< NOTE MCS (Maintien en Condition de Sécurité) >

Groupe d’échange – Transports Collectifs Ferroviaires et Urbains

CAMPUS CYBER

< SOMMAIRE >

Table des matières

< INTRODUCTION >

Objectif du document

Le Maintien en Condition de Sécurité (MCS) constitue une activité primordiale pour la phase opération et maintenance, du fait de la durée de vie des systèmes du secteur ferroviaire.

Cette activité nécessite d'être précisée compte-tenu :

- de standards et règlementations souvent trop génériques,
- du manque d'alignement entre les acteurs du secteur,
- et de la difficulté à combiner MCS et sûreté de fonctionnement.

L'objectif de ce document est de définir les principes et la mise en œuvre du MCS afin de servir de socle harmonisé à utiliser/décliner dans le cadre de la contractualisation de chaque marché de prestation de MCS. Ce document spécifie et cadre les activités et livrables associés, définit des modèles types (activités, responsabilités, niveaux de service) qui puissent être utilisés dans le cadre des marchés et contrats entre les différents acteurs (fournisseur produit, intégrateur système, opérateur/exploitant et mainteneur).

Il est le fruit d'un travail réalisé par le Groupe d'Echange Transports Collectifs Ferroviaires et Urbains (GE TCFU), composé des acteurs suivants :

- Les opérateurs de transports : Keolis, RATP, RATPDev, SNCF, Transdev
- Les industriels : Alstom, Compagnie des Signaux, Hitachi, Siemens

Définition

Le Maintien en Condition de Sécurité (MCS) reprend l'ensemble des mesures organisationnelles et techniques concourant à maintenir le niveau de cybersécurité tout au long du cycle de vie d'un système.

Notamment, il s'appuie sur :

- Une maîtrise de l'inventaire et de la cartographie (technique, physique) des composants matériels et logiciels ; et des processus organisationnels afférents.
- Une veille des vulnérabilités sur ceux-ci.
- Un traitement de celles-ci via des corrections ou des mesures de mitigation/compensation (techniques ou organisationnelles) permettant de maintenir le niveau de cybersécurité dans le temps.

Le MCS doit être anticipé en phase de conception afin de pouvoir être effectif à la date de mise en service du système.

Cadre Réglementaire

Le cadre réglementaire se renforce progressivement sur cette thématique.

Pour ne citer qu'eux, les sujets de veille de vulnérabilités et de traitement/correctif sont repris dans :

- Le décret « LPM » du Code de la Défense paru en Août 2016 :

Annexe 1/Règle 4 (https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033063035)

- La Directive NIS2 parue en décembre 2022 : (https://eur-lex.europa.eu/eli/dir/2022/2555)
- Le guide d'application explicitant les exigences relatives à la Cybersécurité dans le cadre du décret n°2021-873 du 29 juin 2021 concernant la circulation d'un véhicule à délégation de conduite et à ses conditions d'utilisation (décret « STRA ») :

(https://www.strmtg.developpement-durable.gouv.fr/guide-d-application-relatif-a-la-cybersecurite-a807.html)

- Le Règlement européen « Cyber Resilience Act » entré en vigueur en Décembre 2024 :

(https://eur-lex.europa.eu/eli/reg/2024/2847)

Cadre normatif

Le cadre normatif de cybersécurité dans le domaine ferroviaire et routier se renforce également.

- S'agissant du ferroviaire :

La TS 50701 est parue en 2020 puis 2023 au niveau européen (CENELEC). Le chapitre « Operational, maintenance and disposal requirements » introduit cette thématique.
Les travaux se poursuivent actuellement au niveau international (IEC) dans le cadre du Project Team 63452. Une deuxième version Committee Draft for Vote soumise en 2025 aux comités nationaux développe cette thématique dans un chapitre « Operational, maintenance and disposal requirements » enrichi. La version finale IEC 63452 est prévue pour début 2026.
Ces deux textes (TS 50701 / IEC 63452) sont une déclinaison de l'IEC 62443 (standard transverse de cybersécurité industrielle) appliquée au domaine ferroviaire.

- S'agissant du transport routier :

La ISO21434 (https://www.iso.org/fr/standard/70918.html) décrit les exigences concernant les véhicules routiers.

Acteurs

Les acteurs définis sont :

- Fournisseur Produit (FP) : fabricant de matériel, éditeur de logiciel.
- Intégrateur Système (IS) : prestataire de service d'intégration d'une solution ferroviaire[1], comprenant les activités de spécification, conception, implémentation, validation et la préparation de mise en service.
- Opérateur (exploitant) (O) : organisation en charge d'opérer une application ferroviaire[2], dans le cadre de cette note, elle est aussi l'organisation gestionnaire d'actif de cette application.

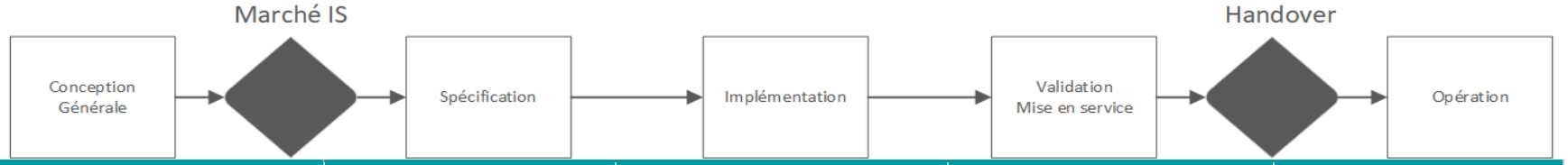
[1] *Solution ferroviaire : ensemble de systèmes de contrôle et de composants matériels et logiciels installés et configurés pour fonctionner dans une application ferroviaire.*

- Mainteneur (M): le mainteneur peut être l'opérateur ou un tiers sous contrat ; dans le cadre du MCS, le mainteneur agit uniquement pour la phase de déploiement de mitigation/correctif.

Le tableau ci-dessous décrit le cycle de vie de projet pour une solution ferroviaire d'un point de vue cybersécurité avec une description sommaire des activités pour chaque acteur.

[2] *Application ferroviaire : ensemble des personnels, matériels, logiciels, procédures et politiques impliqués dans l'exploitation du service ferroviaire et susceptibles d'affecter ou d'influencer son fonctionnement sûr, sécurisé et fiable.*

Ainsi, le système technique solution ferroviaire délivré par l'intégrateur système au moment du handover constitue le système technique de l'application ferroviaire mise en opération dans l'organisation de l'opérateur



	Conception générale	Spécification	Implémentation	Validation Mise en service	Exploitation
Activité Opérateur / Maitrise d'ouvrage	Initie l'analyse de risques Définit les exigences fonctionnelles de cybersécurité	Confirme la liste des CCA	Anticipe les organisations liées aux mesures de MCS en validant leur opérationnalité	Valide les procédures organisationnelles Approuve le Handover et met en service la solution	Décide des déploiements liés au MCS Maintien de l'analyse de risques
Activité IS	Répond à l'appel d'offre avec une liste préliminaire des CCA	Définit les exigences opérationnelles Conçoit la solution Affine la liste des CCA	Implémente les mesures de sécurité	Vérifie les mesures de sécurité Prépare le Handover	Réalise les activités MCS (veille, analyse et propositions) conformément au RACI et au contrat
Activité FP	N/A	Fournit la capacité de sécurité des produits	Fournit les mises à jour des produits	N/A	Réalise les activités MCS (veille, analyse et propositions) conformément au RACI et au contrat
Activités liées au MCS	Vérification conjointe O/IS de la capacité de traiter du MCS et des CCA Initialisation de la stratégie de MCS Contractualisation (au plus tôt) du MCS	Validation conjointe O/IS de la capacité de traiter du MCS et des CCA	Finalisation de la stratégie de MCS	Vérification de la couverture test Contractualisation (au plus tard) du MCS	Exécution du contrat MCS

Tableau 1 : Cycle de vie de projet pour une solution ferroviaire d'un point de vue cybersécurité

Afin de maitriser au mieux et au plus tôt le coût de possession du système, la contractualisation du MCS devrait être réalisée dès la phase d'appel d'offre.

