GUIDE D'APPLICATION

STRMTG
SERVICE TECHNIQUE DES REMONTÉES MÉCANIQUES ET DES TRANSPORTS GUIDÉS

SYSTÈMES DE TRANSPORT ROUTIER AUTOMATISES

Cybersécurité des STRA

MINISTÈRE CHARGÉ DES TRANSPORTS
Liberté
Égalité
Fraternité

Version 3 – février 2026

Objet – Domaine d'application – Destinataires

Le présent guide d'application explicite les exigences relatives à la Cybersécurité pour les systèmes de transport routier automatisés (STRA).

Il est applicable aux STRA de personnes relevant du titre V du livre Ier de la troisième partie de la partie règlementaire du code des transports (articles R. 3151-1 à R. 3153-1) et aux STRA de marchandises relevant du titre V du livre II de la troisième partie de la partie réglementaire du code des transports (articles R. 3251-1 à R. 3253-1).

Il est destiné à l'ensemble des acteurs professionnels du secteur des transports routiers automatisés : organisateurs de service, maîtres d'ouvrage, exploitants, maîtres d'œuvre, bureaux d'études, Organismes qualifiés agréés (OQA), concepteurs de systèmes techniques de transports routiers automatisés, constructeurs de matériels.

Les dispositions du présent guide visent à expliciter et décliner les exigences applicables en termes de moyens à mettre en œuvre pour limiter les risques de cybersécurité. Ces exigences ont été formalisées en concertation avec la profession, offrant ainsi un cadre destiné à faciliter le travail des professionnels. Elles ne présentent pas un caractère réglementaire mais leur respect permet cependant de présumer de la conformité aux exigences réglementaires et/ou de la pertinence de la démarche adoptée.

Leur périmètre est limité aux risques relatifs à la cybersécurité pouvant affecter la sécurité des usagers et des tiers vis-à-vis du fonctionnement du système, lorsque le contrôle dynamique du véhicule n'est pas assuré par un conducteur humain, sur la voirie ouverte à la circulation publique (i.e. sur la voirie dont rien ne s'oppose à l'usage par le public).

Il est précisé que dans ces conditions, les risques de cybersécurité pouvant affecter la sécurité des personnels d'exploitation et de maintenance vis-à-vis du fonctionnement du système sont traités par le présent guide :

- au titre des usagers, lorsqu'ils sont transportés à bord des véhicules du système ou en interaction avec le système en exploitation ;
- et au titre de tiers, lorsqu'ils sont présents sur le parcours.

Par ailleurs, les dispositions du présent guide couvrent également les risques relatifs de cybersécurité pouvant affecter la sécurité des tiers lorsqu'ils sont en interaction avec les équipements et aménagements spécifiquement mis en place pour le système, hors des phases de fonctionnement de ce système.

Elles ne se substituent pas aux éventuelles autres réglementations applicables à de tels systèmes en termes de cybersécurité, et notamment :

- à la transposition de la directive européenne Network and Information System Security (NIS) dans sa version V2 ;
- au règlement européen n°2022/1426 du 5 août 2022 relatif à la réception par type des systèmes de conduite automatisée (ADS) des véhicules entièrement automatisés ainsi qu'aux règlements ONU n°155 et n°156 qui y sont référencés ;
- à la loi de programmation militaire et ses textes d'application, le cas échéant.

Elles ne traitent pas :

- des problématiques de cybersécurité internes aux acteurs extérieurs : services de secours, gestionnaires de voirie, etc. ;
- des problématiques de cybersécurité spécifiques aux ERP de type gare en tant que tels, hormis pour leurs interfaces avec le système de transport ;
- des opérations de chargement et de déchargement des marchandises ;
- de la prise en compte des éventuels risques relatifs à la cybersécurité engendrés par les travaux de réalisation du projet lorsque ceux-ci n'ont pas d'impacts sur un système de transport routier automatisé existant ;
- de la sécurité psychique et mentale à laquelle une cyberattaque pourrait porter atteinte ;
- des éventuels dommages causés aux organisations et à leur image par une cyberattaque ;
- des éventuels dommages causés aux individus par l'atteinte à leurs données personnelles suite à une cyberattaque ;
- des éventuels impacts d'une cyberattaque sur la disponibilité d'un système dès lors que la sécurité des usagers du système et des tiers n'est pas impactée ;
- des éventuels impacts financiers d'une cyberattaque.

Ce guide a vocation à être complété de manière incrémentale au fur et à mesure de l'enrichissement des travaux sur la cybersécurité des STRA.

Historique des mises à jour

N° version	Rédacteur	Date	Nature de la version
1	F. Brun	19/12/2022	Création par GT Cybersécurité des STRA
2	F. Brun	27/11/2024	Mise à jour et ajouts par GT Cybersécurité des STRA
3	F. Brun	06/02/2026	Intégration du transport de marchandises

RÉDACTEUR	VÉRIFICATEUR	APPROBATEUR
François Brun Chargé d'affaires transports publics automatisés	**Pierre Jouve** Chef du département transports publics automatisés	**Daniel Pfeiffer** Directeur
Signature numérique de François BRUN francois.brun Date : 2026.02.06 16:37:39 +01'00'	Signature numérique de Pierre JOUVE pierre.jouve Date : 2026.02.06 17:09:33 +01'00'	Le Directeur du Service Technique des Remontées Mécaniques et de Transports Guidés Daniel PFEIFFER Date : 2026.02.10 10:51:23 +01'00'

Service technique des remontées mécaniques et des transports guidés (STRMTG)
1461 rue de la piscine
38400 Saint Martin d'Hères
tél. : 33 (0)4 76 63 78 78
mèl. : strmtg@developpement-durable.gouv.fr
www.strmtg.developpement-durable.gouv.fr

Table des matières

Table des illustrations

Table des tableaux

Préambule

Le titre V du livre Ier de la troisième partie de la partie règlementaire du code des transports fixe les exigences de sécurité applicables aux systèmes de transport routier automatisés fournissant un service de transport de personnes.

Ces mêmes exigences sont applicables aux systèmes de transport routier automatisés de marchandises relevant du titre V du livre II de la troisième partie de la partie réglementaire du code des transports. Selon ces exigences, la mise en service d'un système de transport routier automatisé sur un parcours ou une zone de circulation prédéfinie est conditionnée à une démonstration de sécurité formalisée au travers d'un Dossier de conception du système technique (DCST), d'un Dossier préliminaire de sécurité (DPS) et d'un Dossier de sécurité (DS). Ces dossiers sont chacun assortis de l'avis d'un Organisme qualifié agréé (OQA) par le STRMTG.

Une fois le STRA mis en service, l'exploitant fait réaliser un audit annuel externe du système de gestion de la sécurité en exploitation par un OQA. Les évaluations réalisées par les OQA portent sur un certain nombre de domaines techniques, dont la cybersécurité.

Le présent guide vise donc à préciser les exigences applicables en termes de cybersécurité tout au long du cycle de vie d'un STRA, d'un système technique, ou d'un de leurs sous-systèmes, que ce soit :

- *au cours de son cycle de développement, des études de conception à la livraison, ou*
- *au cours de son exploitation et de sa maintenance, jusqu'à son retrait du service.*

Avant la mise en service d'un STRA, la démonstration du respect de toutes ces exigences est une partie intégrante de la démonstration de sécurité. Le risque de cybersécurité pouvant concerner l'ensemble des composantes d'un système et l'ensemble de ses phases de développement, les exigences relatives à la cybersécurité peuvent impacter l'ensemble des éléments de la démonstration de sécurité. Les briques de cette démonstration ne sont pas rappelées dans ce guide. Néanmoins, certaines présentent des éléments intéressant la cybersécurité, qu'il convient de prendre en compte avec les précautions suivantes :

- *Les véhicules intégrés dans le STRA doivent faire l'objet d'une réception au titre du Code de la route. La réception (ou homologation) est la certification administrative de la conformité du véhicule aux exigences des règlementations techniques en vue de permettre son immatriculation et sa circulation. Ce processus n'est pas abordé dans le présent guide. La réception est un prérequis à la démonstration de sécurité mais elle ne suffit pas à démontrer la sécurité des systèmes. Par définition, le périmètre de l'homologation est limité au véhicule et à ses éventuelles interfaces. Aussi, si les résultats de l'homologation et ses référentiels associés servent de données d'entrée à la démonstration de sécurité des STRA, les analyses faites dans le cadre de l'homologation des véhicules ne sauraient dispenser des analyses de niveau système ;*
- *Tout comme la démonstration du respect des exigences de sécurité, la démonstration du respect des exigences de cybersécurité applicables au système technique ou au STRA est réalisée au niveau du système. Elle est réalisée :*
    - *Pour chaque système technique, dans son domaine de conception technique ;*
    - *Pour chaque STRA dans son domaine d'emploi pour un parcours ou une zone prédéfinie.*

  La mise en œuvre de ces exigences devra tenir compte des conditions d'exploitation raisonnablement prévisibles, accessibilité des équipements du système, etc.

- *La démonstration GAME fait l'objet d'un guide d'application et d'un guide technique qui n'abordent pas la cybersécurité mais dont certains éléments peuvent servir les exigences applicables décrites dans le présent guide. Ces éléments devront faire néanmoins l'objet d'une analyse spécifique du point de vue de la cybersécurité.*

Après la mise en service d'un STRA, le respect des exigences applicables à la cybersécurité doit être évalué et documenté à différentes occasions :

- *Lors de l'audit annuel externe de sécurité en exploitation, qui doit évaluer l'application du système de gestion de la sécurité en exploitation, l'effectivité du contrôle interne et l'adéquation du système de gestion de la sécurité à l'évolution des enjeux de sécurité en exploitation.*

- *Lors du diagnostic pouvant être demandé par le préfet en cas d'insuffisance du rapport annuel sur la sécurité de l'exploitation du système établi par l'exploitant, ou de doute sérieux sur l'application du système de gestion de la sécurité ou sur le plan d'intervention et de sécurité, ou sur leur adéquation aux enjeux de sécurité.*
- *Sur demande du préfet, lors de l'évaluation de l'analyse, faite par l'exploitant, d'un accident ou incident grave.*

Ce guide a été élaboré en concertation avec les experts de la profession dans le cadre d'un groupe de travail. Les exigences et les méthodologies associées, n'ont, à la date de publication de ce guide, pas encore été mises en pratique sur un système réel. Elles restent donc susceptibles d'évolutions suite aux premières mises en application sur des cas concrets. Ce guide pourra ainsi être complété et amendé afin de prendre en compte les enseignements tirés des premiers cas d'application.

Définitions

Accident	Evénement ou série d'événements inattendus conduisant à des dommages, qui peuvent engager la sécurité des personnes.
Accident de la circulation	Collision entre un véhicule et un autre véhicule ou un obstacle mobile ou fixe.
Activité de cybersécurité	Activité réalisée en application d'une ou plusieurs exigence(s) applicable(s) à la cybersécurité.
Analyse de risque	Utilisation systématique de toutes les informations disponibles pour identifier les dangers et estimer le risque (d'après règlement UE 402/2013 du 30 avril 2013).
Assertion de NICS	Traduction formelle de la définition des NICS en une assertion assumée par l'entité responsable et le cas échéant, les autres entités responsables en interface.
Assurance cybersécurité	Fondement d'une confiance justifiée dans le fait que les exigences applicables à la cybersécurité ont été ou seront satisfaites (d'après ISO IEC 15026-1).
Attaquant	Voir « source de menace ».
Besoin d'en connaître	Nécessité impérieuse de prendre connaissance d'une information dans le cadre d'une fonction déterminée et pour la bonne exécution d'une mission précise (d'après IGI 1300).
Bien support	Bien à protéger, en regard de son rôle dans la sécurité des usagers et des tiers.
Compromission d'une fonction de niveau système	Violation de la cybersécurité d'une fonction au niveau système provoquant la perte, la divulgation et/ou la corruption des données (inspiré de CLC/TS 50701)
Concepteur de système technique	Personne physique ou morale assurant la conception d'ensemble du système technique et définissant notamment ses fonctionnalités et leurs conditions d'utilisation (Article R. 3151-1 du code des transports).
Contrainte	Elément de contexte vis-à-vis duquel on ne peut pas fixer d'objectif de cybersécurité (à l'inverse d'une hypothèse) ; cela peut se traduire par des éléments réglementaires ou factuels qui s'imposent au projet.
Contrôle dynamique	Exécution de toutes les fonctions opérationnelles et tactiques en temps réel nécessaires au déplacement du véhicule. Il s'agit notamment du contrôle du déplacement latéral et longitudinal du véhicule, de la surveillance de l'environnement routier, des réactions aux événements survenant dans la circulation routière et de la préparation et du signalement des manœuvres. (Article R. 311-1-1 du code de la route)
Danger	Circonstance pouvant mener à un accident (d'après règlement UE 402/2013 du 30 avril 2013).
Domaine d'emploi	Conditions d'emploi d'un système technique de transport routier automatisé associées à des parcours ou zones de circulation particulières et respectant son domaine de conception technique (Article R. 3151-1 du code des transports).
Domaine de conception technique du système	Conditions d'opération dans lesquelles un système technique de transport routier automatisé est spécifiquement conçu pour fonctionner, à l'exclusion, pour les systèmes de transport routier automatisé de marchandises, des opérations de chargement et de déchargement des marchandises. (cf. articles R. 3151-1 et R. 3251-2 du code des transports).

Dysfonctionnement	Mauvaise réponse du système dans deux cas possibles : • Lors d'une défaillance, • Lors d'apparition de conditions de fonctionnement qui ne sont pas correctement gérées en raison de limitations fonctionnelles (insuffisances fonctionnelles).
Ecosystème	Ensemble des parties prenantes qui gravitent autour de l'objet de l'étude et concourent à la réalisation de ses missions (d'après guide méthode EBIOS Risk Manager).
Entité responsable	Personne morale étant responsable de livrable(s) ou d'activité(s) impliquant l'évaluation et/ou l'audit par un OQA. Peut désigner le concepteur du système technique, l'organisateur du service, ou l'exploitant de STRA.
Entité tierce	Entité autre qu'une entité responsable, assurant la responsabilité d'activités de cybersécurité sur un système considéré.
Evénement redouté	Événement indésirable qui peut provoquer une situation dangereuse et dans certaines conditions un accident.
Evénement redouté de cybersécurité	Expression de l'effet direct d'une attaque sur une mission ou une fonction du système considéré.
Exigence applicable à la cybersécurité	Exigence formulée dans le présent guide, identifiée par un code de type [EX-N.NN] où N est un chiffre.
Exigence de NICS	Exigence caractérisant la rigueur attendue dans la réalisation des activités de cybersécurité constitutives du cycle de vie du système considéré.
Exigence fonctionnelle de cybersécurité	Eléments requis pour atteindre les objectifs de cybersécurité.
Exploitant	- Pour le transport de personnes : personne physique ou morale assurant directement ou à la demande de l'organisateur du service l'exploitation du système de transport ainsi que la gestion et la maintenance de celui-ci. L'exploitant peut être la même entité que l'organisateur du service ou que le concepteur du système technique. En cas de pluralité d'exploitants, le terme exploitant désigne le chef de file (article R. 3151-1 du code des transports). - Pour le transport de marchandises : personne physique ou morale assurant l'exploitation du système de transport routier automatisé de marchandises, ainsi que la gestion et la maintenance de celui-ci, pour son propre compte ou dans le cadre de prestations de transport public routier de marchandises (article R. 3251-2 du code des transports).
Fonction de niveau système	Action ou activité spécifiée au niveau système qui peut être exécutée par des moyens techniques et/ou des êtres humains et ayant un rendement défini en réponse à une entrée définie (d'après NF EN 50126-1).
Gravité du risque	Estimation du niveau et de l'intensité des effets d'un risque, via la mesure des impacts préjudiciables perçus, qu'ils soient directs ou indirects (d'après guide méthode EBIOS Risk Manager).
Hypothèse	Supposition fondée permettant de s'affranchir d'un objectif de cybersécurité et ainsi réduire le périmètre de l'appréciation des risques de cybersécurité (à l'inverse d'une contrainte). L'hypothèse est notamment formulée dans les cas de partage ou de maintien du risque ; il est recommandé de motiver les raisons qui ont mené à retenir l'hypothèse.
Infrastructure numérique	Ensemble des équipements permettant la communication et la connectivité nécessaires au STRA, i.e. les unités de bords de route, les réseaux de communications 3G/4G/5G, C-ITS, reliant les différents

