

DIRECTIVE N°39

PORTANT SUR
LA SÉCURITE NUMERIQUE DES SYSTEMES INDUSTRIELS
(DIR-SNSI)

2^{EME} ÉDITION
APPROUVEE LE 09 JUIN 2023

ENTRETENUE PAR LA DPID



L'édition en vigueur de ce document est celle accessible *via* le site DGNUM.
S'assurer de la validité de toute copie avant usage.

Rédaction	LCL Jean-Sébastien REVY	DGNUM/SDSN/BCN
Vérification	ICDD Franck ROUSSET	DPID/DSDN
Vérification	ICA Sophie GRIFFE	DPID/FSSI
Approbation	VA Denis BERTRAND	DPID

La présente directive annule et remplace la première édition de la directive n°39
du 1er juillet 2016 relative à la sécurité des systèmes industriels.

Résumé :

Comme tout système numérique, les systèmes industriels peuvent constituer une cible pour des attaques informatiques dont les conséquences pourraient remettre en cause des activités opérationnelles et les missions du ministère. Leur numérisation croissante, leur capacité de communication accrue et l'intégration de nouvelles technologies les rendent particulièrement vulnérables. Cependant, ils demeurent différents des systèmes numériques classiques du fait de leur histoire, de leur conception et de leur fonctionnement.

Après avoir défini et caractérisé le système industriel (§3), la directive 39 précise les responsabilités en matière de sécurité numérique (§4) et décrit un processus (§5) qui prend en compte les enjeux de sécurité et leurs spécificités ainsi que les normes et la réglementation en vigueur. Elle précise des pratiques de sécurisation (§6) à mettre en œuvre de manière globale et selon la phase du cycle de vie du système. Elle a enfin pour objectif de fournir un référentiel unique en matière d'exigences de sécurité pour les systèmes industriels (annexe 5).

Le processus (annexe 2) que décrit la directive 39 s'appuie sur les notions de *classe**, de *zones de sécurité** et de *conduits**.

La *classe** désigne un niveau de sécurité en fonction du risque numérique qu'il représente pour le métier ou les activités auxquelles concourt le système industriel. Pour chaque fonction principale de ce système, un niveau de classe* est déterminé à partir d'une appréciation des risques dont la directive propose une méthode (annexe 2) issue du guide de l'ANSSI portant sur les systèmes industriels.

La *zone de sécurité** est un sous-ensemble des systèmes industriels qui regroupe des ressources logiques ou physiques réalisant une ou des fonctions déterminées. À chaque zone de sécurité* est alors attribué un niveau de classe* correspondant au niveau de classe maximal des fonctions qu'elle réalise. La zone de sécurité* est associée à un ensemble d'exigences de sécurité (annexe 5) qui dépendent de la nature de ses composants et de son niveau de classe*.

Les *conduits** regroupent des canaux de communication* permettant de raccorder les zones de sécurité* entre elles. Ces conduits* nécessitent la mise en place de mesures de sécurité adaptées à leur nature et aux niveaux de classe* des zones qu'ils relient.

Ainsi, ce processus permet d'établir une architecture fonctionnelle de sécurité et un socle de sécurité adapté au système industriel et à ses enjeux de sécurité ainsi que de définir la démarche d'homologation la plus pertinente.

Nota : les termes identifiés par le symbole * sont définis dans le glossaire présent en annexe 1. Le glossaire¹ du Guide 7 définit aussi les termes usuels en matière de sécurité numérique.

Suivi de versions

Edition	Date	Principales évolutions
Edition 1	5 juillet 2016	
Edition 2	Avril 2022	Prise en compte des risques portant sur les données. Mise en place des notions de zone de sécurité* et de conduits*. Définition d'un socle de sécurité générique.

¹ <https://synoptic.intradef.gouv.fr/nouvelle-edition-du-guide-ndeg7-0> ou <https://forge.intradef.gouv.fr/plugins/mediawiki/wiki/guide7/index.php?title=Glossaire>

TABLE DES MATIERES

1. PRÉSENTATION GÉNÉRALE	5
1.1. Enjeux de sécurité.....	5
1.2. Sécurité numérique des systèmes industriels.....	5
1.3. Champ et modalités d'application	5
1.4. Niveaux de préconisation.....	6
1.5. Gestion des dérogations aux règles de la directive	6
2. CADRE DOCUMENTAIRE	7
2.1. Documents applicables	7
2.2. Autres documents et sites de référence.....	8
3. DÉFINITIONS ET CARACTÉRISTIQUES.....	8
3.1. Définition des systèmes industriels	8
3.2. Catégories d'appartenance des systèmes industriels.....	8
3.2.1. Selon leur finalité	8
3.2.2. Selon le domaine métier.....	9
3.3. Périmètre de la sécurité numérique du système industriel.....	10
3.4. Systèmes industriels, cibles ou vecteurs de risques	12
3.5. Sûreté de fonctionnement et sécurité numérique	13
3.6. Système industriel et données	13
3.6.1. Types de données à identifier	13
3.6.2. Sensibilité des données	14
4. ACTEURS EN MATIÈRE DE SÉCURITÉ NUMÉRIQUE.....	14
4.1. Autorité d'homologation (AH).....	14
4.2. Responsables SSI (RSSI).....	15
5. PROCESSUS D'ATTRIBUTION DE CLASSE ET DE SEGMENTATION	15
5.1. Phase d'attribution de classe	16
5.1.1. Définition d'une classe* de sécurité	16
5.1.2. Attribution de classe*	16
5.1.3. Objectifs de l'attribution de classe	17
5.2. Phase de segmentation.....	17
6. PRINCIPES ET DÉMARCHES DE SÉCURISATION.....	18
6.1. Principes de sécurisation.....	18
6.2. Homologation des systèmes industriels.....	19
6.3. Gestion des risques.....	19
6.4. Socle de sécurité.....	20
6.5. Spécification du système industriel	20
6.6. Conception du système industriel	21

6.7. Utilisation du système industriel	22
6.7.1. Principaux acteurs et leur responsabilité.....	22
6.7.2. Maintien en condition de sécurité (MCS).....	23
6.7.3. Contrôle.....	24
6.7.4. Incident de sécurité	24
6.8. Retrait de service.....	25
<i>ANNEXE 1 – GLOSSAIRE</i>	<i>26</i>
<i>ANNEXE 2 – CLASSIFICATION, CATÉGORISATION, SEGMENTATION ET HOMOLOGATION</i>	<i>30</i>
<i>ANNEXE 3 - ÉVALUATION DES IMPACTS</i>	<i>38</i>
<i>ANNEXE 4 – SCHÉMA CLASSIQUE D’UNE DÉMARCHE D’HOMOLOGATION.....</i>	<i>45</i>
<i>ANNEXE 5 – SOCLE DE SÉCURITÉ</i>	<i>47</i>

1. PRÉSENTATION GÉNÉRALE

1.1. Enjeux de sécurité

Comme tous systèmes numériques, les systèmes industriels sont exposés à des risques de source accidentelle ou intentionnelle qui peuvent porter atteinte aux activités et aux missions du ministère, ses personnels et ses infrastructures. Les risques de fuite d'informations ne sont pas non plus négligeables.

Les systèmes industriels concourent aussi au fonctionnement et à la sécurité des systèmes d'information. Leur indisponibilité et leur compromission peuvent avoir de graves impacts sur ces derniers. C'est pourquoi leur identification, leur localisation ainsi que leur niveau de sécurité numérique intéressent aussi les autorités d'homologation (AH) des systèmes d'information.

1.2. Sécurité numérique des systèmes industriels

La sécurité numérique des systèmes industriels est l'ensemble des activités visant à atteindre et maintenir un état de cyber-sécurité des systèmes industriels, présentant le meilleur compromis entre risques et efficience. Elle consiste à identifier et évaluer les risques puis à les réduire à un niveau jugé acceptable par des mesures de sécurité adaptées aux systèmes et à leur environnement. Comme pour tous les systèmes numériques, ce niveau de sécurité doit être maintenu tout au long de leur cycle de vie. Les systèmes industriels font donc l'objet d'une démarche d'homologation et d'une démarche de maintien en condition de sécurité (MCS). Ces démarches doivent prendre en compte leur forte diversité et leurs spécificités tant au niveau de leur réalisation et de leur exploitation qu'au niveau de leur organisation et des acteurs impliqués ainsi que leur environnement, les métiers qu'ils soutiennent et les activités auxquelles ils concourent.

L'objectif de la présente directive est de s'assurer de la prise en compte de la sécurité numérique dans les systèmes industriels par la mise en œuvre d'**une méthodologie qui leur est spécifique** et de définir **des mesures de sécurité adaptées à leurs enjeux de sécurité et aux risques auxquels ils sont exposés**.

À partir d'une analyse fonctionnelle et d'une analyse de risques succincte portée sur ses principales fonctionnalités, un système industriel peut être segmenté en plusieurs zones de sécurité auxquelles il est attribué une classe*, c'est-à-dire un niveau de sécurité. Les mesures de sécurité à appliquer sur les ressources du système dépendent ainsi du niveau de classe* de la zone dans laquelle elles se situent. Ces mesures peuvent être complétées par celles déduites d'une analyse de risques plus approfondie.

Des mesures complémentaires peuvent aussi être appliquées aux systèmes industriels en raison de réglementations particulières (incendie, navigabilité, etc.) qui ne relèvent pas de la sécurité numérique et dont l'application est nécessaire pour autoriser leur utilisation. Les mesures de sécurité ne peuvent aller à l'encontre de ces obligations réglementaires sans lesquelles ces systèmes ne peuvent être mis en service.

La présente directive peut être déclinée par les entités du ministère qui souhaitent préciser leur organisation interne et les éventuelles spécificités de leur secteur d'activité.

1.3. Champ et modalités d'application

La présente directive précise les exigences relatives aux spécificités des systèmes industriels et s'appuie sur les guides de recommandations de l'ANSSI et les standards en vigueur.

La directive s'adresse à tous les acteurs participant à la spécification, à la conception, à la réalisation et à l'utilisation des systèmes industriels, en particulier les personnes en charge des projets, les responsables d'opérations d'infrastructures incluant tout ou partie de ces systèmes

mais également aux acteurs participant à leur maintien en condition de sécurité (MCS). Ces acteurs peuvent être du domaine de la sécurité numérique ou d'autres domaines concourant à la vie des systèmes industriels.

Elle s'adresse également aux autorités qualifiées en matière de SSI (AQSSI), aux autorités d'homologation (AH), aux autorités d'emploi et aux autorités clientes ou bénéficiaires d'un système industriel.

L'autorité d'homologation (AH) ajoute cette directive à son socle de sécurité, en complément des directives n°27 [Dir HSI] et n°47 [Dir MCS] qui portent respectivement sur l'homologation de sécurité des systèmes d'information et sur le maintien en condition de sécurité (MCS).

Les annexes sont destinées à évoluer sous la responsabilité de la DPID sur proposition des états-majors, directions et services. Leur dernière version est accessible sur SYNOPTIC.

Nota : si l'autorité d'homologation (AH) choisit, avec l'accord de son AQSSI, de ne pas ajouter la présente directive à son socle de sécurité, par exemple lorsque la partie industrielle des systèmes est minoritaire, elle s'assure de l'application des documents de référence listés au §2.1.

1.4. Niveaux de préconisation

Les règles définies dans ce document ont différents niveaux de préconisation et sont conformes au [RGI] et à la [RFC 2119]² :

OBLIGATOIRE	Ce niveau de préconisation signifie que la règle édictée indique une exigence absolue de la directive.
RECOMMANDÉ	Ce niveau de préconisation signifie qu'il peut exister des raisons valables, dans des circonstances particulières, pour ignorer la règle édictée, mais les conséquences doivent être comprises et pesées soigneusement avant de choisir une voie différente.
CONSEILLÉ	Ce niveau de préconisation signifie que la règle édictée est une bonne pratique de sécurité numérique. Il n'est pas nécessaire d'instruire une dérogation lorsqu'elle n'est pas respectée.
DÉCONSEILLÉ	Ce niveau de préconisation signifie que la règle édictée indique une prohibition qu'il est toutefois possible, dans des circonstances particulières, de ne pas suivre, mais les conséquences doivent être comprises et le cas soigneusement pesé.
INTERDIT	Ce niveau de préconisation signifie que la règle édictée indique une prohibition absolue de la directive.

1.5. Gestion des dérogations aux règles de la directive

Les règles peuvent s'appliquer sur le système industriel dans son ensemble ou sur un sous-système selon leur niveau de classe*.

Les dérogations :

- aux règles portant sur la classe 1, ou ;

² <https://www.ietf.org/rfc/rfc2119.txt> – *Keywords for use in RFCs to indicate requirement levels.*

- aux règles **RECOMMANDÉES** ou **DECONSEILLÉES** portant sur les classes^{*3} 2 ou 3, ou portant sur le système dans son ensemble.

sont du ressort de l'autorité d'homologation (AH). L'AQSSI en est tenu informée.

Les dérogations :

- aux règles **OBLIGATOIRE** ou **INTERDIT** portant sur les classes* 2 ou 3 , ou portant sur le système dans son ensemble, ou ;
- aux règles relevant des systèmes d'information d'importance vitale (S2IV) ;

sont du ressort de l'AQSSI. Le fonctionnaire SSI (FSSI) en est tenu informé.

2. CADRE DOCUMENTAIRE

2.1. Documents applicables

[PSSIM] Instruction ministérielle n°7326/ARM/CAB relative à la politique de sécurité des systèmes d'information du ministère des Armées du 25 juin 2018.

https://synoptic.intradef.gouv.fr/sites/synoptic/files/im7326_edition_2_du_25_juin_2018.pdf.

[PSSIM-T] Instruction n°7326-2/ARM/CAB du 21 juillet 2021, édition 2 relative au volet technique de la politique de sécurité du système d'information du ministère des Armées (PSSI-M).

<https://synoptic.intradef.gouv.fr/securite-numerique/pssi-m-volet-technique-2nd-edition>.

[DIR HSI] Directive n°27 portant sur l'homologation des systèmes d'information du ministère des armées, 3ème édition, 07 juin 2022.

<https://synoptic.intradef.gouv.fr/securite-numerique/directive-ndeg27dgnum-2eme-edition-du-19-novembre-2019-portant-sur-lhomologation> (Intradef).

[DIR MCS] Directive n°47 portant sur le maintien en condition de sécurité (MCS), Note 200/ARM/DGNUM/DG/DR du 4 juin 2020.

<https://synoptic.intradef.gouv.fr/securite-numerique/publication-de-la-directive-ndeg47-portant-sur-le-maintien-en-condition-de>.

[DIR DEV-SEC] Directive n°40 portant sur le développement d'applications informatiques et des logiciels robustes.

<https://synoptic.intradef.gouv.fr/architecture-technique-generale/directive-ndeg40defdgsic-du-17-mai-2017-portant-sur-le>

[Guide HYG] Guide d'hygiène informatique - ANSSI.

https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf.

[Guide ANSSI] Maîtriser la SSI pour les systèmes industriels - ANSSI.

https://www.ssi.gouv.fr/uploads/IMG/pdf/Guide_securite_industrielle_Version_finale-2.pdf.

[Arrêté SIIV AME] Arrêté du 22 mars 2021 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'importance vitale « Activités militaires de l'État ».

<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043310173>.

³ La notion et les niveaux de classe* sont définis et précisés au paragraphe 5.1.1

[Arrêté SIIV AIA] Arrêté du 8 septembre 2017 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'importance vitale « Activités industrielles de l'armement ».

[IGI 1300] Instruction générale interministérielle n°1300 sur la protection du secret de la défense nationale du 9 août 2021.

<https://synoptic.intradef.gouv.fr/securite-numerique/igi-1300-protection-sur-le-secret-de-la-defense-nationale>.

[II 901] Instruction interministérielle n°901/SGDSN/ANSSI du 28 janvier 2015 portant sur la protection des systèmes d'information sensibles. <https://synoptic.intradef.gouv.fr/securite-des-systemes-dinformation/publication-de-ii-901-sur-la-protection-du-sensible-et-du-dr>

[IM 900] Instruction ministérielle n°900/ARM/CAB/NP du 15 mars 2021, portant sur la protection du secret et des informations diffusion restreinte et sensibles.

http://portail.intradef.gouv.fr/sites/default/files/im_900_du_15_mars_2021_-_np.pdf

2.2. Autres documents et sites de référence

[IEC 62443] Norme ISA/IEC 62443 portant sur la sécurité des systèmes d'automatisation et des systèmes de commande

[ANSSI] Site SSI de l'ANSSI www.ssi.gouv.fr

[DGNUM] SYNOPTIC (Intradef) synoptic.intradef.gouv.fr

3. DÉFINITIONS ET CARACTÉRISTIQUES

3.1. Définition des systèmes industriels

Un système industriel⁴ est un système d'information particulier ayant pour finalité de contrôler ou de commander des installations ou équipements techniques, composés d'un ensemble de capteurs* et/ou d'actionneurs*. Il permet ainsi une interaction entre le monde numérique et le monde réel.

3.2. Catégories d'appartenance des systèmes industriels

3.2.1. Selon leur finalité

Les systèmes industriels sont très présents dans des domaines d'emploi variés comme l'armement, l'énergie, la santé, le bâtiment, la recherche, et dans des activités de conception, de production, de gestion, de supervision. Ils sont également présents au sein des processus de contrôle, de mesure, de prévision, de facturation, d'analyse et de planification.

Un système industriel peut :

- piloter des installations physiques (unité et chaîne de production, unités de distribution d'eau, d'énergie, ...) ou des équipements (armes, transports, outil de laboratoire, robots, ...) ;
- assurer des fonctions de protection des biens et des personnes ou de l'environnement ;
- collecter et traiter des données d'expériences et de mesures...

⁴ Par abus de langage, les termes SCADA* ou SCI* sont souvent utilisés afin de désigner les systèmes industriels alors que ces termes ne représentent qu'un sous-ensemble de ces derniers.