Dans le cas où des évolutions majeures ou un manque de maturité venaient à remettre en cause les hypothèses de la contractualisation initiale, ce point serait à adresser par le management du projet.

Dans tous les cas, la contractualisation du MCS doit être réalisée au plus tard à la mise en service.

< PREALABLE A LA CONTRACTUALISATION >

Strategie de MCS et Cyber critical assets

Une Stratégie de MCS (Maintien en Conditions de Sécurité) doit être établie pour un système ou un ensemble de systèmes.
La Stratégie de MCS a pour but d'établir les :

- Activités réalisées dans le cadre du MCS (étapes ; livrables ; organisations ; comitologie ; …).
- Modalités (périmètre ; critères ; prévenance ; temporalité) des activités de veille.
- Modalités (périmètre ; critères ; prévenance ; temporalité) des activités de traitements (mitigation / correction ; stratégie de validation et moyens de tests).

La Stratégie de MCS est à établir en version initiale et doit être finalisée au plus tard à la mise en service ; ceci permettant d'encadrer un éventuel contrat de maintenance.

La Stratégie de MCS peut évoluer dans le temps, notamment en cas d'évolution du système, de sa capacité, des opportunités et disponibilités de MCS, des modalités de sa maintenance ou de l'organisation mise en place, de la menace ; et donc plus globalement en cas d'évolution des risques SSI pesant sur lui. Les activités du MCS sont définies dans les chapitres ultérieurs de la présente note.

Concernant les activités de veille, plusieurs critères peuvent être pris en compte dont le score de vulnérabilité (CVSS), l'exploitabilité (EPSS, KEV), l'évolution de la menace (threat landscape, ISAC). Les informations pour les activités de veille peuvent être mises à disposition par les éditeurs, fabricants et industriels, voire récupérées au travers de CERT par l'opérateur. Les vulnérabilités de niveau composant demandent à être contextualisées au niveau système en prenant en compte l'architecture et les mesures de sécurité en place. Les hypothèses de contextualisation sont à préciser dans la Stratégie de MCS. L'évolution de la menace est une composante à prendre en compte pour cette contextualisation en s'appuyant, via l'opérateur, sur les éléments de threat intelligence qu'il mesure de manière continue pour son environnement et son écosystème, au travers des sources multiples que peuvent être les agences de cybersécurité, les groupes sectoriels, le partage d'informations, …

Concernant les activités de traitements, la décision de déployer ou non une mesure de mitigation et/ou un correctif appartient à l'opérateur. Des méthodologies d'aide à la décision peuvent être définies (par exemple SSVC).

Cette décision est prise sur la base de la stratégie de remédiation des systèmes exploités par l'opérateur, à partir des éléments issus des activités de veille. Afin de rendre possible et pragmatique le traitement du MCS sur des systèmes complexes tels que les systèmes ferroviaires, une approche CCA (Cyber Critical Asset) est fortement recommandée.

Les CCA (Cyber Critical Asset) sont des composants choisis du système qui doivent faire

prioritairement l'objet d'une veille et de plans de traitement cyber. Cette liste de CCA devrait notamment contenir à minima :

- Les composants les plus exposés (ex : équipements sans-fil type MCG ou Access Point Wi-Fi, équipements disposant de connecteurs facilement accessibles depuis une zone publique, …),
- Les composants assurant des fonctionnalités cybersécurité au sein de l'architecture (ex : secure-gateway portant des fonctionnalités de type filtrage ou shared-cybersecurity-services, équipements réseaux, barrières de sécurité, …),
- Les composants permettant d'accroitre la protection physique et apportant un bénéfice cybersécurité élevé (ex : lecteur de badge protégeant l'accès à une zone technique).

Cette liste devra être complétée et confirmée par les travaux d'Analyse de Risques SSI et validée conjointement par les parties. Ce choix des CCA doit permettre de maintenir sur l'ensemble du système un niveau de sécurité acceptable en concentrant les traitements sur ces composants, permettant d'exclure d'autres composants des activités de traitement et/ou de réduire la liste des composants de l'activité de veille.

Afin de pouvoir maintenir une activité de MCS dans le temps, l'obsolescence des logiciels doit être suivie pour gérer de manière proactive le fait qu'un logiciel deviendra obsolète dans un avenir défini (gestion de la fin de support / fin de vie).

Si un logiciel devient impossible à mettre à jour (du fait que le matériel n'est plus compatible), en cas d'intention de maintenir dans des conditions sécurisées un produit, une mise à jour technologique du matériel peut être nécessaire et doit être anticipée.

Si une décision unilatérale d'un acteur de la chaine de MCS, notamment au niveau produit, impacte la capacité à répondre à la stratégie définie au niveau système (par exemple interruption inopinée du support, décision de détendre le cycle de mise à jour, …), la stratégie de MCS, et par extension le contrat de maintenance associé, pourront nécessiter d'être amendés.

Une évolution de la Stratégie de MCS peut entrainer une évolution du contrat.

Hypothèses et contexte de mise en oeuvre

Cette section décrit les hypothèses d'exécution du contrat de Maintien en Condition de Sécurité entre les acteurs impliqués, notamment fournisseur de produit (product supplier), intégrateur système (system integrator), opérateur (operator).

Le niveau de service pourra être adapté selon le projet ; et notamment des activités pourront être contractualisées au forfait ou au devis. Voir le §4.1 pour plus de détails.

Périmètre du contrat

1.1.1 Périmètre

Le périmètre du contrat doit définir les éléments concernés par tout ou partie des activités du chapitre 3.

Dans le cadre d'une proposition préliminaire, l'approche CCA permet une projection contractuelle. La confirmation du scope de surveillance et/ou de traitement, appuyée par l'analyse de risques du projet, permet de définir le périmètre précis du contrat de MCS à finaliser avant la mise en service.

2.1.1 Recouvrement contractuel

Deux types de recouvrements peuvent exister :

1. Plusieurs contrats de MCS pour un système donné (plusieurs intégrateurs/mainteneurs concernés).
2. Garantie du contrat initial et contrat de MCO/MCS.

Pour le point 1, les points de vigilance essentiels sont sur les périmètres de responsabilités et la gestion des interfaces (ex. tunnel IPsec vulnérable entre deux sous-systèmes faisant l'objet de deux contrats MCS différents).
Pour le point 2, les points de vigilance essentiels reposent sur les conditions d'exécution des contrats et les recouvrements éventuels :

- Les conditions de mise en œuvre de la garantie et du MCS sont portées par chacun des contrats respectifs en s'assurant de leur compatibilité respective (Ex : SLA, durée de réactivité, …).
    - Une mise à jour MCS n'a pas d'impact sur la durée ou l'exécution du contrat de garantie.
    - Une mise à jour MCS ne constitue pas une clause de limitation ou d'arrêt de garantie.
- Une mise à jour fonctionnelle sous garantie peut s'accompagner d'une mise à jour MCS.

Engagement

3.1.1 Durée d'engagement

Le contrat doit prévoir une durée d'engagement.

