

MARCHE PUBLIC DE SERVICE

Cahier des Clauses Techniques Particulières (C.C.T.P.)

Annexe 5 : Exigences de maintien en condition de sécurité.

CONTRAT SENSIBLE

Abréviations :

AH	: Autorité d'homologation
CALID	: Centre d'Analyse en Lutte Informatique Défensive
CERT	: Computer Emergency Response Team
COTS	: Commercial off-the-shelves : composant ou matériel grand public
CSSI	: Correspondant de la sécurité des systèmes d'information
MCO	: Maintien en Condition Opérationnelle
MCS	: Maintien en Condition de Sécurité
OSSI	: Officier de sécurité des systèmes d'information
PAS	: Plan d'assurance
RSSI-A	: Responsable de la sécurité des systèmes d'information aval
S2I	: Sécurité des systèmes industriels d'infrastructure
SSI	: Sécurité des systèmes d'information

Textes applicables :

Référence	Titre
[IGI 1300]	Arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle sur la protection du secret de la défense nationale
[II 901]	Instruction interministérielle n°901/SGDSN/ANSSI du 28 janvier 2015 relative à la protection des systèmes d'informations sensibles
[IM 900]	Instruction ministérielle n°900/DEF/CAB du 26 janvier 2012 relative à la protection du secret de la défense nationale au sein du ministère de la défense
[IM-DS]	Instruction ministérielle n°1544/DEF/CAB/DR du 17 janvier 2017 relative à la défense-sécurité des activités, moyens et installations du ministère de la défense, version du 10 août 2020.
[PSSI-A]	Politique de sécurité des systèmes d'information des armées n°D-16-007151/DEF/EMA/SCOPS/CYBER/DR du 08 juillet 2016
[Dir.39]	Directive DGSIC n°39/DEF/DGSIC/DR du 1 ^{er} juillet 2016 portant sur la sécurité des systèmes industriels
[DIR-MCS]	Directive DGNUM n°47/ARM/DGNUM/SDSNUM/DR du 4 juin 2020 portant sur le maintien en condition de sécurité des systèmes d'information du ministère des armées

Documents de référence

Référence	Titre
IEC 62443	Cybersécurité des installations industrielles
Code pénal	Articles 121-2, 323-1 à 323-3, 411-1 à 411-11, 413-9 à 413-12, 414-7 à 414-9
Guide ANSSI	Guide de l'ANSSI sur la cybersécurité des systèmes industriels Guide de l'ANSSI sur l'hygiène informatique

Glossaire :

Autorité d'homologation (AH): autorité de niveau hiérarchique suffisant qui, sur avis d'une commission d'homologation, signe la décision autorisant l'emploi d'un système industriel d'infrastructure. La démarche d'homologation permet de s'assurer que les risques pesant sur le système, dans son contexte d'emploi, sont connus et acceptés.

Centre d'Analyse en Lutte Informatique Défensive (CALID): Le CALID est chargé d'assurer la coordination technico opérationnelle des actions de lutte informatique défensive pour le ministère de la Défense, c'est le point focal de l'OPVAR. Le CALID dispose d'un site Intradef : <http://portail-calid.intradef.gouv.fr/>

Cybersécurité: vocable regroupant sous un seul terme la cyberprotection (défense en profondeur des systèmes), la cyberdéfense (prévention et réaction en cas d'attaque) et la cyber-résilience (gestion organisationnelle et technologique des modes dégradés).

Maintien en condition de sécurité (MCS): Le MCS est une offre de services réglementaires pour les systèmes d'information industriels complémentaire au maintien en condition de sécurité. Il permet le maintien dans le temps de la sécurité face aux vulnérabilités identifiées.

Plan d'assurance sécurité (PAS): Ce document décrit l'ensemble des actions spécifiques que le candidat doit mettre en œuvre lors de l'exécution du marché pour garantir le respect des exigences de sécurité du donneur d'ordres. Un modèle de PAS est proposé dans le guide de l'ANSSI « Maîtriser les risques de l'infogérance » publié en décembre 2010.

Responsable de la sécurité des systèmes d'information aval: Le RSSI-A est chargé d'assurer le suivi SSI du système en service. À ce titre il assure le secrétariat de la commission d'homologation.