Un système industriel est alors susceptible de :

- concourir directement à la réalisation d'une activité tout comme un système d'information classique (système d'armes, équipements médicaux, machines-outils, ...) ;
- participer au soutien d'une activité en lui fournissant l'environnement dont elle a besoin (infrastructure, énergie, climatisation, chauffage, ...) ;
- assurer la protection des biens et des personnes qui concourent à l'activité (contrôle d'accès, vidéosurveillance, détection d'intrusion, système incendie, etc.) ;
- favoriser une activité en apportant du confort aux biens et personnes.

L'activité à laquelle un système industriel contribue ainsi que sa part de contribution sont à définir pour apprécier l'impact d'un incident sur ce même système industriel.

3.2.2. Selon le domaine métier

Il est aussi possible de regrouper les systèmes industriels en fonction de leur emploi et donc des domaines métiers auxquels ils appartiennent :

- **les systèmes industriels d'infrastructure comprenant :**
 - o ceux qui contribuent à la protection physique des installations et des sites, comprenant les contrôles d'accès, la détection d'intrusion et la vidéosurveillance (CADIVS*) ;
 - o ceux de gestion technique d'infrastructure (GTI), dont la gestion technique de bâtiment (GTB*), la gestion technique centralisée⁵ (GTC*), la gestion technique de site (GTS), la gestion technique énergétique (GTE), etc. ;
 - o ceux de la sécurité incendie (INC) ;
 - o ceux aéroportuaires, industrialo-portuaires, des moyens de manutention et de levage ;
 - o ceux de servitudes dont les systèmes de climatisation, chauffage et ventilation (CVC), les réseaux de desserte électrique, les réseaux de fluides ;
 - o les systèmes de contrôle commande (SCC*), systèmes concourant à l'infrastructure.
- les systèmes de contrôle commande (SCC*) des systèmes d'information embarqués sur système d'arme (SIESA) ;
- **les systèmes industriels de servitude (SIS)**, qui n'entrent pas dans les catégories précédentes comme les systèmes permettant de remplir une ou plusieurs fonctions d'environnement avec des contraintes plus ou moins sévères telles que la consommation, la température, la taille et les performances en temps réels* (réseaux de fluides et réseaux de desserte électrique autres que ceux concourant à l'infrastructure, vannes automatisées utilisées par le SEO, etc.) ;
- **les systèmes industriels de plateforme de test et de mesure** (éléments constitutifs d'outils médicaux, de bancs d'essai, de plateformes d'analyse scientifique, etc.) ;
- **les systèmes industriels dédiés** : simulateurs, machines-outils, etc.

Les systèmes de sûreté au sens de la [PSSI-E] et de la [PSSIM] désignent les systèmes d'information qui contribuent à la protection physique et à la gestion des installations. Ils englobent les CADIVS*, les GTI* et les INC.

En raison du développement de la numérisation des services et produits, il est parfois devenu difficile d'identifier parmi les systèmes numériques ceux qui relèvent des systèmes industriels au sens de la présente directive. Si un système numérique n'est pas identifié parmi ceux répertoriés

⁵ Les systèmes de gestion technique centralisée (GTC*) désignent aussi l'ensemble des ressources qui gère les équipements d'une ou de plusieurs fonctions d'un même domaine métier.

précédemment, l'autorité d'emploi ou bénéficiaire décide si effectivement ce système relève ou non de la présente directive.

3.3. Périmètre de la sécurité numérique du système industriel

Une grande majorité des systèmes industriels est organisée selon une architecture de type CIM⁶, qui répartit les équipements du système en cinq grands niveaux:

- **niveau 0** : composants (capteurs*, actionneurs*) qui assurent des fonctions de mesures et de commandes. Ils assurent le lien entre la partie numérique et la partie physique ;
- **niveau 1** : composants (automates*) qui assurent les fonctions de pilotages des actionneurs* en fonction des données fournies par les capteurs* ;
- **niveau 2** : composants (SCADA⁷) qui réalisent des fonctions de supervision et de contrôle du processus ;
- **niveau 3** : composants (MES⁸) qui assurent l'exécution et la gestion du processus opérationnel ;
- **niveau 4** : composants (ERP⁹) qui assurent la gestion et la planification des ressources (gestion des stocks, commande, facturation , etc.).

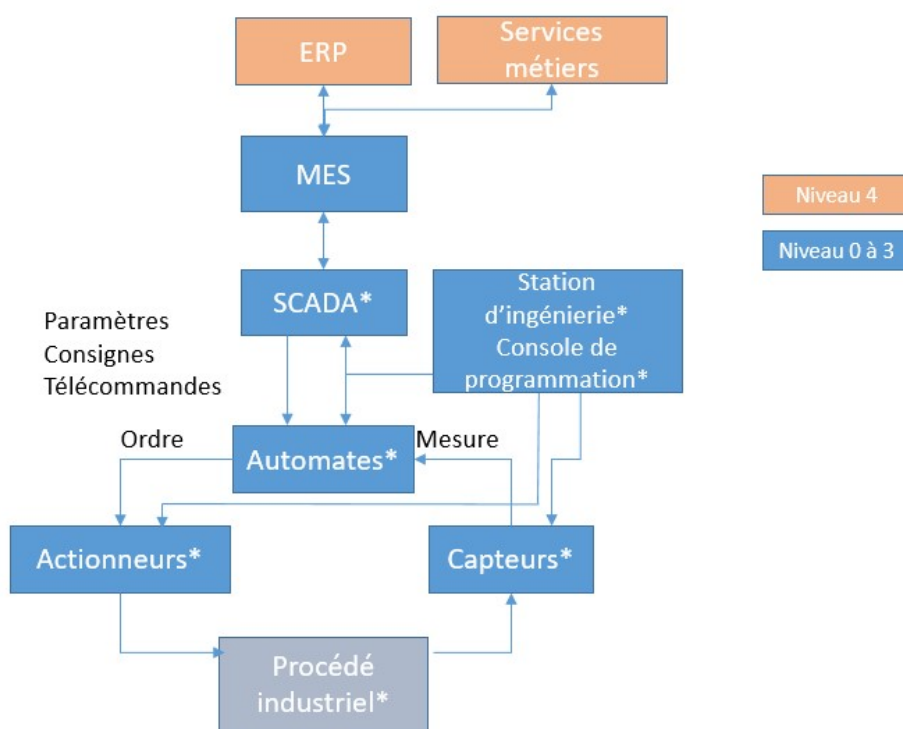


Schéma de fonctionnement d'un système industriel

⁶ Le *computer integrated manufacturing* (CIM) est un concept décrivant l'automatisation des procédés de fabrication.

⁷ *Supervisory Control and Data Acquisition*, équivalent au système de supervision industrielle.

⁸ *Manufacturing Execution System*.

⁹ *Enterprise Resource Planning*.

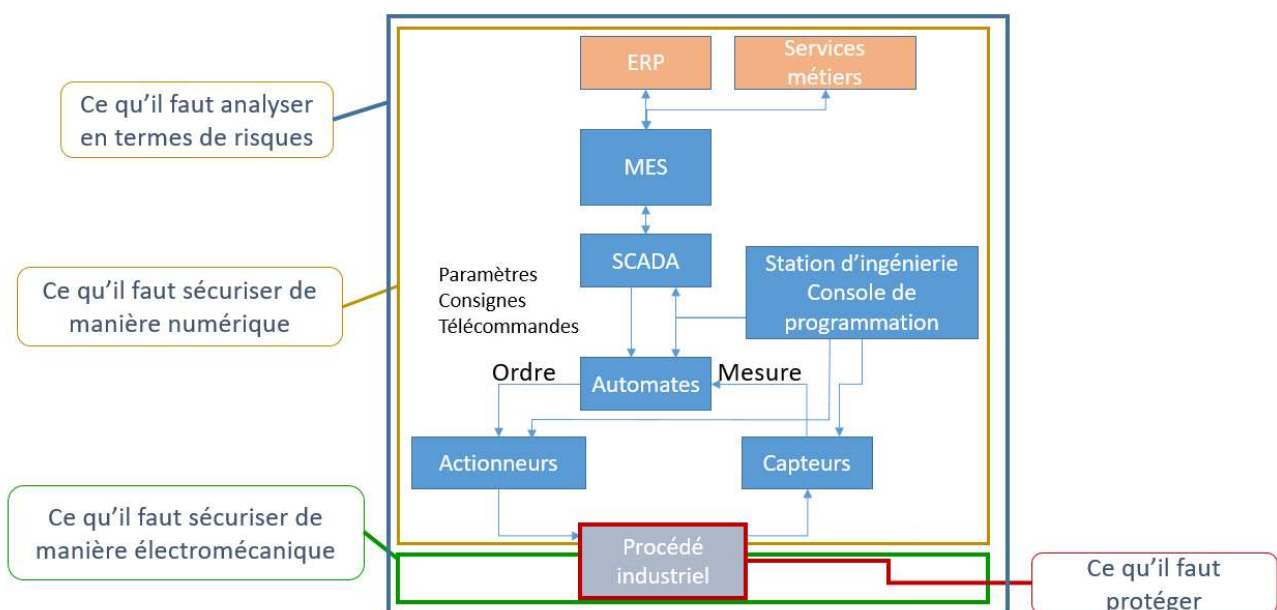
Des canaux de communication* permettent de connecter les différents niveaux entre eux.

Les systèmes industriels font l'objet de nombreuses évolutions qui intègrent des innovations liées à l'Internet des objets (IoT*) et aux technologies numériques (intelligence artificielle, robotique, informatique en nuage, Big Data, réalité augmentée, ...) et qui peuvent alors remettre en cause cette architecture. Les composants de niveau 0 peuvent ainsi directement être connectés avec des composants de niveau 4.

La sécurité numérique d'un système industriel doit être globale et se fonder sur une démarche de gestion de risques. Cette démarche inclut dans son analyse :

- tous les éléments intervenant dans le processus métier (matériel, logiciel, organisation, personnel, formation), du capteur* jusqu'au poste de gestion des ressources (du CIM 0 au 4), de sa conception jusqu'à son retrait de service sans oublier les opérations de maintenance ;
- l'environnement dans lequel le système est déployé ;
- les besoins de sécurité des métiers et des activités ainsi que des systèmes numériques qu'il supporte ;
- les impacts d'attaques informatiques sur les métiers, les activités et les systèmes numériques qu'il supporte.

Plus standardisés, les composants de niveau 4 (stations d'ingénierie* les consoles de programmation*, les postes de maintenance, ...) ainsi que leurs connexions avec les autres niveaux doivent faire l'objet d'une grande attention. **Ils sont à inclure dans la démarche d'homologation et dans l'analyse de risques.** Néanmoins, leur intégration dans le périmètre d'homologation¹⁰ du système industriel n'est pas systématique. S'ils ne sont pas inclus dans l'homologation du système industriel, ils doivent nécessairement relever d'un système homologué ou en cours d'homologation. Les mesures génériques de sécurité portant sur tout système numérique doivent leur être appliquées autant que cela est possible dans une démarche de gestion de risque.



¹⁰ Si les composants du niveau 4 ne sont pas inclus dans le périmètre d'homologation, ils sont alors considérés comme partie prenante [au sens EBIOS RM] dans l'analyse de risques.

3.4. Systèmes industriels, cibles ou vecteurs de risques

Les systèmes industriels se sont rapprochés tardivement mais progressivement des standards du monde numérique et notamment du protocole IP¹¹. Des systèmes hétérogènes ont été ainsi interconnectés dans un souci majeur de productivité, tout en cherchant à préserver la sûreté de fonctionnement* mais sans prise en compte systématique de la sécurité numérique. Les interconnexions avec des réseaux non maîtrisés, comme Internet, la multiplication des applications numériques et l'usage croissant des technologies de communication dans les équipements font croître la numérisation des systèmes industriels et leur capacité de communication. Les dernières technologies (informatique en nuage, Internet des objets connectés (IoT*), robotique, SmartGrid, ...) contribuent également à cette tendance.

La numérisation des systèmes industriels les rend ainsi particulièrement vulnérables aux incidents en matière numérique, notamment aux attaques informatiques. L'intrusion dans un système de vidéosurveillance, l'infection virale dans un système de production ou encore le piratage d'une chaîne de production par un objet connecté à l'Internet sont désormais des modes d'actions d'attaques courantes.

Or par leur rôle, les systèmes industriels **constituent une cible privilégiée pour les attaquants informatiques**. Leurs actions peuvent en effet avoir un impact direct et conséquent sur les missions du ministère, voire porter atteinte à l'intégrité des personnes et des biens.

Pourtant, les systèmes industriels ne sont guère reconnus comme des systèmes d'information à part entière, ce qui explique une moindre vigilance sur leur niveau de sécurité et sur les risques qui pèsent sur eux.

Pour autant, les systèmes industriels ne peuvent être considérés comme des systèmes numériques classiques. Ils demeurent spécifiques de par leur histoire, leur conception, et leur fonctionnement. Pour mettre en place des mesures efficaces, il est donc nécessaire de prendre en compte leurs spécificités, leurs contraintes et leurs exigences particulières, parmi lesquelles :

- une difficulté à appliquer les mesures classiques de sécurité (antivirus, correctifs, ...) ;
- des vulnérabilités techniques spécifiques liées aux composants et protocoles employés ;
- une architecture peu sujette aux modifications dans le temps ;
- une nécessité de fonctionnement en continu, avec seulement des arrêts planifiés (maintenance, ...) ;
- une nécessité de durée (très courte) de traitement déterminée et non sujette aux interférences pour certains systèmes fonctionnant en temps réel* ;
- une durée de vie pouvant –être conséquente (supérieure à 20 ans et parfois même au-delà de 40 ans) ;
- un besoin croissant d'interconnexions avec d'autres systèmes, cette interdépendance augmentant le risque mutuel sur l'ensemble des systèmes ;
- la nécessité fréquente, parfois contractuelle, d'une interconnexion avec Internet pour garantir la maintenance du système.

La démarche d'homologation doit identifier et prendre en compte les différents impératifs et contraintes qui s'imposent au système industriel afin de mettre en place des mesures répondant aux justes besoins.

¹¹ IP : *Internet Protocol*

RO 1. Il est **OBLIGATOIRE** pour la chaîne fonctionnelle de sécurité numérique de prendre en compte dans son périmètre de responsabilité tous les systèmes identifiés comme systèmes industriels et de les intégrer dans la cartographie des systèmes d'information.

3.5. Sûreté de fonctionnement et sécurité numérique

La sûreté de fonctionnement* est l'aptitude d'un bien à remplir une fonction requise dans des conditions données pendant un temps donné. Elle a donc pour but d'empêcher les défaillances et les pannes qui peuvent compromettre le fonctionnement d'un service, notamment jugé critique. Elle peut aussi se définir comme « la propriété qui permet aux utilisateurs de placer une confiance justifiée dans le service qu'il leur délivre »¹². À ce titre, les critères de maintenabilité et de fiabilité, de disponibilité et d'intégrité sont les critères primordiaux pour un système industriel. **La sûreté de fonctionnement* est alors un atout pour la sécurité numérique.**

Cependant, les mesures préconisées dans le domaine de la sûreté de fonctionnement* peuvent également favoriser des risques numériques en permettant la réalisation de nouveaux scénarios d'attaques, en tant que vecteurs ou cibles d'attaque. Afin de réduire ces risques, **les moyens garantissant la continuité d'activité doivent, dans la mesure du possible, ne pas s'appuyer sur des dispositifs numériques.** Des risques numériques peuvent être supprimés par la mise en place de ressources ne disposant d'aucun composant numérique. Si, toutefois, ces moyens comprennent une composante numérique, ils doivent être insérés dans le périmètre d'homologation.

En outre, la sûreté de fonctionnement* ne couvre pas l'ensemble des risques portant sur le système industriel. Elle prend en compte les dysfonctionnements de source involontaire (erreurs, pannes). **Les risques de menaces intentionnelles** (attaques informatiques par exemple) ou **les risques n'impactant pas directement le fonctionnement du système industriel** (fuites d'informations sensibles, divulgations ou encore vols de données) **relèvent de la sécurité numérique.**

La couverture de l'ensemble des risques pesant sur un système industriel impose donc de traiter conjointement la sécurité numérique et la sûreté de fonctionnement* dans **une approche harmonisée.**

Cependant, des mesures préconisées par la sécurité numérique peuvent interférer avec celles proposées par la sûreté de fonctionnement*. Il s'agit alors, dans la mesure du possible, d'arbitrer un équilibre, en s'appuyant sur l'avis de l'autorité d'homologation (AH). Ces décisions sont insérées dans le dossier d'homologation.

Le responsable de projet/programme d'un système industriel veille à traiter les risques numériques, non de manière isolée, mais au niveau global de la gestion de risques, afin de garantir la cohérence et la complémentarité de la démarche d'homologation et de celle mise en œuvre dans le cadre de la sûreté de fonctionnement*.

L'autorité d'homologation (AH) tient compte des risques traités par la sûreté de fonctionnement* et leur traitement avant de prononcer une décision.

3.6. Système industriel et données

3.6.1. Types de données à identifier

Les systèmes industriels traitent différents types de données portant sur le procédé industriel* et le système numérique en lui-même, dont certaines sont relatives à la sécurité numérique. Au sein

¹² Guide de la sûreté de fonctionnement, sous la direction de Jean-Claude Laprie, Toulouse, Capacduès, mai 1995, 2^{ème} édition.

de chaque domaine, se distinguent des données de fonctionnement, de supervision, d'exploitation et d'administration fonctionnelle et technique, de maintenance, de sauvegarde et de journalisation.

À ces différentes données s'ajoutent les informations portant sur le projet ou le système industriel (cartographie, dossier de configuration, documents techniques, procédures, etc.).

3.6.2. Sensibilité des données

La sensibilité des données dépend de plusieurs facteurs :

- leur nature et leur confidentialité (confidentiel médical, données à caractère personnel, données classifiées, ...) qui peuvent induire des obligations réglementaires ou légales ;
- la catégorie d'appartenance du système industriel (cf. 3.2) ;
- les activités auxquelles concourt ce système.

Le système industriel peut contenir des informations sensibles qui impliquent réglementairement la mise en œuvre de mesures de sécurité, notamment pour garantir leur confidentialité et leur traçabilité.