4.1.1 Divulgation des vulnérabilités

La divulgation des vulnérabilités entre les parties prenantes doit être définie dans le contrat et respecter à minima les obligations règlementaires (ex : vulnérabilités exploitables connues au titre du CRA).

Dans le cas de source publique (Renseignements d'Origine Sources Ouvertes -ROSO-, ou en anglais Open Source Intelligence -OSINT-) , l'ensemble des renseignements sont disponibles et accessibles à toutes les parties prenantes du contrat MCS.

Au-delà des communications de vulnérabilités en source ouverte, il peut y avoir certaines vulnérabilités dont le fournisseur a connaissance, mais qu'il ne souhaite communiquer qu'à une communauté limitée, on parlera dans ce cas de sources discrètes (ex : incident survenu sur système similaire, résultat de pentests…).
Le choix de communiquer ou non est à la discrétion du fournisseur ; néanmoins, ce choix doit faire l'objet d'un processus formel, partagé avec le client ; notamment car la visibilité sur les sources discrètes est importante pour la décision de contre-mesures par l'Opérateur.

Ces informations ayant un niveau de sensibilité élevé, le contrat devra définir le principe de manipulation de l'information, ainsi que le public habilité (SOC , CERT, …).

Ces sources discrètes feront l'objet d'un accord de confidentialité sur la durée du contrat.

5.1.1 Gestion des modifications

La gestion des modifications dans le cadre du MCS est à considérer comme toute gestion du changement appliquée au système considéré. Aussi, la gestion de configurations, la documentation, … doivent suivre les processus de gestion du changement en place sur le système dans le cadre de l'application du contrat de MCS.

6.1.1 Périmètre et gestion du matériel obsolète

Les hypothèses de Stratégie de MCS, de liste des composants éligibles à l'activité de veille et/ou de traitement doivent être précisées dans les éléments contractuels.

Si des équipements doivent être remplacés de manière iso-fonctionnelle dans le cadre de l'application du contrat de MCS, ces nécessités de mise à jour technologique doivent être précisées dans les éléments contractuels au travers d'hypothèses chiffrées (fréquence, contenu, testabilité, interopérabilité avec le système existant).

Ces hypothèses doivent s'enrichir du retour d'expérience des MCS d'autres systèmes ou d'incidents récents dans le but d'établir une correcte appréciation des coûts associés.

7.1.1 Stratégie de gestion des correctifs de sécurité

Les hypothèses concernant notamment l'homologation de sécurité, la sûreté de fonctionnement, l'interopérabilité et l'intégration / déploiement doivent être prises en compte dans le contrat.

Au niveau produit, la gestion des correctifs de sécurité devrait être optimisée en cohérence avec les baselines produits.

Au niveau système, la gestion des correctifs de sécurité relevant du MCS devrait être optimisée en cohérence avec les évolutions fonctionnelles, éventuellement prévues par ailleurs (optimisation des développements, des validations, des démonstrations, et des déploiements).

Moyens de test et validation

La bonne mise en œuvre du MCS pourra être très dépendante des moyens de tests et validation disponibles. Ces moyens de tests / bancs de tests peuvent servir à l'analyse des vulnérabilités, la validation des mitigations ou correctifs, démonstration d'absence d'impacts fonctionnels, …

Ils peuvent :

- exister au niveau produit, sous-système, système,
- exister chez un fournisseur, système intégrateur, opérateur, mainteneur,
- être maintenus dans le cadre d'un contrat différent du contrat de MCS.

Pour construire la Stratégie de MCS, il faut prendre en compte l'existence et le maintien (dans une durée adéquate et avec une représentativité compatible) de ces capacités de tests et validation existantes.

La Stratégie de MCS peut conduire à une modification dans la stratégie de conservation des bancs de tests existants ou à la création / adaptation de bancs nécessaires au MCS. La mise à disposition de plateformes hors production dont l'architecture, les cas d'usages et la charge simulés doivent bénéficier de la représentativité nécessaire aux tests.

La stratégie de validation des correctifs de sécurité doit identifier le niveau de couverture cible des tests permis par des moyens de tests / capacités de validation (Ex : fonction, robustesse, performance, maintenabilité, sécurité, rendement, fiablité, …) en adéquation avec le périmètre des modifications envisageables.

< ACTIVITES MCS >

Les activités présentées dans ce paragraphe peuvent s'entendre pour le traitement individuel d'une vulnérabilité. Toutefois il est évident que pour des raisons d'efficacités opérationnelles et économiques, les activités de veille de vulnérabilités et de traitements associés sont à envisager en traitements par lots/packages/versions, notamment s'agissant des livraisons intermédiaires entre acteurs.

Les paragraphes suivants ont vocation à :

- 3.1 : identifier le chemin décisionnel correctif/mitigation/contrôle.
- 3.2 : présenter la succession macroscopique des travaux des acteurs impliqués dans la démarche.
- 3.3 : présenter en détail la liste des activités à mener.

Les différentes activités identifiées dans ces 3 paragraphes se recoupent de manière cohérente mais ne présentent pas le même niveau de détail.

Vue graphique et décisionnelle

Le schéma ci-dessous n'attribue pas la responsabilité des tâches, mais identifie les tâches à accomplir et ne dépend pas des personnes qui les accomplissent, cela dépendant de l'organisation du projet.

Le processus est déclenché par la divulgation d'une vulnérabilité concernant un bien qui doit être maintenu en condition de sécurité.
La divulgation des vulnérabilités peut provenir de bases de données publiques (ex : NVD), d'informations fournisseurs, du partage d'informations par la communauté (ex : ISAC), par des tiers de confiance (ex : CERT, CSIRT), de rapports de tests (ex : pentests, scan de vulnérabilités aux interfaces), de rapports d'incidents et de partage d'informations internes.

Une vérification initiale doit écarter les éléments qui ne constituent pas une vulnérabilité (ex : mauvaise attribution de la vulnérabilité qui n'affecterait finalement aucun bien dans le champ de l'analyse, vulnérabilité déjà signalée auparavant et déjà traitée ou remédiée, …). Cette analyse peut conduire à quitter le processus.

Les données d'entrée pertinentes pour l'analyse de la vulnérabilité sont, entre autres, le rapport ou l'avis de vulnérabilité, l'inventaire des actifs, la Stratégie de MCS et la liste des CCA, l'analyse des risques de l'application, le CyberSecurity Case incluant le contexte de cybersécurité et les SecRACs.

Si l'analyse de la vulnérabilité et l'application des critères de priorisation (exemples : impacts cyber importants sur l'architecture, conséquences indirectes sur la sureté de fonctionnement, …) concluent à une gravité très élevée et à un traitement prioritaire, l'application immédiate de contre-mesures peut s'avérer nécessaire.

Les trois principales catégories de contre-mesures sont les suivantes :

- Application d'un correctif
  Si cela est compatible avec la stratégie de MCS et appuyé par une décision de l'opérateur, le déploiement d'un correctif est un moyen de résoudre définitivement une vulnérabilité.

- Mesures de mitigation
  Les mesures de mitigation permettant de réduire ou de supprimer le risque (comme le filtrage, la désactivation de ports, …) peuvent s'avérer tout aussi efficaces ; notamment si un correctif est disponible mais que les conditions de son déploiement ne sont pas acceptables, que le correctif n'est pas compatible ou n'est pas pertinent (techniquement, calendairement, économiquement) ou tout simplement si un correctif n'est pas disponible.

- Mesures de compensation
  Les mesures de compensation permettant de contenir ou de contrôler le risque (comme des activités de surveillance ou de contrôle, …) peuvent également être définies pour maîtriser le risque lié à l'existence d'une vulnérabilité non corrigée ou non mitigée.