	composants connectés du système ou de l'écosystème et les équipements dédiés à la supervision.
Interface	Point d'entrée ou de sortie logique et/ou physique qui donne accès au système pour des flux d'informations (inspiré d'IEC 62443-1-1 :2009).
Intervention à distance	Action exercée par la personne habilitée mentionnée à l'article L. 3151-3, située à l'extérieur du véhicule, dans le cadre d'un système de transport routier automatisé, aux fins : a) D'activer, de désactiver le système, de donner l'instruction d'effectuer, modifier, interrompre une manœuvre, ou d'acquitter des manœuvres proposées par le système ; b) De donner instruction au système de navigation opérant sur le système de choisir ou de modifier la planification d'un itinéraire ou des points d'arrêt pour les usagers. (Article R. 3151-1 du code des transports)
Maintien en condition de cybersécurité	Ensemble d'activités visant à assurer que le système conserve un niveau de cybersécurité constant, adapté à l'évolution de la menace (inspiré des règles de sécurité de l'ANSSI concernant la protection des OIV).
Menace	Terme générique utilisé pour désigner toute intention hostile de nuire dans le cyber espace. Une menace peut être ciblée ou non sur l'objet de l'étude (d'après guide méthode EBIOS Risk Manager).
Mesure de cybersécurité	Eléments identifiés pour répondre aux exigences fonctionnelles de cybersécurité.
Mesure de réduction des risques	Série de mesures permettant de réduire la fréquence d'occurrence d'un danger ou d'en atténuer les conséquences afin d'atteindre et/ou de maintenir un niveau de risque acceptable (règlement UE 402/2013).
Mission du système considéré	Fonction, finalité, raison d'être du système considéré (d'après guide méthode EBIOS Risk Manager).
Modification substantielle	Toute modification d'un système de transport routier automatisé ou d'une partie de système existant, dès lors qu'elle modifie l'évaluation de la sécurité (article R. 3151-1 du code des transports);
Module	Unité architecturale, fonctionnelle ou technique, spécifiée à un niveau approprié pour la mise en œuvre du système considéré.
Niveaux d'Intégrité Cybersécurité Système	Système de classification décrivant les exigences à respecter pour assurer que les activités relatives aux exigences applicables de à la cybersécurité sont réalisées avec un niveau d'effort suffisant en regard du niveau de risque.
Objectif de cybersécurité	But à atteindre pour amener un risque identifié à un niveau acceptable, en agissant sur la vraisemblance et la gravité du risque et sur les variables qui les composent.
Organisateur du service	- Pour le transport de personnes : pour les services de transport public collectif exécutés dans le cadre de l'article L. 1221-3 du code des transports, l'autorité territorialement compétente au sens de l'article L. 1221-1 ou L. 1241-1 du code des transports ; pour les services de transport publics collectifs organisés en application de la section 3 du titre premier du livre premier de la troisième partie du présent code, l'entreprise citée à l'article L. 3111-17 du code des transports; pour les services de transport public particulier, l'exploitant au sens de l'article L. 3122-1 du code des transports; pour les services privés, les personnes physiques ou morales visées au R. 3131-1 et R. 3131-2 du code des transports (article R. 3151-1 du code des transports).

	- Pour le transport de marchandises : l'entreprise de transport routier de marchandises, le commissionnaire de transport, au sens de l'article L. 1411-1, ou l'autorité territorialement compétente, au sens de l'article L. 1231-1 (article R. 3251-2 du code des transports).
Organisme qualifié agréé	Organisme agréé pour procéder à l'évaluation de la sécurité de la conception, de la réalisation et de l'exploitation des systèmes de transport routiers automatisés (article R. 3151-1 du code des transports).
Parcours ou zone de circulation prédéfini	Ensemble des sections routières ou espace dont les limites géographiques sont définies, sur lesquelles est prévue la circulation ou l'arrêt d'un ou plusieurs véhicules d'un système de transport routier automatisé. (Article R. 3151-1 du code des transports) *Note : dans la suite du document, le terme "parcours" est communément utilisé en lieu et place de "parcours ou zone de circulation prédéfinie ».*
Partie prenante	Personne ou organisme de l'écosystème susceptible d'affecter, d'être affecté ou de se sentir lui-même affecté par une décision ou une activité (inspiré de l'ISO 31073 : 2022).
Passager	Catégorie d'usager situé à l'intérieur d'un véhicule du système qui ne peut prendre part à aucune action de contrôle dynamique de ce véhicule.
Potentiel d'attaque	Combinaison de la motivation et des capacités d'une source de menace. Les capacités incluent les ressources disponibles et l'expertise de la source de menace (inspiré de ISO 18045).
Risque de cybersécurité	Scénario, avec un niveau donné, combinant un événement redouté de cybersécurité avec un scénario de menaces et un scénario de conséquences. Son niveau correspond à l'estimation de sa gravité et de sa vraisemblance.
Risque résiduel	Risque subsistant après le traitement du risque. [ISO 31073 : 2022]
Situation dangereuse	Situation dans laquelle des personnes sont (ou auraient pu être) exposées à un ou plusieurs dangers.
Serveur dorsal	Couche logicielle ou matérielle accédant à des données mais ne gérant pas d'interface utilisateur.
Source de menace	Chose ou personne à l'origine de menaces. Elle peut être caractérisée par son type (humain ou environnemental), par sa cause (accidentelle ou délibérée) et selon le cas par ses ressources disponibles, son expertise, sa motivation (d'après ISO 27005 :2022).
Sous-système	Partie d'un système, qui est elle-même un système (EN 50126-1:2017).
Station	Point d'arrêt prédéfini des véhicules destiné à permettre l'accès des usagers aux véhicules dans un système de transport routier automatisé de personnes. Par extension, ce terme désigne également un point d'arrêt destiné à permettre le chargement ou le déchargement des marchandises dans un système de transport routier automatisé de marchandises.
Stratégie de collecte	Spécification de la liste des sources de collecte, des collecteurs, des évènements à collecter, des méthodes de collecte (protocoles, applications, propriétés de sécurité, etc.) et des fréquences de collecte dans le cadre de la surveillance des performances de cybersécurité. [Référentiel d'exigences PDIS v2.0]
Stratégie d'analyse	Spécification de la mise en œuvre de règles de détection permettant de détecter les incidents de sécurité sur la base des évènements collectés au titre de la stratégie de collecte dans le cadre de la surveillance des performances de cybersécurité. [Référentiel d'exigences PDIS v2.0]

Stratégie de notification	Spécification des incidents de sécurité à notifier, incluant le format, le contenu, le délai, le niveau de sensibilité ou de classification des notifications ainsi que les personnes à notifier notamment en fonction de l'incident de sécurité et de son niveau de gravité. [Référentiel d'exigences PDIS v2.0]
Système	Ensemble d'éléments (matériels, logiciels ou humains) reliés entre eux, considéré comme un tout dans un contexte défini et organisé de sorte à atteindre un objectif donné, dans certaines conditions (Guide Technique relatif à la démonstration GAME pour les STRA). Les éléments composants un système peuvent être de différentes natures : • Technique : logiciel, composant, équipement, réseau… • Fonctionnel : fonction, mode opérationnel… • Organisationnel : règles, processus… Un système peut désigner un système complet de transport routier automatisé, un système technique, ou un de leurs sous-système.
Système considéré	Système identifié comme étant l'objet des exigences applicables à la cybersécurité.
Système de conduite automatisé	Système associant des éléments matériels et logiciels, permettant d'exercer le contrôle dynamique d'un véhicule de façon prolongée (Article R. 311-1-1 du code de la route).
Système de transport routier automatisé de marchandises	Système technique de transport routier automatisé, déployé sur des parcours ou zones de circulation prédéfinis, et complété de règles d'exploitation, d'entretien et de maintenance, aux fins de réaliser une activité de transport routier de marchandises ». (Article R. 3251-2 du code des transports)
Système de transport routier automatisé de personnes	Système technique de transport routier automatisé, déployé sur des parcours ou zones de circulation prédéfinis, et complété de règles d'exploitation, d'entretien et de maintenance, aux fins de fournir un service de transport routier public collectif ou particulier de personnes, ou de service privé de transport de personnes, à l'exclusion des transports soumis au décret no 2017-440 du 30 mars 2017 relatif à la sécurité des transports publics guidés (Article R. 3151-1 du code des transports).
Système de transport routier automatisé	Système de transport routier automatisé de personnes ou système de transport routier automatisé de marchandises. *Note : la définition de « système de transport routier automatisé » utilisée dans ce guide est volontairement plus large que celle de l'article R.3151-1 du code des transports. Elle recouvre à la fois les systèmes de transport routier automatisés de personnes qui relèvent du titre V du livre Ier de la troisième partie de la partie réglementaire du code des transports et les systèmes de transport routier automatisés de marchandises qui relèvent du titre V du livre II de la troisième partie de la partie réglementaire du code des transports.*
Système technique de transport routier automatisé	Ensemble de véhicules hautement ou totalement automatisés, tels que définis aux 8.2 et 8.3 de l'article R. 311-1 du code de la route, et d'installations techniques permettant une intervention à distance ou participant à la sécurité (Article R. 3151-1 du code des transports).

	Note : dans la suite du document, la formulation « Système technique » est communément utilisée en lieu et place de « Système technique de transport routier automatisé ».
Traitement du risque	Sous-processus de la gestion des risques permettant de choisir et de mettre en œuvre des mesures de sécurité visant à modifier les risques de sécurité de l'information. [ISO 31073 :2022]
Usager (du système)	Terme général faisant référence au rôle de l'humain par rapport à la délégation de conduite (SAE J3016). *Note : Dans ce document, le terme « usager » est employé pour désigner l'usager du système, par opposition aux « autres usagers » de la route (ou de la voirie)[1].*
Usager de la route	Toute personne faisant l'usage de la route (y compris les trottoirs et autres espaces adjacents) (EN ISO TR 4804 : 2020). *Note : les usagers du système sont une catégorie d'usagers de la route. Par opposition aux usagers du système, les « autres » usagers de la route représentent les tiers.*
Véhicule hautement automatisé	Véhicule équipé d'un système de conduite automatisé exerçant le contrôle dynamique d'un véhicule dans un domaine de conception fonctionnelle particulier, pouvant répondre à tout aléa de circulation ou défaillance, sans exercer de demande de reprise en main pendant une manœuvre effectuée dans son domaine de conception fonctionnelle. Ce véhicule peut être intégré dans un système technique de transport routier automatisé tel que défini au 1o de l'article R. 3151-1 du code des transports (Article R. 311-1-1 du code de la route).
Véhicule totalement automatisé	Véhicule équipé d'un système de conduite automatisé exerçant le contrôle dynamique d'un véhicule pouvant répondre à tout aléa de circulation ou défaillance, sans exercer de demande de reprise en main pendant une manœuvre dans le domaine de conception technique du système technique de transport routier automatisé auquel ce véhicule est intégré, tels que définis aux 1° et 4° de l'article R. 3151-1 du code des transports (Article R. 311-1-1 du code de la route).
Vraisemblance du risque	Estimation de la faisabilité ou de la probabilité qu'un risque se réalise. [EBIOS RM]
Vulnérabilité	Propension d'un milieu, d'un bien ou d'une personne à subir des conséquences dommageables à la suite d'un événement. Elle ne produit pas les conséquences par elle-même.

[1] L'usager du système peut être par exemple le passager à bord d'un véhicule du système, la personne en attente d'être prise en charge, les personnes en charge du chargement et du déchargement des marchandises, etc.
Par ailleurs, même si elle peut être rattachée à l'usager, la notion de personnel d'exploitation est préférée à celle d'usager du système pour désigner les personnels en charge de l'exploitation et de la maintenance du système : opérateur d'intervention à distance, opérateur d'intervention locale, etc.

Liste des abréviations

AFNOR	Association Française de NORmalisation
AFO	Agent des Forces de l'Ordre
AMDEC	Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API	Application Programming Interface
CERT	Computer Emergency Response Team
CMDB	Configuration Management Database
DCST	Dossier de Conception du Système Technique
DORESE	Doctrine Organisation Ressources humaines Entraînement Soutien Equipement
DPS	Dossier Préliminaire de Sécurité
DS	Dossier de Sécurité
DSI	Direction des Systèmes d'Information
EDP	Engin de Déplacement Personnel
EFR	Etat Final Recherché
ER	Evénement Redouté
ERP	Etablissement Recevant du Public
GAME	Globalement Au Moins Equivalent
GIP ACYMA	Groupement d'Intérêt Public d'Action contre la CYberMAlveillance
IEC	International Electrotechnical Commission
ISO	International Standard Organisation
LPM	Loi de Programmation Militaire
MRM	Manœuvre à Risque Minimal
NICS	Niveau d'Intégrité Cybersécurité Système
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
OIV	Opérateur d'Importance Vitale
OQA	Organisme Qualifié Agréé
ORSEC	Organisation de la Réponse de SEcurité Civile
OSI	Open Systems Interconnection
PIS	Plan d'Intervention et de Sécurité
PMR	Personne à Mobilité Réduite
PCC	Poste de Commande Centralisé
REX	Retour d'EXpérience
SGS	Système de Gestion de la Sécurité
SOC	Security Operations center
SSI	Sécurité des Systèmes d'Information
ST	Système Technique de transport routier automatisé
STRA	Système de Transport Routier Automatisé
STRA-M	Système de transport routier automatisé de marchandises
STRA-P	Système de transport routier automatisé de personnes
TC	Transport en Commun
UNR	United Nations Regulation
VP	Véhicule Prioritaire
VSR	Vérification de Service Régulier
V2X	Vehicle To Everything

1 Champ d'application

1.1 Eléments constitutifs ou en interface

Un STRA peut être constitué de différents éléments spécifiques :

- des véhicules hautement et / ou totalement automatisés ;
- des installations techniques spécifiques au système permettant une intervention à distance ou participant à la sécurité, déployées sur le parcours ;
- des installations techniques permettant une intervention à distance ou participant à la sécurité, dédiées à la supervision, déployées en dehors du parcours ;
- des règles d'exploitation et de maintenance (aspect organisationnel supporté par le SGS en exploitation) ;
- un parcours et ses aménagements.

Il est également en interface avec différents éléments qui contribuent à son fonctionnement :

- des équipements de communication et de localisation partagés extérieurs au système ;
- des équipements permettant les opérations de chargement et le déchargement des marchandises (STRA-M, le cas échéant) ;
- la chaussée routière sur laquelle peuvent circuler les véhicules du système ;
- des installations techniques génériques (préexistantes et partagées avec d'autres usagers de la route) ;
- des services extérieurs (forces de l'ordre, services de secours, services de la voirie, services de prévision et d'information météo, services d'information trafic, etc.) ;
- des règles de circulation applicables sur le parcours ;
- etc.