Les données peuvent aussi être sensibles en raison des informations qu'elles peuvent apporter aux attaquants pour la préparation de leurs attaques, en particulier en absence de standardisation de certaines composantes du système industriel.

RO 2. Il est **OBLIGATOIRE** de prendre en compte les risques de fuites ou de divulgations d'informations ainsi que les exigences de sécurité relatives aux données sensibles dans la démarche d'homologation.

4. ACTEURS EN MATIÈRE DE SÉCURITÉ NUMÉRIQUE

Les responsabilités et les rôles des acteurs en matière de sécurité numérique (autorité d'emploi, autorité qualifiée, autorité d'homologation (AH), responsable SSI¹³, ...) sont définies dans la [PSSIM], dans la directive [DIR HSI] pour la démarche d'homologation et la directive pour le maintien en condition de sécurité [DIR MCS]. D'autres responsabilités et rôles peuvent aussi être définis par secteurs d'activité et par catégories de systèmes industriels.

4.1. Autorité d'homologation (AH)

L'autorité d'homologation d'un système industriel doit être choisie à un niveau hiérarchique suffisant pour porter les risques et donc assumer les responsabilités en cas de conséquences d'une défaillance du système industriel et pour décider de l'ouverture et de la fermeture de son utilisation. En outre, elle doit pouvoir intervenir dans le maintien en condition opérationnelle (MCO) afin de garantir les composants techniques du maintien en condition de sécurité (MCS).

L'autorité d'homologation est l'autorité d'emploi du système industriel ou une autorité dont dépend l'autorité bénéficiaire.

Ces autorités maîtrisent en effet les enjeux de sécurité portant sur le système industriel et les ressources. Ce principe garantit en outre une unicité de responsabilité et une cohérence dans la prise en compte des risques de toute nature. Par exemple, selon ce principe, l'autorité d'homologation (AH) d'un CADIVS* déployé sur un site est l'autorité responsable de la sécurité

¹³ Le responsable SSI (RSSI) désigne le RSSI Projet (RSSI-P) ou le RSSI aval (RSSI-A). Cf. §4.2. Les deux fonctions peuvent être cumulées par une même personne.

physique de ce site ou une autorité dont elle dépend. En cas de besoin d'arbitrage, le FSSI propose une désignation en privilégiant l'unicité de la chaîne de responsabilité.

En cas de systèmes industriels similaires prévus d'être déployés sur plusieurs sites ou au sein de plusieurs entités distinctes, la démarche d'homologation doit être menée sous la responsabilité d'une seule autorité d'homologation (AH), ou du maître d'ouvrage au profit de l'autorité d'homologation (AH) si celle-ci l'autorise. Dans ce dernier cas, le RSSI en charge de la démarche d'homologation du SI en cours de conception et de réalisation (RSSI-P) relève alors du maître d'ouvrage ou du maître d'ouvrage délégué.

Lorsque l'autorisation d'emploi d'un système industriel nécessite la tenue d'une commission (par exemple une commission de sécurité, de sûreté, une revue de réception, etc.), la décision d'homologation (ou à défaut l'état actuel de la démarche d'homologation) doit être connue de cette même commission afin que le besoin en sécurité numérique y soit pris en compte dans sa décision ou son avis comme pour tout besoin fonctionnel. En outre, les livrables nécessaires à ces commissions doivent inclure des aspects de sécurité numérique. Réciproquement, les décisions prises lors de ces commissions doivent enfin être connues des acteurs de la démarche d'homologation.

4.2. Responsables SSI (RSSI)

La démarche d'homologation (ou de ré-homologation) d'un système industriel est conduite par un RSSI, formellement désigné, au profit de l'autorité d'emploi, même s'il ne relève pas de son autorité ou de l'autorité bénéficiaire.

Le RSSI doit être sensibilisé à la sécurité des systèmes industriels et à leurs spécificités. Pour les systèmes complexes ou à forts enjeux de sécurité, s'il n'est pas accompagné d'un spécialiste en ce domaine, le RSSI doit être formé à la sécurité des systèmes industriels de manière à mener une démarche d'homologation pertinente.

Sauf réglementations ou politiques particulières propres à une activité ou à un métier, le RSSI est en charge de **la définition de la stratégie de maintien en condition de sécurité (MCS) et de sa mise en œuvre sous la responsabilité de l'autorité d'emploi ou bénéficiaire**. Il peut s'appuyer sur la directive [DIR MCS]. Cette activité, dont l'objectif est de maintenir dans le temps le niveau de sécurité atteint au prononcé de l'homologation du SI, peut engendrer des indisponibilités incompatibles avec l'activité du site où il est déployé. Il appartient alors au RSSI de reporter ou refuser les interventions liées au MCS en relation avec l'autorité d'homologation (AH) et l'autorité d'emploi ou bénéficiaire, tout en mettant éventuellement en œuvre des mesures organisationnelles visant à maîtriser les risques identifiés. **Les responsabilités du RSSI en matière de maintien en condition de sécurité (MCS) doivent être clairement définies et connues.**

5. PROCESSUS D'ATTRIBUTION DE CLASSE ET DE SEGMENTATION

À partir d'une appréciation des risques, un niveau de sécurité, appelé **classe***, est attribué aux principales fonctions d'un système industriel (phase d'attribution de classe, cf. §5.1). Le système industriel peut alors être segmenté en groupements de ressources physiques et logiques qui réalisent des fonctions bien définies et partagent des exigences de sécurité communes (phase de segmentation*, cf. §5.2). Les sous-ensembles sont appelés **zones de sécurité** auxquelles est attribuée un niveau de classe*. Les zones de sécurité communiquent entre elles, de manière permanente ou temporaire, par des canaux de différentes natures, qui peuvent aussi partager des exigences de sécurité communes, constituant alors des **conduits***. Le système industriel est

alors segmenté en zones de sécurité* homogènes et distinctes, raccordées entre elles par des conduits*. **L'architecture technique est ainsi définie en cohérence avec le besoin de sécurité de chaque zone de sécurité* portant les fonctions principales du système industriel.**

5.1. Phase d'attribution de classe

5.1.1. Définition d'une classe* de sécurité

L'attribution de classe consiste à estimer le niveau de sécurité numérique attendu **à partir d'une appréciation de risques**.

La classe* peut être attribuée à :

- un système industriel réparti sur plusieurs sites ;
- un système industriel déployé sur un site ;
- un sous-ensemble du système qui correspond à une zone de sécurité*.

La classe* attribuée à un système industriel ou à une zone de sécurité* est déterminée à partir de la criticité des fonctions et de leur exposition aux menaces.

La criticité des fonctions est évaluée à partir des impacts :

- d'une fuite, d'un vol ou d'une divulgation d'informations (criticité en matière de **confidentialité**) ;
- d'une défaillance ou d'une conséquence d'une défaillance du système industriel sur les fonctions qu'il réalise, sur les missions auxquelles il contribue, sur l'activité et les systèmes d'information dont ils garantissent le bon fonctionnement, que l'impact soit le résultat d'une attaque, d'une erreur ou d'une panne (criticité en matière de **disponibilité** et d'**intégrité**).

La criticité d'un système est évaluée à partir de la criticité de ses fonctions principales.

L'exposition aux menaces (ou la surface d'attaques) est évaluée à partir de l'environnement du système industriel, de ses interconnexions avec d'autres systèmes ou de sa connectivité avec l'extérieur, de son niveau de standardisation et de complexité, de sa taille, de son hétérogénéité et de son niveau d'accessibilité. D'autres facteurs peuvent être pris en compte.

Il existe trois niveaux de classes* de sécurité :

- **classe 1** pour des systèmes industriels ou sous-ensembles pour lesquels la criticité du SI **ET** son exposition aux menaces sont **faibles** ;
- **classe 2** pour des systèmes industriels ou sous-ensembles pour lesquels la criticité du SI **OU** son exposition aux menaces est **significative** ;
- **classe 3** pour des systèmes industriels ou sous-ensembles pour lesquels la criticité du SI **ET** son exposition aux menaces sont **critiques**.

Afin de simplifier l'appréciation de risques, il est possible d'attribuer une classe 0 à un sous-ensemble qui n'est pas exposé aux attaques informatiques de par l'absence de composants numériques.

5.1.2. Attribution de classe*

Les classes* de sécurité doivent être estimées à partir de la méthode définie en annexe 2 ou par toute autre méthode autorisée par l'autorité d'homologation (AH). La catégorie d'appartenance du système industriel (cf. §3.2) est nécessairement un élément à prendre en compte dans l'attribution d'une classe*.

Une liste d'impacts génériques par catégorie d'appartenance du système d'information est définie dans l'annexe 3. Elle est amenée à évoluer au fur et à mesure de l'expérience. Toute proposition de modification est à transmettre à la DPID.

Une modification fonctionnelle ou technique apportée au système industriel nécessite une revue de l'estimation du niveau de classe*.

Le niveau de classe* d'une zone de sécurité* n'est pas figé. Le changement du contexte ou la définition des ressources pour assurer des fonctions peut par exemple modifier ce niveau de classe*. Les documents contractuels doivent alors prendre en compte les possibilités d'évolution de classe* dans la mesure du possible.

5.1.3. Objectifs de l'attribution de classe

Le niveau de classe* permet de définir :

- **le socle de sécurité**, c'est-à-dire l'ensemble des exigences de sécurité techniques et organisationnelles à appliquer sur les ressources, visant à répondre aux besoins de sécurité en matière de confidentialité, d'intégrité, de disponibilité, voire de traçabilité ;
- **les possibilités de dérogation** à la présente directive et les modalités dérogatoires.

Le socle de sécurité comprend aussi :

- les exigences propres aux composants de niveau 4 selon la réglementation en vigueur et les diverses recommandations (DGNUM, ANSSI, CNIL, etc.) ;
- les exigences spécifiques selon la nature des données et le niveau de confidentialité.

L'autorité d'homologation (AH) s'assure que le socle de sécurité reste applicable, cohérent et vérifiable.

5.2. Phase de segmentation

La segmentation d'un système industriel consiste à :

- regrouper les fonctions principales du système industriel en zones de sécurité homogènes et distinctes, auxquelles est attribué un niveau de classe* ;
- identifier les conduits* qui raccordent les zones de sécurité entre elles.

Une zone de sécurité* est associée à un socle de sécurité qui dépend de la nature de ses composants et de son niveau de classe*.

Les conduits* impliquent aussi la mise en place de mesures de sécurité adaptées à leur nature et aux niveaux de classe* des zones qu'ils raccordent.

Le regroupement de l'ensemble des ressources en une seule zone ou leur répartition en plusieurs zones de sécurité présentent des avantages et des inconvénients. La solution qui consiste à réduire le système industriel à une seule zone et donc à imposer à tous les équipements les mêmes règles rationalise les infrastructures, simplifie la conception et l'exploitation du système industriel mais elle impose à tous les équipements les mêmes contraintes, ce qui peut impliquer des surdimensionnements en matière de sécurité et des coûts excessifs. Le découpage du système industriel en zones de sécurité réduit la prise en compte de certaines contraintes sur une partie du système industriel mais complexifie l'infrastructure à maintenir. L'effort porte notamment sur les interfaces entre les zones.

Le choix dépend fortement du système industriel, de sa complexité et de son architecture, des conditions d'emploi, des ressources disponibles ainsi que des périmètres de responsabilité.

6. PRINCIPES ET DÉMARCHES DE SÉCURISATION

La présente directive définit les principes et démarches à mettre en œuvre en matière de sécurité numérique d'un système industriel de manière globale ou selon la phase du cycle de vie du système. Ces principes et démarches donnent lieu à des exigences définies en annexe 5 et les précisent.

6.1. Principes de sécurisation

Les principes de sécurisation applicables sur un système numérique sont à mettre en œuvre dans la conception d'un système industriel **de manière pragmatique** afin de prendre en compte ses spécificités et ses particularités qu'il faut donc identifier **de manière globale**, c'est-à-dire sans le séparer de la sécurité numérique des systèmes qu'il soutient et de son environnement.

La sécurité numérique d'un système industriel est souvent très dépendante de sa conception¹⁴. Un des principaux efforts de sécurisation porte donc sur la phase de conception et de réalisation. Elle engendre nécessairement des coûts, parfois difficiles à estimer. **La définition d'objectifs de sécurité** clairs et atteignables est donc primordiale.

Selon la nature du système industriel, l'application d'une mesure de sécurité propre au numérique peut mettre le maître d'œuvre face à une impossibilité technique. **Le principe de la défense en profondeur**¹⁵ doit donc être appliqué avec rigueur et englober la protection physique, la sensibilisation et la formation des utilisateurs ainsi qu'un corpus documentaire complet et exact, et une cartographie bien documentée et associée à une localisation des ressources en sont aussi des éléments majeurs.

Compte tenu de la durée de vie particulièrement longue de certains systèmes industriels, **la gestion des compétences et la gestion de la cartographie du système industriel** sont des points essentiels de leur maintien en condition de sécurité (MCS). Il est nécessaire d'y veiller tout au long de leur cycle de vie. La documentation apparaît alors un élément clé dans son suivi. Les risques de rupture de compétences sont aussi à prendre en compte, notamment dans une analyse de risques.

Afin d'éviter que **les dispositifs de continuité d'activité** prévus en cas de dysfonctionnement soient de nouvelles sources de risques en matière de sécurité numérique, ils doivent, dans la mesure du possible, ne pas contenir des composants numériques afin de ne pas être vulnérables aux attaques informatiques.

Si le système industriel est segmenté en zones de sécurité, la sécurisation porte sur chaque zone de sécurité* en fonction de son niveau de classe* mais aussi sur les conduits* ou interactions entre les zones de sécurité selon **le principe de filtrage*** de flux initiés depuis une zone de classe* élevée vers une zone de classe* moindre (voire équivalente).

Enfin, des négligences peuvent conduire à la réalisation d'attaques informatiques ou à la diffusion des codes malveillants sur le système industriel, engendrant des impacts bien réels. L'analyse de risques portant sur les systèmes industriels doit donc prendre en compte ces risques. Les mesures à mettre en œuvre comprennent alors nécessairement **des actions durables sur le personnel** (formation, sensibilisation, ...).

¹⁴ Ou des choix d'intégration avant sa mise en œuvre.

¹⁵ La défense en profondeur consiste en la combinaison de dispositifs juridiques, organisationnels, techniques et humains, distribués en lignes successives, visant à affaiblir l'agression en vue d'en prévenir ou d'en limiter les effets (Source : Instruction ministérielle n°1544 relative à la défense sécurité).

Enfin, une attention doit aussi porter sur **les clauses contractuelles** notamment en terme de sous-traitance, d'hébergement et de transfert de données, de télémaintenance* et de maintien en condition de sécurité (MCS).

6.2. Homologation des systèmes industriels

Le processus d'homologation et les principes définis dans [Dir HSI] sont applicables aux systèmes industriels. La présente directive la précise et la complète.

Le type de démarche d'homologation d'un système industriel ainsi que ses modalités dépendent de sa classe* et de sa segmentation*.

La stratégie d'homologation :

- précise la procédure d'attribution de classe appliquée sur le système industriel ainsi que l'outil utilisé pour la mettre en œuvre ;
- définit clairement les modalités de la démarche et veille à les adapter aux ressources qui lui sont consacrées ;
- définit la classe* du système industriel ;
- décrit les différentes zones de sécurité en cas de segmentation* ;
- précise les conduits* et leur nature.

Comme tous systèmes d'information, les systèmes industriels font aussi l'objet d'une catégorisation qui peut éventuellement impliquer le choix de la démarche conformément à [PSSIM-T]. La catégorisation en système standard, important ou essentiel peut être déterminée à partir de la classe* du système conformément à l'annexe 2.

La démarche d'homologation prend en compte les modalités de déploiement. En cas de déploiements de systèmes industriels similaires ou dans un environnement similaire, les méthodes pouvant faciliter le processus sont à rechercher afin de réduire les efforts, rationaliser le dossier d'homologation et faciliter son suivi.

Selon [Dir HSI], l'homologation d'un système numérique nécessite au préalable son enrôlement dans l'outil de suivi ministériel du patrimoine applicatif. Cependant, en raison du nombre important de systèmes industriels, cet enrôlement n'est applicable qu'aux systèmes industriels de classe 2 ou 3. Le suivi des systèmes industriels de classe 1 est alors assuré par l'AQSSI selon les modalités qu'elle définit. Ce suivi est rendu disponible au FSSI et au COMCYBER.

Le certificat d'usage et de conformité (CUC) est élaboré à partir des exigences de sécurité du socle de sécurité, tel que celui proposé en annexe 5, réactualisé le cas échéant. Selon la nature du système industriel, des activités qu'il porte, et des données qu'il traite, il peut être complété par d'autres exigences de sécurité.

Le dossier d'homologation contient, en plus des éléments définis dans [Dir HSI], tout élément justifiant la catégorisation et la segmentation* du système industriel.

L'autorité bénéficiaire du système industriel, si elle n'est pas l'autorité d'homologation (AH), est invitée à participer à la commission d'homologation. Le RSSI s'assure que l'invitation est transmise à l'autorité bénéficiaire.

La liste des risques résiduels ainsi que le plan d'amélioration continue de sécurité (PACS) sont suivis par le RSSI tout le long du cycle de vie du système industriel, et plus particulièrement lors du renouvellement d'homologation.

6.3. Gestion des risques

Les risques numériques suivants sont à prendre en compte dans toute analyse de risques portant sur un système industriel :

- les risques d'intrusion et de corruption du système industriel en provenance d'une source de menace intentionnelle externe ou interne ;
- la propagation d'une infection virale non ciblée ;
- la fuite ou la divulgation d'informations sensibles.

Les risques peuvent survenir lors de la réalisation ou de l'utilisation du SI mais **surtout lors des opérations de maintenance**.

L'analyse de risques portant sur un système industriel ne peut être générique en raison de la multiplicité et de l'hétérogénéité des systèmes industriels. Elle s'appuie notamment sur un socle de sécurité et un référentiel (impact, menace, vraisemblance, etc.) adaptés à la nature du système, aux activités auxquelles il contribue et à sa catégorie d'appartenance.