Les mesures de mitigations et/ou de compensation peuvent être temporaires (en attente de mieux ou d'un correctif à venir/à déployer dans un temps long) ; ou définitives (si pérennes et suffisantes et/ou plus pertinentes qu'un correctif sur le long terme).

À l'issue du traitement (qu'il s'agisse de correctif, mitigation ou mesure de compensation), la documentation de l'application doit être mise à jour (notamment les évolutions de configurations ou fonctionnelles associées aux correctifs / aux mitigations ; les évolutions de SecRACs associées aux actions de compensation).

Dans le cas extrême où une vulnérabilité ne pourrait être résolue ou suffisamment surveillée, et que l'équipe de sécurité ne pourrait plus appliquer la stratégie de MCS établie, une décision concernant cette vulnérabilité devrait être portée au niveau décisionnel suffisant dans l'organisation (à définir par celle-ci) pour acceptation (temporaire ou non) ou une autre décision, par exemple, l'interruption d'une fonctionnalité.

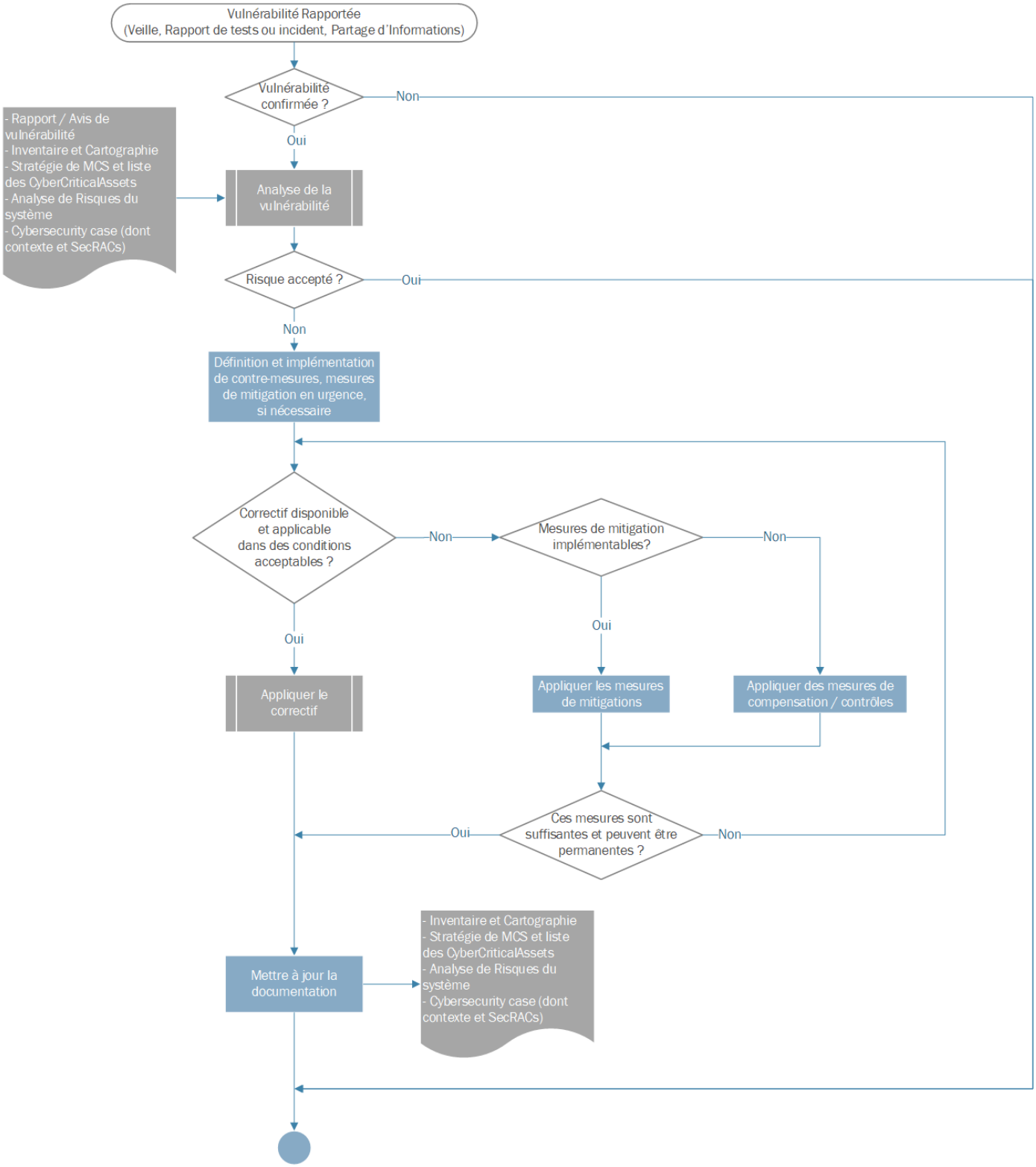


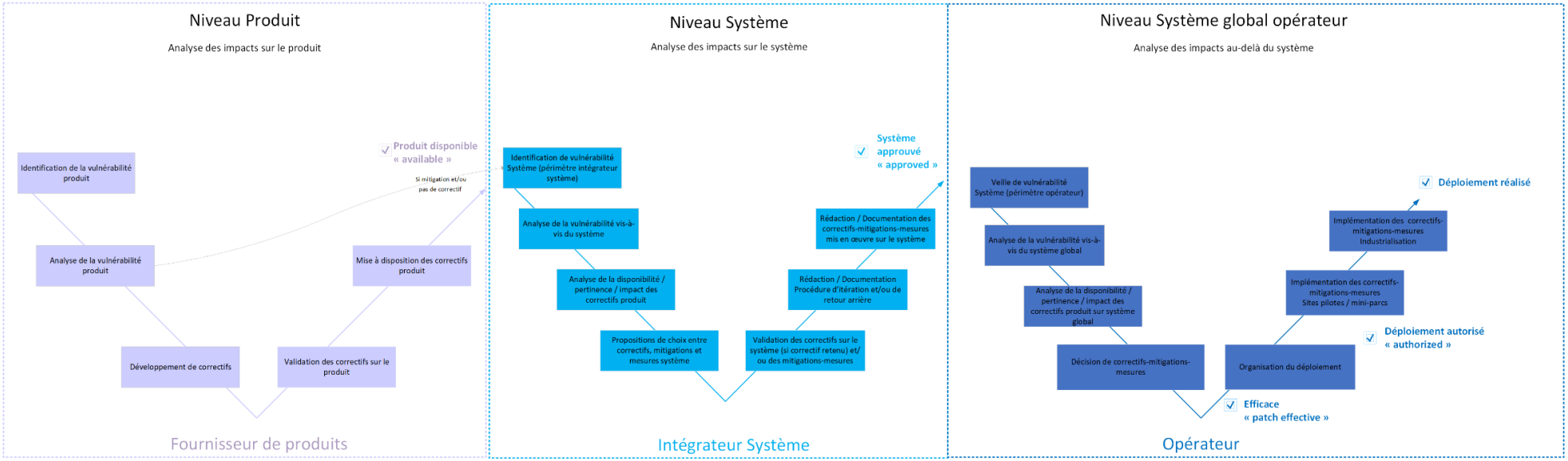
Figure 1 : Vue graphique et décisionnelle

Vue graphique par acteurs

Le schéma ci-dessous a pour vocation de détailler les activités principales type permettant d'aboutir au traitement d'une vulnérabilité au travers d'un correctif ou d'une mitigation ; avec trois acteurs principaux engagés dans le processus :

- Le fournisseur de produit (product supplier) dont le champ d'action se limite au produit non intégré dans une architecture système.
- L'intégrateur système (system integrator) dont le champ d'action concerne l'intégration des éléments « produit » dans l'architecture système.
- L'opérateur (operator) dont le champ d'action concerne la mise en œuvre finale dans le système en production, sur la base des éléments d'entrée du fournisseur de produit et/ou de l'intégrateur système (l'opérateur peut solliciter le mainteneur pour la mise en œuvre du déploiement).