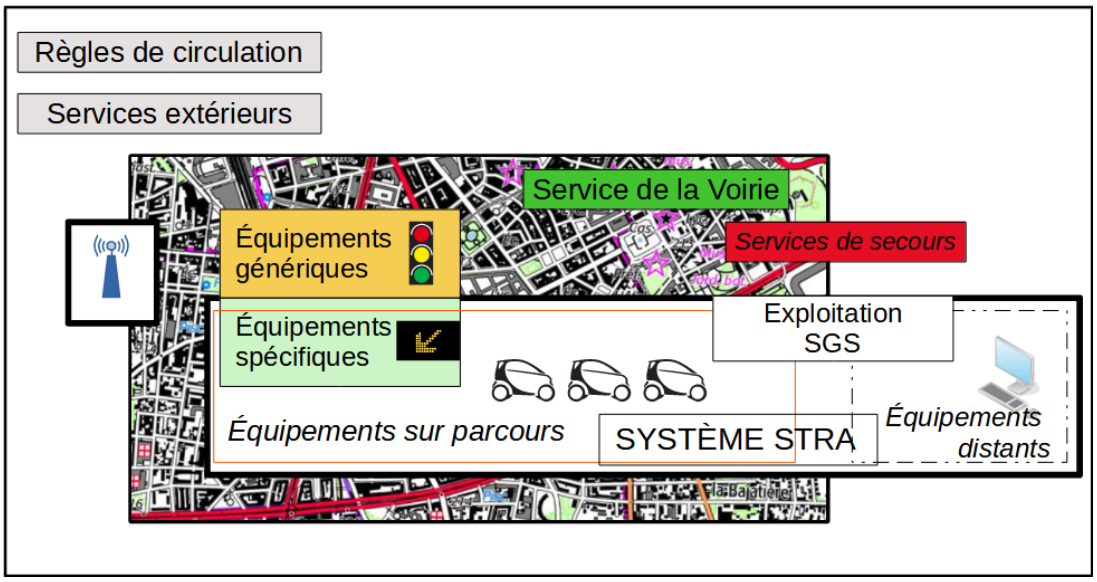


Figure 1 : Décomposition organique d'un STRA

1.2 Contexte réglementaire

Le présent guide est applicable aux systèmes de transport routier automatisés de personnes relevant du titre V du livre Ier de la troisième partie de la partie règlementaire du code des transports (articles R. 3151-1 à R. 3153-1) et aux systèmes de transport routier automatisés de marchandises relevant du titre V du livre II de la troisième partie de la partie réglementaire du code des transports (articles R. 3251-1 à R. 3253-1).

Le code des transports introduit l'obligation que les systèmes techniques de transport routiers automatisés et que les systèmes de transport routier automatisés soient évalués à différentes étapes

de leur cycle de vie par des organismes qualifiés agréés (OQA). La cybersécurité est un des domaines techniques pour lesquels les agréments de ces organismes sont délivrés.

Pour les systèmes de transport routier automatisés de personnes (STRA-P), cette exigence est formalisée par les articles R.3152-26 et R.3152-28 du code des transports, exposés ci-après.

> Art. R.3152-26
>
> L'organisme dont l'avis est joint aux dossiers mentionnés aux articles R. 3152-6 à R. 3152-8, est agréé par l'autorité mentionnée à l'article R. 3152-1. […]

> Art. R.3152-28
>
> I. - L'agrément est délivré par l'autorité mentionnée à l'article R. 3152-1, qui s'assure que l'organisme dispose des compétences nécessaires à l'accomplissement de ses missions dans les domaines techniques considérés.
>
> II. - L'agrément est délivré pour un ou plusieurs des domaines techniques suivants :
>
> 1. Sûreté de fonctionnement des systèmes embarqués ;
> 2. Sûreté de fonctionnement des équipements de connectivité ou de positionnement ;
> 3. **Cybersécurité** ;
> 4. Sécurité des infrastructures et des équipements de la route ;
> 5. Sécurité du comportement routier des véhicules ;
> 6. Systèmes de gestion de la sécurité en exploitation ;
> 7. Evaluation globale de la sécurité des systèmes.

Cette même exigence est ensuite transposée pour les systèmes de transport routier automatisés de marchandises (STRA-M) par l'article R.3251-1 du code des transports :

> Art. R. 3251-1
>
> Les dispositions du titre V du livre premier de la troisième partie du présent code sont applicables au transport routier de marchandises, lorsqu'il est effectué au moyen d'un système de transport routier automatisé, sous réserve des dispositions prévues au présent titre.

Les missions de l'organisme qualifié agréé pour le domaine technique 3. Cybersécurité sont précisées dans le « Guide d'application relatif à la mission de l'organisme qualifié agréé pour l'évaluation de la sécurité et pour l'audit de sécurité en exploitation des STRA » du STRMTG.

1.3 Exigences applicables à la cybersécurité

Le présent guide vise à expliciter les exigences applicables aux entités responsables et aux systèmes considérés (cf. section 1.4) en termes de cybersécurité, appelées dans la suite du présent document « exigences applicables à la cybersécurité », ainsi que les conditions de la démonstration du respect de ces exigences.

Il fournit également les principes méthodologiques contribuant au respect de certaines exigences.

Le présent document ne saurait prétendre être exhaustif :

- Certains éléments mériteront d'être détaillés dans les évolutions du présent document ou dans des documents complémentaires ;
- Les éléments fournis devront être enrichis au fur et à mesure des retours d'expérience des acteurs issus des différents cas d'application.

Il appartient toujours aux entités responsables (cf. section 1.4) de compléter en tant que de besoin les différents éléments de ce guide, dans le but de couvrir les spécificités d'un système considéré.

Dans le même esprit, il est toujours possible de justifier de la non-prise en compte d'un élément du présent document qui serait « non-applicable » en raison des spécificités d'un système considéré.

Exigences selon la nature du service de transport

Par défaut, les éléments présentés dans la suite de ce document concernent les STRA au sens général.

Lorsque cela est pertinent, le document précise pour certains éléments s'ils concernent plus spécifiquement les STRA-P ou plus spécifiquement les STRA-M.

Cette précision reste indicative, en particulier pour les systèmes prévoyant un transport effectué à titre accessoire. En application de l'article R. 3252-12 du code des transports, ces systèmes sont concernés par l'ensemble des éléments :

- Le transport routier automatisé de marchandises effectué à titre accessoire au moyen d'un STRA-P est également concerné par les éléments du guide spécifiques aux STRA-M ;

- Le transport routier automatisé de personnes effectué à titre accessoire au moyen d'un STRA-M est également concerné par les éléments du guide spécifiques aux STRA-P.

1.4 Périmètre d'application

1.4.1 Entités responsables

Les exigences applicables à la cybersécurité sont en premier lieu opposables aux entités responsables, qui sont seules garantes de leur respect. Ces exigences couvrent l'ensemble du cycle de vie d'un système considéré et sont identifiées par un code de type [EX-N.NN] où N est un chiffre (cf. Annexe A).

Entité responsable	Système considéré
Concepteur du système technique	Système technique de transport routier automatisé
Organisateur du service	STRA
Exploitant	STRA

Tableau 1 : Système considéré en fonction de l'entité responsable

Chaque entité responsable doit s'assurer des compétences des organismes et / ou des personnes qui sont chargés des activités de cybersécurité.

1.4.2 Entités tierces

Ce référentiel d'exigences applicables à la cybersécurité peut aussi être utilisé par toute entité tierce qui le souhaite, par exemple dans le cadre de la fourniture d'équipements ou sous-systèmes pouvant être intégrés à un STRA. Dans ce cas, cette entité tierce doit fournir un livrable contenant une démonstration du respect des exigences applicables à la cybersécurité pour le système considéré.

Également, dans l'exercice de sa responsabilité, une entité responsable peut imposer tout ou partie de ces exigences à une entité tierce (fournisseur, sous-traitant, etc.), exception faite du constructeur du véhicule qui est soumis à des exigences spécifiques dans le cadre de l'homologation. Dans ce cas, l'entité responsable doit exiger un livrable contenant la démonstration du respect des exigences applicables à la cybersécurité par l'entité tierce concernée.

Dans les deux cas précités :

- Le système considéré doit être défini ;
- L'entité tierce assure le rôle de l'entité responsable en respectant les exigences applicables à la cybersécurité pour ce système considéré.

1.5 Articulation avec la démonstration de sécurité

Dans le cas où le système considéré est le STRA complet ou le système technique de transport routier automatisé, il doit faire l'objet d'une démonstration de sécurité, introduite dans les termes ci-après à l'article R.3152-5 du code des transports.

> Art. R. 3152-5
>
> La démonstration de la sécurité est établie préalablement à la mise en service du système de transport routier automatisé, en vérifiant que, dans son domaine d'emploi prévu, les réponses du système à l'ensemble des risques liés au fonctionnement du système et des risques de circulation raisonnablement prévisibles et identifiables, satisfont aux conditions prévues aux articles R. 3152-2 à R. 3152-4.
>
> Cette démonstration est conduite sur la base des dossiers prévus aux articles R. 3152-6 à R. 3152-8, assortis des avis des organismes qualifiés agréés prévus aux articles R. 3152-25 et R. 3152-26. […]

Comme indiqué en préambule, la démonstration du respect des exigences applicables à la cybersécurité est une partie intégrante de la démonstration de la sécurité.

A ce titre :

- Les exigences applicables à la cybersécurité visent à garantir que tout système de transport routier automatisé ou tout système technique de transport routier automatisé est conçu pour éviter les accidents pouvant résulter de situations raisonnablement prévisibles, pour ce qui concerne la cybersécurité, dans son domaine d'emploi ou dans son domaine de conception technique (article R3152-2. II. 1) ;
- Le champ, le périmètre et les limites d'application des exigences applicables à la cybersécurité sont ceux de la démonstration de sécurité (article R3152-2 II, III et IV). Dans le cas des systèmes de transport routier automatisés de marchandises (STRA-M), les opérations de chargement et de déchargement des marchandises, y compris les opérations d'arrimage des marchandises, sont exclues du domaine de conception technique du système et ne font pas partie du périmètre de la démonstration de sécurité (Art R. 3251-2. 2. du code des transports). Seules leurs interfaces avec les fonctions de conduite automatisée sont prises en compte et décrites dans le dossier de conception du système technique (Art. R. 3252-2 du code des transports). ;
- La démonstration du respect de toutes les exigences applicables à la cybersécurité doit apparaître dans les dossiers réglementaires faisant l'objet d'un avis de l'OQA : DCST, DPS et DS (articles R3152-25 et R3152-26). Etant donné que la démonstration du respect des exigences applicables à la cybersécurité n'est pas formalisée de manière explicite dans la composition des dossiers réglementaires (DCST, DPS et DS respectivement aux articles R. 3152-6 à R. 3152-8) prévue par le décret, plusieurs possibilités sont proposées :
    - Rajouter un ou des chapitres contenant les éléments relatifs à la cybersécurité ;
    - Inclure dans des chapitres définis dans le décret les éléments relatifs à la cybersécurité ;
    - Créer un sous-dossier à chaque dossier réglementaire contenant les éléments relatifs à la cybersécurité.

Cela signifie qu'en cas de modifications jugées substantielles (cf. section 1.6), les dossiers réglementaires concernés doivent être remis à jour par l'entité responsable et réévalués par un OQA.

Le champ de la démonstration du respect des exigences applicables à la cybersécurité doit intégrer l'ensemble des éléments qui participent à la sécurité du système de transport STRA parmi ceux constitutifs ou en interface présentés à la section 1.1.

Parmi ces éléments, il convient de distinguer :

- Les éléments qui font partie du système et sont directement intégrés dans la démonstration. Par exemple, les exigences relatives à un feu de circulation spécifique au système analysé sont directement spécifiées et résolues dans le cadre de la démonstration de sécurité ;
- Les éléments qui ne font pas partie du système mais qui participent à sa sécurité, pour lesquels la démonstration de sécurité pourra spécifier des exigences exportées, lesquelles devront être vérifiées par l'entité responsable. Par exemple, les exigences relatives à un feu de circulation préexistant et non spécifique au système analysé sont spécifiées sous forme d'exigences exportées et résolues dans un second temps sous la responsabilité de l'organisateur du service au stade du déploiement.

Aussi, les études concernant la sûreté de fonctionnement du système considéré doivent être prises en compte pour la mise en œuvre des exigences applicables à la cybersécurité.

A ce titre :

- Si disponibles et pertinentes au sens de la cybersécurité, les modélisations du système considéré (par exemple les différents types d'architecture : opérationnelle, technique, fonctionnelle, organique, etc.) devront être prises en considération ;
- Les cas de dysfonctionnements identifiés lors de ces études, lorsqu'ils peuvent résulter d'une cyberattaque, devront être pris en compte dans les analyses de risque cyber.

1.6 Opérations concernées

Les exigences applicables à la cybersécurité doivent être mises en œuvre dans le cadre :

- De tout nouveau système technique de transport routier automatisé ;
- De tout nouveau système de transport routier automatisé ;
- De toute modification, même non substantielle d'un système technique de transport routier automatisé existant ;
- De toute modification, même non substantielle d'un système de transport routier automatisé existant ;
- De l'exploitation, de la maintenance et du retrait de service d'un système de transport routier automatisé existant, nouveau, ou modifié.

La modification substantielle est définie dans les termes suivants à l'article R.3151-1 du code des transports : « 18. Modification substantielle : toute modification d'un système de transport routier automatisé ou d'une partie de système existant, dès lors qu'elle modifie l'évaluation de la sécurité. »

Les exigences applicables à la cybersécurité en phase exploitation peuvent amener à devoir modifier substantiellement ou non le système considéré. Chaque modification du système considéré doit alors faire l'objet d'une analyse préalable de son impact sur l'évaluation de la sécurité.

Deux cas sont toutefois à traiter spécifiquement :

- Le maintien en condition de cybersécurité (cf. section 4.5) : installation de mises à jour, application de correctifs, réponse aux incidents, etc. Dans ce cas, la modification peut ne pas être considérée comme substantielle :
    - Si ses impacts concernent uniquement le champ de la cybersécurité ;
    - Et si elle ne sert pas à réduire un risque inacceptable.
- La réappréciation des risques en phase exploitation, suite à une évolution de l'environnement du système considéré, révélant un ou plusieurs risque(s) inacceptable(s). Dans ce cas, la modification du système considéré qui en résulte vient modifier l'évaluation de la sécurité

formalisée dans les dossiers réglementaires faisant l'objet d'un avis de l'OQA. Elle doit être considérée comme substantielle.

1.7 Périmètre de la cybersécurité

L'article R.3152-2 du code des transports définit 3 grandes « populations » pour la sécurité desquelles il convient de protéger le système considéré dans le cadre de tout nouveau système et de toute modification d'un système existant :

- Les usagers du système de transport ;
- Les personnels d'exploitation ;
- Les tiers.

Les exigences explicitées dans le présent guide visent à assurer la sécurité des usagers et des tiers vis-à-vis du fonctionnement du système en exploitation, y compris les personnels d'exploitation et de maintenance dès lors qu'ils sont transportés à bord des véhicules du système ou en interaction avec le système en exploitation au même titre que les usagers du système de transport, ou qu'ils sont présents sur le parcours au même titre que les tiers.

1.8 Preuves

Pour toutes les phases du cycle de vie du système considéré, les preuves du respect des exigences applicables à la cybersécurité doivent être formalisées et tracées par chaque entité responsable, et, le cas échéant, par toute entité tierce (cf. §1.4.2), dans le ou les dossier(s) ou document(s) dont elle est responsable.

