécurité du MI concernant les logiciels/micrologiciels ainsi que leurs composants et dépendances (modules, librairies), les programmes et configurations/paramétrages, pendant toute la durée du contrat.

Via sa chaine CYBER, le client peut émettre une demande formelle au titulaire de correction d’une vulnérabilité jugée critique par le Commandement : le titulaire est tenu de déployer le correctif si existant ou une solution de contournement sous 72 heures.

Dans tous les cas, suite à identification des correctifs, le titulaire est tenu :

* en amont de la correction, d’apporter au client les preuves d’innocuité virale des solutions et de leur bon fonctionnement, de prouver qu’elles proviennent de sources sûres ; d’effectuer les sauvegardes adéquates pour s’assurer du retour-arrière,
* suite à la correction, d’apporter au client les preuves de bon fonctionnement et de non-régression et d’effectuer les sauvegardes ; mettre à jour la documentation impactée ; livrer les supports numériques utilisés.

Par ailleurs, sur sollicitation du client, le titulaire est tenu de fournir tout élément lui permettant de constituer le dossier d’homologation du MI.

### Gestion de l’obsolescence et des faits techniques

Le titulaire s’engage à mettre en place un plan de gestion des matériels et des applications en cas d’obsolescence et de tout constat d’anomalie (fait technique) sur tous les composants du MI (fait technique émis par le client ou le titulaire). Les faits techniques sont classés sur une échelle de criticité (mineur/majeur/bloquant) nécessitant une réponse adaptée et leurs impacts doivent être analysés pour correction.

En cas de changement de matériel ou de logiciel, d’application de correctifs, le titulaire s’assure de l’interopérabilité du matériel et de la compatibilité des logiciels (aucune régression n’est acceptée).

De plus le titulaire s’engage à vérifier et démontrer le bon fonctionnement de l’ensemble des composants une fois les changements opérés ; effectuer les sauvegardes nécessaires et mettre à jour la documentation impactée ; livrer les supports numériques utilisés.

### Incidents

Sur le système d’information du client

Le titulaire s’engage à signaler au client au plus tôt, et en moins de soixante-douze heures (72h), tout incident de sécurité ou anomalies, qu’il serait amené à rencontrer ou observer durant l’exécution des prestations qui lui sont confiées.

Sur le système d’information du titulaire

Le titulaire s’engage à signaler au client au plus tôt, tout incident de sécurité susceptible d’affecter directement ou indirectement les données ou les systèmes d’information du client.

LIVRABLES

Le titulaire doit fournir :

* Le MI avec les matériels informatiques et programmables installés et configurés conformément aux exigences du présent clausier ;
* L’ensemble des systèmes d’exploitations, logiciels/micrologiciels (et leurs licences et signatures numériques), pilotes, librairies, programmes, fichiers d’installation, configurations, permettant une réinstallation complète du MI ;
* Les mises à jour, les matériels et logiciels suite à évolution, correctif, traitement d’obsolescence et de fait technique ;
* Les supports de données nécessaires au MCO/S du MI, a minima :
* Un disque dur de secours identique au disque installé dans chaque poste informatique, maintenu à jour des évolutions et correctifs, des évolutions de programme/configuration effectués sur le disque du MI ;
* Un disque externe permettant les sauvegardes de tous les systèmes, programmes et configurations ;
* Pour chaque automate, une carte mémoire de secours identique à celle installée, maintenue à jour des évolutions de programme/configuration ;
* Les outils de supervision, administration, paramétrage, diagnostic, sauvegarde/ restauration et de contrôle des signatures numériques des composants du MI ;
* La documentation technique et de maintenance en conformité avec les exigences définies supra ; les livrables [MDP] et [INV], de par leur sensibilité, sont en particulier à transmettre directement lors de la livraison du MI, ou bien sous une forme chiffrée avec un moyen MINARM agréé ;
* Les supports de formation (support informatique au format bureautique standard et papier) ;
* La matrice de conformité aux exigences ;
* Les PV de conformité de recette industrielle et cahiers de tests associés ;
* Avant chaque intervention sur le MI, une fiche FiSSII remplie par l’intervenant et signée avec le client selon le modèle en [DA2] .