NB : Les activités illustrées ici ne se veulent pas exhaustives (plus de détails disponibles dans le §3.3) et permettent une vision macroscopique des étapes clefs et points de passage entre ces trois acteurs principaux.



N.B. : Les termes entre guillemets sont les équivalents des notions dans la norme IEC 62443.

Figure 2 : Vue graphique par acteurs

Par « **Produit disponible** » :

L'éditeur ou Fournisseur Produit responsable met à disposition une nouvelle version (correctif) officielle reconnue par l'Intégrateur Système.
L'éditeur ou Fournisseur Produit responsable propose des mitigations sur la version existante.

Par « **Système approuvé** » :

L'Intégrateur Système responsable met à disposition une nouvelle version Système (intégrant le correctif ou la mitigation qui modifie le système) officielle reconnue par l'Opérateur du Système global.

Par « **Déploiement réalisé** » :

L'Opérateur met en place une nouvelle version Système (intégrant le correctif ou la mitigation qui modifie le système) officielle mise à disposition par l'Intégrateur Système.

Tableau des activités

Le tableau ci-après a pour vocation de détailler les activités et sous-activités à mener.

Les activités clefs sont :

1. La comitologie et suivi associés à la prestation de MCS
2. La veille de vulnérabilités produit
3. La veille de vulnérabilités système
4. Le développement et validation du correctif produit
5. Le traitement des vulnérabilités (proposition de correctifs-mitigations-mesures, fiche de vulnérabilité complétée)
6. Le traitement des vulnérabilités (validations des correctifs)
7. Le traitement des vulnérabilités (déploiement)
8. La mise à jour de l'analyse de risques

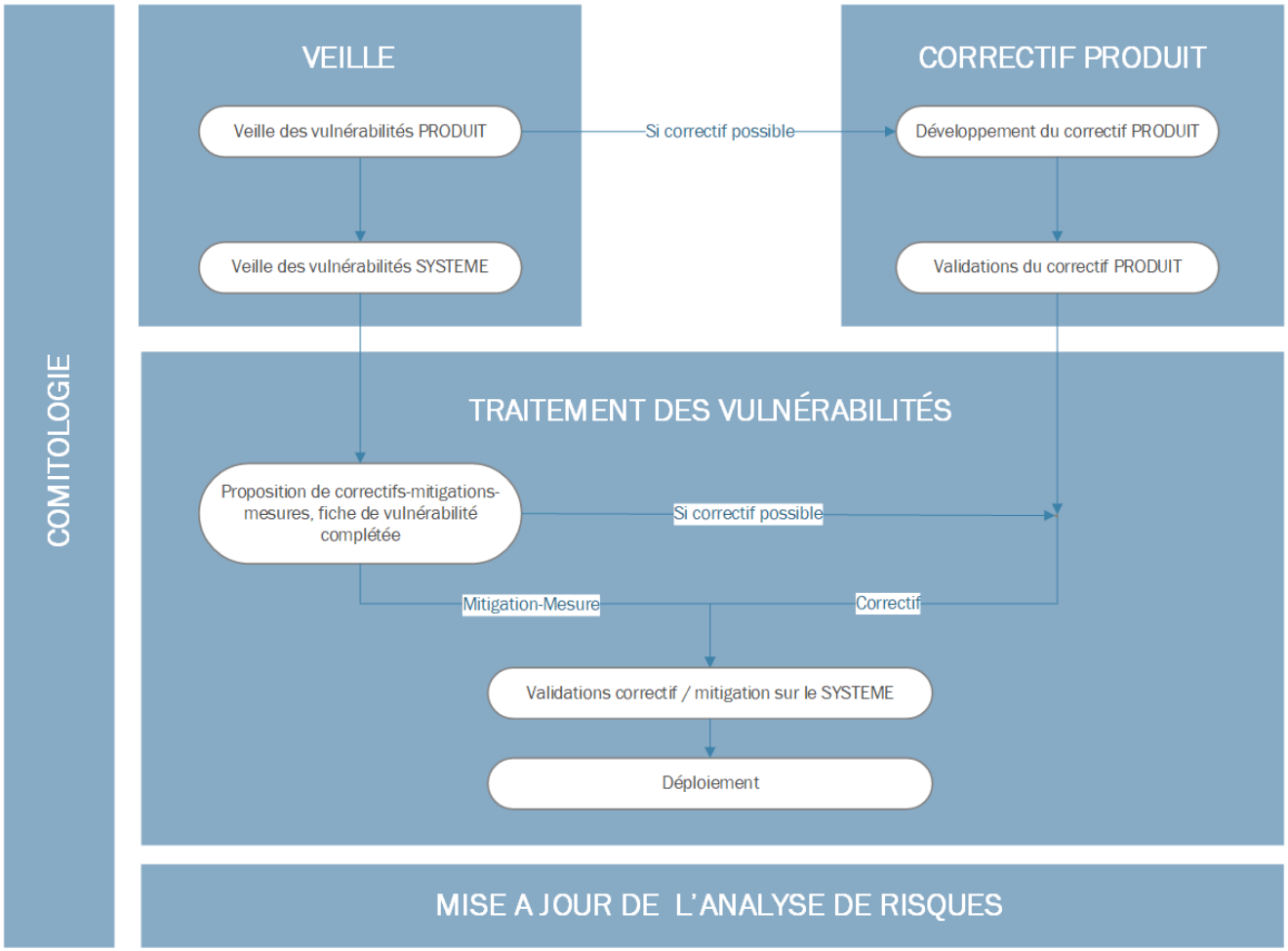


Figure 3 : Vue graphique des activités clefs

NB : Le reste de la documentation impactée (cybersecurity case, documentation technique du produit, du système, …) par un changement lié à une modification MCS doit également être considéré, et est défini par l'analyse d'impact de la modification mais n'est pas détaillé ici.

	Activité		Sous-Activité	Input	Output	Commentaire
1	Comitologie et suivi associés à la prestation de MCS	1.1	**Comité de suivi**	• Liste des vulnérabilités dont nouvelles ou ayant évolué • Bulletin obsolescence et End of life • REX incident	Décisions de traitement	Trimestriel à semestriel
		1.2	**Comité exceptionnel**	• Vulnérabilité très critique • Évolution de périmètre • Incident	Décisions de traitement	Exceptionnel
2	Veille des vulnérabilités produit	2.0	**Inputs préalables**	• Inventaire • Base de vulnérabilités, rapport d'audit, partage d'informations • Critères de traitement et analyses (définis dans la stratégie de MCS)		
		2.1	**Identification / intégration des sources** Identification des sources fiables et intégration dans un outil pour automatisation	• NVD • Service du fournisseur de COTS / OSS • CERTs • Service d'intelligence sur la menace • Incident de sécurité • Rapport d'audit, de pentests	Sources dans la fiche de vulnérabilités	
		2.2	**Analyse des vulnérabilités** Tri des vulnérabilités affectant réellement un produit à l'aide d'un SBOM détaillé, filtrant les librairies non installées / inactives en fonction du durcissement, ou écartant celles qui doivent être filtrées à cause des « security related application conditions »	• SBOM • Durcissement produit • SecRAC du produit	Liste filtrée des vulnérabilités affectant une (ou plusieurs) version(s) du produit	