Les impacts sur un système industriel ne peuvent être identifiés, définis et évalués sans l'avis de l'autorité d'emploi ou bénéficiaire, voire d'interlocuteurs représentatifs du secteur d'activité. Les RSSI des systèmes d'information qui dépendent de systèmes industriels prennent en compte dans leur démarche les risques induits par une attaque informatique sur ces systèmes industriels.

L'autorité d'emploi ou bénéficiaire du système industriel est nécessairement impliquée dans la gestion de risques portant sur le système industriel. Si elle n'est pas l'autorité d'homologation (AH) du SI, les décisions portant sur les objectifs de sécurité et les risques nécessitent sa validation.

Le traitement des risques ne peut être réalisé sans le concours d'interlocuteurs qualifiés (ingénierie sûreté de fonctionnement*, responsable sûreté physique, etc.) afin de s'assurer de sa pertinence avec des domaines connexes (sûreté de fonctionnement*, sûreté des bâtiments, etc.) et d'éviter la redondance des mesures, voire leurs contradictions.

6.4. Socle de sécurité

Le socle de sécurité d'un système industriel comporte l'ensemble des exigences de sécurité qu'il convient de respecter. Il est associé de manière globale à tout le système industriel ou par zones de sécurité selon leur niveau de classe*. **La liste des règles telles que définies en annexe 5 constitue le socle de sécurité générique de tout système industriel.**

RO 3. Il est **OBLIGATOIRE** de définir et d'utiliser un socle de sécurité, tel que celui défini en annexe 5 (ou équivalent), en prenant en compte le niveau de classe* des zones de sécurité qui le constituent.

6.5. Spécification du système industriel¹⁶

La sécurité numérique est prise en compte dès la spécification du besoin. Elle est établie à partir :

- de la réglementation applicable, à partir de laquelle est constitué le socle de sécurité ;
- des résultats d'une analyse de risques, même succincte portant sur un périmètre précis et des contextes d'emploi ;
- des exigences de sécurité spécifiques au métier ;
- des dispositifs de sécurité apportés par l'environnement ainsi que ses contraintes.

¹⁶ Selon la nature du système industriel et du référentiel qui s'applique à son développement, la spécification peut avoir lieu soit en phase de préparation soit en phase de réalisation. La directive porte sur l'activité même de la spécification.

Elle peut nécessiter des dispositifs particuliers à mettre en œuvre tels que les dispositifs d'authentification et les systèmes de supervision de sécurité à déployer (sonde de détection d'intrusion, système de gestion des événements et des informations de sécurité (SIEM, etc.).

Les exigences de sécurité numérique portent sur :

- les données traitées en fonction de leur nature et de leur niveau de confidentialité ;
- le corpus documentaire, qui, en raison de la durée d'exploitation généralement longue du système industriel, porte la connaissance du système ;
- le personnel qui, par ses fonctions, peut être vecteur de risques ou cibles d'attaques en cas de négligence ou d'incompétence ;
- la sécurité physique des locaux qui peut, dans certains cas, être la seule barrière de sécurité efficace ;
- les équipements, y compris ceux qui se connectent de manière temporaire sur le système industriel, tels qu'un poste de diagnostic dans le cadre d'une maintenance ;
- le système industriel en lui-même sous trois aspects :
 - les moyens de communication mis en œuvre entre :
 - le système industriel et son environnement ;
 - le système industriel et d'autres systèmes numériques ;
 - le groupement de fonctions en zone de sécurité*, permettant d'appliquer des mesures de sécurité distinctes et homogènes, communes aux ressources constitutives, dont nécessairement :
 - le durcissement des équipements ;
 - le cloisonnement* et le filtrage* du réseau ;
 - la mise en place d'un contrôle d'accès physique ;
 - la surveillance au sein d'une zone ;
 - la mise à jour des équipements (fréquence, démarche) ;
 - les règles d'authentification sur les équipements ;
 - les conduits* (interactions et échanges entre les zones de sécurité).

Les responsabilités des différents acteurs, y compris des tierces parties (prestataires), en matière de sécurité numérique, sont définies au plus tôt.

La mise en place de profils de protection standardisés est une bonne pratique. Elle permet de définir les exigences de sécurité applicable à un modèle de système industriel utilisé dans un certain contexte d'emploi. Cela facilite la prise en compte et l'intégration de la sécurité numérique dans les projets ou programmes de systèmes industriels.

6.6. Conception du système industriel

La maîtrise d'œuvre fournit des solutions pour répondre aux besoins et aux objectifs de sécurité formellement définis.

Afin de limiter l'exposition aux menaces et l'introduction de vulnérabilités lors de l'implémentation, elle veille à limiter les interfaces et la complexité du système au strict nécessaire.

Elle intègre dès la conception du système des outils et des mécanismes qui permettent de faciliter la gestion de la sécurité numérique et l'application des exigences telles que :

- le durcissement et la maîtrise des configurations ;
- la gestion des vulnérabilités ;

- la gestion des obsolescences.

Elle fournit aussi :

- la documentation décrivant les mesures de sécurité mises en œuvre ;
- des processus de maintien en condition de sécurité (MCS) sous toutes ses formes (techniques, documentaires, compétences, traces, etc.) après avoir identifié les composants du système industriel à maintenir impérativement ;
- une cartographie du système industriel présentant :
 - les équipements réseau et de sécurité avec leur configuration (pare-feu, commutation réseau, sonde réseau, etc.) ;
 - les différents équipements avec leur configuration logique ;
 - les différents environnements physiques avec leur localisation ;
 - les autres systèmes auxquels le système industriel est connecté ;
 - une matrice des flux.

La cartographie inclut nécessairement un périmètre physique, une zone géographique, des biens et des flux physiques. Elle est établie selon les visions métier, applicative, infrastructure et sécurité. **Le niveau de détail est suffisant et adapté aux enjeux de sécurité du système industriel.**

Un dispositif est mis en œuvre pour garantir la mise à jour de la cartographie, en particulier lors des évolutions du système. Il est intégré dans le processus de maintenance. Une vérification à fréquence régulière de l'inventaire des actifs permet de **disposer d'une cartographie pérenne** et de **garantir son exactitude**.

La maîtrise d'ouvrage (ou maîtrise d'ouvrage déléguée) vérifie que les exigences de sécurité définies dans la spécification du système et celles fixées par le plan d'assurance sécurité (PAS) en cas d'infogérance externe soient respectées à partir de contrôles de conformité et de tests de robustesse pour vérifier la configuration des équipements, y compris sur les plateformes de test (ou d'essai), et de l'ensemble des équipements sur site. Elle s'assure que le système fourni est conforme aux spécifications définies en matière de sécurité numérique. Les résultats de tests en matière de sécurité numérique sont à insérer dans le dossier d'homologation.

La maîtrise d'ouvrage ou l'autorité bénéficiaire du système industriel s'assure que :

- le personnel en charge de son exploitation ou de son utilisation est compétent et dispose des supports nécessaires pour maintenir cette compétence et réagir en cas d'incidents de sécurité (fiches réflexes) ;
- les composants du système industriel sont protégés par un dispositif de sécurité physique correspondant aux besoins de sécurité. Les serveurs et éléments actifs du réseau ne doivent pas être accessibles aux personnes n'ayant pas le besoin d'y accéder.

La confidentialité des différents documents est à garantir contre toute divulgation ou fuite d'informations. Concernant la cartographie, celle-ci n'est pas stockée sur le système industriel en question mais sur un système d'information qui répond aux besoins de sécurité pour en garantir la confidentialité, la disponibilité, l'intégrité et la traçabilité.

6.7. Utilisation du système industriel

6.7.1. Principaux acteurs et leur responsabilité

Comme tous systèmes numériques et en matière de sécurité, les systèmes industriels déployés au profit d'un organisme sont sous la responsabilité de l'autorité d'emploi ou/et bénéficiaire. Pour assurer leur responsabilité, ces autorités disposent :

- d'un RSSI-A pour son maintien en condition de sécurité (MCS) sous tous les aspects, le renouvellement de la décision d'homologation et pour tout événement de sécurité impactant le système du SI de manière significative ;
- d'un ou plusieurs OSSI (ou CSSI) qui inscrivent le système industriel dans leur périmètre de responsabilité et veillent au respect des mesures de sécurité au niveau local.

Le RSSI-A et les OSSI s'appuient sur un ou plusieurs administrateurs (réseau, système, sécurité, fonctionnel, etc.) en charge de l'administration technique ou fonctionnelle du système industriel.

Les tierces parties (notamment prestataires) portent aussi des responsabilités en matière de sécurité numérique selon un périmètre de responsabilités bien définies et connues des autres acteurs.

Les utilisateurs du système industriel sont aussi responsables de l'usage des moyens qui leur sont fournis ainsi que des données traitées ou générées.

Toute personne accédant au système est informée de ses responsabilités et doit être sensibilisée aux risques spécifiques induits par sa fonction. La sensibilisation sur les risques portant sur un système numérique générique est nettement insuffisante. L'autorité d'emploi ou bénéficiaire veille donc à maintenir **un niveau de sensibilisation adapté aux risques qui pèsent sur ses systèmes industriels**.

6.7.2. Maintien en condition de sécurité (MCS)

Certaines actions du maintien en condition de sécurité (MCS) peuvent avoir un impact sur le processus industriel (ralentissement, redémarrage). Elles sont identifiées puis encadrées par des procédures qui détaillent le protocole d'intervention, définissent la fenêtre de maintenance et d'intervention possible et précisent le protocole à suivre pour un retour à un état normal. La définition de la fenêtre de maintenance est réalisée avec le métier dont le système supporte les activités. Des procédures de maintenance immédiates sont définies.

Le maintien en condition de sécurité (MCS) ne se réduit pas à l'aspect technique mais s'étend à tous les aspects de la sécurité numérique (cartographie, compétence, documentaire, etc.). La directive [Dir MCS], qui s'applique aux systèmes d'information et de communication, définit des principes et des mesures qui peuvent être appliqués aux systèmes industriels.

En raison de la durée de vie d'un système industriel, il est parfois impossible d'assurer la maintenance des composants du système industriel sur toute la durée de son cycle de vie. Il convient alors d'identifier les composants obsolètes, de mettre à jour l'analyse des risques, de mettre en œuvre des contre-mesures compensatoires adaptées lorsqu'elles sont possibles, et de renforcer leur surveillance.

Les risques au cours des maintenances du système industriel sont identifiés et évalués afin de prendre des mesures adaptées, notamment en cas de télémaintenance* ou d'intervention d'agents ou de tierces parties sur le système.

Toute intervention de maintenance nécessite :

- le contrôle de l'habilitation des intervenants et de celle de leur société ;
- une sensibilisation des intervenants adaptée au système ;
- la mise à jour de la cartographie et l'inventaire des équipements ainsi que leur vérification ;
- la définition des fenêtres de maintenance ;
- le cloisonnement* des données afin de faire respecter le principe du besoin d'en connaître ;
- la revue des règles de filtrage* avec définition du processus de modification ;
- la revue des accès logiques aux ressources ;
- la modification de la configuration par défaut des équipements et applicatifs, ainsi que le contrôle d'intégrité des correctifs appliqués ;

- la mise en place d'équipements dédiés à la maintenance (équipements sécurisés, durcis) dont l'intégrité et l'innocuité sont vérifiés avant intervention ;
- la sécurisation des systèmes obsolètes, par durcissement, cloisonnement* ou surveillance spécifique ;
- la désactivation des ports et le déploiement des bouchons de protection des ports ;
- le verrouillage des câbles ;
- la sauvegarde des systèmes et le stockage sur des supports hors-ligne.

En cas de télémaintenance* à partir d'un réseau non maîtrisé sans passerelle sécurisée, les mesures suivantes sont applicables *a minima* afin de réduire les risques :

- la connexion sur le réseau non maîtrisé, limitée au temps de la maintenance ;
- le filtrage* des flux ;
- la traçabilité des actions menées.

6.7.3. Contrôle

Avant un renouvellement d'homologation, l'autorité d'homologation (AH) met en place un contrôle adapté aux enjeux de sécurité du système industriel afin d'évaluer son niveau de conformité au socle de sécurité ou son niveau de risque. Elle vérifie au moins :

- la réévaluation du socle de sécurité ;
- la mise à jour de l'analyse des risques (cycle opérationnel *a minima*) ;
- l'actualisation de la cartographie ;
- la désignation et la présence de personnel intervenant compétent et sensibilisé, habilité et qualifié ;
- la connaissance et l'application des mesures de sécurité de nature organisationnelle ;
- l'efficacité de la défense en profondeur ;
- la sécurité physique des installations ;
- l'application du maintien en condition de sécurité (MCS) préalablement défini ;
- les procédures de maintenance portant sur la sécurité numérique.

Le renouvellement d'homologation s'appuie nécessairement sur les résultats de ce contrôle. Les points de contrôle vérifiés sont insérés dans le dossier d'homologation.

6.7.4. Incident de sécurité

Les autorités impactées par un incident de sécurité jugé grave ainsi que la procédure d'alerte doivent être définies et connues avant l'utilisation du système. Les autorités pouvant être impactées ainsi que la procédure d'alerte sont précisées dans les procédures d'exploitation de sécurité (PES) du système. La procédure d'alerte est adaptée au système industriel, à son environnement et à son organisation. L'autorité d'homologation (AH) vérifie sa mise en place et sa pertinence.

Les risques d'attaques informatiques sur les systèmes industriels sont pris en compte dans les plans de reprise et de continuité d'activité des organismes. Des modes dégradés sont définis pour assurer la continuité des activités auxquelles ils contribuent, notamment au travers de dispositifs de nature non numérique.

En cas d'attaques informatiques, des mesures sont mises en œuvre afin de les endiguer et de limiter leurs impacts sur les activités et sur le système en lui-même ainsi que sur les systèmes auxquels il est connecté.

Un incident de sécurité donne lieu à une analyse et à un retour d'expérience afin de déterminer son origine et d'améliorer la sécurité numérique.

6.8. Retrait de service

Le démantèlement d'un système industriel est une phase délicate et sensible en matière de sécurité numérique. Le RSSI-A est informé de son lancement comme de la fin de l'opération.

Les RSSI-P et le RSSI-A connaissent la procédure de retrait de service mise en place afin de la prendre en compte dans la démarche d'homologation ou dans son renouvellement. Compte tenu des spécificités des systèmes industriels, notamment leur longévité, les modalités de retrait de service sont suivies lors des renouvellements d'homologation.

Des mesures sont prises pour garantir les besoins de sécurité des données en matière de disponibilité, de confidentialité et d'archivage, et pour assurer, si nécessaire, la reprise des données.

Selon son importance et sa complexité, le démantèlement nécessite parfois la mise en place d'un vecteur contractuel. Celui-ci insère des exigences de sécurité pour répondre aux besoins de sécurité du système industriel et des données traitées.

ANNEXE 1 – GLOSSAIRE

Actionneur

Un actionneur est l'élément opposé au capteur* physique. Il introduit une action physique dans un procédé industriel*. Dans un système numérique, l'actionneur est souvent associé à un convertisseur numérique / analogique, ou à une sortie tout ou rien (TOR). Exemple : ouverture de gâche de porte, commande de débit, commande de moteur pas à pas.

Le terme actionneur ne doit pas être confondu avec le terme « effecteur », caractéristique d'un système d'arme.

Automate

Un automate est un dispositif se comportant de manière automatique, c'est-à-dire sans intervention humaine. Ce comportement peut être figé, le système fera toujours la même chose. On nomme Automate Programmable Industriel (API) un dispositif électronique programmable destiné à la commande de processus industriels par un traitement séquentiel. Il envoie des ordres vers les pré-actionneurs (Partie Opérative ou PO côté actionneur) à partir de données d'entrées (capteurs*, Partie Commande ou PC côté capteur*), de consignes et d'un programme informatique.

CADIVS Contrôles d'accès, détection d'intrusion, et vidéosurveillance.

Canal de communication

Liaison spécifique de communication logique ou physique entre les actifs.

Capteur physique (ou capteur)

Le capteur physique est le composant matériel qui mesure une grandeur ou un état physique dans un procédé physique*. Dans un système numérique, le capteur physique est généralement associé à un convertisseur analogique / numérique ou à une entrée tout ou rien (TOR). Exemple : détecteur de porte ouverte ou fermée, mesure de température, de courant. Le terme capteur physique ne doit pas être confondu avec le terme « capteur » utilisé dans les systèmes d'arme pour identifier les composants ou sous-systèmes qui permettent de constituer la situation tactique ou opérative.

Classe de sécurité (ou classe)

Niveau de sécurité attribué à des fonctions d'un système industriel, à des zones de sécurité* ou à un système industriel réparti sur plusieurs sites ou déployé sur un site. Le terme de « classe » peut être équivalent à « niveau de classe ».

Cloisonnement

Fait de mettre en place des séparations logiques ou physiques au sein ou entre des systèmes d'information pour créer des zones homogènes distinctes.

Cloisonnement physique : mise en place de réseaux physiquement distincts, utilisant notamment des éléments actifs dédiés à chaque réseau.

Cloisonnement logique : mise en place par exemple de VLAN, de VPN.

Conduit

Groupement de canaux de communication* partageant des exigences de sécurité communes et connectant deux ou plusieurs zones.

Console de programmation

Poste contenant les outils permettant de programmer, de configurer et de réaliser des opérations d'administration sur un automate* industriel.

Filtrage

Le filtrage, notamment le filtrage de flux, est un mécanisme permettant de gérer les flux autorisés à circuler au sein et entre les systèmes. Il s'agit alors de n'autoriser que les flux nécessaires au fonctionnement du système.

Gestion technique de bâtiment (GTB)

Système industriel permettant la gestion de l'ensemble des installations techniques d'un bâtiment (électricité, climatisation, aération, ascenseurs, ...).

Gestion technique centralisée (GTC)

Système de conduite d'un seul domaine technique (chauffage ou éclairage ou climatisation, etc.) provenant d'un même site.