A. Généralités

Le maintien en condition de sécurité est le processus qui permet d'obtenir l'assurance que le niveau de sécurité du système industriel d'infrastructure ne se dégrade pas au cours de sa phase d'utilisation. Le niveau d'exigences de sécurité dépendra de la classe du S2I évalué selon la [Dir.39]

Une dégradation du niveau de sécurité peut provenir, par exemple, de la découverte d'une vulnérabilité technique dans un logiciel ou de tout changement de contexte qui augmenterait la vraisemblance d'une menace.

La notion de MCS comprend, de façon classique, les activités suivantes :

- La collecte d'informations décrivant toute évolution des vulnérabilités et de la menace (veille),
- L'analyse des risques, dans le contexte des systèmes utilisés et de leurs configurations,
- La proposition de recommandations (correctifs de programmes ou mesures de contournement, recommandations techniques et organisationnelles),
- Le déploiement de correctifs de sécurité,
- Le contrôle à tout moment du niveau de sécurité des systèmes et de l'intégrité des fichiers.

Le MCS est une activité complémentaire du maintien en condition opérationnelle (MCO), la sécurité étant l'un des aspects des conditions opérationnelles. En effet, une cyberattaque rend souvent le système indisponible. Comme le MCO, le MCS impose des évolutions du système pour corriger les failles identifiées et réduire les risques pesant sur le système d'information industriel, contribuant ainsi à garantir son bon fonctionnement.

B. Exigences de management

B.1. Suivi du MCS

- [MCS-001] Le titulaire doit décrire, dans un plan d'assurance sécurité (PAS), l'organisation et les procédures définies pour la réalisation du maintien en condition de sécurité du système.
- [MCS-002] Pour les systèmes de classe 2 et 3, le titulaire désigne un « Correspondant SSI », point de contact dans le cadre du marché pour les questions d'organisation générale et de coordination.
- [MCS-003] Les travaux de maintien en condition de sécurité forment un sous-ensemble du maintien en condition opérationnelle. Les résultats et le suivi de ces travaux doivent être fournis dans le cadre du MCO.
- [MCS-004] Dans le cadre du suivi du MCO, le titulaire doit également intégrer dans les comptes rendus périodiques d'activité du MCO, un rapport d'activité sur le MCS.
- [MCS-005] La veille technologique assurée au titre du MCO, les détections et traitements d'obsolescences (matérielles ou logicielles) doivent prendre en compte l'impact prévisible sur le MCS du système.
- [MCS-006] Toute modification du périmètre de maintien en condition de sécurité conduisant à une régression en matière de cybersécurité doit être validé par l'autorité d'homologation.

B.2. Ressources humaines

- [MCS-007] L'ensemble du personnel intervenant sur le système doit être sensibilisé à l'hygiène de cybersécurité et à la sécurité des S2I.
- [MCS-008] Le personnel intervenant directement sur le système d'information industriel doit être formé au bon niveau à la SSI.
- [MCS-009] Le plan d'assurance sécurité précise la liste nominative des intervenants et les documents SSI réglementaires afférents (habilitation du niveau de classification adapté au système, attestation de reconnaissance de responsabilité renseignée et signée, attestation de formation à la SSI). Le titulaire veillera à maintenir et anticiper les risques de perte des compétences spécifiques en lien avec le S2I. Cette liste est mise à jour annuellement.

B.3. Gestion documentaires

- [MCS-010] L'ensemble des documents relatifs à la conception, à la configuration ou au fonctionnement du système industriel doit être considéré, a minima, comme sensible.
- [MCS-011] Les documents doivent être stockés dans un système d'information dont le niveau de sensibilité est adapté aux S2I.
- [MCS-012] Le titulaire proposera une périodicité pour la revue documentaire afin de s'assurer que les documents nécessaires existent bien et que les documents inutiles soient éliminés.
- [MCS-013] Le transfert des faits techniques, pouvant révéler des vulnérabilités, doit être géré avec le niveau de protection adéquat conformément à l'annexe de sécurité. A minima, le transfert via un support « public » doit être réalisé au moyen du logiciel *Zed! Entreprise* ou *ACID Cryptofiler*.
- [MCS-014] Le titulaire procédera à l'inventaire de l'ensemble des procédures organisationnelles et des fiches de tâches à appliquer sur le S2I. Au besoin, il les créera, les complètera, et assurera leur mise à jour.