	Activité		Sous-Activité	Input	Output	Commentaire
		2.3	**Fiche de vulnérabilité** Description de vulnérabilité, de son score de base, de son score revu en fonction des critères de la politique de gestion de vulnérabilité du domaine, exploitabilité, impact	• Sources de vulnérabilités • Méthode de calcul de score pour le domaine (standard, règlementation, politique fournisseur)	Fiche de vulnérabilité complétée Bulletin de sécurité produit (périodique)	Identification des informations sensibles TLP RED nécessaire et diffusion adéquate
3	Veille des vulnérabilités système	3.0		• Inventaire • Base de vulnérabilités, rapport d'audit, partage d'informations • Critères de traitement et analyses • Bulletin de sécurité produit (périodique) • Résultats audits, pentests, etc.	Fiche de vulnérabilité complétée	Fréquence : Inclus dans un bulletin périodique (ensemble des fiches des nouvelles vulnérabilités ou ayant évolué) trimestriel à semestriel
		3.1	**Identification et intégration des produits** Identification des fournisseurs, de leurs engagements de MCS Intégration des différents rapports pour analyse système	• SBOM système • Scope de chaque fournisseur / RACI	Cartographie MCS du système avec les fournisseurs	

	Activité		Sous-Activité	Input	Output	Commentaire
		3.2	**Analyse système** Analyse contextuelle des vulnérabilités de l'ensemble des produits en prenant en compte : • L'architecture, les zones de sécurités (IEC62443) • La stratégie de MCS avec la notion de cyber critical asset • Les parties prenantes et les processus métiers • L'analyse de risques et les scénarios de menaces • L'intelligence sur la menace	• Architecture • Stratégie de MCS • Parties prenantes et processus métiers • Analyse de risques • Intelligence sur la menace	Bulletin de sécurité système	
4	Développement et validation du correctif produit	4.0		• Description de la vulnérabilité • Disponibilité de correctif d'un composant tiers si à l'origine de la vulnérabilité (librairie OSS ou COTS)	Correctif Note de déploiement du correctif et des éventuelles contraintes associées (prérequis, dépendances, méthode de déploiement…) Cas de test démontrant l'efficience du correctif quand c'est possible (par exemple quand l'exploitation de la vulnérabilité est outillée ou quand il s'agit d'une violation d'une règle de codage)	Activité de développement classique de correctif pour défaut

	Activité		Sous-Activité	Input	Output	Commentaire
5	Traitement des vulnérabilités (proposition de correctifs-mitigations-mesures, fiche de vulnérabilité complétée)	5.1	**Réponse immédiate** Lorsque la vulnérabilité le nécessite, des mesures de réponse immédiate peuvent être déclenchées pour limiter au plus tôt les impacts de la vulnérabilité, sans attendre de connaître précisément les correctifs applicables.	• Stratégie de MCS (incluant les inputs opérateurs aux interfaces pour la mise en œuvre de la prestation MCS) • Inventaire, architecture et Analyse de Risques • Vulnérabilité très critique (selon critère défini dans la Stratégie de MCS)	• Réunion immédiate • Décision immédiate	Les critères d'une réponse/réunion immédiates sont notamment des impacts élevés de cybersécurité ou sûreté de fonctionnement.

	Activité		Sous-Activité	Input	Output	Commentaire
		5.2	**Proposition de correctifs-mitigations-mesures** La mise en œuvre de correctifs de sécurité est la solution privilégiée, en priorisant les situations pour lesquelles le niveau de vulnérabilité est élevé, et en recherchant l'optimum coûts/délais des activités de tests et déploiements. À défaut de correctif disponible ou déployable dans des conditions acceptables (ces conditions pouvant être techniques, calendaires, économiques, …), des mitigations temporaires ou définitives doivent être recherchées. Celles-ci peuvent être techniques et/ou organisationnelles ; en prévention, contrôle ou réaction.	• Stratégie de MCS (incluant les inputs opérateurs aux interfaces pour la mise en œuvre de la prestation MCS) • Inventaire, architecture et Analyse de Risques • Vulnérabilité et criticité (selon critère défini dans la Stratégie de MCS) • Disponibilité de correctif	La fiche de vulnérabilité est complétée dès que possible ; de manière itérative ou complète ; des éléments de mitigation et/ou correction possibles : • Solutions de traitement envisagées, soit : ○ Une/des mesure(s) de réponse immédiate, ○ Un/des correctif(s), ○ Une/des mesures(s) de mitigation (en cas d'absence de correctif(s) suffisant(s)), ○ Une/des mesures(s) de compensation (en cas d'absence de palliatif(s) suffisant(s)), • Risques ou vulnérabilités résiduels • Déviation fonctionnelle Les éléments relatifs à l'impact de la vulnérabilité, les solutions de traitement envisagées et les risques ou vulnérabilités résiduels doivent être argumentés, expliqués. Cette fiche de vulnérabilité complétée doit être établie aussi vite que possible ; et dans un délai maximum convenu (par ex un mois).	

	Activité		Sous-Activité	Input	Output	Commentaire
		5.3	**Procédure d'itération et/ou de retour arrière lors de la mise en œuvre** Les propositions doivent être accompagnées d'une stratégie d'implémentation (par exemple implémentation en Y ; nombre d'assets considérés, …) et de retour arrière (capacité à revenir à l'état initial en cas de problème). Ces éléments permettront d'enrichir la décision et l'organisation de la mise en œuvre de(s) mesure(s).	• Fiche de vulnérabilité • Organisation (y compris contraintes opérationnelles de l'opérateur – ex : exploitation HO/HNO …) • Stratégie / Hypothèses de déploiement	• Procédure d'itération et/ou de retour arrière	
		5.4	**Décision de correctifs-mitigations-mesures sur le système** Sur la base des deux points précédents, prise de décision sur la mise en œuvre des mesures / plan d'actions.	• Fiche de vulnérabilité • Procédure d'itération et/ou de retour arrière	• Décision(s) de mise(s) en œuvre / Plan d'actions • Planning(s) de mise(s) en œuvre • Acteur(s) de la mise(s) en œuvre	

	Activité		Sous-Activité	Input	Output	Commentaire
6	Traitement des vulnérabilités (validations des correctifs / mitigations)	6.1	**Validation des correctifs produit / mitigations sur le système** Les correctifs/ mitigations doivent être validés. Cette validation comprend les tests des correctifs / mitigations (et/ou leur intégration), la non-régression fonctionnelle (ou démonstration d'innocuité) ainsi que la maîtrise de la performance du système vis-à-vis de la mise en place des correctifs / mitigations. La fiche de vulnérabilité doit identifier toute déviation (fonctionnelle, régression, limitation…). La procédure de retour arrière doit également être testée.	• Fiche de vulnérabilité • Procédure d'itération et/ou de retour arrière • Banc ou système représentatif ; système de production • Correctif / mitigation	• Validation du correctif / mitigation dans le système ; Cahiers de recette et complétude de la couverture de tests • Démonstration d'innocuité ou de la compatibilité du correctif / mitigation avec le fonctionnel • Procédure d'itération et/ou de retour arrière testée et validée	Le périmètre des tests à effectuer est établi à partir de l'analyse d'impact du correctif / mitigation Les validations et intégrations techniques et documentaires doivent s'inscrire dans la gestion des changements applicable au système concerné (processus, acteurs, …) Tout impact sur le système doit être confirmé avec les équipes fonctionnelles système / ingénieurs système