Intervenant

Toute personne étant amenée à intervenir sur un système d'information. Ceci comprend le personnel chargé de l'opération du système mais également les intégrateurs, les mainteneurs, etc.

Internet des objets (IoT)

Dispositif connecté sur Internet (ou sur un réseau spécifique au ministère) et qui dispose d'une liaison numérique avec son environnement, généralement sous la forme d'un protocole qui n'est pas seulement point-à-point et qui supporte plusieurs rôles (transfert de données, commande, mise à jour, etc.).

Ils sont souvent en mesure d'interagir physiquement avec leur environnement à travers des capteurs* et/ou actionneurs*.

Label (certification, agrément), qualification)

Par niveau de confiance décroissant, le label peut correspondre à :

- un agrément de l'ANSSI ;
- une qualification standard ou renforcée de l'ANSSI ;
- une approbation par l'OTAN, l'UE, une certification par l'ANSSI, une qualification élémentaire par l'ANSSI ou une certification reconnue au titre de l'accord international SOG-IS17 ;
- une certification reconnue au titre de l'accord international CCRA18.

Opérateur

Intervenant* en charge de l'exploitation d'un système industriel pour réaliser une des tâches du processus industriel.

Procédé industriel (ou physique)

Ensemble matériel qui peut produire ou transformer de la matière, de l'énergie, ou rendre un service physiquement mesurable en transformant de la matière ou de l'énergie sous toutes ses formes.

SCADA Supervisory Control and Data Acquisition

Voir système de supervision industrielle.

SCC Systèmes de contrôle commande

Système numérique qui implémente des automatismes de régulation, de contrôle, de pilotage de procédé physique* de toute nature. Un système de contrôle commande (SCC) contient généralement un (ou plusieurs) automate(s)* ou calculateur(s) relié(s) à des capteurs* permettant

¹⁷ Senior Officials Group Information Systems Security

¹⁸ Criteria Commun Risk Assessment

de caractériser l'état du procédé physique*, et d'actionneurs*, permettant de faire évoluer cet état.

SCI Système de contrôle industriel

Système comprenant des équipements et des logiciels conçus pour surveiller et contrôler le fonctionnement de machines-outils et des appareils qui leur sont associés dans les environnements industriels. Il comprend des SCC*, SCADA* et API.

Segmentation

La segmentation d'un système industriel consiste à regrouper les ressources d'un système industriel en zones de sécurité*, auxquelles est attribué un niveau de classe* et à identifier les conduits* qui raccordent les zones de sécurité* entre elles.

Station d'ingénierie

Équipement informatique disposant des logiciels de paramétrage, de conception, de programmation, d'administration des équipements industriels comme les automates* et les SCADA*. Cet équipement est connecté sur le réseau industriel et mis à disposition des équipes de maintenance, d'ingénierie, de support, etc.

Sûreté de fonctionnement

Étude des défaillances et des pannes d'un système visant à s'assurer de l'aptitude de celui-ci à accomplir des fonctions, dans des conditions définies et durant un intervalle de temps donné.

La sûreté de fonctionnement traite en particulier les propriétés de fiabilité, maintenabilité, disponibilité et sécurité (FMDS). La sécurité est entendue ici au sens des biens et des personnes.

Système industriel

Système d'information particulier ayant pour finalité de contrôler ou de commander des installations ou équipements techniques, composées d'un ensemble de capteurs* et/ou d'actionneurs*.

Système d'information de gestion

Système d'information comprenant les services et applications destinés à la gestion (bureautique, ressources humaines, relation clients...).

Système de supervision industrielle

Système permettant d'acquérir et de traiter un grand nombre de données (télémessures, télésignalisations et télé-alarmes) et de contrôler des équipements industriels (automates*, capteurs*, actionneurs*...) en leur envoyant des télécommandes et téléajustages.

Traduction anglaise : *Supervisory Control and Data Acquisition* (SCADA).

Système industriel distribué

Un système industriel est considéré comme distribué dès lors que des mesures de protection physique ne sont pas applicables à l'ensemble des équipements et lient le composant.

Télediagnostic

Action d'effectuer à distance, sous-entendu depuis l'extérieur des systèmes d'information de l'entité responsable, un diagnostic d'installation technique. Ceci n'inclut pas de modification de paramétrage (lecture seule).

Télégestion

Action de prendre le contrôle à distance, sous-entendu depuis l'extérieur des systèmes d'information de l'entité responsables, d'installations techniques géographiquement réparties (lecture/écriture).

Télémaintenance

Action d'effectuer à distance, sous-entendu depuis l'extérieur des systèmes d'information de l'entité responsable, des tâches de maintenance sur des installations techniques. Ceci implique notamment de pouvoir faire des modifications de paramètres ou de programmes (lecture/écriture).

Temps réel (dur, mou)

On parle de mécanisme « temps réel » lorsqu'une contrainte de temps caractérise le mécanisme. Le terme « temps réel » a été souvent employé à tort en informatique de gestion pour identifier des traitements qui doivent être réalisés dans des délais contraints, pour le confort de l'utilisateur. On parle de temps réel dur quand les événements traités trop tardivement ou perdus provoquent des conséquences catastrophiques pour la bonne marche du système (perte d'informations cruciales, plantage, etc.). Les systèmes à contraintes dures ne tolèrent qu'une gestion stricte et bornée du temps afin de conserver l'intégrité du service rendu et sont toujours respectés. Pour le temps réel dur, sont souvent cités en exemple, les contrôles de processus industriels sensibles comme la régulation des centrales nucléaires ou les systèmes embarqués utilisés dans l'aéronautique.

On parle de temps réel mou quand les événements traités trop tardivement ou perdus sont sans conséquence catastrophique pour la bonne marche du système. On peut citer l'exemple des systèmes multimédia : si quelques images ne sont pas affichées, cela ne met pas en péril le fonctionnement correct de l'ensemble du système.

Zone de sécurité

Sous-ensemble d'un système industriel qui regroupe des ressources logiques ou physiques selon leur niveau de risques ou sur d'autres critères tels que la fonction opérationnelle, l'emplacement physique ou logique, ou l'organisation responsable.

ANNEXE 2 – CLASSIFICATION, CATÉGORISATION, SEGMENTATION ET HOMOLOGATION

L'annexe décrit la méthode d'attribution de classe* à partir d'une analyse fonctionnelle du système, ce qui permet ensuite de le catégoriser selon les critères de la [PSSIM], puis de le segmenter en zones de sécurité si cela s'avère nécessaire avant de déterminer la démarche d'homologation la plus pertinente. L'annexe 4 décrit sous forme de logigramme la démarche idéale du processus de l'analyse fonctionnelle à l'homologation du SI.

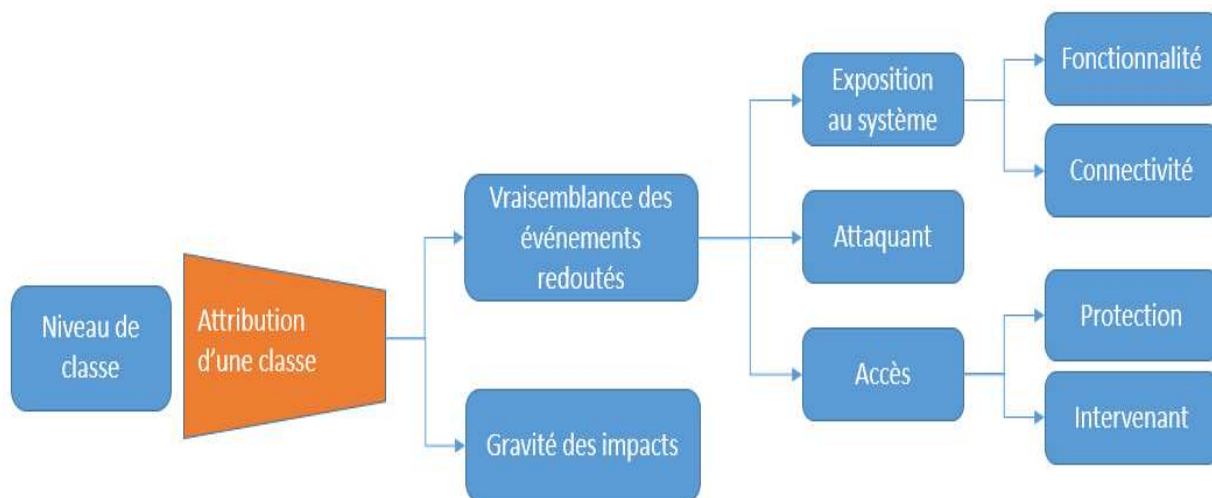


1. Analyse fonctionnelle

L'analyse fonctionnelle du système consiste à rechercher, à caractériser et à hiérarchiser les fonctions remplies par le système pour répondre aux besoins exprimés par l'autorité bénéficiaire.

L'analyse fonctionnelle est le support à partir duquel il est possible de mener une analyse de risques. Il s'agit d'établir les fonctions assurées par le système industriel afin d'identifier les risques auxquels elles sont associées. Chacune des fonctions est alors associée à une classe*.

2. Attribution de classe*



Facteurs déterminant un niveau de classe

2.1. Généralités

L'attribution de classe* consiste à attribuer pour chaque fonction du système un niveau de risque puis à retenir le niveau de classe maximal attribué aux fonctions comme niveau de classe du système.

Le niveau de risques est déterminé à partir de :

- **la gravité des impacts** sur les activités auxquelles la fonction concourt en cas d'événements redoutés ;

- la vraisemblance des événements redoutés, définie à partir :
 - de l'exposition du système industriel à la menace, elle-même déterminée à partir de la complexité du système et de ses connectivités ;
 - du niveau d'expertise des attaquants ;
 - des exigences d'accessibilité au système industriel au niveau des intervenants et de la protection physique.

Gravité des impacts Vraisemblance des événements redoutés	1	2	3	4	5	6
1	Classe 1	Classe 1	Classe 1	Classe 2	Classe 2	Classe 2
2	Classe 1	Classe 1	Classe 1	Classe 2	Classe 2	Classe 2
3	Classe 1	Classe 1	Classe 2	Classe 2	Classe 2	Classe 2
4	Classe 1	Classe 2	Classe 2	Classe 2	Classe 2	Classe 3
5	Classe 1	Classe 2	Classe 2	Classe 2	Classe 2	Classe 3
6	Classe 1	Classe 2	Classe 2	Classe 2	Classe 3	Classe 3
7	Classe 1	Classe 2	Classe 2	Classe 2	Classe 3	Classe 3
8	Classe 1	Classe 2	Classe 2	Classe 3	Classe 3	Non autorisé
9	Classe 1	Classe 2	Classe 2	Classe 3	Non autorisé	Non autorisé

2.2. Détermination de la gravité des impacts

Les impacts sont différents selon la catégorie d'appartenance du système industriel et des activités auxquelles concourt le système industriel. L'annexe 3 propose des listes d'impacts différenciées selon ces critères.

Niveau	Intitulé
1	Insignifiant

2	Mineur
3	Modéré
4	Majeur
5	Critique
6	Intolérable

2.3. Détermination de la vraisemblance des événements redoutés

La vraisemblance est déterminée par la formule suivante :

$$\text{Vraisemblance} = \text{Exposition} + \text{arrondi.entier.sup}\left(\frac{\text{Attaquant} + \text{Accès} - 2}{2}\right)$$

$$\text{Dont Accès} = \text{Max}(\text{Intervenant}, \text{Protection})$$

Les différents termes utilisés dans la formule sont définis dans les paragraphes suivants.

2.3.1. Détermination du facteur « Exposition »

Connectivité Fonctionnalité	C1	C2	C3	C4	C5	C6
F1	1	1	2	3	Non applicable	
F2	1	2	3	4	4	5
F3	2	3	3	4	4	5
F4	3	3	4	4	5	5

2.3.1.1. Détermination du facteur « Fonctionnalité »

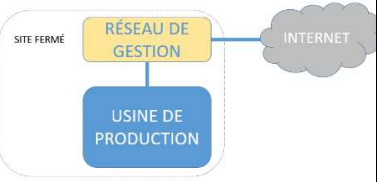
Le critère évalue le niveau de complexité du système.

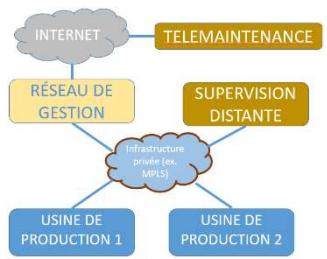
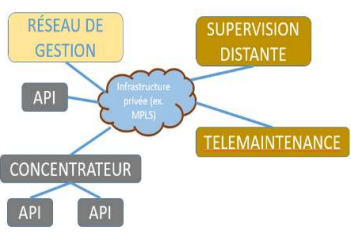
N.	Intitulé	Définition
F1	Système minimal	Système contenant uniquement des éléments de niveau CIM 0 et 1 (contrôle commande) à l'exclusion des consoles de programmation, à savoir : capteurs*/actionneurs*, entrées/sorties déportées, automates*, pupitres, systèmes embarqués, analyseurs.
F2	Système complexe	Système contenant des éléments de niveau CIM 0, 1 et 2 (contrôle-commande et SCADA*). S'ajoutent aux éléments de niveau 1 : station de supervision, serveurs d'historique local (Historian), base de données locales.

F3	Système très complexe	Système comprenant des éléments de niveau CIM 3 et/ou 4. En particulier, système avec console de programmation*, système connecté à un système d'exécution des fabrications, système comportant des bases de données d'historiques centralisées. Le système industriel peut être interconnecté avec d'autres systèmes pour partager des données.
F4	Système mutualisé	La fonction de supervision, de pilotage ou d'historisation est mutualisée avec d'autres systèmes industriels. Le système n'est plus autonome.

2.3.1.2. Détermination du facteur « Connectivité »

Le niveau de « Connectivité » correspond à la catégorie la plus élevée définie dans le tableau précédent.

N.	Intitulé	Besoins fonctionnels	Remarques
C1	Système isolé 	Le système est dédié à un site, à un ou plusieurs bâtiments. Il ne sort pas du site, du ou des bâtiment(s). OU La maintenance est réalisée sur site et directement sur les équipements, si nécessaire au moyen d'un poste de maintenance maîtrisé (sans déport).	Le réseau de production est complètement fermé. Les services sont réalisés directement sur le système ou à distance au moyen d'un réseau local dédié. La maintenance n'est pas déportée dans une autre pièce ou bâtiment ou elle est déportée par une liaison point à point. Si le système utilise des technologies sans fil, le niveau est de 3. Le système peut utiliser la technologie sans contact.
C2	Système connecté à un réseau d'information de gestion maîtrisé 	Le système échange des données avec un système d'information de gestion* au moyen d'un réseau local relevant du ministère. ET Les données sont traitées et stockées sur le site. ET Aucun service n'est réalisé à partir de l'extérieur du système industriel. OU La maintenance sur site est réalisée à partir d'équipements maîtrisés	Le réseau de production est connecté au système d'information de gestion* de l'entreprise. Celui-ci peut être interconnecté avec Internet. Cependant aucune opération depuis l'extérieur du système d'information de gestion* n'est autorisée. Si le système utilise des technologies sans fil, le niveau est de 3. Le système peut utiliser la technologie sans contact.

N.	Intitulé	Besoins fonctionnels	Remarques
		(avec déport sans liaison sans fil).	
C3	Système utilisant une technologie sans fil (hors technologie sans contact) 	Des services utilisent des moyens de liaison sans fil. OU La maintenance est réalisée sur site avec des équipements relevant du ministère pouvant utiliser des liaisons sans fil.	Le système industriel faisant usage de technologie sans fil, les technologies sans contact ne doivent pas être prises en compte.
C4	Système connecté à des postes non maîtrisés	La maintenance sur site est réalisée à partir d'équipements non maîtrisés.	
C5	Système distribué* sous maîtrise du ministère 	Le système s'étend sur plusieurs sites relevant tous du ministère. ET La maintenance est réalisée sur site ou par un contrôle à distance à partir d'un site du ministère.	Le système distribué* utilise une infrastructure privée. Celle-ci pourra être complètement privée ou être louée auprès d'un opérateur de télécommunications.
C6	Système distribué* 	Le système s'étend sur plusieurs sites qui ne relèvent pas tous du ministère. OU La maintenance peut être réalisée par un contrôle à distance à partir d'un site ne relevant pas du ministère.	Le système utilise une infrastructure publique, comme celle d'un opérateur de télécommunications.

2.3.2. Attaquant

N.	Définition	Moyens	Détermination
1	Attaque non ciblée (infection virale non ciblée, ...)	Aucun	Aucune

2	Personne avec des moyens très limités, pas nécessairement de volonté de nuire. Exemples : hacktivistes, hackers blancs, amateurs...	Faibles	Faible
3	Personne ou organisme avec des moyens limités mais avec une certaine détermination. Exemples : employés licenciés, mécontents, concurrents.	Faibles	Forte
4	Organisme aux moyens conséquents. Exemples : organisations de cybercriminalité, terroristes.	Importants	Forte
5	Organisme aux moyens illimités et à la détermination très forte. Exemple : organisme étatique.	Très importants	Très forte

2.3.3. Accès

2.3.3.1. Intervenant*

N.	Intitulé	Définition
1	Habileté, autorisé, contrôlé	L'ensemble des intervenants autorisés sont habilités (au sens métier et/ou sens protection du secret) et contrôlés. Une intervention non-autorisée n'est pas possible sans intrusion physique (accompagnement, authentification des utilisateurs, journalisation des actions).
2	Habileté et autorisé	L'ensemble des intervenants autorisés sont habilités (au sens métier et/ou sens protection du secret) mais au moins une partie des opérations possibles n'est pas tracée. Une intervention non autorisée n'est pas possible sans intrusion physique (accompagnement, authentification des utilisateurs, ...).
3	Autorisé	Il n'y a pas d'exigence particulière sur les intervenants autorisés mais une intervention non autorisée n'est pas possible sans intrusion physique (authentification des utilisateurs).
4	Non autorisé	Cette catégorie contient tous les systèmes industriels dans lesquels une intervention non autorisée est possible (système industriel accessible au public).