C. Exigences de maintien en condition de sécurité

L'efficacité du MCS repose sur l'existence impérative d'une cartographie complète du système industriel et la maîtrise de la configuration logicielle. Elles permettent d'évaluer l'impact d'une vulnérabilité découverte sur un produit ou de mesurer les conséquences de la concrétisation d'une menace.

C.1. Gestion des actifs

- [MCS-015] Si elle n'existe déjà, le titulaire doit établir en début de contrat une cartographie physique du système industriel (équipements réseaux, automates, postes de maintenance, ...).
- [MCS-016] S'il n'existe déjà, le titulaire doit établir en début de contrat un référentiel de configuration qui indiquera tous les logiciels présents, les versions de firmware, les versions des programmes automates, les paramétrages au niveau des systèmes de conduite, des installations, des matériels, des rechanges ou outillages.
- [MCS-017] Une fois le référentiel de configuration établi, le client indiquera au titulaire les logiciels et exécutables à la bonne version ainsi que les outils de rechargement dont il dispose. Le titulaire doit alors fournir au client les logiciels, exécutables, outils de rechargement et procédures de restauration des systèmes manquants. En cas d'impossibilité de fourniture, le titulaire le signale au client en apportant des justificatifs.

- [MCS-018] Pour les systèmes de classe 2 et 3, si elle n'existe déjà, le titulaire doit établir en début de contrat une cartographie des applications (matrice des flux).
- [MCS-019] La cartographie et la documentation du S2I doivent être revues à chaque modification du système industriel.
- [MCS-020] L'ensemble des données produites par les différents outils de MCS (configuration, développement applicatif, documentations, ...) sont la propriété de l'administration. Le titulaire en assure la qualité, la disponibilité et l'accessibilité.

C.2. Sécurisation des systèmes

- [MCS-021] Le titulaire s'assurera que l'accès aux équipements du système industriel est limité par des dispositifs physiques (ports physiques non utilisés scellés, ports physiques utilisés verrouillés, baies techniques sécurisées, locaux fermés, systèmes d'alarme, ...) conformément à la réglementation en vigueur. Le cas échéant, le titulaire proposera aux clients les solutions adéquates pour s'y conformer.
- [MCS-022] Le titulaire vérifiera que des dispositifs d'intégrité physique (étiquette d'intégrité numérotée avec code couleur), en conformité avec la PSSI-A, sont présents sur les stations de supervision, les serveurs, les équipements réseaux et tous éléments actifs afin de contrôler l'intégrité physique. Le cas échéant, le titulaire proposera aux clients les solutions adéquates pour s'y conformer.
- [MCS-023] La séquence de démarrage de chaque équipement (y compris le PC de maintenance) doit être protégée (mot de passe au BIOS, boot par USB ou CD-Rom désactivés, ...). Le titulaire recense les équipements protégés et met en œuvre des protections pour ceux qui n'en ont pas, sauf impossibilité ou difficulté technique majeure à justifier auprès du client.
- [MCS-024] Chaque équipement du système dispose d'un moyen d'authentification protégé conformément à la PSSI-A. Ces mots de passe doivent pouvoir être modifiés à volonté par les utilisateurs authentifiés. Si le logiciel est hébergé sur un système d'exploitation alors le titulaire met en place deux sessions distinctes : une pour le client accessible par un mot de passe modifiable par le client, l'autre pour le titulaire avec un mot de passe propre au titulaire dans l'objectif de permettre l'authentification et l'identification individuelle des intervenants. Le titulaire recense les équipements protégés et met en œuvre des protections pour ceux qui n'en ont pas. Si un équipement présente une difficulté particulière rendant ce besoin difficilement réalisable techniquement, le titulaire doit le justifier auprès du client.
- [MCS-025] Dans la mesure du possible, le principe du moindre privilège doit être appliqué pour chacun des profils déclarés sur un système.
- [MCS-026] Lorsque la fonctionnalité existe, les modes de configuration et/ou de programmation à distance des automates sont désactivés.
- [MCS-027] Le système industriel ne doit pas être interconnecté à Internet.
- [MCS-028] L'usage des technologies sans-fil est interdit. En cas de nécessité, le titulaire soumettra le besoin auprès du client pour validation.
- [MCS-029] Si le S2I utilise des fonctions, des protocoles, des services, des algorithmes obsolètes ou vulnérables, le titulaire proposera leur remplacement par des solutions plus sûres, pérennes et soutenues. S'il est nécessaire de développer de nouvelles fonctionnalités, le titulaire s'appuiera uniquement sur des solutions sûres, pérennes et soutenues.