		6.2	**Rédaction / Documentation des correctifs et du système**
			Les correctifs doivent être documentés.
			Les documentations du système doivent être mises à jour.
				• Documentation du correctif
				  ○ Principes généraux du correctif
				  ○ Référentiel documentaire impacté avec une description des impacts
				  ○ Impacts sur la maintenance
					• Documentation de conception du système à jour
					• Documentation de maintenance du système à jour
					• Mode opératoire d'installation, paramétrage compris, en environnement de production (en accord avec procédure d'itération et/ou de retour arrière)
					• Binaires logiciels
						Les validations et intégrations techniques et documentaires doivent s'inscrire dans la gestion des changements applicable au système concerné (processus, acteurs, …)

	Activité		Sous-Activité	Input	Output	Commentaire
7	Traitement des vulnérabilités (déploiement)	7.1	**Organisation du déploiement dans le système global** Réunions préparatoires pour l'implémentation de la solution (mode opératoire, dates d'intervention, modalités de retour arrière, réservation des ressources, …) Définition des sites pilotes, des mini-parcs de tests avant généralisation du déploiement	• Mode opératoire d'installation, paramétrage compris, en environnement de production (en accord avec procédure d'itération et/ou de retour arrière) • Procédure d'itération et/ou de retour arrière • Planning(s) de mise(s) en œuvre • Acteur(s) de la mise(s) en œuvre	• Planification • Réservation des ressources (techniques et humaines) • Validation go site pilote / mini-parc opérateur	Sous la responsabilité de l'opérateur, l'organisation et la mise en œuvre du déploiement peut faire intervenir le mainteneur sous contrat ou le système intégrateur en prévisionnel ou sur demande
		7.2	**Implémentation des correctifs sites pilotes / mini-parcs**	• Binaires • Planification • Réservation des ressources (techniques et humaines)	• Suivi site pilote / mini-parc • Validation go industrialisation opérateur	En cas de dysfonctionnement lors d'un déploiement, la procédure de retour arrière technique doit être mise en œuvre pour une remise en service rapide du système. En complément, une réitération du processus de traitement de la vulnérabilité doit être mis en œuvre pour envisager un nouveau traitement pérenne et sans dysfonctionnement.
		7.3	**Implémentation des correctifs industrialisation**	• Binaires • Planification • Réservation des ressources (techniques et humaines)	• Suivi industrialisation • Validation finale opérateur	

	Activité		Sous-Activité	Input	Output	Commentaire
8	Mise à jour de l'analyse de risques			• Analyse de risques	• Analyse de risques	La pertinence de la mise à jour de l'analyse de risques doit être adressée selon les critères suivants : • Est-ce que le traitement de la vulnérabilité influe sur le contenu et les conclusions de l'analyse ? • Est-ce que plusieurs analyses sont impactées ? • Est-ce que cette mise à jour peut être mutualisée avec d'autres mises à jour ?

Tableau 2 : Tableau des activités

Compétences en lien avec les activités

Le tableau ci-dessous associe les acteurs et compétences à mobiliser pour chacune des activités spécifiques au MCS. Dans un contexte plus global, l'annexe H de la norme IEC 63452, « Cybersecurity roles and competence profiles », présente les différents métiers requis pour réaliser les activités de cybersécurité dans le contexte d'un système ferroviaire.

Activités	Sous-activités	Opérateur		Intégrateur système					Fournisseur produit (hors COTS)					Fournisseur produit (COTS)
		Resp. du système	Resp. SSI sur le périmètre du système	Pôle de compétence MCO/MCS (Cellule de veille)	Expert cyber "Généraliste"	Architecte cyber du système	Ingénieur projet (système)	Resp. FMDS	Pôle de compétence MCO/MCS (Cellule de veille)	Expert cyber produit	Resp. Ligne produit	Développeur	Resp. FMDS	Resp. Compte client
Comitologie et suivi associés à la prestation de MCS	Comité de suivi	X	X			X	X							
	Comité exceptionnel	X	X		X	X	X			X	X			
Veille des vulnérabilités produit	Identification / intégration des sources								X	X	X	X		X
	Corrélation des vulnérabilités => CVSS contextualisation produit									X	X	X		X
	Fiche de vulnérabilité => Synthèse des vulnérabilités retenues					X				X	X			X
Veille des vulnérabilités système	Identification et intégration des produits => CVSS contextualisation système					X	X							
	Analyse système (global)		X			X	X							

Activités	Sous-activités	Opérateur		Intégrateur système					Fournisseur produit (hors COTS)					Fournisseur produit (COTS)
		Resp. du système	Resp. SSI sur le périmètre du système	Pôle de compétence MCO/MCS (Cellule de veille)	Expert cyber "Généraliste"	Architecte cyber du système	Ingénieur projet (système)	Resp. FMDS	Pôle de compétence MCO/MCS (Cellule de veille)	Expert cyber produit	Resp. Ligne produit	Développeur	Resp. FMDS	Resp. Compte client
Développement et validation du correctif produit	Développement							Si composant certifié SIL>=1			X	X	Si composant certifié SIL>=1	X
	Validation							Si composant certifié SIL>=1			X		Si composant certifié SIL>=1	
Traitement des vulnérabilités (propositions de correctifs-mitigations-mesures, fiche de vulnérabilité complétée)	Réponse immédiate	X	X			X	X							
	Proposition de correctifs-mitigations-mesures		X		X	X	X			X	X	X		
	Procédure d'itération et/ou de retour arrière lors de la mise en œuvre		X			X	X							
	Décision de correctifs-mitigations-mesures sur le système	X	X											

Activités	Sous-activités	Opérateur		Intégrateur système					Fournisseur produit (hors COTS)					Fournisseur produit (COTS)
		Resp. du système	Resp. SSI sur le périmètre du système	Pôle de compétence MCO/MCS (Cellule de veille)	Expert cyber "Généraliste"	Architecte cyber du système	Ingénieur projet (système)	Resp. FMDS	Pôle de compétence MCO/MCS (Cellule de veille)	Expert cyber produit	Resp. Ligne produit	Développeur	Resp. FMDS	Resp. Compte client
Traitement des vulnérabilités (validations des correctifs / mitigations)	Validation des correctifs produit sur le système		X			X	X							
	Rédaction / Documentation des correctifs et du système					X		Si composant certifié SIL>=1						
Traitement des vulnérabilités (déploiement)	Organisation du déploiement dans le système global	X	X			Sur demande Opérateur	Sur demande Opérateur							
	Implémentation des correctifs sites pilotes / mini-parcs	X*	X*			Sur demande Opérateur	Sur demande Opérateur							
	Implémentation des correctifs industrialisation	X*	X*			Sur demande Opérateur	Sur demande Opérateur							
Mise à jour de l'analyse de risques	Mise à jour de l'analyse de risques	X	X			X	Sur demande Opérateur	Si composant certifié SIL>=1					Si composant certifié SIL>=1	

Tableau 3 : Compétences en lien avec les activités

** L'opérateur peut solliciter le mainteneur pour la mise en œuvre du déploiement.*

- *Exemples « Responsable du système » : Responsable de l'exploitation / Responsable de l'actif, …*

< NIVEAU DE SERVICE ET RACI >

Niveaux services types

Dans cette section, plusieurs niveaux de services sont proposés afin de guider l'opérateur dans les différentes variantes possibles en fonction du périmètre et des enjeux.