2.3.3.2. Protection

N.	Intitulé	Définition
1	Protection forte	L'intrusion dans le système <i>via</i> l'accès physique aux équipements est rendue difficile par une protection, comprenant plusieurs barrières physiques avec contrôle d'accès, alarme, détection et réaction. Le système comprend en outre un contrôle d'accès logique (authentification).

2	Protection moyenne	L'intrusion dans le système <i>via</i> l'accès physique aux équipements est possible mais nécessite de contourner plusieurs barrières physiques munies d'un dispositif de contrôle d'accès sans dispositif de détection ou de réaction. S'il n'existe qu'une seule barrière physique munie d'un contrôle d'accès, le système dispose d'un contrôle d'accès logique (authentification).
3	Protection minimale	L'intrusion physique dans le système <i>via</i> un accès physique aux équipements nécessite de contourner une seule barrière physique munie au moins d'un contrôle d'accès.
4	Protection absente	Il n'existe aucune barrière physique avec contrôle d'accès avant d'accéder physiquement aux équipements.

3. Catégorisation d'un système d'information

Le niveau de classe* d'un système industriel correspond au niveau de classe* maximal attribué aux fonctions qu'il assure.

Un système peut être caractérisé au minimum selon l'équivalence suivante :

Niveau de classe* du système industriel	Niveau de catégorisation du système industriel
Classe 1	Standard
Classe 2	Important
Classe 3	Essentiel

4. Segmentation en zones de sécurité

Il est possible de découper un système industriel en différents ensembles de ressources réalisant une fonction. Cette zone fonctionnelle se voit alors attribuer le niveau de classe* associé à cette fonction. Elle est alors appelée zone de sécurité*. Il est possible de fusionner des zones de sécurité selon une analyse architecturale. Le niveau de classe* de la nouvelle zone est alors le niveau de la classe* maximale des zones fusionnées.

Les zones de sécurité* échangent des données entre elles par des conduits*. Une matrice des échanges entre les zones permet d'identifier les flux et leur sens, et par conséquent les conduits* ainsi que leur nature (sans fil, câble). Si deux zones de sécurité sont liées par des conduits* différents, il est alors pertinent de dissocier chacune des zones selon la nature des conduits*.

Les exigences et mesures définies en annexe 5 sont appliquées sur les éléments d'une zone de sécurité* en fonction de son niveau de classe* et sur les conduits*.

5. Démarche d'homologation

Conformément à [Dir HSI] et au chapitre §5.1 de la présente directive, il est recommandé que la démarche d'homologation soit définie à partir de la classe* du système selon le tableau suivant :

Niveau de classe* du système industriel	Démarche d'homologation
Classe 1	Sommaire

Classe 2	Simplifiée
Classe 3	Standard

Les modalités de la segmentation* du système industriel peuvent aussi définir les démarches d'homologation selon les deux cas suivants :

- si le système industriel est réduit à une zone de sécurité* ou un ensemble de zones de même classe*, la méthode d'homologation est classique. Elle correspond à une démarche portée sur un périmètre d'homologation bien défini ;
- si le système industriel est segmenté en plusieurs zones de sécurité, il est possible d'homologuer le système comme un système de systèmes, chacune des zones constituant un système à homologuer. Cette méthode permet alors de porter une plus grande attention sur les conduits*.

ANNEXE 3 - ÉVALUATION DES IMPACTS

L'impact désigne les conséquences directes ou indirectes d'un événement qui remet en cause des besoins de sécurité du système industriel, des activités auxquelles il concourt, de l'organisme, du personnel ou encore de l'environnement. Il peut toucher les besoins de disponibilité, d'intégrité et de confidentialité, voire de traçabilité. C'est **par l'évaluation des impacts** qu'il est alors possible d'**estimer le niveau de gravité** d'un événement survenant sur le système industriel.

Plusieurs critères permettent d'évaluer un impact, des critères d'ordre opérationnel, financier, sanitaire, etc. L'importance de ces critères varie selon la catégorie d'appartenance du système et les activités auxquelles il concourt. Par exemple, si le système contribue à une activité relevant du médical, le critère « humain » est primordial.

Exemples de critères permettant d'évaluer un impact :

- les activités des bénéficiaires ainsi que le système auquel concourt directement ou indirectement le système industriel ;
- la santé et l'intégrité physique du personnel ou des personnes concernées ;
- les aspects financiers ;
- les aspects environnementaux ;
- les aspects juridiques ;
- la crédibilité du système et des bénéficiaires.

L'impact est jugé plus grand quand le dysfonctionnement ou la perte de fonctions n'est pas perceptible. Le niveau est alors au minimum de 5.

L'annexe présente des exemples à partir desquels il est possible de construire l'échelle d'impact propre à un système industriel. Néanmoins, il est indispensable de **définir des impacts correspondant aux spécificités du système et des activités auxquelles il concourt directement ou indirectement en relation avec les acteurs opérationnels, et leur contexte d'emploi.**

1. Exemples d'impacts génériques

N.	Intitulé	Impact sur l'activité portée par le système	Coût humain	Coût financier	Impact environnemental	Données perdues, divulguées ou interceptées	Impact sur l'image
1	Insignifiant	Impacts négligeables	Aucune blessure n'est envisagée.	Coût pris en charge par la maintenance ou le projet	Dépassement limité et passager d'une norme de rejet sans exigence légale de déclaration aux autorités	Données publiques	Impact négligeable
2	Mineur	Impacts acceptables sur les activités	Blessures légères ne conduisant pas à un arrêt ou à un traitement médical	Coût induit par l'événement inférieur à 100 K€	Dépassement d'une norme de rejet exigeant une déclaration aux autorités mais sans conséquence pour l'environnement	Données ou informations sans impact sur la sécurité du système, des activités ou du personnel	Mise en cause de la crédibilité du système
3	Modéré	Impacts sérieux ou répétés sur les activités sans néanmoins les compromettre	Blessures pouvant conduire à un arrêt temporaire ou à un traitement médical	Coût induit par l'événement entre 100 K€ et 1M€	Pollution modérée limitée au site	Données ou informations sensibles avec impact modéré sur la sécurité du système, des activités ou du personnel	Mise en cause de la crédibilité de l'activité au sein de l'organisme
4	Majeur	Impact graves pouvant compromettre les activités	Blessures pouvant conduire à un traitement de longue durée ou à une invalidité permanente	Coût induit par l'événement entre 1M€ et 10M€	Pollution significative limitée au site ou externe au site Évacuation de personnes	Données ou informations sensibles avec fort impact pour la sécurité du système, des activités ou du personnel. Données diffusion restreinte, données de santé, données à caractère personnel (RGPD), données portant sur la protection du potentiel scientifique et technologique (PPST)	Mise en cause de la crédibilité de l'activité hors de l'organisme au sein du ministère

N.	Intitulé	Impact sur l'activité portée par le système	Coût humain	Coût financier	Impact environnemental	Données perdues, divulguées ou interceptées	Impact sur l'image
5	Critique	Impacts graves conduisant à l'annulation ou des activités	Décès	Coût induit par l'événement entre 10M€ et 100M€	Pollution majeure avec conséquences environnementales durables externes au site (petite étendue)	Données classifiées (S).	Mise en cause de la crédibilité du ministère
6	Intolérable	Impacts graves remettant en cause d'autres activités jugées critiques	Plusieurs décès	Coût induit par l'événement supérieur à 100M€	Pollutions majeures avec conséquences environnementales durables externes au site (grande étendue)	Données classifiées (TS)	Mise en cause de la crédibilité de l'État

2. Exemples d'impacts sur un CADIVS*

Les impacts dépendent surtout de la :

- localisation du système au sein de la défense en profondeur physique mise en place ;
- sensibilité des biens à protéger (humain, infrastructure, activités, systèmes, informations).

N	Intitulé	Impact opérationnel
1	Insignifiant	Dysfonctionnement momentané, non perceptible, sans conséquences sur la sécurité physique.
2	Mineur	Dysfonctionnement occasionnel, rapidement détecté et limité. Aucune conséquence en matière de sécurité si ce n'est une plus grande surveillance.
3	Modéré	Dysfonctionnement répété et durable, qui implique une grande surveillance, voire des mesures palliatives, limitée pour le bénéficiaire. Impossibilité d'accéder au site sans intervention humaine, provoquant retard, discrédit. Impact limité sur l'organisation des activités pour garantir sa sécurité.
4	Majeur	Dysfonctionnement ou perte de service détectable avec impact sur la sécurité avec capacité de réaction rapide possible en cas de détection. Nécessiter de modifier de manière importante l'organisation des activités pour garantir la sécurité par la mise en place de mesures palliatives fortes. Réduction de l'efficacité de la défense en profondeur. Mais nécessité de traverser d'autres barrières de sécurité indépendantes pour accéder aux zones ou éléments sensibles. Multiplication de faux positifs, entraînant une perte de confiance dans le système. Impossibilité de découvrir les auteurs d'intrusion et leurs modes d'action. Perte de confidentialité des données sensibles accessibles sur le système.
5	Critique	Dysfonctionnement ou perte de service non détectable de la sécurité ou détectable mais sans capacité d'intervention rapide. Possibilité de pénétrer dans le site ou dans une zone sans capacité de détection et de réaction. Présence d'une barrière de sécurité indépendante encore à franchir avant d'accéder à des éléments à protéger.
6	Intolérable	Possibilité d'accéder directement à des zones ou éléments à protéger sans détection. Aucune barrière de sécurité à franchir.

3. Exemples d'impacts sur un système industriel de type GTI

Les impacts dépendent surtout de la nature des systèmes soutenus et de leurs besoins de disponibilité.

N.	Intitulé	Conséquences
----	----------	--------------

1	Insignifiant	Quelques difficultés, occasionnelles, sans conséquences perceptibles sur les activités ou les systèmes.
2	Mineur	Dysfonctionnement occasionnel, rapidement détecté et réparable, causant des impacts limités et peu durables sur les activités et systèmes sans gravité. Besoin possible d'intervention d'intervenants ou du prestataire.
3	Modéré	Dysfonctionnement provoquant des gênes sans gravité auprès des activités et systèmes. Aucune charge de travail constatée. Intervention nécessaire du prestataire.
4	Majeur	Dysfonctionnement ou perte de services causant des effets significatifs sur les systèmes ou activités. Possibilité de réduire les activités ou de mettre le système en mode dégradé, voir en arrêt pour un temps déterminé et tolérable. Charge de travail conséquent. Modification de l'organisation du bénéficiaire. Intervention nécessaire du prestataire.
5	Critique	Impact grave sur les activités des bénéficiaires, remettant en cause leurs missions. Remise en cause du niveau de disponibilité des systèmes jugés critiques. Remise en cause de l'aptitude du système.
6	Intolérable	Impact sur la santé et l'intégrité physique du personnel.

4. Exemples d'impacts sur le système Incendie

Les impacts dépendent surtout des activités et des biens protégés par le système incendie.

N.	Intitulé	Conséquences
1	Insignifiant	Quelques difficultés, non perceptibles, sans conséquences sur la sécurité et sur les bénéficiaires
2	Mineur	Difficulté occasionnelle et limitée, rapidement détectée et réparée. Besoin possible d'intervention d'intervenants ou du prestataire.
3	Modéré	Dysfonctionnement provoquant quelques gênes sans gravité sur l'activité des bénéficiaires Intervention nécessaire du prestataire.
4	Majeur	Dysfonctionnement provoquant des gênes sans gravité mais pouvant remettre en cause l'activité des bénéficiaires de manière encore tolérable. Génération de faux positifs remettant en cause la crédibilité du système.
5	Critique	Perturbation durable, voire arrêt, des activités du bénéficiaire, remettant ainsi en cause ses missions. Remise en cause de la sécurité physique des systèmes et des données des bénéficiaires. Remise en cause de l'aptitude du système.

		Perte d'aptitude du système.
6	Intolérable	Mise en danger du personnel.

5. Exemples d'impacts sur un système industriel de plateforme de test et de mesure

L'impact porte surtout sur :

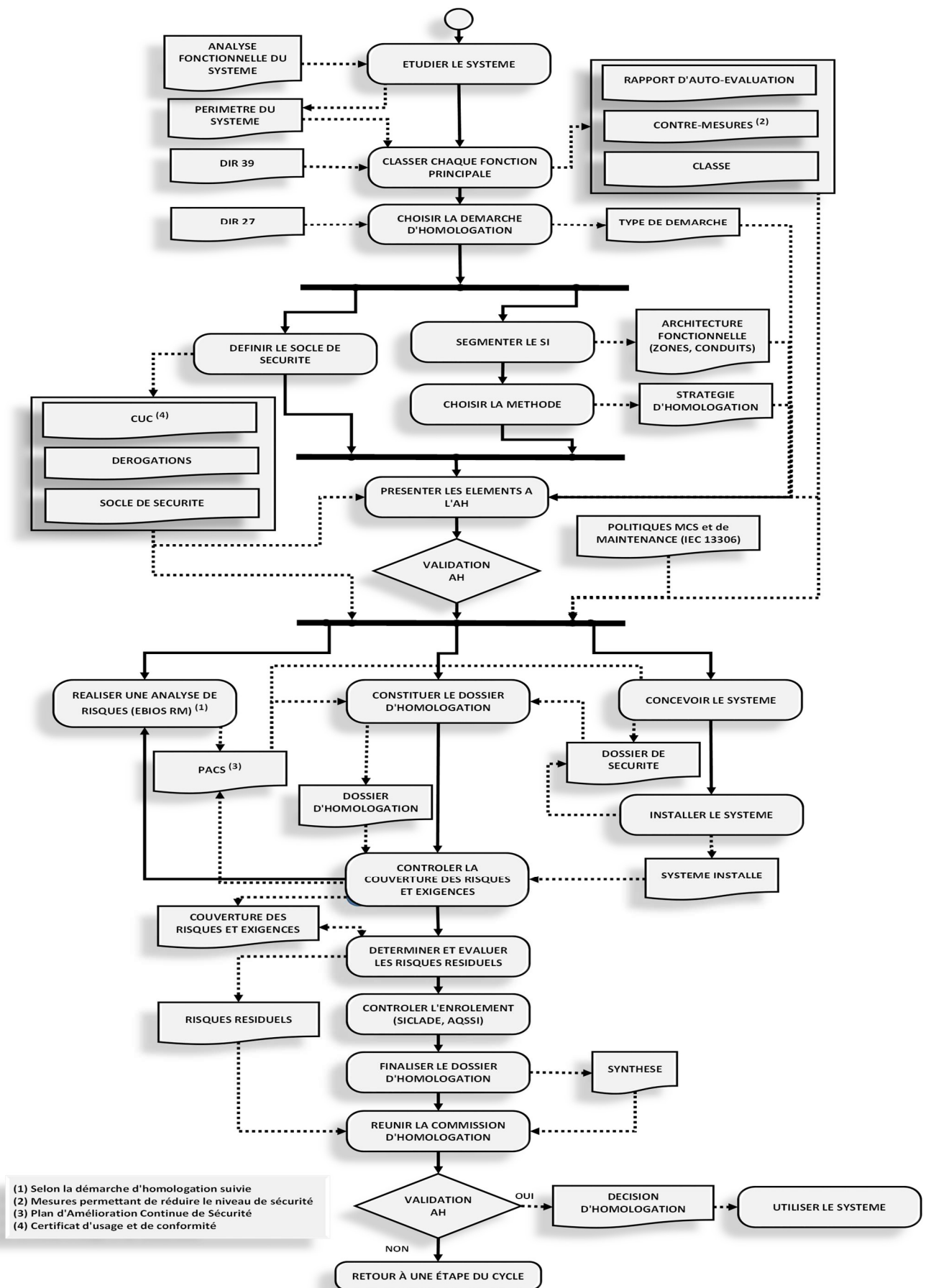
- les résultats et l'interprétation qui peut en être faite ;
- la confidentialité des tests réalisés ;
- l'efficacité des tests réalisés.

N.	Intitulé	Conséquences
1	Insignifiant	Dysfonctionnement imperceptible, n'ayant aucun impact sur les mesures et les résultats.
2	Mineur	Dysfonctionnement perceptible, ne remettant pas en cause la poursuite des tests et des mesures.
3	Modéré	Dysfonctionnement perceptible qui provoque le retard de l'activité, jugé tolérable par les utilisateurs. Les erreurs des résultats produits sont détectées. Possibilité de refaire les tests et les mesures. Perte de crédibilité du système.
4	Majeur	Dysfonctionnement qui remet en cause de manière limitée les activités de l'utilisateur. Délai d'interruption jugé non tolérable. Erreurs encore détectables. Perte financière jugée majeure.
5	Critique	Dysfonctionnement qui remet en cause une activité ou un service jugé critique pour le bénéficiaire. Dysfonctionnement imperceptible, non détectable, conduisant à des pertes financières non tolérables ou à des destructions. Résultats erronés non détectables qui impliquent des erreurs d'interprétation et des décisions faussées. Perte de crédibilité du bénéficiaire. Crise médiatique par divulgation d'informations sensibles. Recours judiciaire suite à une perte de données sensibles.
6	Intolérable	Mise en danger du personnel.

6. Exemples d'impacts sur un système industriel dédié

Les impacts dépendent de la nature des activités industrielles et d'entraînement supportées (criticité par rapport aux missions opérationnelles et d'entraînement du ministère, ...), et de leur dangerosité pour les personnes, les infrastructures et l'environnement...