Entité responsable ou entité tierce	Dossiers ou documents contenant les preuves et leur traçabilité
Concepteur du système technique	DCST
Organisateur du service	DPS, DS
Exploitant	SGS, PIS + toute trace de leur application.
Entité tierce (cf. §1.4.2)	Livrable contenant une démonstration du respect des exigences applicables à la cybersécurité

Tableau 2 : Dossiers ou documents contenant les preuves et leur traçabilité

2 Activités de cybersécurité

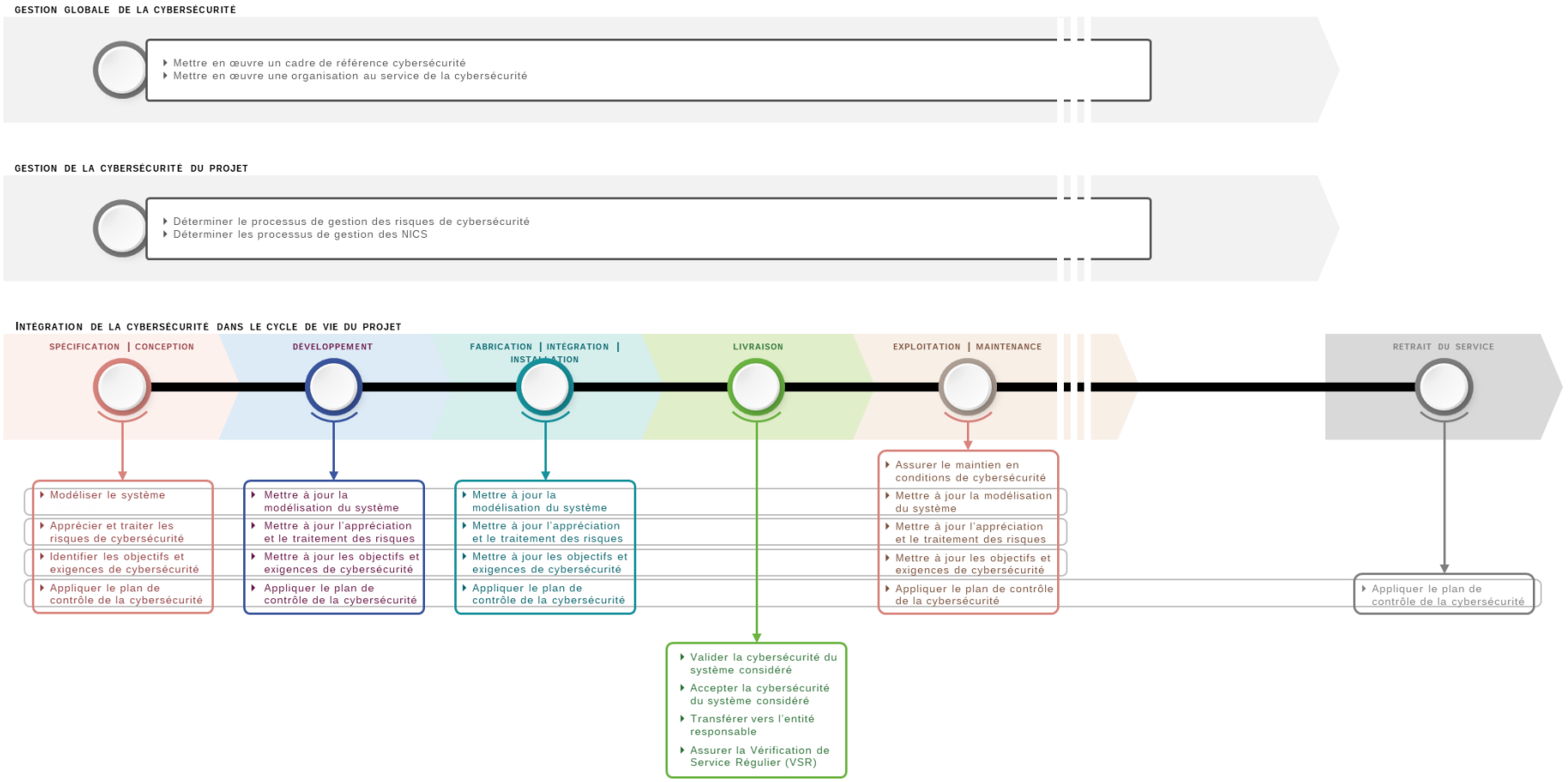


Figure 2 : Activités de cybersécurité intégrées au cycle de vie du système considéré

3 Exigences pour les activités de cybersécurité transverses et continues

La présente section décrit les exigences relatives aux activités de cybersécurité transverses et continues, applicables à l'entité responsable qui doivent être mises en œuvre sur le périmètre du système considéré. Certaines activités de cybersécurité peuvent par ailleurs être « non applicables » au regard de la nature du système considéré ; dans ce cas, le caractère « non applicable » de l'activité de cybersécurité doit être justifié.

3.1 Gestion globale de la cybersécurité

3.1.1 Objectifs

L'objectif de cette thématique est d'assurer le bon fonctionnement des processus-cadre de gestion de la cybersécurité au sein de l'entité responsable, en soutien des activités de cybersécurité réalisées en mode projet, quelle que soit la phase du cycle de vie du système considéré.

3.1.2 Activités de cybersécurité

[EX-0.01] Définir et mettre en œuvre un cadre de référence cybersécurité	
Un cadre de référence cybersécurité doit être élaboré et mis en œuvre afin d'assurer une gouvernance de la cybersécurité au sein de l'entité responsable.	
Entrées	**Sorties**
EX-0.10	*EX-0.09* | *EX-1.02* | *EX-1.03*| *EX-2.02* | *EX-3.02* *EX-5.02* | *EX-5.06* | *EX-5.07* | *EX-5.12*

Le cadre de référence cybersécurité intègre notamment :

- La documentation relative à la gouvernance de la cybersécurité (schéma directeur cybersécurité, politique générale ou thématique cybersécurité, etc.) ;
- La documentation opérationnelle de mise en œuvre de la cybersécurité (tous les documents d'application : politique locale cybersécurité, processus propres à la cybersécurité, etc.).

La documentation opérationnelle inclut notamment l'ensemble des processus-cadre de la cybersécurité, qui sont applicables et appliqués à toutes les différentes phases du cycle de vie, dont notamment :

- Le processus de gestion des risques de cybersécurité (cf. Annexe C) ;
- Le processus de gestion des incidents de cybersécurité ;
- Le processus de gestion des crises cybersécurité ;
- Le processus de gestion des vulnérabilités et correctifs.

La direction générale de l'entité responsable doit formellement attester de son appropriation du cadre de référence cybersécurité et du soutien à sa mise en application, via notamment une compréhension explicite des risques de cybersécurité et un engagement à gérer ces risques.

[EX-0.02] Définir et mettre en œuvre une organisation au service de la cybersécurité	
Une organisation au service de la gouvernance et de la mise en œuvre de la cybersécurité doit être définie et mise en œuvre au sein de l'entité responsable.	
Entrées	**Sorties**
	EX-5.01 | *EX-5.02* | *EX-5.06* | *EX-5.07*

L'organisation de la cybersécurité spécifie notamment :

- L'organisation et la composition de la filière hiérarchique cybersécurité, et, le cas échéant, d'une filière fonctionnelle cybersécurité adaptée à l'organisation de l'entité responsable ;
- La description des missions relatives à la cybersécurité de chacune des parties prenantes de ces filières, sous la forme de fiches de poste ou de fiches de mission ;
- La description (composition, fréquence et ordre du jour) des comités de cybersécurité nécessaires à la gouvernance et à la mise en œuvre de la cybersécurité.

La direction générale de l'entité responsable doit formellement valider la définition de ce schéma d'organisation et attester du soutien à sa mise en application, via notamment l'attribution explicite des postes définis dans la filière et un engagement à donner les moyens pour réaliser les missions.

[EX-0.03] Développer une culture de la cybersécurité à tous les niveaux	
Un plan de sensibilisation à la cybersécurité et un plan de gestion des compétences en matière de cybersécurité doit être élaboré et mis en œuvre afin de développer en continu une culture de la cybersécurité au sein de l'entité responsable.	
Entrées	**Sorties**
	EX-5.04

Le plan de sensibilisation à la cybersécurité concerne l'ensemble des personnels de l'entité responsable ; les thématiques et les moyens de sensibilisation peuvent varier en fonction des missions exercées mais doivent assurer :

- La compréhension du risque de cybersécurité (cf. Annexe C) ;
- La compréhension de leurs rôles et responsabilités en matière de cybersécurité ;
- La connaissance des règles d'hygiène et des bonnes pratiques en matière de cybersécurité.

Le plan de gestion des compétences en matière de cybersécurité concerne les personnels de l'entité responsable dont la mission nécessite des compétences dans le domaine (ex. : administrateur technique).

Les plans de sensibilisation et de gestion des compétences doivent prendre en compte, pour les personnels concernés, des enjeux propres et des spécificités (technologiques, règlementaires, etc.) des STRA.

[EX-0.04] Réaliser une veille continue et en exploiter les résultats	
Un processus de veille cybersécurité doit être élaboré et mis en œuvre, afin d'assurer une approche proactive de la cybersécurité au sein de l'entité responsable.	
Entrées	**Sorties**
sources internes ; sources ouvertes ; sources gouvernementales et organismes spécialisés	*EX-1.01* | *EX-1.02* | *EX-2.01* | *EX-3.01* *EX-5.08* | *EX-5.10* | *EX-5.11*

Le processus de veille précise l'organisation et les flux d'échange d'information mis en œuvre au sein de l'entité responsable. Le processus de veille doit spécifier :

- Les thématiques de veille, dont :
  - Une veille globale cybersécurité ;
  - Une veille sectorielle dans le domaine du transport ;
  - Une veille spécifique pour chaque type de sous-système ou composant.
- Les types de veille, dont une :
  - Veille juridique et réglementaire ;
  - Veille documentaires (normes, publications, etc.) ;
  - Veille événementielle (actualité cybersécurité, veille menace, etc.) ;
  - Veille outils ;
  - Veille vulnérabilités et correctifs.
- Les sources de veille (parties prenantes de l'écosystème, cf. Annexe B) :
  - Sources internes (direction juridique, direction technique, etc.) ;
  - Sources ouvertes (dont réseaux sociaux) ;
  - Autorités (dont ANSSI) ou organismes spécialisés (dont CERT) ;
  - Éditeurs / Mainteneurs de solutions matérielles ou logicielles.

Le processus de veille spécifie par ailleurs les actions à mener suite à une remontée d'information issue de la veille :

- Tri et priorisation des informations ;
- Remontée d'information ou remontée d'alerte si nécessaire.

Le processus de veille doit prendre en compte les enjeux propres et les spécificités (technologiques, règlementaire, etc.) des STRA.

[EX-0.05] Définir et mettre en œuvre un système de management de la cybersécurité	
Un système de management de la cybersécurité doit être élaboré et mis en œuvre afin d'assurer l'amélioration continue de la cybersécurité au sein de l'entité responsable.	
Entrées	**Sorties**
EX-0.01 | *EX-0.04*	*EX-0.06* | *EX-0.07* | *EX-0.08* | *EX-0.12* *EX-4.01* *EX-5.01* | *EX-5.05* | *EX-5.06* | *EX-5.07* *EX-6.01*

Le système de management de la cybersécurité doit être conforme aux normes internationales ou équivalent. Il s'appuie notamment sur :

- Un système de gestion documentaire ;

- Une mesure de l'efficacité de la cybersécurité, via :
    - Des indicateurs et tableaux de bord cybersécurité ;
    - Des informations issues du retour d'expérience sur la gestion des incidents ou presqu'incidents de cybersécurité ;
    - Des résultats d'audits cybersécurité ;
    - Des informations issues de la veille cybersécurité.
- Une comitologie de la cybersécurité assurant l'amélioration continue, via :
    - La prise en compte des retours des parties prenantes ;
    - La définition de plans d'action correctifs ;
    - La définition de plans d'action préventifs ;
    - La définition de plans d'action d'amélioration.

3.2 Gestion de la cybersécurité du projet

3.2.1 Objectifs

L'objectif de cette thématique est d'assurer la bonne intégration de la cybersécurité dans les processus de gestion du projet au sein de l'entité responsable, en soutien des activités de cybersécurité réalisées en mode projet, quelle que soit la phase du cycle de vie du système considéré.

3.2.2 Activités de cybersécurité

[EX-0.06] Etablir le plan qualité cybersécurité du projet	
Un plan qualité cybersécurité doit être élaboré et mis en œuvre afin d'assurer que les activités de cybersécurité à réaliser au titre du projet soient attribuées et intégrées au cycle de vie du projet.	
Entrées	**Sorties**
EX-0.05	*EX-0.07* | *EX-0.13* *EX4.01* | *EX-5.01*

Le plan qualité cybersécurité permet de maîtriser la mise en application des exigences du présent référentiel. Il spécifie notamment :

- Les documents ou éléments en entrée nécessaires à la réalisation de chaque activité de cybersécurité ;
- Les livrables ou éléments en sortie attendus de chaque activité de cybersécurité ;
- Les plans de contrôle réalisés en sortie de chaque activité de cybersécurité ;
- Les éléments de preuve de conformité aux exigences du présent référentiel ;
- Les ressources nécessaires pour la réalisation de chaque activité de cybersécurité ;
- La planification de chaque activité de cybersécurité ;
- Les rôles et responsabilités associées à chaque activité de cybersécurité du projet.

Le plan qualité cybersécurité spécifie la comitologie du projet, notamment la comitologie nécessaire pour la validation des objectifs de cybersécurité et l'acceptation des risques résiduels, à chaque phase du cycle de vie.

Le plan qualité cybersécurité est élaboré au début du projet et est mis à jour à chaque phase du cycle de vie du projet par l'entité responsable dépositaire des activités de cybersécurité de la phase concernée.

[EX-0.07] Etablir le plan de contrôle de la cybersécurité du projet	
Un plan de contrôle de la cybersécurité doit être élaboré afin d'assurer que les mesures de cybersécurité existantes ou implémentées à chaque phase du cycle de vie respectent leurs spécifications.	
Entrées	**Sorties**
EX-0.05 | *EX-0.06*	*EX-1.10* | *EX-2.09* | *EX-3.09* | *EX-6.01*

Le plan de contrôle de la cybersécurité permet d'assurer, à chaque phase du cycle de vie, que les mesures de cybersécurité mises en œuvre respectent leurs spécifications. Il inclut la vérification de l'application du plan qualité cybersécurité et les contrôles propres à chaque phase du cycle de vie.

Le plan de contrôle de la cybersécurité est élaboré au début du projet et est mis à jour à chaque phase du cycle de vie du projet par l'entité responsable dépositaire des activités de cybersécurité de la phase concernée.

[EX-0.08] Gérer la documentation du projet du point de vue de la cybersécurité	
La documentation du projet doit faire l'objet de mesures de protection nécessaires et suffisantes, en lien avec la sensibilité des informations dans les documents, pour toutes les phases du cycle de vie documentaire.	
Entrées	**Sorties**
EX-0.05 | *EX-0.06*	*Toute documentation*

La documentation propre au projet et la documentation utile au projet appartenant à des tiers doit faire l'objet des mesures de protection nécessaires, en lien avec la sensibilité des informations dans les documents :

- Mesures de classification de l'information et de marquage des documents ;
- Mesures de protection des données stockées ou archivées ;
- Mesures de protection des données lors du transfert de données.

La documentation propre au projet et la documentation utile au projet appartenant à des tiers doit être facilement disponible à toute partie prenante du projet ayant le besoin d'en connaître, selon des processus et des moyens d'échange d'informations définis dans le plan qualité cybersécurité.

[EX-0.09] Identifier les contraintes et les hypothèses du système considéré	
Toutes les contraintes et toutes les hypothèses ayant une incidence sur la gestion des risques de cybersécurité du système considéré doivent être identifiées et caractérisées.	
Entrées	**Sorties**
EX-0.01 | *EX-0.06*	*EX-1.01* | *EX-1.02* *EX-2.01* | *EX-3.01* | *EX-5.11*

Les contraintes qui pèsent sur le système considéré peuvent être de nature très diverses (réglementaires, organisationnelles, budgétaires, calendaires, techniques, etc.). Les contraintes à

prendre en compte pour le système considéré et pour l'ensemble des sous-systèmes et composants qui le composent intègrent notamment :

- Les contraintes qui pèsent sur l'entité responsable ;
- Les contraintes qui pèsent spécifiquement sur le système considéré.

Les hypothèses à prendre en compte pour le système considéré et pour l'ensemble des sous-systèmes et éléments qui le composent sont imposées par l'entité responsable. Les hypothèses peuvent aussi consister en un risque accepté a priori sur un environnement donné. Si des hypothèses portent sur une autre entité responsable ou une partie prenante, elles doivent être formalisées et transmises.

Certaines contraintes et hypothèses peuvent être héritées du domaine de conception fonctionnelle si le système considéré est le véhicule automatisé, du domaine de conception technique si le système considéré est le système technique, ou du domaine d'emploi si le système considéré est le STRA.