C.3. Sauvegarde des données

- [MCS-030] Le titulaire fournira un plan de sauvegarde des données qui lui semble les plus importantes dans le cadre d'une restauration du système après incident.
- [MCS-031] Les configurations des différents matériels actifs (automates, switches, postes de supervision, ...) doivent être sauvegardées avant et après toutes modifications y compris lorsque celles-ci ont été apportées « à chaud ».
Le propriétaire des supports de sauvegardes est le MINARM, ils doivent être stockés dans un lieu sécurisé au sein de l'emprise militaire.
- [MCS-032] Le processus de restauration des sauvegardes sera testé régulièrement selon une périodicité proposée par le titulaire. Les données concernées sont toutes les données nécessaires à la reconstruction de l'installation après un sinistre (les firmwares, les programmes automates, les fichiers de configuration, les paramètres de procédé).

C.4. Intervention

- [MCS-033] Le titulaire doit obtenir un accord formel du client pour tout déploiement d'un correctif, qu'il soit de sécurité ou non, ou d'une nouvelle version du système. L'application d'un correctif est traitée de la même façon que toute évolution du système.
- [MCS-034] Avant chaque intervention sur un système industriel d'infrastructure, le titulaire ou ses sous-traitants renseigne un certificat de cybersécurité (annexe 6 du CCTP).
- [MCS-035] Pour chaque intervention, le titulaire utilise obligatoirement lorsqu'elles existent les consoles de maintenance détenues par le client.
- [MCS-036] Lorsque les consoles de maintenance ne sont pas détenues par le client, le titulaire recensera annuellement l'ensemble des équipements matériels et logiciels afin qu'ils soient identifiés auprès du client.
- [MCS-037] L'utilisation d'outils particuliers hors d'un cadre prévu par la politique de sécurité du système industriel est interdite.
- [MCS-038] Tout support de stockage numérique amovible ne doit contenir que des données dédiées à l'intervention sur l'unité.
- [MCS-039] Selon la politique SSI du site, le titulaire et ses sous-traitants peuvent devoir déclarer auprès de l'OSSI ou du CSSI du site, tout mouvement d'entrée et de sortie d'un support de stockage numérique. Les informations ou supports classifiés doivent être marqués ou détruits conformément à la réglementation en vigueur.
- [MCS-040] Le titulaire et ses sous-traitants doivent être en mesure de justifier au RSSI-A, responsable du système, de l'innocuité de son propre matériel de maintenance/dépannage (PV et rapport de l'antivirus interne ou externe, à jour et lancé moins de 48h avant l'intervention, et après toute connexion sur un autre système).
- [MCS-041] Tout poste de maintenance intervenant sur le système dans le cadre de son maintien en condition de sécurité doit être à jour de ses correctifs de sécurité.
- [MCS-042] Le titulaire et ses sous-traitants passent sur un sas antivirus du site tous leurs supports de stockage numériques amovibles.
- [MCS-043] À la demande de l'OSSI/CSSI du site ou du RSSI-A, le titulaire et ses sous-traitants peuvent devoir mettre à disposition leurs supports numériques à l'entrée et à la sortie du site, à des fins de vérification des contenus. Cette

vérification, en présence du détenteur, se traduit de deux façons : un passage sur un antivirus d'une « station blanche » du site et/ou un contrôle pour s'assurer qu'aucune donnée n'a été sortie du site sans autorisation.