N.	Intitulé	Conséquences
1	Insignifiant	Dysfonctionnement imperceptible, n'ayant aucun impact sur les activités supportées.
2	Mineur	Dysfonctionnement occasionnel, rapidement détecté et réparable, causant des impacts limités et peu durables sur les activités supportées et sans gravité. Besoin possible d'intervention de personnels ou du prestataire.
3	Modéré	Dysfonctionnement perceptible qui provoque le retard de l'activité, jugé tolérable par les utilisateurs. Besoin opératoire d'intervention de personnels ou du prestataire à moyen terme.
4	Majeur	Dysfonctionnement qui remet en cause de manière limitée les activités industrielles et d'entraînement. Délai d'interruption jugée non tolérable. Besoin obligatoire d'intervention de personnel ou du prestataire à court terme
5	Critique	Impact sur la santé et atteinte possible de manière temporaire à l'intégrité physique des personnes. Dysfonctionnement qui remet en cause une activité ou un service jugé critique pour le bénéficiaire. Délais d'interruption jugés inacceptables. Dysfonctionnement imperceptible, non détectable pouvant conduire à des destructions, des ruptures de service et des pertes financières importantes. Besoin obligatoire d'intervention de personnes ou du prestataire à court terme.
6	Intolérable	Impact grave sur la santé et l'intégrité physique des personnes, l'environnement, les infrastructures, les missions opérationnelles et d'entraînement du ministère. Besoin immédiat d'intervention de personnels ou du prestataire. Crise médiatique et recours judiciaire suite accident majeur. Pertes financières majeures.



ANNEXE 5 – SOCLE DE SÉCURITÉ

Lorsque l'utilisation d'un dispositif labellisé* est imposée par une règle, cette exigence de labellisation ne s'applique que si un tel dispositif existe. Le niveau de confiance le plus adapté aux enjeux de sécurité doit être recherché.

Si des exigences ne peuvent être appliquées en raison de besoins dûment justifiés, notamment techniques, des mesures palliatives doivent être mises en place dans le cadre d'une gestion de risque. Elles doivent faire l'objet d'une dérogation selon les règles définies au chapitre §1.4 et sont mentionnées dans le dossier d'homologation.

L'annexe 5 est associée à un fichier Excel qui reprend l'ensemble des exigences avec les références réglementaires d'où elles sont extraites et les phases du cycle de vie du système au cours desquelles elles s'appliquent.

Légendes :

Nature O et T : Règle de nature organisationnelle (ORG) et/ou technique (TECH).

SI Règle portant sur le SI dans son ensemble, quel que soit sa classe*.

C1, C2, C3 Règle portant sur la zone de sécurité* de classe 1, 2 ou 3

I Interdite, O Obligatoire, R Recommandée, C Conseillée, D Déconseillée

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
Gérer le risque							
RISQ1	ORG	Attribuer une ou des classes* à un système industriel, soit en l'attribuant dans sa totalité, soit en le segmentant en zones de sécurité.	O				Voir méthode décrite dans l'annexe 2
RISQ2	ORG	Sur proposition du RSSI en charge de la démarche d'homologation, l'attribution de classe est validée par l'autorité d'emploi ou bénéficiaire puis par l'autorité d'homologation (AH). Toute évolution de classe* nécessite une nouvelle validation.	O				
RISQ3	ORG	Pour le responsable de projet/programme d'un système industriel, traiter les risques numériques, non de manière isolée, mais au niveau global de la gestion de risques, afin de garantir la cohérence et la complémentarité de la démarche d'homologation et de celle mise en œuvre dans le cadre de la sûreté de		R	O	O	

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
		fonctionnement*. Le traitement de risques ne se limite pas à la sécurité du numérique.					
RISQ4	ORG	Mener une analyse de risques suivant une méthode autorisée par le ministère et selon la démarche d'homologation appropriée. Prendre en compte dans l'analyse de risques : - les risques d'intrusion et de corruption du système industriel en provenance d'une source de menace externe ou interne ; - la propagation d'une infection virale non ciblée ; - la fuite ou la divulgation d'informations pouvant conduire à la mise en œuvre d'une attaque ou à une infraction. Cette analyse de risques est à réactualiser en cas de changement substantiel du SI (évolution du SI ou de l'environnement), d'incident de sécurité et systématiquement lors du renouvellement d'homologation.	O				
RISQ5	ORG	En cas d'analyse de risques contractualisée, prendre un prestataire labellisé.		C	R	O	
RISQ6	ORG	Réaliser une analyse de risques avec le concours d'interlocuteurs qualifiés (ingénierie sûreté de fonctionnement*, responsable sûreté physique, etc.).		C	O	O	
Maîtriser l'organisation de la sécurité numérique							
ORG1	ORG	En complément de la directive 27, préciser de manière formelle les responsabilités en matière de sécurité numérique : - de l'autorité d'exploitation du système ; - de la maîtrise d'ouvrage et de la maîtrise d'ouvrage déléguée ; - de la maîtrise d'œuvre, des fournisseurs et intégrateurs ; - des opérateurs*. Les responsabilités sont régulièrement revues et mises à jour, en particulier lors des renouvellements d'homologation.	O				
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.		R	O	O	Le point de contact pourrait être chargé de : - la liaison avec la chaîne de responsabilité de l'entité responsable ;

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
							- la garantie du respect de la politique de cybersécurité ; - la communication sur les divergences par rapport aux exigences et les autres non-conformités.
ORG3	ORG	Le prestataire doit désigner en son sein un point de contact en matière de sécurité numérique qui sera 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				
ORG4	ORG	Enrôler les systèmes industriels dans l'outil ministériel de suivi du patrimoine applicatif. Pour les SI de classe 1, l'enrôlement relève de l'AQSSI.	O				
ORG5	ORG	Mettre à jour les données de l'outil de suivi du patrimoine applicatif du ministère des Armées (ou de l'outil de suivi de l'AQSSI) avant toute homologation ou renouvellement d'homologation.	O				
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 cybersécurité des systèmes industriels pourraient être dispensées en même temps que les formations de sûreté et de sécurité du site.

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
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				
PERS3	ORG	Disposer d'administrateurs techniques et fonctionnels compétents et qualifiés. Tout système industriel doit être en effet administré par des personnels formés à cet effet.	O				
PERS4	ORG	Pour un système Non Protégé, disposer d'un contrôle élémentaire pour détenir des privilèges particuliers (compte administrateur).	R				
Maîtriser les données							
INFO1	ORG	Identifier les données portant sur le procédé industriel*, le système numérique en lui-même, la sécurité numérique ou encore sur le projet, puis leur niveau de classification et enfin leur sensibilité en termes de confidentialité, de disponibilité, d'intégrité et de traçabilité. Les traiter en conséquence.	O				Voir §3.6 de la directive 39.
INFO2	ORG	Définir le niveau de sensibilité de la documentation et le faire apparaître clairement sur les documents. L'ensemble des documents relatifs à la conception, à la configuration ou au fonctionnement du système industriel sont à considérer comme des informations <i>a minima</i> sensibles. Les documents devraient être traités en conséquence.	O				
INFO3	ORG	Stocker les documents relatifs à la conception, à la configuration ou au fonctionnement dans un système d'information externe au système industriel. Le système doit satisfaire à leurs besoins de sécurité en matière de disponibilité, d'intégrité et de confidentialité.	O				

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
INFO4	TECH	Lorsqu'un équipement présente des risques non négligeables de perte, de vol ou de sabotage susceptibles de porter atteinte au système industriel, et qu'il contient des données <i>a minima</i> Diffusion Restreinte, chiffrer la mémoire de stockage. Cette règle est notamment applicable sur les postes de maintenance et les équipements mobiles susceptibles de quitter une zone sécurisée.	R				
Intégrer la sécurité numérique dans le projet							
ISSIP1	ORG	Identifier la réglementation relative aux activités auxquelles concourt le système industriel et intégrer leurs exigences dans le socle de sécurité du SI (ensemble des exigences de sécurité applicables sur le système).	O				
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 pourraient être prévus pour réaliser des mises à jour. On pourra configurer les sorties d'un automate* pour qu'elles restent sur leurs derniers états, pendant la mise à jour de son <i>firmware</i> .
ISSIP3	ORG	Prendre en compte le besoin de sécurité physique des équipements pour définir leur localisation et les moyens de protection physique.		R	O	O	
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 devraient pas être présents sur le système industriel. À titre d'exemple, des postes bureautiques non connectés au système industriel devraient être prévus pour permettre la consultation de la documentation, le remplissage de feuilles de suivi, etc.	R				
ISSIP5	ORG	Insérer dans le cahier des charges la liste des documents attendus, au moins : - une analyse fonctionnelle ou organique ; - un dossier d'exploitation et de maintenance ; - une ou des cartographies adaptées à la complexité du système et aux enjeux de sécurité.	O				

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
ISSIP6	ORG	Insérer dans le cahier des charges des clauses demandant des tests de sécurité numérique, notamment lors des recettes usine et plateforme. Des procédures de test de conformité en matière de cybersécurité doivent être définies et mises en place.		C	R	O	
ISSIP7	ORG	En cas de prestation externalisée, insérer dans le cahier des charges un plan d'assurance sécurité (PAS). Celui-ci décrit toutes les mesures répondant aux exigences de sécurité numérique demandées.		R	O	O	
ISSIP8	ORG	Insérer dans le cahier des charges une clause exigeant la fourniture d'équipements matériels et logiciels labellisés sur le plan de la sécurité numérique.		C	C	R	
ISSIP9	ORG	Inclure dans une clause que les supports d'un équipement informatique comportant une mémoire physique rémanente ayant vocation à stocker ou traiter des informations sensibles (DR, DCP) ou classifiées soient identifiables et ne retournent pas chez les tiers en cas de maintenance ou réparation. Cette mesure ne s'applique pas aux dispositifs agréés.	O				Les mémoires rémanentes des composants systèmes (de type disques durs, mémoires flash, etc.) qui contiennent ou ont contenu des données classifiées de défense doivent pouvoir être extraites des équipements. Les modalités pratiques d'extraction dans le cas de l'envoi en maintenance ou de recyclage doivent être décrites dans les procédures d'exploitation et de soutien.
ISSIP10	ORG	Définir, dès la phase de spécification, les modalités de démantèlement du système industriel, notamment la gestion des données et des procédés classifiés. Elles sont précisées au fur et à mesure du cycle de vie du système.	O				
ISSIP11	ORG	Intégrer au processus de choix les caractéristiques de sécurité numérique des équipements répondant aux clauses de sécurité.	O				
ISSIP12	ORG	Intégrer dans chaque temps contractuel, notamment lors du choix du candidat, le RSSI ou un expert en sécurité numérique selon la complexité du système et les enjeux de sécurité.	O				
ISSIP13	ORG	Définir des rôles pour les personnels accédant aux systèmes industriels.	O				

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
		Les rôles doivent correspondre strictement aux missions de chacun selon la politique des moindres privilèges. Les rôles d'utilisateurs et d'administrateurs (techniques, fonctionnels) doivent être distincts. Intégrer les rôles dans la gestion des comptes informatiques. Les documenter et les implémenter.					
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).		R	O	O	Voir Directive DGNUM n°40 sur le développement robuste
ISSIP15	TECH	Dédier un environnement de développement aux opérations de développement du système industriel. Cet environnement ne peut être utilisé pour d'autres activités.		R	O	O	
ISSIP16	TECH	Séparer l'environnement de développement de l'environnement de production.	O				
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				
ISSIP18	ORG	Vérifier le niveau de sécurité de l'environnement de développement.		C	R	R	
ISSIP19	ORG	Intégrer dans le contrat une clause pour que l'entité responsable puisse auditer le contractant ou les fournisseurs afin de vérifier que l'ensemble des mesures de sécurité numérique demandées sont bien appliquées.		C	R	R	
ISSIP20	TECH	Mettre en œuvre une analyse statique du code et des tests de robustesse avant la mise en production et préalablement à l'intégration de changements majeurs.	C				
ISSIP21	ORG	Effectuer un audit de code par des prestataires labellisés.		C	C	R	
Protéger physiquement le système et les contrôles d'accès aux locaux, aux équipements et aux câblages							

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
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				
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				
PHY3	ORG	Définir et mettre en œuvre une politique de contrôle d'accès aux locaux, aux armoires et aux coffrets abritant des équipements du système industriel (gestion des accès aux locaux, mécanismes de contrôle d'accès, gestion des clés et des codes d'alarme, etc.). Les mécanismes de contrôle d'accès sont adaptés aux enjeux de sécurité du système industriel ou conformes aux réglementations selon la nature du système et son niveau de confidentialité.	O				
PHY4	ORG	Définir le personnel explicitement autorisé, voire habilité, à accéder sans accompagnement aux locaux abritant des équipements du système industriel. La liste de ce personnel doit être tenue à jour.	O				
PHY5	ORG TECH	Tracer l'accès aux locaux, notamment les locaux techniques, armoires, coffrets abritant des éléments sensibles du système industriel, y compris pour le personnel accompagné. Les traces sont conservées un an.	O				
PHY6	ORG	Mettre en place un dispositif de détection d'intrusion et de vidéosurveillance pour les locaux ou zones physiques les plus sensibles en cas de risques d'intrusion physique jugés non négligeables, en particulier pour les locaux et zones non occupés de manière permanente.		C	R	O	
PHY7	ORG	Déployer les serveurs et les postes d'exploitation dans des locaux différents.		R	O	O	
PHY8	ORG	Installer les serveurs dans des locaux fermés sous contrôle d'accès, si possible dans des salles informatiques ou locaux techniques.		R	O	O	

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
PHY9	ORG	Insérer les locaux techniques et les locaux abritant des serveurs dans des zones protégées (ZP).		R	R	O	
PHY10	ORG	Ne rendre accessibles les unités centrales des stations, les équipements réseaux industriels et les automates* qu'au personnel autorisé et ayant besoin d'y accéder.	O				
PHY11	TECH	Mettre en place un dispositif de détection d'ouverture avec remontée d'alarme sur les armoires des équipements sensibles. <i>A minima</i> , 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.		C	R	O	
PHY12	ORG	Interdire la libre accessibilité aux prises d'accès au système industriel si les équipements sont accessibles au public ou dans des zones sans surveillance.	O				
PHY13	ORG	Protéger le câblage du système industriel pour prévenir ou détecter tout accès en vue d'une écoute, d'une modification ou d'une perturbation du fonctionnement du système.		R	O	O	Par exemple, mise en place du capotage pour le câblage. Il est possible de s'inspirer des exigences portant sur les circuits approuvés (cf. DTM 63). Dans le cas de systèmes classifiés, ces exigences sont obligatoires.
PHY14	TECH	Obturer les prises dédiées à la maintenance lorsqu'elles ne sont pas utilisées (bouchons, plaques d'occultation, etc.). Le retrait de l'obturateur suit une procédure bien définie et il est soumis à autorisation préalable.	O				
PHY15	ORG	En cas de locaux mutualisés ou partagé avec un organisme, mettre en place une convention de services définissant les responsabilités en matière de sécurité entre entité hébergée et hébergeant.	O				
PHY16	ORG	En cas de locaux mutualisés ou partagés avec un autre organisme, mettre en place des réseaux physiquement séparés.	O				

Maîtriser les zones de sécurité au sein du système industriel

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
RSO1	TECH	Découper les systèmes industriels par zones de sécurité auxquelles est attribué un niveau de classe*.	O				Un système industriel peut être réduit à une seule zone de sécurité*.
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				
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.		R	O	O	
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.		R	O	O	
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 pourra 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 ; - 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 ;

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
							- 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.
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.		R	O	O	Dans le cas d'Ethernet, on pourra effectuer le filtrage* sur les adresses MAC source et destination.
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 pourra être assurée par un pare-feu.
RSO8	TECH	Former au moins une zone de sécurité* à part entière pour le réseau d'administration.		R	O	O	
RSO9	TECH	Cloisonner le réseau d'administration des équipements des autres réseaux de manière physique.		C	R	O	Le périmètre porte sur les équipements d'informatique classique comme les commutateurs, passerelles, routeurs, pare-feu, etc.
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.		R	O	O	
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				

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
Maîtriser l'accès au réseau							
RSO12	ORG	Identifier, localiser et recenser les points d'accès réseau ainsi que leur statut (obstrué, désactivé, etc.)	O				
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				
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 devrait être positionné derrière un pare-feu ne laissant passer que les flux strictement indispensables. En particulier, le trafic externe au VPN devrait être bloqué.		R	O	O	
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.		R	O	O	
RSO16	TECH	Remonter une alerte en cas de tentative de connexion et de déconnexion sur les ports réseau, et la traiter.		R	R	O	
Maîtriser les interconnexions							
RSO17	TECH	Assurer un cloisonnement* entre le système industriel et d'autres systèmes (industriels ou d'information).	O				
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.		R	O	O	

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
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.		R	O	O	On pourra utiliser un VPN IPsec par exemple.
RSO20	TECH	Dans le cadre d'interconnexions entre des systèmes répartis sur des localisations différentes, mettre en place un dispositif de filtrage* (pare-feu).		R	O	O	
RSO21	TECH	Configurer les passerelles d'interconnexion selon le guide de l'ANSSI relatif à l'interconnexion d'un système d'information à Internet.		R	O	O	Guide ANSSI relatif à l'interconnexion d'un SI à Internet.
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				
RSO23	TECH	Ne pas autoriser une interconnexion directe entre un système industriel de classe 3 (ou zones de classe 3) et Internet.	O				
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				
RSO25	TECH	Réciproquement, limiter les accès depuis Internet vers le système industriel au strict nécessaire.	O				
RSO26	TECH	Pour l'interconnexion, utiliser des équipements labellisés.		C	R	O	
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				
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.