[EX-0.10] Etablir un processus de gestion des risques de cybersécurité pour le projet	
Un processus de gestion des risques de cybersécurité doit être élaboré et mis en œuvre, afin d'assurer que les risques de cybersécurité sont maîtrisés sur l'ensemble du cycle de vie du projet.	
Entrées	**Sorties**
Annexe C *EX-0.04*	*EX.0.11* *EX-1.03* | *EX-1.04* | *EX-2.02* | *EX-2.03* *EX-3.02* | *EX-3.03* | *EX-5.12* | *EX-5.13*

Le processus de gestion des risques doit notamment spécifier :

- Que l'appréciation des risques de cybersécurité est réalisée dès la phase de spécification / conception du projet et mise à jour à chaque phase du projet ;
- Que l'appréciation des risques est documentée et que l'ensemble des décisions sont formellement tracées ;
- Que les risques de cybersécurité identifiés lors de l'appréciation des risques de cybersécurité sont répertoriés, et que le répertoire ainsi constitué est mis à jour après chaque réévaluation de l'appréciation des risques ;
- Que les critères d'acceptation des risques sont définis ;
- Que les critères de réappréciation des risques incluent, sans s'y limiter, les conditions de déclenchement suivantes :
    - La modification du contexte des menaces ou d'une tendance émergente mise en exergue par les résultats de la veille
    - La connaissance d'une nouvelle vulnérabilité pouvant affecter un système en fonctionnement
- Que toute modification majeure du contexte qui surviendrait après la phase de spécification / conception est susceptible de nécessiter un retour sur cette phase
- Que la répétition des appréciations des risques produit des résultats cohérents, valides et comparables ;
- Que le résultat de l'appréciation des risques de cybersécurité doit être soumis à la personne responsable en charge de l'acceptation des risques, dans le cadre de la gouvernance cybersécurité mise en œuvre au titre du plan qualité cybersécurité, pour acceptation du plan de traitement des risques et des risques résiduels ;
- Que toutes les modifications résultant du traitement des risques sont documentées et tracées.

Le processus de gestion des risques doit être conforme aux principes décrits à l'Annexe C du présent document pour ce qui concerne l'identification, l'analyse, l'évaluation et le traitement des risques de cybersécurité.

[EX-0.11] Définir les Niveaux d'Intégrité Cybersécurité Système (NICS) pour le projet	
Un ensemble de NICS et d'exigences de NICS doit être défini pour assurer que les exigences applicables à la cybersécurité sont respectées, à chaque étape du cycle de vie du système considéré, proportionnellement aux risques de cybersécurité sur le système considéré.	
Entrées	**Sorties**
Annexe D *EX-0.05* | *EX-0.06* | *EX-0.10*	*EX-0.12* | *EX-0.13*

La définition des NICS et des exigences de NICS est réalisée selon les principes définis à l'annexe D du présent document. Elle comprend :

- La formulation d'une assertion de NICS, qui doit servir de base :
  - À l'établissement de la matrice de NICS ;
  - À l'association des exigences de NICS à chaque NICS ;

  et qui doit permettre d'en justifier la pertinence ;

- L'établissement de la matrice de NICS ;
- Les échelles d'exigences de NICS pour le projet, couvrant l'ensemble des exigences applicables du présent guide. Des exemples d'échelles d'exigences de NICS sont données à l'annexe K, à titre indicatif.

[EX-0.12] Etablir un processus de détermination et de réévaluation des NICS pour le projet	
Un processus de détermination et de réévaluation du [des] NICS doit être élaboré et mis en œuvre, afin d'assurer que le ou les NICS requis au niveau du système et, le cas échéant, de ses éléments, soit [soient] initialement déterminé[s] au début du projet et réévalué[s] à la suite de chaque itération de l'appréciation des risques.	
Entrées	**Sorties**
Annexe D *EX-0.06* | *EX.0.11*	

Le processus est élaboré selon les principes définis à l'annexe D du présent document. Le système considéré doit se voir attribuer un NICS. Des éléments du système considéré peuvent se voir allouer un NICS.

Le [les] NICS ainsi déterminé[s] est [sont] le[s] NICS requis. La détermination initiale du [des] NICS s'effectue à la suite de la première appréciation des risques sur le système considéré. Une réévaluation du [des] NICS doit être réalisée après chaque itération de l'appréciation des risques sur le système considéré.

[EX-0.13] Etablir un processus permettant de démontrer le respect des exigences de NICS	
Un processus permettant de démontrer le respect des exigences de NICS doit être élaboré et mis en œuvre, afin d'assurer que les exigences de NICS associées au NICS déterminé pour le système considéré et, le cas échéant, aux NICS alloués aux éléments du système considéré, sont satisfaites.	
Entrées	**Sorties**
Annexe D *EX-0.11*| *EX-0.13*	*EX-0.06*

Le processus est élaboré selon les principes définis à l'annexe D du présent document. Le processus définit les éléments de preuves objectives permettant de démontrer que les exigences de NICS sont respectées et que le (ou les) NICS requis sont ainsi atteints.

4 Exigences pour les activités de cybersécurité relatives au cycle de vie du système considéré

La présente section décrit les exigences relatives aux activités de cybersécurité intégrées au cycle de vie du système considéré. Chaque activité de cybersécurité est applicable à l'entité responsable. Certaines activités de cybersécurité peuvent être « non applicables » au regard de la nature du système considéré ; dans ce cas, le caractère « non applicable » de l'activité doit être justifié et tracé.

L'ordre des activités de cybersécurité présenté ne préjuge pas de l'ordre chronologique dans lequel elles sont effectuées. Certaines activités peuvent être réalisées en parallèle ou de manière itérative.

4.1 Phase de spécification / conception

4.1.1 Objectifs

La phase de spécification / conception du système considéré intègre les activités de modélisation du système et d'appréciation initiale des risques de cybersécurité. A l'issue de cette phase, les objectifs de cybersécurité et les mesures de cybersécurité applicables au système considérée sont spécifiés.

L'objectif en matière de cybersécurité de cette phase du cycle de vie est de spécifier les mesures de cybersécurité du système considéré, sur la base d'une appréciation des risques. Ces spécifications seront déclinées en propriétés, intrinsèques ou exportées, du système considéré dans les phases ultérieures. Elles pourront être affinées ou réévaluées lors des phases ultérieures.

4.1.2 Activités de cybersécurité

<table>
<tr><td colspan="2">[EX-1.01] Modéliser le système considéré et son écosystème</td></tr>
<tr><td colspan="2">Tous les sous-systèmes et éléments constituant le système considéré doivent être identifiés et caractérisés, l'ensemble constituant la modélisation du système considéré. Toutes les parties prenantes impliquées dans le système considéré doivent être identifiées et caractérisées, l'ensemble constituant l'écosystème du système considéré.</td></tr>
<tr><td>Entrées</td><td>Sorties</td></tr>
<tr><td>Annexe B
EX-0.04 | EX-0.06 | EX-0.09</td><td>EX-1.02 | EX-1.03 | EX-2.01</td></tr>
</table>

Le système considéré doit être modélisé selon les principes décrits à l'annexe B du présent document. Les composantes suivantes doivent notamment être caractérisées :

- Les missions du système considéré, qui portent les enjeux propres à la sécurité des usagers et des tiers ;
- Le contenu du système considéré et les éventuelles exceptions (ex. : un sous-système faisant l'objet d'une règlementation particulière) ;
- Les limites du système considéré et ses interfaces externes, en lien avec l'écosystème ;
- Les biens supports, incluant :
    - Sous-systèmes et composants du système considéré ;
    - Utilisateurs et communautés d'utilisateurs du système considéré ;
    - Interfaces internes du système considéré (interfaces entre un bien support et un autre) ;
    - Informations relatives à la nature de ces biens supports (bien physique, bien logiciel, etc.) ;
    - Informations relatives à la localisation de ces biens supports ;

- Données sensibles au sens de la sécurité.

A ce stade de la modélisation, les informations pertinentes sur l'environnement opérationnel (incluant les installations partagées – feux, par exemple – ou même de service partagé – communication 5G, localisation GPS, etc.) du système en matière de cybersécurité doivent être décrites et les relations entre les éléments doivent être explicitées.

L'écosystème du système considéré doit être modélisé selon les principes décrits à l'annexe B du présent document. Les composantes suivantes doivent être analysées :

- Les relations entre les différentes parties prenantes du système considéré ;
- Les interfaces entre les parties prenantes et le système considéré ;
- Les enjeux et préoccupations de cybersécurité des parties prenantes ;
- Les rôles et responsabilités en matière de cybersécurité des parties prenantes ;
- Les politiques de cybersécurité mises en œuvre par les parties prenantes concernant le système considéré.

[EX-1.02] Identifier l'existant à prendre en compte pour le système considéré	
Toutes les contributions existantes ayant une incidence sur la gestion des risques de cybersécurité du système considéré doivent être identifiées et caractérisées.	
Entrées	**Sorties**
EX-0.06 | *EX-0.09* | *EX-1.01*	*EX-1.03* | *EX-2.01*

L'existant à prendre en compte pour le système considéré et pour l'ensemble des sous-systèmes et éléments qui le composent intègrent notamment :

- Les références internes de l'entité responsable relatives à la cybersécurité à considérer :
  - Politique de cybersécurité ou assimilée ;
  - Documents d'applications (processus, procédures et modes opératoires, etc.).
- Les références externes relatives à la cybersécurité à appliquer :
  - Références légales et règlementaires ;
  - Références normatives ;
  - Références communautaires ;
  - Références sectorielles.
- Les retours d'expérience sur des STRA ou des systèmes similaires :
  - Les objectifs de cybersécurité ;
  - Les éléments d'entrée ;
  - Les exigences de NICS ;
  - Les indicateurs et de tableaux de bord ;
  - Les menaces et les sources de menaces considérées (cf. Annexe F).
- Les informations existantes concernant le système considéré :
  - Les activités de cybersécurité déjà réalisées ;
  - Les résultats d'audit cybersécurité déjà réalisés dans le cadre du projet ;
  - Les qualifications déjà obtenues (certification, homologation, etc.) pour un sous-système ou un élément du système considéré.

[EX-1.03] Réaliser l'appréciation des risques de cybersécurité du système considéré	
Une appréciation des risques de cybersécurité du système considéré doit être réalisée et documentée conformément au processus de gestion des risques.	
Entrées	**Sorties**
Annexe C, Annexe H *EX-0.06* | *EX-0.09* | *EX-0.10* | *EX-1.01* | *EX-1.02*	*EX-1.04* | *EX-2.02*

Le système considéré doit faire l'objet d'une appréciation des risques selon les principes décrits à l'Annexe C du présent document. Cette appréciation des risques doit être documentée de manière à pouvoir fournir des preuves claires et complètes des méthodologies, données, jugements et interprétations utilisées pour la réaliser, notamment pour que la répétition des appréciations des risques produise des résultats cohérents, valides et comparables.

En phase de spécification / conception, le système considéré n'est modélisable qu'à un niveau d'abstraction élevé. En conséquence, l'ensemble des vulnérabilités exploitables par les sources de menace n'est pas totalement identifiable. L'appréciation des risques mettra en évidence des scénarios de menace de haut niveau (cf. Annexe H) qui seront affinés dans les phases suivantes du cycle de vie du système considéré.

Dans le cas où on hérite d'une appréciation des risques réalisée par ailleurs pour un sous-système ou un élément du système considéré, il est attendu de vérifier que :

- Le contexte du système considéré est compatible avec l'appréciation des risques de cybersécurité ;
- L'objet de l'appréciation des risques de cybersécurité est adapté au contexte d'application spécifique prévu.

Les risques identifiés doivent être répertoriés, conformément au processus de gestion des risques.

[EX-1.04] Elaborer un plan de traitement des risques de cybersécurité du système considéré	
Un plan de traitement des risques de cybersécurité du système considéré doit être élaboré, afin d'amener les risques à un niveau acceptable selon des critères formellement définis, conformément au processus de gestion des risques.	
Entrées	**Sorties**
Annexe C *EX-0.06* | *EX-0.10* | *EX-1.03*	*EX-1.05* | *EX-2.03*

Le système considéré doit faire l'objet, pour chaque risque identifié, d'un plan de traitement des risques de cybersécurité selon les principes décrits à l'Annexe C du présent document.

Le plan de traitement des risques doit notamment formaliser les principes d'acceptation des risques de cybersécurité et les critères d'acceptation des risques de cybersécurité dérivés de ces principes.

[EX-1.05] Définir les objectifs de cybersécurité du système considéré	
Les objectifs de cybersécurité du système considéré permettant de réduire ou maintenir les risques de cybersécurité du système considéré à un niveau acceptable doivent être définis, en lien avec l'appréciation des risques.	
Entrées	**Sorties**
EX-0.06 | *EX-0.10* | *EX-1.04*	*EX-1.06* | *EX-2.04* | *EX-3-04*

Si la décision de traitement d'un risque de cybersécurité consiste à réduire ou maintenir le risque considéré, un ou plusieurs objectifs de cybersécurité correspondants doivent être spécifiés. De manière adaptée au système considéré les objectifs de cybersécurité visent :

- Dans le cas de la réduction d'un risque, à réduire le risque à un niveau acceptable ;
- Dans le cas du maintien d'un risque, à maintenir le risque à un niveau acceptable.

Les objectifs de sécurité visent à agir sur les variables constitutives du risque (vraisemblance et gravité, qui sont des variables composites dépendant elles-mêmes de variables intermédiaires : difficulté de l'attaque, attractivité de la cible, etc.). Les objectifs de cybersécurité peuvent concerner :

- Les éléments constitutifs du système considéré et de son écosystème (cf. Annexe B) et /ou les éléments constitutifs du risque (source de menace (cf. Annexe F), événements redoutés (cf. Annexe J), etc.) ;
- Tout ou partie des phases du cycle de vie, y compris les phases ultérieures à la phase pendant laquelle ils sont spécifiés ;
- Tout ou partie des aspects de l'implémentation des biens supports (cf. Annexe B) (conception technique, architecture technique, localisation physique ou géographique, nature des utilisateurs, etc.).

Les objectifs de cybersécurité du système considéré doivent être répertoriés en lien avec les risques qu'ils traitent, conformément au processus de gestion des risques.

[EX-1.06] Décliner les objectifs de cybersécurité du système considéré en exigences fonctionnelles de cybersécurité	
Les objectifs de cybersécurité du système considéré doivent être déclinés en exigences fonctionnelles de cybersécurité.	
Entrées	**Sorties**
EX-0.06 | *EX-1.05*	*EX-1.07* | *EX-2.04*

Les objectifs de cybersécurité déclinés en exigences fonctionnelles de cybersécurité constituent le concept de cybersécurité qui doit garantir :

- L'adéquation avec les objectifs de cybersécurité ;
- L'exhaustivité de la prise en compte des objectifs de cybersécurité ;
- La prise en compte des dépendances entre les exigences fonctionnelles de cybersécurité ;
- L'adéquation avec les hypothèses et les contraintes du système considéré.

Une attention particulière doit être portée à la spécification des exigences fonctionnelles de cybersécurité relatives au contrôle des interfaces dont la cybersécurité peut être compromise.

La description des exigences fonctionnelles de cybersécurité doit porter à la fois sur le comportement attendu en matière de cybersécurité du système considéré et sur les activités à engager pour obtenir le NICS approprié.

Le niveau de détail élémentaire de l'architecture fonctionnelle de cybersécurité correspond a minima à celui de la modélisation du système et de son écosystème (EX-1.01).

Les exigences fonctionnelles de cybersécurité peuvent être à prendre en compte par l'entité responsable du système considéré ou être exportées vers les différents acteurs de l'écosystème.

[EX-1.07] Spécifier l'architecture fonctionnelle de cybersécurité du système considéré	
L'attribution des exigences fonctionnelles de cybersécurité aux sous-systèmes, aux éléments du système considéré et à leurs interfaces, constituant l'architecture fonctionnelle de cybersécurité, doit être spécifiée.	
Entrées	**Sorties**
EX-0.06 | *EX-0.10* | *EX-1.06*	*EX-1.08* | *EX-2.05*

L'architecture fonctionnelle de cybersécurité doit être exprimée et structurée de façon claire, précise, univoque, vérifiable, évaluable, maintenable et réalisable et doit favoriser la compréhension par les parties prenantes susceptibles d'utiliser ces informations à l'une ou l'autre des phases du cycle de vie.

Chaque sous-système ou élément du système considéré appartenant à l'architecture fonctionnelle de cybersécurité doit satisfaire aux exigences suivantes :

- S'il n'est pas préexistant, sa spécification fonctionnelle doit satisfaire aux exigences fonctionnelles de cybersécurité du système considéré, en prenant en compte l'impact des vulnérabilités partagées et des chemins d'attaque multiples ;
- S'il est préexistant, les exigences d'intégration qui le concernent doivent être clairement identifiées et satisfaites.