Les niveaux de services types sont :

Niveaux de services	A	B	C	D
Comitologie et suivi associés à la prestation de MCS	Forfait	Forfait	Forfait	Forfait
Veille des vulnérabilités produit	Forfait	Forfait	Forfait	Forfait
Veille des vulnérabilités système	Devis	Forfait	Forfait	Forfait
Traitement des vulnérabilités (proposition de correctifs-mitigations-mesures, fiche de vulnérabilité complétée)	Devis	Devis	Forfait	Forfait
Traitement des vulnérabilités (validations des correctifs / mitigations, documentation)	Devis	Devis	Devis	Forfait
Traitement des vulnérabilités (déploiement)	Hors contrat MCS (Activité Mainteneur sur décision Opérateur)			

Tableau 4 : Niveaux de services types

Le choix peut se faire en fonction de la nature du système à maintenir.

Le modèle à privilégier en réponse à l'Appel d'Offres est le Niveau B pour les systèmes à fort enjeux :

- Veille des vulnérabilités (produit + système) => Inclus au forfait
- Traitement des vulnérabilités (proposition de correctifs-mitigations-mesures, fiche de vulnérabilité complétée) => Inclus au devis
- Traitement des vulnérabilités (validations des correctifs / mitigations, documentation) => Inclus au devis
- Traitement des vulnérabilités (déploiement) => Exclu

Pour les prestations envisagées au devis, des estimations annuelles doivent être proposées sur la base du retour d'expérience ; et des taux journaliers doivent être précisés.

Pour un produit simple non vital, le niveau A peut être considéré. Les niveaux C ou D peuvent être envisagés pour un périmètre limité où il existe une maturité suffisante pour estimer les forfaits de traitement des vulnérabilités.

RACI types

Le tableau ci-dessous présente le RACI des activités (cf §3.3) liées au déroulement du processus MCS :

Activités	FP	IS	O	M
Comitologie et suivi associés à la prestation de MCS	C	R	A	I
Veille des vulnérabilités produit	R/A	I	I	I
Veille des vulnérabilités système	I***	R/A	I	I
Traitement des vulnérabilités (proposition de correctifs-mitigations-mesures, fiche de vulnérabilité complétée)	C	R*	A	C
Traitement des vulnérabilités (validations des correctifs / mitigations, documentation)	C	R/C**	R/A	C
Traitement des vulnérabilités (déploiement)		C	A	R

Tableau 5 : RACI activités

* Les sous-activités suivantes peuvent nécessiter la participation de, ou la prise en charge par l'opérateur :

- *5.3 Procédure d'itération et/ou de retour arrière lors de la mise en œuvre*
- *5.4 Décision de correctifs-mitigations-mesures sur le système*

*** Suivant où se situent les équipements et moyens de tests.*

**** L'intégrateur système informe le fournisseur de produit du résultat de l'activité analyse système (3.2) uniquement pour les vulnérabilités du produit de ce fournisseur. Le niveau d'information partagée avec le fournisseur dépend de la nature du produit car le fournisseur du produit n'a pas forcément besoin de connaître l'architecture système.*

R : Responsible - Le ou les R (le A peut aussi jouer le rôle de R) réalisent l'activité. Il doit y avoir au moins un R pour chaque activité.
A : Accountable (on utilise aussi parfois le terme Approver) - Le A s'organise comme il le souhaite pour sous-traiter au(x) R, mais l'activité reste de sa responsabilité. Si les R ne remplissent pas leurs objectifs (ou n'existent pas), c'est au A d'assumer. Le A est, comme son nom l'indique, celui qui doit rendre des comptes sur l'avancement de l'activité. Il y a toujours un A (et un seul) pour chaque activité. « Avoir le A » signifie être totalement responsable de l'activité.
C : Consulted - Les C sont les entités (personnes, groupes) qui doivent être consultées.
I : Informed - Les I sont les entités qui peuvent ou doivent être informées.

Le A (Accountable) lié à l'opération et maintenance du système, en lien avec les décisions de traitement prises dans le cadre du processus de MCS, est porté par l'opérateur.

< ACRONYMES ET ABREVIATION >

Acronyme	Définition
CCA	Cyber Critical Asset (voir chapitre 2.1)
CRA	Cyber Resilience Act
CENELEC	Comité européen de normalisation en électronique et en électrotechnique
CERT	Computer Emergency Response Team (Centre d'alerte et de réaction aux attaques informatiques)
CISO	Chief Information Security Officer (Responsable Sécurité des Systèmes d'Informations)
COTS	Commercial-off-the-shelf (Produit informatique standard / étagère / catalogue)
CSIRT	Computer Security Incident Response Team (Centre de réaction aux attaques informatiques)
CVE	Common Vulnerabilities and Exposures (Vulnérabilités publiques)
CVSS	Common Vulnerabilities Scoring System (Système de notation des vulnérabilités publiques)
C-CVSS	CVSS contextualisé
EPSS	Exploit Prediction Scoring System (Système de notation de la prédiction d'exploitation de vulnérabilités)
ISO	Information Security Officer (Responsable CyberSécurité)
FIRST	Forum of Incident Response and Security Teams (Forum des réponses aux incidents et des équipes de (cyber)sécurité).
FMDS	Fiabilité Maintenabilité Disponibilité Sécurité
HO/HNO	Heures Ouvrées / Heures Non Ouvrées
IEC	International Electrotechnical Commission (Commission électrotechnique internationale)
ISAC	Information Sharing and Analysis Center (Organisation de partage d'informations cybersécurité)
KEV	Known Exploited Vulnerabilities (vulnérabilités exploitables connues)
LPM	Loi de Programmation Militaire
MCG	Mobile Communication Gateway (Passerelle de communication mobile ; dans le cadre d'une communication bord-sol par exemple)
MCO	Maintien en Conditions Opérationnelles
MCS	Maintien en Conditions de Sécurité
NIS2	Directive Européenne "Network and Information Security" 2
NVD	National Vulnerability Database (Base de données de vulnérabilités américaine)
OSINT	Open Source Intelligence (ROSO en français)
OSS	Open Source Software (Logiciel Open-Source)
RACI	Responsible, Accountable, Consulted et Informed (Matrice des responsabilités)
REX	Retour d'EXpériences

Acronyme	Définition
ROSO	Renseignements d'Origine Sources Ouvertes (OSINT en anglais)
RSSI	Responsable Sécurité des Systèmes d'Informations
SBOM	Software Bill Of Materials (Inventaire des composants logiciels)
SecRACs	Security Related Application Conditions (Conditions d'application nécessaire en lien avec la CyberSécurité ; voir IEC62443/IEC63452)
SIL	Safety Integrity Level
SLA	Service Level Agreement (Niveau de service contractualisé)
SOC	Security Operation Center (Centre des opérations cybersécurité)
SSI	Sécurité des Systèmes d'Information
SSVC	Stakeholder-Specific Vulnerability Categorization (Méthode du CISA permettant une aide à la décision pour une vulnérabilité)
STRA	Systèmes de Transport Routier Automatisés
TLP	Traffic Light Protocol (Système pour classifier une information sur 4 niveaux : White/Clear, Green, Amber, Red)

< HISTORIQUE DES VERSIONS DU DOCUMENT >

Version	Date	Auteur	Commentaire
1.2	24/07/2025	Opérateurs et Industriels du Groupe d'échange Transports Collectifs Ferroviaires et Urbains (GE TCFU) (*KEOLIS, RATP, RATPDEV, SNCF, TRANSDEV, ALSTOM, COMPAGNIE DES SIGNAUX, HITACHI, SIEMENS*)	

.

< Studio des Communs >

POUR EN SAVOIR PLUS : **WIKI.CAMPUSCYBER.FR**
ADRESSE MAIL DE CONTACT : COMMUNAUTES@CAMPUSCYBER.FR
5 - 7 RUE BELLINI 92800, PUTEAUX

CAMPUS CYBER