- [MCS-044] Les supports de stockage d'informations sensibles non chiffrés doivent être réparés, soit en local, sous le contrôle d'un responsable sécurité, soit par du personnel habilité dans des locaux protégés.
- [MCS-045] L'ajout et le retrait d'équipements ne doivent être effectués que par des intervenants habilités à le faire et désignés nominativement par le titulaire.
- [MCS-046] Les systèmes envoyés en réparation doivent pouvoir être « blanchis » de façon à ne laisser aucune information sensible ou classifiée. En particulier, quand cela est possible, l'usage des fonctions de sécurité doit être verrouillé par l'administrateur du système afin d'interdire l'utilisation ou l'étude de ces fonctions en dehors du contrôle du système (excepté si elles sont directement concernées par la réparation).
- [MCS-047] Un contrôle de la configuration matérielle et logicielle d'un équipement est effectué lors d'un retour de réparation et avant sa remise en service. Le titulaire vérifie qu'elle est conforme à la configuration initiale avant envoi du matériel et justifie les éventuels écarts.
- [MCS-048] Lorsque cela est techniquement possible, les supports d'informations sensibles sont extraits des matériels envoyés en réparation. Dans le cas contraire, la réparation doit avoir lieu sur site ou selon les règles liées à la confidentialité du matériel.
- [MCS-049] L'installation ou la modification d'un logiciel ne peut être effectuée que par le responsable désigné par le titulaire et habilité à le faire. Les logiciels ainsi installés doivent avoir été préalablement vérifiés par un logiciel antivirus sur un poste non connecté au système en exploitation.
- [MCS-050] Le titulaire doit maintenir la cohérence entre les versions logicielles livrées au titre du MCO et les correctifs fournis au titre du MCS.
- [MCS-051] Le titulaire doit s'assurer qu'aucun composant logiciel ne soit vulnérable ou obsolète à la livraison de chaque version du système.
- [MCS-052] En cas de découverte de vulnérabilités, le titulaire doit immédiatement informer le RSSI-A.

- [MCS-053] Le titulaire proposera une procédure de gestion des interventions afin de pouvoir identifier :
- La personne qui exécute le travail et son donneur d'ordre ;
 - La date et l'heure de l'intervention ;
 - Le périmètre sur lequel le travail est exécuté ;
 - Les actions réalisées ;
 - La liste des équipements retirés ou remplacés (y compris le cas échéant les numéros d'identification) ;
 - Les modifications apportées et leur impact.

C.5. Antivirus

- [MCS-054] Le titulaire étudie la mise en place, sur tous les systèmes disposant d'un système d'exploitation, y compris, le cas échéant sur les plateformes de test et/ou de pré-production, d'un antivirus conforme aux exigences fixées par la PSSI-A.
- Le titulaire propose au client la liste des systèmes devant bénéficier de la mise en place d'un antivirus pour validation.
- [MCS-055] La mise en œuvre des antivirus est déclenchée manuellement par un administrateur de sécurité. Toute détection de menace doit faire remonter une alerte vers l'utilisateur ; aucune suppression, mise en quarantaine, désinfection ne peut avoir lieu sans autorisation expresse d'un administrateur de sécurité.
- [MCS-056] Le titulaire fournit, selon une périodicité définie par le client, sur support amovible, toutes les mises à jour de cet antivirus en ayant pris soin, au préalable, de valider sur une plate-forme représentative du système, si elle existe, les correctifs de sécurité et de s'assurer de la non-régression des fonctions de sécurité lors de l'intégration des correctifs de sécurité.
- Le titulaire précise pour chaque mise à jour la source de son téléchargement ainsi que la signature numérique liée au contrôle d'intégrité.
- [MCS-057] Les bases de signatures antivirus sont mises à jour selon une périodicité définie par le client. Le titulaire précise pour chaque mise à jour la source de son téléchargement ainsi que la signature numérique liée au contrôle d'intégrité. Ces mises à jour ne demandent aucune action autre que l'acceptation de la mise à jour de la part des exploitants sur les postes de travail.