Si de nouveaux risques de cybersécurité sont identifiés à partir de l'architecture fonctionnelle de cybersécurité, l'appréciation des risques de cybersécurité, le plan de traitement des risques de cybersécurité, les objectifs de cybersécurité et les exigences fonctionnelles de cybersécurité du système considéré doivent être mis à jour.

[EX-1.08] Spécifier les mesures de cybersécurité applicables au système considéré	
Les mesures de cybersécurité permettant de maintenir ou réduire les risques de cybersécurité du système considéré à un niveau acceptable, en lien avec les objectifs de cybersécurité, doivent être spécifiées.	
Entrées	**Sorties**
EX-0.06 | *EX-0.10* | *EX-1.07*	*EX-1.09* | *EX-2.06*

Les mesures de cybersécurité peuvent être intégrées aux spécifications du système considéré ou faire l'objet d'une spécification distincte.

Les mesures de cybersécurité peuvent être à appliquer par l'entité responsable du système considéré ou décrire des mesures exportées vers différents acteurs de l'écosystème.

Au même titre que les objectifs de cybersécurité, les mesures de cybersécurité peuvent concerner :

- Les éléments constitutifs du système considéré, de son écosystème, du risque ;
- Tout ou partie des phases du cycle de vie ;
- Tout ou partie des aspects de l'implémentation des biens supports.

Les mesures de cybersécurité peuvent être de nature technique, fonctionnelle, organisationnelle ou contextuelle ; elles peuvent traiter de différents aspects du système considéré :

- Les aspects de cybersécurité des fonctions du système ;
- Les aspects de cybersécurité des interfaces internes et externes ;
- Les aspects de cybersécurité de l'architecture ;
- Les aspects relatifs aux performances de cybersécurité ;
- Les aspects relatifs à l'exploitation et à la maintenance ;
- Les aspects relatifs aux usagers du système de transport et aux tiers ;
- La prise en compte des systèmes connexes qui fournissent des services de cybersécurité.

Une attention particulière doit être portée à la spécification des mesures de cybersécurité relatives au contrôle des interfaces dont la cybersécurité peut être compromise.

Les acteurs en charge de l'application des mesures de traitement du risque, quelle que soit la phase du cycle de vie considérée, doivent être formellement identifiés.

Dans le cas où on hérite d'une appréciation des risques réalisée par ailleurs pour un sous-système ou un élément du système considéré, il est attendu de vérifier que :

- Les exigences fonctionnelles de cybersécurité importées peuvent être respectées et déclinées en mesures de cybersécurité sur le système considéré ;
- La documentation disponible est suffisante pour soutenir les activités de cybersécurité. La documentation disponible doit notamment spécifier les hypothèses, les contraintes, les composantes du risque (en particulier les sources de risques).

[EX-1.09] Spécifier l'architecture technique de cybersécurité du système considéré	
L'architecture technique des éléments du système considéré liés aux mesures de cybersécurité, constituant l'architecture technique de cybersécurité, doit être spécifiée.	
Entrées	**Sorties**
EX-0.06 | *EX-1.08*	*EX-2.07*

L'architecture technique de cybersécurité doit être exprimée et structurée de façon claire, précise, univoque, vérifiable, évaluable, maintenable et réalisable et doit favoriser la compréhension par les parties prenantes susceptibles d'utiliser ces informations à l'une ou l'autre des phases du cycle de vie. Elle doit respecter les exigences suivantes :

- Les mesures de cybersécurité ne doivent pas pouvoir être contournées dans le fonctionnement nominal du système considéré (un élément ne peut pas utiliser un autre chemin de communication, y compris des mécanismes de niveau inférieur);
- Les mesures de cybersécurité doivent être inviolables dans le fonctionnement nominal du système considéré (le système contrôle les droits de modification des éléments liés aux mesures de cybersécurité, de la configuration et des données, pour empêcher les modifications non autorisées).

Le niveau de détail élémentaire utilisé pour l'architecture technique de cybersécurité correspond a minima à celui de la modélisation du système et de son écosystème (EX-1.01).

Chaque sous-système ou élément du système considéré appartenant à l'architecture technique de cybersécurité doit satisfaire aux exigences suivantes :

- S'il n'est pas préexistant, sa spécification technique doit prendre en compte les spécifications des mesures auxquelles il est lié, en tenant compte de l'impact des vulnérabilités partagées et des chemins d'attaque multiples.
- S'il est préexistant, les exigences d'intégration qui le concernent doivent être clairement identifiées et satisfaites

Si de nouveaux risques de cybersécurité sont identifiés à partir de l'architecture technique de cybersécurité, l'appréciation des risques de cybersécurité le plan de traitement des risques de cybersécurité, les objectifs de cybersécurité, les exigences fonctionnelles de cybersécurité et les mesures de cybersécurité du système considéré doivent être mis à jour.

[EX-1.10] Appliquer le plan de contrôle de la cybersécurité du système considéré	
Le plan de contrôle de la cybersécurité du système considéré doit être mis en œuvre en phase de spécification / conception afin de livrer un système conformément aux spécifications et conforme au plan qualité cybersécurité.	
Entrées	**Sorties**
EX-0.06 | *EX-0.07*	*EX-2.09*

Le contrôle de la cybersécurité en phase de spécification / conception consiste à vérifier que les mesures respectent leurs spécifications, et doit notamment inclure la vérification de l'application du plan qualité cybersécurité (cf. EX-0.06).

4.2 Phase de développement

4.2.1 Objectifs

La phase de développement du système considéré intègre de manière indifférenciée les aspects de développement de l'architecture des systèmes d'information, de composants matériels ou de composants logiciels du système considéré.

L'objectif en matière de cybersécurité de cette phase du cycle de vie est de mettre en œuvre les mesures de cybersécurité exprimées en phase de spécification / conception dans le cadre de ces développements. Les spécifications de cybersécurité deviennent, au titre de la phase de développement, des propriétés spécifiques, intrinsèques ou exportées, du système considéré.

4.2.2 Activités de cybersécurité

[EX-2.01] Mettre à jour la modélisation du système considéré et de son écosystème	
La modélisation du système et de son écosystème doit être mise à jour en prenant en compte les nouvelles données en entrée induites par la réalisation de la phase de développement.	
Entrées	**Sorties**
Annexe B *EX-0.04* | *EX-0.06* | *EX-0.09* | *EX-1.01* | *EX-1.03*	*EX-2.02* | *EX-3.01*

La phase de développement peut permettre de disposer de nouvelles données d'entrée permettant d'effectuer une itération de la modélisation du système considéré et de son écosystème, selon les principes décrits à l'Annexe B du présent document, en identifiant notamment :

- De nouveaux biens supports, incluant les :
  - Éléments du système considéré ;
  - Utilisateurs et communautés d'utilisateurs du système considéré ;
- De nouvelles interfaces et dépendances du système considéré :
  - Interfaces et dépendances internes du système considéré (entre les éléments du système considéré) ;
  - Interfaces externes du système considéré (écosystème, environnement) ;
- De nouvelles parties prenantes impliquées dans le système considéré ;
- D'éventuels choix d'implémentation technique non identifiés à la phase précédente ;
- De nouvelles informations issues de l'architecture fonctionnelle de cybersécurité du système considéré ;
- etc.

[EX-2.02] Mettre à jour l'appréciation des risques de cybersécurité du système considéré	
L'appréciation des risques de cybersécurité du système considéré doit être mise à jour en prenant en compte les évolutions du système considéré et les contraintes et hypothèses spécifiques de la phase de développement, conformément au processus de gestion des risques.	
Entrées	**Sorties**
Annexe C | *Annexe H* *EX-0.06* | *EX-0.09* | *EX-0.10* *EX-1.02* | *EX-1.03* | *EX-2.01*	*EX-2.03* | *EX-3.02*

La phase de développement peut permettre de disposer de nouvelles données d'entrée qui caractérisent mieux les risques de cybersécurité, notamment sur les aspects suivants :

- Via l'analyse des choix technologiques effectués pour le développement du système considéré ou de ses interfaces ;
- Via l'analyse de l'évolution du contexte (ex. : activité accrue d'une source de menace, découverte d'une vulnérabilité majeure, etc.) ;
- Via le raffinement des chemins d'attaque suite à la mise en œuvre technique de la phase de développement (ex. : choix technologiques, vulnérabilité par conception, etc.).

Ces données d'entrée s'inscrivent dans la méthodologie d'appréciation des risques dont les principes sont décrits à l'Annexe C du présent document.

Le répertoire des risques de cybersécurité doit être mis à jour.

[EX-2.03] Mettre à jour le plan de traitement des risques de cybersécurité du système considéré	
Le plan de traitement des risques de cybersécurité du système considéré doit être mis à jour en prenant en compte les évolutions de l'appréciation des risques de cybersécurité en phase de développement, conformément au processus de gestion des risques.	
Entrées	**Sorties**
Annexe C *EX-0.06* | *EX-0.10* | *EX-1.04* | *EX-2.02*	*EX-2.04* | *EX-3.03*

L'appréciation des risques en phase de développement doit permettre de mettre à jour, pour chaque risque nouveau ou modifié (EX-2.02), le plan de traitement des risques de cybersécurité selon les principes décrits à l'Annexe C du présent document.

[EX-2.04] Mettre à jour les exigences fonctionnelles de cybersécurité du système considéré	
Les exigences fonctionnelles de cybersécurité du système considéré doivent être mises à jour et affinées relativement aux objectifs de cybersécurité en prenant en compte les évolutions du plan de traitement des risques en phase de développement.	
Entrées	**Sorties**
EX-0.06 | *EX-1.05* | *EX-1.06* | *EX-2.03*	*EX-2.05* | *EX-2.06* | *EX-3.04*

Les exigences fonctionnelles de cybersécurité ainsi mises à jour font évoluer le concept de cybersécurité qui doit garantir :

- L'adéquation avec les objectifs de cybersécurité ;
- L'exhaustivité de la prise en compte des objectifs de cybersécurité ;
- L'adéquation avec les hypothèses et les contraintes du système considéré.

[EX-2.05] Mettre à jour l'architecture fonctionnelle de cybersécurité du système considéré	
L'architecture fonctionnelle de cybersécurité du système considéré être mise à jour en prenant en compte les évolutions des exigences fonctionnelles de cybersécurité en phase de développement.	
Entrées	**Sorties**
EX-0.06 | *EX-0.10* | *EX-1.07* | *EX-2.05*	*EX-2.07* | *EX-3.05*

Si de nouveaux risques de cybersécurité sont identifiés à partir de l'architecture fonctionnelle de cybersécurité, l'appréciation des risques de cybersécurité, le plan de traitement des risques de cybersécurité, les objectifs de cybersécurité et les exigences fonctionnelles de cybersécurité du système considéré doivent être mis à jour.

[EX-2.06] Mettre à jour les mesures de cybersécurité applicables au système considéré	
Les mesures de cybersécurité applicables au système considéré issues de l'appréciation des risques doivent être mises à jour en prenant en compte les évolutions de l'appréciation des risques de cybersécurité en phase de développement.	
Entrées	**Sorties**
EX-0.06 | *EX-0.10* | *EX-1.08* | *EX-2.04*	*EX-2.07* | *EX-3.05*

Les mesures de cybersécurité et l'architecture technique de cybersécurité doivent être mises à jour en prenant en compte notamment :

- Les mesures de cybersécurité issues de la phase précédente du cycle de vie ;
- Les mesures de cybersécurité issues des dossiers règlementaires déjà réalisés ;
- Les mesures de cybersécurité importées du fait des interfaces avec de nouveaux systèmes ;
- La maintenabilité des mesures de cybersécurité implémentées en phase de développement ;
- Les contraintes pesant sur l'architecture technique qui limitent les fonctions de cybersécurité ;
- Les contraintes pesant sur le développement qui limitent les fonctions de cybersécurité ;
- Les opportunités offertes par le développement qui proposent des fonctions de cybersécurité ;
- Les opportunités offertes par l'architecture qui proposent des fonctions de cybersécurité.

Les acteurs en charge de l'application des mesures de traitement du risque, quelle que soit la phase du cycle de vie considérée, doivent être formellement identifiés.

Les mesures de cybersécurité mises à jour en phase de développement peuvent aussi concerner les mesures de cybersécurité applicables à la phase d'exploitation / maintenance.

[EX-2.07] Mettre à jour l'architecture technique de cybersécurité du système considéré	
L'architecture technique de cybersécurité du système considéré être mise à jour en prenant en compte les évolutions de l'appréciation des risques de cybersécurité en phase de développement.	
Entrées	**Sorties**
EX-0.06 | *EX-0.10* | *EX-1.09* | *EX-2.05*	*EX-2.08* | *EX-3.05*

Pour chaque mesure de cybersécurité, une description de l'architecture technique de cybersécurité doit être fournie. Son niveau de détail doit correspondre à celui de l'exigence (des exigences) fonctionnelle(s) de cybersécurité à laquelle (auxquelles) cette mesure répond. Cette description doit démontrer comment la mesure met en œuvre les stratégies décrites en phase de spécification/conception.

Si de nouveaux risques de cybersécurité sont identifiés à partir de l'architecture technique de cybersécurité, l'appréciation des risques de cybersécurité le plan de traitement des risques de cybersécurité, les objectifs de cybersécurité, les exigences fonctionnelles de cybersécurité et les mesures de cybersécurité du système considéré doivent être mis à jour.

[EX-2.08] Mener à bien le développement du système considéré conformément aux spécifications de cybersécurité	
Le développement du système considéré doit mettre en œuvre les spécifications de cybersécurité applicables à la phase de développement.	
Entrées	**Sorties**
EX-0.06 | *EX-2.07*	*EX-3.01*

Les mesures de cybersécurité applicables à la phase de développement sont appliquées aux éléments du système considéré et en deviennent des propriétés spécifiques.

[EX-2.09] Appliquer le plan de contrôle de la cybersécurité du système considéré	
Le plan de contrôle de la cybersécurité du système considéré doit être mis en œuvre en phase de développement afin de livrer un système conformément aux spécifications et conforme au plan qualité cybersécurité.	
Entrées	**Sorties**
EX-0.06 | *EX-0.07*	*EX-3.09*

Le contrôle de la cybersécurité en phase de développement consiste à vérifier que les mesures respectent leurs spécifications, et doit notamment inclure :

- La vérification de l'application du plan qualité cybersécurité (cf. Ex-0.06) ;
- La vérification de l'absence de failles de cybersécurité dans les développements réalisés ;
- La vérification de l'absence de fonctionnalités non attendues au sein du système considéré.

4.3 Phase de fabrication / intégration / installation

4.3.1 Objectifs

La phase de fabrication / installation / intégration du système considéré intègre de manière indifférenciée les aspects de fabrication, de configuration, d'assemblage, d'intégration ou d'installation du système considéré, incluant l'architecture du système d'information en soutien du système considéré.

L'objectif en matière de cybersécurité de cette phase du cycle de vie est de mettre en œuvre les spécifications de cybersécurité exprimées aux phases précédentes dans le cadre de la fabrication / intégration / installation du système considéré. Les spécifications de cybersécurité deviennent, au titre de la phase de fabrication / intégration / installation, des propriétés spécifiques, intrinsèques ou exportées, du système considéré.