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
RSO29	TECH	Constituer une zone de sécurité* contenant le réseau sans-fil.	O				Les communications sans fil devraient être cloisonnées au maximum en isolant les périphériques sans fil dans un réseau physique ou logique séparé.
RSO30	TECH	Les points d'accès sans fil devraient 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.		R	O	O	
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.		R	O	O	
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.		R	O	O	
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.		R	O	O	Mesures possibles : Par exemple, on pourrait 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 ;

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
							- le retrait ou la déconnexion des lecteurs de médias amovibles.
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.		R	O	O	
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	R	O	
EXP5	TECH	Sur les automates* et les applications SCADA*, ne pas charger dans les équipements les mnémoniques et commentaires		R	O	O	
EXP6	ORG	Privilégier les équipements labellisés.		R	R	O	
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
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				

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
EXP9	TECH	Appliquer le principe du moindre privilège sur les applications. Elles doivent s'exécuter avec des privilèges strictement nécessaires à leur fonctionnement.		R	O	O	
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	R	O	
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.		C	R	O	Éléments concernés : <i>firmwares</i> , systèmes d'exploitation et logiciels standards, progiciels SCADA*, programmes d'automates et de SCADA*, fichier de configuration des équipements réseau, etc.
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 <i>firmware</i> ; - les logiciels et progiciels SCADA* ; - les paramètres de configuration durcis.		R	O	O	
EXP13	TECH	Ne pas installer d'outils de développement sur les machines de production. Seuls les environnements de production (<i>runtime</i>) 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.		R	O	O	
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				
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				

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
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				
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				
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				
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				
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				
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				

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
EXP22	ORG	Effectuer une revue régulière des intervenants et de leurs comptes, au minimum une fois par an pour vérifier : - l'application des règles portant sur les comptes et les accès ; - la pertinence des comptes. Si des comptes appartiennent à des personnels n'intervenant plus sur le système industriel, ils sont désactivés et supprimés au bout d'un temps défini afin de garantir la traçabilité de leurs actions.. Porter une attention particulière sur les comptes d'administration.	O				Les comptes doivent être désactivés dès le départ d'un personnel. Le circuit départ de l'entité prévoit une notification aux administrateurs des systèmes.
EXP23	ORG	Dans le cas où un appel doit être fait, exceptionnellement et pour des raisons de savoir-faire exclusif, à des personnes non habilitées (étrangères par exemple) pour effectuer un dépannage ou une opération particulière sur des matériels ou logiciels, mettre en place toutes mesures utiles pour qu'elles ne puissent avoir connaissance, même fortuitement d'informations sensibles ou classifiées. De plus, leur accès physique et leur intervention doivent être effectués sous la surveillance continue de personnels habilités et qualifiés.	O				
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.
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.		R	O	O	

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
EXP26	TECH	Interdire les comptes génériques disposant de privilèges comme les comptes administrateurs .	O				
EXP27	TECH	Pour les comptes ne disposant pas de privilèges, ne pas employer de compte générique ou fonctionnel sauf besoins dûment justifiés.		R	O	O	
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.		R	O	O	
EXP29	TECH	Protéger les comptes, et plus particulièrement les comptes à privilège (comptes administrateur, comptes de service), par un mécanisme d'authentification.	O				
EXP30	TECH	Séparer strictement les comptes utilisateurs et administrateurs.	O				
EXP31	TECH	Mettre en place un audit des événements liés à l'utilisation des comptes.	O				
EXP32	ORG	Valider l'usage de comptes à privilèges par le responsable hiérarchique de l'utilisateur.	R				
EXP33	TECH	Lorsque cela est possible, configurer un accès en lecture seule pour les interventions de maintenance de premier niveau.	R				
EXP34	TECH	Si la gestion des comptes est centralisée, contrôler régulièrement, au moins une fois par an, la configuration de l'annuaire centralisé.	O				
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				

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
EXP36	TECH	Mettre en place une authentification forte (carte à puce, OTP) ou multifacteur 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.).		N A	R	R	
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				
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).		C	O	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.
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				
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				
EXP41	TECH	Privilégier une temporisation d'inhibition par rapport au blocage en cas d'échec d'authentification.	R				

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
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				
EXP43	ORG	Définir une procédure garantissant la sécurité pour la réinitialisation des mots de passe en cas de perte ou d'oubli.	R				
EXP44	TECH	Enregistrer les échecs d'authentification et les authentification réussies des comptes à privilèges.		R	O	O	
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.		R	O	O	Voir la liste d'événements possibles en annexe B du guide ANSSI sur les mesures détaillées à appliquer sur les systèmes industriels.
EXP46	TECH	Activer les fonctions de traçabilité sur les équipements et logiciels s'ils le permettent (Syslog, Windows Event, etc.).		R	O	O	
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.		C	R	O	
EXP48	TECH	Journaliser les modifications de paramètres des capteurs*, actionneurs*, fonctions d'asservissement et de régulation.		C	R	O	
EXP49	TECH	Analyser régulièrement les journaux d'événements de sécurité selon une fréquence adaptée aux besoins. Les fréquence de l'analyse ainsi que les événements recherchés doivent être préalablement définis par le RSSI.		R	O	O	
Maîtriser l'usage des supports amovibles							

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
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				
EXP52	ORG	Définir explicitement l'emploi des supports amovibles, notamment : - les supports autorisés ; - le personnel autorisé à les utiliser ; - les procédures de gestion et de contrôles ; - les utilisations légitimes.	O				
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				
EXP54	ORG	Avant toute connexion sur le système industriel, contrôler l'innocuité du contenu du support et « décontaminer » les supports amovibles sur une station blanche.	O				
EXP55	ORG	En cas d'échange de données à partir d'un support amovible non dédié vers le système industriel, transférer les données depuis une station blanche vers un support dédié au système industriel après avoir effectué un contrôle d'innocuité.	O				
Maîtriser l'usage des équipements mobiles							
EXP56	ORG	Faire prendre en compte les équipements mobiles (supports amovibles, poste de maintenance, nomadisme, etc.).	O				
EXP57	ORG	Identifier les équipements mobiles nécessaires au système industriel et limiter leur usage au strict nécessaire.	O				
EXP58	ORG	Définir l'emploi des équipements mobiles autorisés à se connecter sur le système en s'assurant de leur traçabilité.	O				

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
EXP59	ORG	Dédier les équipements mobiles autorisés à se connecter sur le système industriel, y compris ceux utilisés par des prestataires extérieurs.		R	O	O	
EXP60	ORG	Proscrire la connexion ou le raccordement d'équipements personnels sur le système industriel.	O				
EXP61	TECH	Faire signer par le fournisseur les éléments dont l'intégrité et l'authenticité doivent être vérifiées (équipementier, développeur, intégrateur, etc.). La signature doit être vérifiée par l'entité responsable à la réception et par l'équipement au chargement. Le fournisseur doit 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.		C	R	O	
Maîtriser la maintenance							
MAINT1	ORG	Mettre en place une procédure de gestion des interventions afin de pouvoir les tracer en identifiant : - 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. Ces informations sont enregistrées dans un registre d'accès qui peut être sous forme numérique.	O				Pour certaines emprises, certaines de ces informations seront déjà enregistrées via les procédures inhérentes aux sites. Les entités déclineront ces règles en fonction de leurs spécificités et procédures afin d'éviter des redondances inutiles.
MAINT2	ORG	Définir les modalités des interventions, en particulier le processus d'autorisation, et les faire valider par le RSSI.		R	O	O	
MAINT3	ORG	Interdire l'utilisation d'outils particuliers hors d'un cadre prévu par les politiques de sécurité mises en place.	O				
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		R	O	O	

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
		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.					
MAINT5	ORG	Contrôler le processus d'intervention avant d'homologuer ou de ré-homologuer le système industriel.	O				
MAINT6	ORG	Assurer la protection du système industriel et des données sensibles en respectant les exigences minimales suivantes : - cloisonnement* des informations ; - habilitation des entreprises responsables de l'exécution des prestations ; - habilitation et qualification des intervenants ; - surveillance de l'intervention et contrôle des travaux réalisés.	O				
Maîtriser la télémaintenance							
MAINT7	ORG	Insérer dans le périmètre d'homologation les fonctions de télégestion*, de télémaintenance* ou de télédiagnostic*.	O				
MAINT8	TECH	Insérer les dispositifs de télégestion*, de télémaintenance* ou de télédiagnostic* dans une ou des zones de sécurité spécifiques.	O				
MAINT9	ORG	Vérifier les exigences d'habilitation (au sens métier et de la protection du secret de la défense nationale) des intervenants et des entreprises responsables de l'exécution des prestations (télégestion*, télémaintenance* ou télédiagnostic*) et des personnels effectuant les prestations.	O				
MAINT10	TECH	Limiter les prestations (télégestion*, télémaintenance* ou télédiagnostic*) au strict nécessaire et pendant une durée limitée.	O				
MAINT11	TECH	Activer la liaison de télémaintenance* autant que de besoin sous la responsabilité d'un administrateur du système industriel. La liaison ne doit pas être permanente.	O				
MAINT12	TECH	En cas d'opérations de télégestion*, télémaintenance* ou télédiagnostic*, appliquer les règles suivantes :	O				

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
		- les modalités de l'intervention (motif, durée, fichiers modifiés, procédure de tests, procédure de restauration) doivent être définies et autorisées ; - les connexions doivent être réalisées à la demande de l'entité responsable ; - le télémainteneur doit utiliser un ID de connexion nominatif, non générique ; - l'équipement de connexion distant et l'administrateur distant doivent être authentifiés ; - le mot de passe de connexion doit être changé régulièrement ; - la journalisation des événements de sécurité doit être activée ; - après un délai précis d'inactivité, la connexion doit être fermée ; - l'équipement doit être cloisonné du reste du système industriel et seuls les flux indispensables pour l'opération doivent être autorisés entre l'équipement et le reste du système industriel ; - les opérations de télémaintenance* ne doivent être réalisées qu'à l'aide de protocoles sécurisés, assurant notamment l'intégrité, la confidentialité et l'authenticité des échanges.					
MAINT1 3	TECH	Mettre en œuvre une authentification forte à deux facteurs pour opérer la télémaintenance*.		R	O	O	
MAINT1 4	ORG	Dans le cas d'une connexion par modem n'offrant pas de système d'authentification satisfaisant, utiliser un système de rappel (<i>call-back</i>) pour valider le numéro de téléphone appelant.		R	O	O	
MAINT1 5	TECH	Utiliser pour la télémaintenance* un équipement de connexion labellisé.		C	R	O	
MAINT1 6	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				
MAINT1 7	TECH	Déployer une sonde de détection au niveau de la passerelle de connexion pour pouvoir analyser l'ensemble du trafic entrant et sortant.		C	R	O	
MAINT1 8	TECH	Si des opérations de télémaintenance* sont impérativement nécessaires, les équipements distants et la liaison doivent être intégrés dans le périmètre et être		C	R	O	

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
		inclus dans une zone de classe 3. L'ensemble des mesures de classe 3 doivent leur être appliquées.					
MAINT1 9	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.		N A	C	O	
MAINT2 0	ORGT ECH	En cas d'opérations de télégestion*, télémaintenance* ou télédiagnostic*, contrôler les travaux réalisés.	O				
MAINT2 1	TECH	Dans le cas d'un système industriel classifié ou portant une mention spécifique (Spécial France, Diffusion Restreinte), utiliser une passerelle homologuée pour réaliser des actions de télémaintenance*, de télégestion* ou de télédiagnostic*.	O				
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
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				
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				
MCS4	ORG	Mettre à jour les informations insérées dans l'outil ministériel de patrimoine applicatif (ou de l'outil de suivi de l'AQSSI).	O				

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
MCS5	ORG	Définir un processus (responsabilité, fréquence, ...) garantissant le maintien dans le temps de la cartographie du système, en particulier après des actions de maintenance et d'évolution. Le maintenir et le contrôler avant de ré-homologuer le système industriel.	O				
MCS6	ORG	Mettre à jour la cartographie du système industriel à chaque évolution du système et avant le renouvellement d'homologation.	O				
MCS7	ORG	Définir la liste de la documentation relative au système industriel.	R				
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				
Garantir les compétences							
MCS9	ORG	Identifier les compétences critiques à détenir.	O				
MCS10	ORG	Mettre en place un processus de gestion des compétences afin de s'assurer que les intervenants disposent des compétences nécessaires pour leurs missions. Ce processus devrait en particulier intégrer le transfert de compétences, en cas de départ ou de changement de poste, des personnes en charge du système.	O				
Maîtriser la configuration et son évolution							
MCS11	ORG	Suivre les configurations des serveurs, des équipements réseaux et des équipements. Ce suivi est mis à disposition du RSSI-A.	O				
MCS12	TECH	Contrôler les différences entre la version courante et la version à installer et s'assurer que seules les modifications nécessaires et demandées ont été appliquées.		C	R	O	

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
MCS13	ORG TECH	Tracer les mises à jour et modifications apportées au système industriel.	O				
MCS14	ORG	Avant mise en production, valider les impacts des modifications par le RSSI et l'autorité d'emploi ou bénéficiaire.		R	O	O	
MCS15	ORG	Mettre en place un processus de vérification des versions de programme en cours d'exécution par rapport à une version de référence.		C	R	O	
MCS16	TECH	Faire évaluer et valider les modifications ou évolutions dans un environnement de test préalable avant leur déploiement.		C	R	O	
MCS17	ORG	Mettre en place un processus de test pour évaluer les impacts de toute modification, notamment de l'application de correctifs de sécurité.		C	R	O	
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.		C	R	O	
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.		R	O	O	
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.		C	R	O	

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
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.).		R	O	O	Voir Directive 47 portant sur le MCS
MCS23	ORG TECH	Vérifier et valider les correctifs de sécurité avant leur déploiement.		R	O	O	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.).
MCS23	ORG	Mettre en place un suivi des déploiements des correctifs.	O				
Maîtriser l'obsolescence							
MCS24	ORG	Intégrer dans les contrats avec les fournisseurs des clauses relatives à la gestion de l'obsolescence.	O				Par exemple, indiquer la date à laquelle les équipements ne seront plus pris en charge.
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.	O				

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
MCS26	ORG	Mettre en place un plan de gestion de l'obsolescence pour remplacer les équipements et applications obsolètes.	O				
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				
MCS28	ORG	Recenser l'ensemble des équipements matériels et logiciels dans la gestion du parc afin qu'ils soient bien identifiés et maintenus à jour.	O				
Assurer la continuité de l'activité et sa reprise							
CONT1	ORG	Mettre en place un plan de sauvegarde et de restauration des données sensibles afin de permettre leur restauration en cas d'incident et en fonction du besoin de disponibilité. Il précise les moyens utilisés, les modalités et les fréquences de mises en œuvre des sauvegardes, des tests, et des restaurations ainsi que le nombre de sauvegardes à conserver. Il doit être adapté aux événements et sinistres redoutés.		R	O	O	
CONT2	TECH	Sauvegarder les configurations <i>a minima</i> avant et après toutes modifications. Les configurations sont sauvegardées hors du système industriel.		R	O	O	
CONT3	ORG	Tester régulièrement le processus de sauvegarde et de restauration des données et des configurations <i>a minima</i> avant toute évolution ou modification majeure. Le processus pourrait être testé sur un échantillon limité mais représentatif du système industriel dans son ensemble.		R	O	O	
CONT4	ORG	Mettre en place un plan de reprise et de continuité d'activité lié au fonctionnement du procédé industriel*.		C	R	O	Selon le besoin de disponibilité du SI.
CONT5	TECH	Intégrer des modes dégradés du système industriel, leur permettant soit de s'arrêter sans provoquer de dégâts, matériels ou humains, soit de continuer à fonctionner par un pilotage en mode manuel. Les modes dégradés ne doivent pas s'appuyer sur des dispositifs numériques.		C	R	O	Selon le besoin de disponibilité du SI.

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
CONT6	ORG	Intégrer dans les plans de reprise et de continuité d'activité les cyberattaques et tout incident remettant en cause l'intégrité du système industriel (infection virale par exemple).		C	R	O	
CONT7	ORG	Tester le plan de reprise et de continuité d'activité selon une fréquence adaptée aux besoins de disponibilité. La fréquence est définie dans les procédures d'exploitation de sécurité (PES).	O				
CONT8	ORG	Archiver les outils numériques et données nécessaires à une réinstallation. Ces archives doivent bénéficier d'une protection en intégrité, disponibilité et confidentialité.	O				
CONT9	ORG	Intégrer dans les procédures d'intervention un mode d'urgence (« procédure bris de glace ») pour pouvoir intervenir rapidement en cas de besoin sans dégrader significativement le niveau de cybersécurité du système industriel. En particulier, cette procédure d'urgence ne devrait pas affecter la traçabilité des interventions.		R	O	O	
CONT10	ORG	Insérer dans l'analyse de risques les fonctionnalités liées aux modes d'urgence initialement prévus dans le projet ou les réglementations.		R	R	O	
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.		C	R	O	
INC2	ORG	Utiliser des moyens de détection labellisés.		C	R	O	

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
INC3	TECH	Mettre en place une solution de SIEM ainsi que les ressources (RH, matérielles, etc.) pour garantir son efficience.		D	C	R	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).
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.		C	R	O	Voir Doctrines de détection pour les systèmes industriels , ANSSI, 3 décembre 2020.
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				
INC6	ORG	Adapter la procédure d'alerte au système industriel et à son organisation. Les autorités d'emploi et bénéficiaires y sont intégrés. Ils sont informés des incidents avérés et de leurs conséquences sur leurs activités et les systèmes auxquels il concourt.		C	R	O	
INC7	ORG TECH	Un incident donne lieu à une analyse dont le but est de déterminer l'origine de l'incident et d'améliorer la cybersécurité du système industriel.		C	R	O	
INC8	ORG	Le processus de gestion de crise doit également contenir une procédure d'escalade pour gérer les incidents au bon niveau de responsabilité et décider en conséquence : - s'il faut déclencher un plan de reprise d'activité ; - si une action judiciaire est nécessaire.		C	R	O	
Contrôler l'état de sécurité du système							
CTRL1	ORG	En cas d'audit, les tests doivent être réalisés dans le cadre de la maintenance ou avant la mise en production du système industriel, voire sur une plateforme de test s'ils présentent des risques de dysfonctionnement.	O				Les audits peuvent comprendre - des tests aux limites ; - des tests d'erreur des fonctions métier

N°	Nature	Intitulé	SI	C1	C2	C3	Remarque
							; - des tests de la vérification et de la gestion des exceptions ; - le déroulement de scénarios de menace (tests de pénétration et tentatives de prise de contrôle) ; - la vérification des mécanismes de sécurité (déploiement de correctifs ; - analyse de journaux d'événements ; - restauration de sauvegarde.
CTRL2	ORG	Réaliser un contrôle de conformité avant toute homologation ou renouvellement d'homologation.	O				
CTRL3	ORG	En cas d'externalisation, la prestation d'audit est réalisée par des prestataires externes labellisés.	O				Un contrôle de conformité est inclus dans l'audit d'homologation.