C.6. Veille de sécurité

- [MCS-058] Le titulaire doit proposer pour chaque système une liste des constituants matériels et logiciels pour lesquels il fournira les activités de veille de sécurité, d'alerte et de réponse. Cette liste doit être soumise au client pour acceptation.
- [MCS-059] Le titulaire doit mettre en œuvre une veille de sécurité permanente, pour l'ensemble des constituants matériels et logiciels pris en compte dans le cadre du MCS, permettant de recueillir les bulletins de sécurité et les correctifs disponibles pour chaque constituant, et d'identifier les bulletins de sécurité ayant un impact sur le niveau de sécurité du système.
- [MCS-060] Pour réaliser cette veille, le titulaire doit utiliser plusieurs sources distinctes, dont il fournit la liste (éditeurs des constituants, sites institutionnels, ...) incluant le CERT-FR. Si le titulaire ne souhaite pas utiliser directement la source d'information du CERT-FR, il doit en apporter la justification et assurer

la couverture de l'ensemble des COTS pris en compte dans le cadre du MCS par les sources retenues.

- [MCS-061] En cas d'évolution du système ou de traitement d'obsolescence, le périmètre de veille de sécurité doit être mis à jour.
- [MCS-062] Les développements (langages, logiciels, technologies, ...) effectués au titre du marché sous la responsabilité du titulaire font partie du périmètre de l'activité de veille de sécurité.
- [MCS-063] Pour les systèmes de classe 2 et 3, le titulaire doit analyser, dans le cadre de la veille de sécurité, l'impact de l'évolution des méthodes d'attaques sur les technologies utilisées afin d'identifier des vulnérabilités potentielles.
- [MCS-064] Lorsqu'une vulnérabilité ne possède pas de correctif, le titulaire proposera au RSSI-A des mesures organisationnelles et/ou techniques adaptées aux ressources du S2I.

C.7. Évolution et application des correctifs

- [MCS-065] Lorsque le S2I s'appuie sur des produits qualifiés, agréés ou certifiés dans le domaine de la SSI, le titulaire proposera un déploiement rapide des mises à jour de sécurité. Toutefois, il est déconseillé d'installer des mises à jour ou des versions postérieures visant à apporter des améliorations fonctionnelles si aucun agrément, qualification ou certification ne couvre ces nouvelles fonctionnalités.
- [MCS-066] Le titulaire doit prendre les dispositions pour que l'approvisionnement des correctifs de sécurité soit de confiance, et que la garantie d'origine et un contrôle d'intégrité soient assurés. Ces dispositions doivent être acceptées par le client.
- [MCS-067] Le titulaire prend toutes les dispositions permettant d'éviter que les livraisons ne contiennent un code malicieux. Cela se traduit par un passage sur plusieurs antivirus décrits nommément (avec leur version et la date de mise à jour de leur base antivirus) sur un PV fourni avec les livraisons.
- [MCS-068] Le titulaire doit effectuer la validation des correctifs de sécurité et vérifier la non régression des services et des fonctions de sécurité du système impactés par la mise en œuvre des correctifs de sécurité sur des plateformes représentatives des systèmes quand elles existent ou sur un périmètre réduit du S2I avec une garantie de capacité de restauration en cas de dysfonctionnement. Le titulaire doit obtenir au préalable l'accord du RSSI-A.
- [MCS-069] Chaque correctif de sécurité est dédié à une unique vulnérabilité. Plutôt que fournir de nouvelles versions du système, les correctifs peuvent éventuellement être regroupés sous forme de « service pack » (SP).
- [MCS-070] Le titulaire doit fournir la procédure de déploiement de chaque correctif de sécurité ainsi que la procédure de retour en arrière. Cette procédure indique en particulier l'impact du processus de déploiement sur la disponibilité du système (dont le délai nécessaire de mise en œuvre). S'il n'est pas en charge du déploiement des correctifs de sécurité, le titulaire doit apporter sur site une assistance et un accompagnement à la demande du client pour le réaliser.
- [MCS-071] Lorsque le S2I le permet, le titulaire privilégiera le déploiement automatique des correctifs de sécurité.
- [MCS-072] Le déploiement de correctifs se fait sans ajouter d'interconnexion au système ou à ceux qui lui sont connectés (à Internet, par exemple).