4.3.2 Activités de cybersécurité

<table>
<tr><th colspan="2">[EX-3.01] Mettre à jour la modélisation du système considéré et de son écosystème</th></tr>
<tr><td colspan="2">La modélisation du système considéré et de son écosystème doit être mise à jour en prenant en compte les nouvelles données en entrée induites par la réalisation de la phase de fabrication / intégration / installation.</td></tr>
<tr><th>Entrées</th><th>Sorties</th></tr>
<tr><td>Annexe B
EX-0.06 | EX-0.09 | EX-2.01| EX-2.02 | EX-2.07 | EX-2.08</td><td>EX-3.02 | EX-5.11</td></tr>
</table>

La phase de fabrication / intégration / installation peut permettre de disposer de nouvelles données d'entrée permettant d'effectuer une itération de la modélisation du système considéré et de son écosystème, selon les principes décrits à l'Annexe B du présent document, en identifiant notamment :

- De nouveaux biens supports spécifiques à la phase de fabrication/ intégration/ installation, incluant les :
    - Eléments du système considéré
    - Utilisateurs et communautés d'utilisateurs du système considéré
- De nouvelles interfaces et dépendances du système considéré :
    - Interfaces et dépendances internes du système considéré (entre les éléments du système considéré)
    - Interfaces externes du système considéré (écosystème, environnement)
- De nouvelles parties prenantes impliquées dans le système considéré ;
- D'éventuels choix d'implémentation technique non identifiés à la phase précédente ;
- Etc.

[EX-3.02] Mettre à jour l'appréciation des risques de cybersécurité du système considéré	
L'appréciation des risques de cybersécurité du système considéré doit être mise à jour en prenant en compte les évolutions du système considéré et les contraintes et hypothèses spécifiques de la phase de fabrication / intégration / installation, conformément au processus de gestion des risques.	
Entrées	**Sorties**
Annexe C | *Annexe H* *EX-0.06* | *EX-0.09* | *EX-0.10* | *EX-1.02* | *EX-3.01*	*EX-3.03* | *EX-5.12*

La phase de fabrication / intégration / installation peut permettre de disposer de nouvelles données d'entrée pouvant aider à mieux caractériser les risques de cybersécurité, notamment sur les aspects suivants :

- Via l'analyse de l'évolution du contexte (ex. : activité accrue d'une source de menace, découverte d'une vulnérabilité majeure, etc.) ;
- Via le raffinement des chemins d'attaque suite à la mise en œuvre technique de la phase de fabrication (ex. : exposition particulière au risque, vulnérabilité par conception, etc.).

Ces données d'entrée s'inscrivent dans la méthodologie d'appréciation des risques dont les principes sont décrits à l'Annexe C du présent document.

Le répertoire des risques de cybersécurité doit être mis à jour.

[EX-3.03] Mettre à jour le plan de traitement des risques de cybersécurité du système considéré	
Le plan de traitement des risques de cybersécurité du système considéré doit être mis à jour en prenant en compte les évolutions de l'appréciation des risques de cybersécurité en phase de fabrication / intégration / installation, conformément au processus de gestion des risques.	
Entrées	**Sorties**
Annexe C *EX-0.06* | *EX-0.10* | *EX-2.03* | *EX-3.02*	*EX-3.04* | *EX-15.13*

L'appréciation des risques en phase de fabrication / intégration / installation doit permettre de mettre à jour, pour chaque risque nouveau ou modifié, le plan de traitement des risques de cybersécurité selon les principes décrits à l'Annexe C du présent document.

[EX-3.04] Mettre à jour les exigences fonctionnelles de cybersécurité du système considéré	
Les exigences fonctionnelles de cybersécurité du système considéré doivent être mise à jour relativement aux objectifs de cybersécurité en prenant en compte les évolutions du plan de traitement des risques en phase de fabrication / intégration / installation.	
Entrées	**Sorties**
EX-0.06 | *EX-1.05* | *EX-2.04* | *EX-3.03*	*EX-3.05* | *EX-15.15*

Les exigences fonctionnelles de cybersécurité ainsi mises à jour font évoluer le concept de cybersécurité qui doit garantir :

- L'adéquation avec les objectifs de cybersécurité ;
- L'exhaustivité de la prise en compte des objectifs de cybersécurité ;
- L'adéquation avec les hypothèses et les contraintes du système considéré.

[EX-3.05] Mettre à jour l'architecture fonctionnelle de cybersécurité du système considéré	
L'architecture fonctionnelle de cybersécurité du système considéré doit être mise à jour en prenant en compte les évolutions des exigences fonctionnelles de cybersécurité en phase de fabrication / intégration / installation.	
Entrées	**Sorties**
EX-0.06 | *EX-0.10* *EX-2.05* | *EX-3.04*	*EX-3.06*

Si de nouveaux risques de cybersécurité sont identifiés à partir de l'architecture fonctionnelle de cybersécurité, l'appréciation des risques de cybersécurité, le plan de traitement des risques de cybersécurité, les objectifs de cybersécurité et les exigences fonctionnelles de cybersécurité du système considéré doivent être mis à jour.

[EX-3.06] Mettre à jour les mesures de cybersécurité applicables au système considéré	
Les mesures de cybersécurité applicables au système considéré issues de l'appréciation des risques doivent être mises à jour en prenant en compte les évolutions de l'appréciation des risques de cybersécurité en phase de fabrication / intégration / installation.	
Entrées	**Sorties**
EX-0.06 | *EX-0.10* *EX-2.05* | *EX-3.04*	*EX-3.07* | *EX-15.16*

Les mesures de cybersécurité et l'architecture technique de cybersécurité doivent être mises à jour en prenant en compte notamment :

- Les mesures de cybersécurité issues de la phase précédente du cycle de vie ;
- Les mesures de cybersécurité issues des dossiers règlementaires déjà réalisés ;
- Les mesures de cybersécurité importées du fait des interfaces avec de nouveaux systèmes ;
- La maintenabilité des mesures de cybersécurité implémentées en phase de fabrication / intégration / installation ;
- Les contraintes pesant sur l'architecture technique qui limitent les fonctions de cybersécurité ;
- Les contraintes pesant sur la fabrication / intégration / installation qui limitent les fonctions de cybersécurité ;
- Les opportunités offertes par la fabrication / intégration / installation qui proposent des fonctions de cybersécurité ;
- Les contraintes issues de l'environnement opérationnel, dont :
    - L'environnement physique ou géographique des environnements opérationnels ;
    - Les parties prenantes des environnements opérationnels.

Les acteurs en charge de l'application des mesures de traitement du risque, quelle que soit la phase du cycle de vie considérée, doivent être formellement identifiés.

Les mesures de cybersécurité mises à jour en phase de fabrication / intégration / installation peuvent aussi concerner les mesures de cybersécurité applicables à la phase d'exploitation / maintenance.

[EX-3.07] Mettre à jour l'architecture technique de cybersécurité du système considéré	
L'architecture technique de cybersécurité du système considéré doit être mise à jour en prenant en compte les évolutions de l'appréciation des risques de cybersécurité en phase de fabrication / intégration / installation.	
Entrées	**Sorties**
EX-0.06 | *EX-0.10* | *EX-2.07* | *EX-3.06*	*EX-3.08* | *EX-15.18*

Si de nouveaux risques de cybersécurité sont identifiés à partir de l'architecture technique de cybersécurité, l'appréciation des risques de cybersécurité le plan de traitement des risques de cybersécurité, les objectifs de cybersécurité, les exigences fonctionnelles de cybersécurité et les mesures de cybersécurité du système considéré doivent être mis à jour.

[EX-3.08] Mener à bien la phase de fabrication / intégration / installation conformément aux spécifications de cybersécurité	
La fabrication, l'intégration et l'installation du système considéré doivent mettre en œuvre les spécifications de cybersécurité applicables à la phase de fabrication / intégration / installation.	
Entrées	**Sorties**
EX-0.06 | *EX-3.06*	*EX-4.01*

Les mesures de cybersécurité applicables à la phase de fabrication / intégration / installation sont appliquées aux éléments et aux sous-systèmes du système considéré et en deviennent des propriétés spécifiques.

[EX-3.09] Appliquer le plan de contrôle de la cybersécurité du système considéré	
Le plan de contrôle de la cybersécurité du système considéré doit être mis en œuvre en phase de fabrication, intégration, installation afin de livrer un système conformément aux spécifications et conforme au plan qualité cybersécurité.	
Entrées	**Sorties**
EX-0.06 | *EX-0.07* | *EX-2.09*	*EX-4.01*

Le contrôle de la cybersécurité en phase de fabrication / intégration / installation consiste à vérifier que les mesures de cybersécurité respectent leurs spécifications et doit notamment inclure :

- La vérification de l'application du plan qualité cybersécurité (cf. EX-0.06) ;
- La vérification du fonctionnement sécurisé des fonctions embarquées dans les éléments du système considéré ;
- La vérification du comportement des éléments du système considéré en matière de cybersécurité ;
- La vérification du fonctionnement en matière de cybersécurité des interfaces et des interactions entre les éléments du système considéré ;
- La vérification du fonctionnement des systèmes considérés supportant des services de cybersécurité ;
- La vérification du comportement du système considéré en matière de cybersécurité et les interactions entre le système considéré et l'environnement.

4.4 Phase de livraison

4.4.1 Objectifs

La phase de livraison du système considéré intègre les activités de validation, d'acceptation et de transfert vers l'entité responsable du système considéré. En particulier, lors de cette phase, l'acceptation du système considérée est formellement prononcée.

Les objectifs en matière de cybersécurité de cette phase du cycle de vie sont les suivants :

- Au titre de la validation du système considéré, fournir des preuves objectives que le système considéré répond aux exigences fonctionnelles de cybersécurité et implémente les mesures spécifiées en matière de cybersécurité, et que la gestion de la cybersécurité respecte le plan qualité de cybersécurité ;
- Au titre de l'acceptation du système considéré, valider formellement que le système considéré remplit les objectifs de cybersécurité dans son environnement opérationnel ;
- Au titre de la livraison du système considéré, assurer la capacité du système considéré à maintenir les risques de cybersécurité à un niveau acceptable.

4.4.2 Activités de cybersécurité

<table>
<tr><td colspan="2">[EX-4.01] Valider la cybersécurité du système considéré</td></tr>
<tr><td colspan="2">Un plan de validation de la cybersécurité du système considéré intégrant les méthodes et techniques appropriées doit être élaboré et mis en œuvre, afin d'assurer que les mesures de cybersécurité sont bien mises en œuvre et répondent aux objectifs de cybersécurité.</td></tr>
<tr><td>Entrées</td><td>Sorties</td></tr>
<tr><td>Résultats des tests des phases précédentes
EX-0.06 | EX-0.13 | EX-4.01</td><td>EX-4.02</td></tr>
</table>

Le plan de validation est mis en œuvre à la fin des activités d'intégration / installation et avant l'acceptation du système. Il intègre notamment :

- La nature des méthodes et techniques utilisées parmi :
    - Des actions de recette cybersécurité ;
    - Des audits techniques (audit d'architecture, audit de configuration, audit de code, etc.) ;
    - Des audits organisationnels (audit physique, audit de processus, etc.) ;
    - Des tests d'intrusion (les tests d'intrusion constituent la base d'une évaluation de robustesse en matière de cybersécurité) ;
    - Des tests « *red team* » ;
    - Des tests de sécurité du personnel.
- La profondeur des méthodes et techniques utilisées :
    - Audits documentaires ;
    - Audits déclaratifs ;
    - Constats terrain et tests techniques.
- La qualification des intervenants en charge de la réalisation des actions de validation :
    - Leur indépendance vis-à-vis des parties prenantes du système considéré ;
    - Leurs compétences sur les méthodes et techniques utilisées ;
    - Leurs compétences en matière de cybersécurité technique et organisationnelle ;
    - Leur déontologie professionnelle.
- La planification des tâches de validation.

Il est par ailleurs nécessaire de prendre des mesures de protection suffisantes pour éviter d'éventuelles compromissions durant les tests réalisés au titre du plan de validation.

[EX-4.02] Accepter le système considéré sur le domaine cybersécurité	
L'acceptation du système considéré sur le domaine cybersécurité doit être formellement prononcée, en acceptant en connaissance de cause les risques de cybersécurité résiduels, en lien avec l'appréciation des risques et les actions de validations réalisées.	
Entrées	**Sorties**
EX-0.06 | *EX-0.10* | *EX-3.02* | *EX-4.01*	*EX-4.03* | *EX-4.04*

L'acceptation du système considéré sur le domaine cybersécurité fait l'objet d'une décision formelle dans un comité ad hoc qui induit :

- La définition formelle de critères d'acceptation, intégrant le niveau de risque acceptable ;
- La désignation formelle de la personne responsable en charge de l'acceptation ;
- La définition formelle d'une comitologie en charge de l'acceptation.

Cette comitologie est définie dans le plan qualité de cybersécurité.

L'acceptation du système considéré sur le domaine cybersécurité est réalisée sur la base d'éléments de preuve tangibles, dont la traçabilité doit être maintenue.

L'acceptation du système considéré peut faire état d'une dette de cybersécurité (actions contribuant à la maîtrise des risques sur le système considéré non encore réalisées, incluant les actions identifiées issues du plan de validation). Cette dette de cybersécurité doit :

- Être formalisée, en incluant la date de clôture des actions ;
- Être acceptée au titre de l'acceptation du système considéré.

[EX-4.03] Intégrer la cybersécurité dans les actions de transfert vers l'entité responsable	
Un plan de livraison de la cybersécurité du système considéré doit être élaboré et mis en œuvre, afin d'assurer que le niveau des risques pesant sur le système considéré est à un niveau acceptable lors du transfert vers l'exploitation / maintenance.	
Entrées	**Sorties**
Projet de SGS *EX-0.06* | *EX-4.02*	*Si système considéré = STRA : SGS mis à jour (exploitant, en tant qu'entité responsable)* *Si système considéré = ST : processus de livraison, manuel utilisateur etc. (à définir) à l'OS (en tant qu'entité responsable)* *EX-4.04* | *EX-5.01*

Le plan de livraison du système considéré doit intégrer les actions relatives à la cybersécurité à réaliser dans le cadre du transfert vers l'entité responsable, intégrant :

- Le détail des plans d'actions relatifs au traitement de la dette de cybersécurité issue de la phase de validation du système considéré ;
- La livraison de la documentation relative à la cybersécurité du système concerné (processus, procédures, modes opératoires, guides) ;
- La formation des intervenants de la phase d'exploitation / maintenance aux actions de cybersécurité propres au système considéré.

[EX-4.04] Intégrer la cybersécurité dans la période de Vérification de Service Régulier	
La période de Vérification de Service Régulier (VSR) doit permettre de constater que les moyens mis en œuvre au titre de la cybersécurité permettent de maintenir les risques de cybersécurité à un niveau acceptable.	
Entrées	**Sorties**
EX-0.06 | *EX-4.02* | *EX-4.03*	*EX-5.01* | *EX-5.02* | *EX-5.03*

Les moyens mis en œuvre au titre de la période de Vérification de Service Régulier doivent être formalisés et doivent notamment intégrer :

- Des dispositions particulières de surveillance des performances de cybersécurité ;
- Une implication des parties prenantes des phases précédentes ;
- Une capacité à faire appel à des compétences particulières ;
- La mise en place d'une organisation spécifique.

Les exigences de la phase d'exploitation / maintenance (cf. section 4.5) doivent être mises en œuvre.

4.5 Phase d'exploitation / maintenance

4.5.1 Objectifs

L'objectif de cette phase du cycle de vie est d'exploiter et de maintenir le système considéré de façon à assurer que le niveau des risques pesant sur le système considéré est maintenu à un niveau acceptable après sa mise en service.

Les exigences applicables lors de cette phase devront être traduites dans les procédures d'exploitation / maintenance du système considéré et apparaître, à ce titre, dans le ou les dossiers réglementaire(s) fourni(s) à l'appui du système considéré, et élaboré(s) avant la mise en service.

4.5.2 Activités de cybersécurité

[EX-5.01] Etablir le plan de maintien en conditions de cybersécurité du système considéré	
Un plan de maintien en conditions de cybersécurité du système considéré intégrant l'ensemble des processus attendus pour maintenir le niveau des risques pesant sur le système considéré à un niveau acceptable doit être élaboré et mis en œuvre.	
Entrées	**Sorties**
EX-0.01 | *EX-0.04* | *EX-0.05* | *EX-0.06* | *EX-0.08* *EX-4.03* | *EX-4.04*	*EX-5.02* | *EX-5.03*

Le plan de maintien en conditions de cybersécurité du système intègre notamment :

- Les attendus en termes de compétences cybersécurité en phase d'exploitation maintenance ;
- Le processus et les moyens de surveillance des performances de cybersécurité ;
- Le processus et les moyens de veille sur les évolutions du système et de son environnement ;
- Le processus et les moyens de veille sur les vulnérabilités et les correctifs ;
- Le processus et les moyens de mise à jour ;
- Le processus et les moyens de gestion des incidents de cybersécurité ;
- Le processus et les moyens de réponse aux incidents de cybersécurité ;
- Le processus et les moyens de gestion de crise cybersécurité.