- [MCS-073] L'application d'un lot de correctifs sur une machine doit être tracée dans l'identification de la version de référence déployée sur cette machine (ajout d'un identifiant de lot de correctifs par exemple). Les correctifs étant eux-mêmes identifiés et tracés de manière individuelle.
- [MCS-074] Les logiciels antimalware et les autres équipements de sécurité sur étagères (firewall, IDS, ...) éventuellement utilisés, doivent être mis à jour régulièrement par le titulaire selon la criticité des alertes et une périodicité indiquée par le client. Ces mises à jour demandent un minimum d'actions pour leur déploiement de la part des utilisateurs.
- [MCS-075] L'ensemble des mises à jour doit être protégé en intégrité et leur origine doit être vérifiable.
- [MCS-076] Le titulaire fournira un plan de gestion de l'obsolescence des équipements et des logiciels qui indiquera notamment les dates auxquelles ils ne seront plus soutenus par le fournisseur et les modalités techniques ou organisationnelles pour y palier.
- [MCS-077] Le titulaire proposera les mesures d'isolement (cloisonnement, filtrage) de nature logique ou physique sur les composants techniques (matériels, logiciels) obsolètes ou pour lesquels les vulnérabilités ne peuvent être corrigées à un niveau jugé acceptable. Il suggèrera la surveillance particulière à mettre en œuvre sur ces éléments.
- [MCS-078] En cas d'évolution importante du S2I, le titulaire fournira ou procédera à la mise à jour de la documentation en précisant notamment le contexte, les risques induits par les vulnérabilités, l'organisation mise en place, les mesures déployées ou à déployer ainsi que les corrections apportées.
- [MCS-079] Lorsque les solutions techniques (matérielles ou logicielles) d'amélioration du niveau de sécurité du système industriel ne permettent pas d'assurer la réalisation du service, le titulaire en documentera les raisons dans une fiche de fait technique et proposera des solutions de réduction des risques.

C.8. Renouvellement d'homologation du système

- [MCS-080] En cas de modification importantes du système (modification des conditions d'exploitation, utilisation de nouvelles fonctionnalité ou application, interconnexion à d'autres systèmes,...) ou d'une évolution de l'appréciation des menaces sur le système (vulnérabilités à forte criticité, incident de sécurité majeur, impossibilité d'application de correctifs de sécurité majeurs), le titulaire apportera son expertise au RSSI-A pour l'accompagner dans une éventuelle démarche de renouvellement d'homologation.

C.9. Lutte informatique défensive

- [MCS-081] Dans la mesure du possible, chaque équipement du système doit journaliser les interventions qui y sont effectuées, en identifiant précisément l'intervenant. Si cette journalisation n'existe pas, le titulaire proposera une procédure permettant de l'assurer.
- [MCS-082] La journalisation des différents événements de sécurité générés par le système, si elle existe, doit être activée pour en permettre l'analyse et la conservation sur une période minimale d'un an. Sa configuration doit permettre de garantir qu'elle n'entraînera pas de surcharge des disques ni d'impact sur la disponibilité et la réactivité du système.
- [MCS-083] Le système doit analyser automatiquement l'activité système et les journaux d'événements, afin de détecter de potentielles ou réelles violations de

sécurité. Si cette fonction n'existe pas, le titulaire proposera une procédure et, le cas échéant, une périodicité afin d'assurer l'analyse des journaux d'évènements.

[MCS-084] Lorsqu'elle existe, le titulaire vérifiera que la journalisation des événements de sécurité enregistre les échecs d'authentification et les authentifications réussies des comptes à privilèges.

[MCS-085] Le titulaire proposera une procédure d'intervention d'urgence afin d'intervenir rapidement en cas d'incident ou sur demande d'intervention du CALID. Cette procédure d'urgence ne doit pas affecter la traçabilité des interventions.

[MCS-086] S'il n'existe pas, le titulaire participera à la définition d'un processus de gestion de crise afin de déterminer que faire lors de la détection d'un incident, qui alerter, quelles sont les premières mesures à appliquer.

Le titulaire proposera un quota d'heures annuel réservé aux interventions d'urgence.