[EX-5.02] Réaliser les opérations courantes concourant à la cybersécurité du système considéré	
Les opérations courantes concourant à la cybersécurité du système considéré doivent être documentées et réalisées en continu.	
Entrées	**Sorties**
EX-0.06 | *EX-5.01* | *EX-5.04* | *EX-5.05* | *EX-5.06* *EX-5.07* | *EX-5.08* | *EX-5.09*	*EX-5.03*

Les opérations courantes concourant à la cybersécurité du système intègrent notamment :

- Les activités opérationnelles en tant que telles, notamment pour la prise en compte des erreurs (cas de vulnérabilités liées à une mauvaise configuration) ;
- Les mises à jour des signatures de l'ensemble des moyens de détection (antivirus, détection d'intrusion, etc.) ;

- Les activités de gestion des configurations, afin de maintenir une base de configuration complète et à jour ;
- Les activités de réalisation et de gestion des sauvegardes et les activités de test et de gestion des restaurations ;
- Les activités de gestion dans le temps des habilitations d'accès, prenant en compte notamment les mouvements de personnel.

[EX-5.03] S'assurer que les risques pesant sur le système considéré sont maintenus à un niveau acceptable lors des opérations de maintenance et à la suite de celles-ci	
Les opérations de maintenance ne doivent pas augmenter le niveau des risques de cybersécurité pesant sur le système considéré ou exposer le système considéré à de nouveaux risques de cybersécurité.	
Entrées	**Sorties**
EX-0.05 | *EX-0.06* | *EX-5.01* | *EX-5.02* | *EX-5.05* | *EX-5.08*	

L'ensemble des aspects relatifs à la cybersécurité des opérations de maintenance doit être pris en compte, notamment :

- Assurer l'authenticité et l'intégrité des mises à jour ;
- Assurer la confiance dans les personnels intervenants en maintenance ;
- Assurer une exposition maîtrisée en cas de maintenance connectée.

Par ailleurs, la maintenance d'une fonction de cybersécurité ne doit pas dégrader les performances du fonctionnement du système (ex. : fonction de filtrage sur un équipement temps réel).

[EX-5.04] Assurer la compétence en matière de cybersécurité des personnels intervenants sur le système considéré	
Les personnels intervenants sur le système considéré doivent être formés et sensibilisés de manière continue en matière de cybersécurité en rapport avec leur fonction et les tâches qu'ils réalisent.	
Entrées	**Sorties**
EX-0.03 | *EX-0.06* | *EX-4.01*| *EX-5.01*	*EX-5.02*

La nature des actions de formation et de sensibilisation doit être adaptée :

- A la nature et à la criticité des éléments sur lesquels ils interviennent ;
- Au niveau de privilèges sur les éléments sur lesquels ils interviennent.

La qualification cybersécurité des personnels s'effectue via :

- Un plan de formation à la cybersécurité dans les tâches courantes ;
- Un plan de sensibilisation à la cybersécurité, intégrant :
    - La sensibilisation aux bases de l'hygiène cybersécurité ;
    - La sensibilisation aux risques de cybersécurité.

[EX-5.05] Surveiller les performances de cybersécurité du système considéré	
Un système de surveillance des performances cybersécurité du système considéré doit être mis en œuvre et exploité en continu afin de détecter les événements de cybersécurité en continu, de déclencher des actions correctives ou préventives si nécessaire et mesurer le niveau de risque cybersécurité.	
Entrées	**Sorties**
EX-0.06 | *EX-5.01* | *EX-5.04* | *EX-5.05* | *EX-5.12*	*EX-5.03*

Le système de surveillance des performances de cybersécurité doit permettre de détecter et de réagir aux événements relatifs à des incidents redoutés en rapport avec les risques de cybersécurité pesant sur le système considéré. En conséquence, il doit mettre en œuvre :

- Une stratégie de collecte de données adapté aux événements à détecter, et en corollaire, une capacité de stockage de ces événements ;
- Une stratégie d'analyse des données collectées adaptée aux événements à détecter, et en corollaire, des moyens d'indexation et de requête dans ces données ;
- Une stratégie de notification des événements détectés, intégrant l'ensemble des parties prenantes du système considéré en fonction de la nature de l'événement ;
- Les procédures en soutien de l'application opérationnelle des stratégies de collecte, d'analyse et de notification ;
- La production d'indicateurs et de tableaux de bord permettant de mesurer des tendances et de détecter des signaux faibles.

[EX-5.06] Assurer la gestion des incidents de cybersécurité du système considéré	
Un processus de gestion des incidents de cybersécurité du système considéré doit être spécifié et mis en œuvre afin d'assurer leur prise en charge et de déclencher des actions correctives ou préventives nécessaires pour leur résolution.	
Entrées	**Sorties**
Plan d'Intervention et de secours *EX-0.01* | *EX-0.02* | *EX-0.05* | *EX-0.06* | *EX-5.01* | *EX-5.04*	*EX.5-02* | *EX-5.03* | *EX-5.09*

Le processus de gestion des incidents de cybersécurité doit intégrer :

- Les modalités de qualification de l'incident et les critères de qualification de l'incident ;
- Les modalités d'analyse de l'incident ;
- Les rôles et responsabilités associées aux actions à mener ;
- Les modalités de communication sur l'incident ;
- Les modalités de suivi des actions ;
- Les modalités de déclenchement d'une investigation numérique ;
- Les modalités de déclenchement d'un dispositif de crise de cybersécurité ;
- Les modalités de clôture de l'incident et les critères de clôture.

Le processus de gestion des incidents de cybersécurité doit prévoir l'appui éventuel de services spécialisés privés ou publics.

Le processus de gestion des incidents de cybersécurité doit permettre la capitalisation sur les incidents de cybersécurité, et par conséquent collecter et conserver les informations nécessaires.

Le processus de gestion des incidents doit respecter les articles R.3152-20 à R.3152-22 du code des transports.

[EX-5.07] Assurer la gestion des crises de cybersécurité du système considéré	
Un processus de gestion des crises de cybersécurité du système considéré doit être spécifié et mis en œuvre afin d'assurer la maîtrise des situations de crise cybersécurité.	
Entrées	**Sorties**
Plan d'Intervention et de secours *EX-0.01* | *EX-0.02* | *EX-0.05*| *EX-0.06* | *EX-5.01*	*EX.5-02* | *EX-5.03*

Le processus de gestion des crises de cybersécurité doit intégrer :

- Les critères de décision de déclenchement de la crise ;
- L'organisation spécifique à la gestion de crise ;
- Les dispositions relatives à l'organisation de la cellule de crise ;
- Les dispositions relatives à la communication de crise ;
- Les moyens nécessaires au support de crise ;
- Les critères de décision de clôture de la crise ;
- Les dispositions relatives à la capitalisation (analyse à chaud, analyse à froid).

Le processus de gestion des crises de cybersécurité doit être intégré dans le PIS (Plan d'Intervention et de Sécurité) du système considéré.

[EX-5.08] Assurer une veille continue sur les vulnérabilités et correctifs de ces vulnérabilités du système considéré	
Un processus de veille sur les vulnérabilités et correctifs des éléments du système considéré doit être spécifié et mis en œuvre afin d'assurer l'identification et la prise en compte sans délai des cas d'éléments vulnérables et / ou obsolètes.	
Entrées	**Sorties**
EX-0.04 | *EX-5.05 EX-0.06* | *EX-5.01* | *EX-5.05*	*EX-5.03*

Le processus de veille sur les vulnérabilités doit intégrer :

- La prise en compte de l'ensemble des vulnérabilités sur les éléments du système considéré, et en corollaire, le lien avec la gestion des configurations du système considéré ;
- La qualification de la criticité intrinsèque de la vulnérabilité (sans contexte) et la qualification de la criticité contextuelle de la vulnérabilité (au sein du système considéré) ;
- La décision tracée d'acceptation de la vulnérabilité, de correction de la vulnérabilité ou d'application de mesures compensatoires.

En outre, le processus de veille doit intégrer les cas d'obsolescence ou de fin de support dans les alertes qu'il remonte à la cellule de veille.

[EX-5.09] Assurer les mises à jour des éléments du système considéré	
Un processus de gestion des mises à jour des éléments du système considéré doit être spécifié et mis en œuvre afin d'éviter les cas d'obsolescence et / ou d'assurer l'application dans les meilleurs délais des correctifs de cybersécurité sur les éléments vulnérables du système considéré.	
Entrées	**Sorties**
EX-0.06 | *EX-5.01* | *EX-5.05* | *EX-5.06* | *EX-5.08*	*EX-5.02* | *EX-5.03*

Le processus de gestion des mises à jour doit intégrer :

- Les modalités de test ;
- Les dispositions permettant de garantir la non-régression des performances opérationnelles du système considéré à la suite des mises à jour.

[EX-5.10] Assurer une veille continue sur les évolutions du système considéré et de son environnement	
Un processus de veille sur les évolutions du système considéré et de l'environnement du système considéré doit être spécifié et mis en œuvre afin de réévaluer la modélisation du système considéré et les risques de cybersécurité pesant sur le système considéré.	
Entrées	**Sorties**
EX-0.04 | *EX-0.06* | *EX-0.10* *Rapport circonstancié et autres remontées d'information* *Rapport annuel de l'exploitant* *EX-5.01*	*EX-5.11*

Les évolutions du système considéré ou de son environnement ont un lien fort avec les risques de cybersécurité. Les critères de réévaluation de l'appréciation des risques doivent être spécifiés dans le processus de veille.

On intègre notamment dans les évolutions à considérer :

- Les évolutions du système considéré lui-même :
  - Evolutions fonctionnelles ;
  - Evolutions des objectifs de cybersécurité (issues de résultats non satisfaisants d'un contrôle ou d'un audit, d'un rapport d'analyse d'incidents, etc.) ;
  - Evolutions de l'architecture technique ou d'un des éléments du système considéré (ex. : nouvelle interconnexion logicielle ou matérielle) ;
- Les évolutions de l'environnement du système considéré :
  - Evolution de l'écosystème ;
  - Evolution du domaine de conception fonctionnelle ;
  - Evolution du parcours ;
  - Evolution de la menace / des sources de menaces ;
  - Evolution des vulnérabilités.

[EX-5.11] Mettre à jour la modélisation du système considéré et de son écosystème	
La modélisation du système considéré et de son écosystème doit être mise à jour périodiquement et lorsque l'évolution du système considéré ou de son environnement induit une modification de la modélisation du système considéré.	
Entrées	**Sorties**
Annexe B *EX-0.04* | *EX-0.06* | *EX-0.09* | *EX-3.01* | *EX-5.09* | *EX.5.10*	*EX-5.12*

La veille sur les évolutions du système considéré et de son environnement peut permettre de disposer de nouvelles données d'entrée permettant d'effectuer une itération de la modélisation du système considéré et de son écosystème, selon les principes décrits à l'Annexe B du présent document, en identifiant notamment :

- De nouveaux biens supports spécifiques à la phase d'exploitation/maintenance, incluant les :
    - Eléments du système considéré ;
    - Utilisateurs et communautés d'utilisateurs du système considéré ;
- De nouvelles interfaces et dépendances du système considéré :
    - Interfaces et dépendances internes du système considéré (entre les éléments du système considéré) ;
    - Interfaces externes du système considéré (écosystème, environnement) ;
- De nouvelles parties prenantes impliquées dans le système considéré ;
- Etc.

[EX-5.12] Réapprécier les risques de cybersécurité du système considéré	
L'appréciation des risques de cybersécurité du système considéré doit être refaite périodiquement et lorsque l'évolution du système considéré ou de l'environnement du système considéré induit une modification des risques de cybersécurité pesant sur le système considéré, conformément au processus de gestion des risques.	
Entrées	**Sorties**
Annexe C | *Annexe H* *EX-0.06* | *EX-0.09* | *EX-0.10* | *EX-1.02* | *EX-3.02*	*EX-5.09* | *EX-5.13*

La réappréciation des risques porte sur l'ensemble des étapes décrites à l'Annexe C du présent document.

La réappréciation des risques de cybersécurité vise en outre à vérifier :

- La prise en compte des mesures issues de la phase précédente du cycle de vie ;
- La prise en compte des mesures issues des dossiers règlementaires déjà réalisés ;
- Les hypothèses prises et la cohérence des hypothèses entre elles.

Elle est déclenchée conformément aux critères décrits dans le plan de gestion des risques de cybersécurité.

Les acteurs en charge de l'application de nouvelles mesures de traitement du risque, quelle que soit la phase du cycle de vie considérée, doivent être formellement identifiés. L'entité responsable doit se prononcer sur la substantialité de la mesure de traitement du risque, c'est-à-dire si elle implique une

modification substantielle du système de transport routier automatisé (cf. section 1) au sens de l'article R.3152-18 IV du code des transports.

Elle est un prérequis au diagnostic de la cybersécurité du système décrit à l'article R3152-16 du code des transports, dans le cas où ce diagnostic porterait sur l'aspect cybersécurité.

Le répertoire des risques de cybersécurité doit être mis à jour.

[EX-5.13] Mettre à jour le plan de traitement des risques de cybersécurité du système considéré	
Le plan de traitement des risques de cybersécurité du système considéré doit être mis à jour en prenant en compte les évolutions de l'appréciation des risques de cybersécurité en phase d'exploitation / maintenance, conformément au processus de gestion des risques.	
Entrées	**Sorties**
Annexe C *EX-0.06* | *EX-0.10* | *EX-3.03* | *EX-5.12*	*EX-5.14*

L'appréciation des risques en phase d'exploitation / maintenance doit permettre de mettre à jour, pour chaque risque nouveau ou modifié, le plan de traitement des risques de cybersécurité selon les principes décrits à l'Annexe C du présent document.

[EX-5.14] Mettre à jour les objectifs de cybersécurité du système considéré	
Les objectifs de cybersécurité du système considéré doivent être mis à jour en prenant en compte les évolutions du plan de traitement des risques de cybersécurité en phase d'exploitation / maintenance.	
Entrées	**Sorties**
EX-0.06 | *EX-1.05* | *EX-5.13*	*EX-5.15*

Le plan de traitement des risques en phase d'exploitation / maintenance doit permettre de mettre à jour, dès lors que la décision de traitement d'un risque nouveau ou modifié de cybersécurité consiste à réduire ou maintenir le risque considéré, les objectifs de cybersécurité correspondants.

Tout ou partie des aspects de l'implémentation des biens supports (conception technique, architecture technique, localisation physique ou géographique, nature des utilisateurs, etc.).

Le répertoire des objectifs de cybersécurité doit être mis à jour.

[EX-5.15] Mettre à jour les exigences fonctionnelles de cybersécurité du système considéré	
Les exigences fonctionnelles de cybersécurité du système considéré doivent être mises à jour relativement aux objectifs de cybersécurité.	
Entrées	**Sorties**
EX-0.06 | *EX-3.04* | *EX-5.14*	*EX-5.16* | *EX-5.17*

Les exigences fonctionnelles de cybersécurité ainsi mises à jour font évoluer le concept de cybersécurité qui doit garantir :

- L'adéquation avec les objectifs de cybersécurité ;
- L'exhaustivité de la prise en compte des objectifs de cybersécurité ;
- L'adéquation avec les hypothèses et les contraintes du système considéré.

[EX-5.16] Mettre à jour l'architecture fonctionnelle de cybersécurité du système considéré	
L'architecture fonctionnelle de cybersécurité du système considéré être mise à jour en prenant en compte les évolutions des exigences fonctionnelles de cybersécurité.	
Entrées	**Sorties**
EX-0.06 | *EX-0.10* | *EX-3.05* | *EX-5.15*	*EX-5-17*

Si de nouveaux risques de cybersécurité sont identifiés à partir de l'architecture fonctionnelle de cybersécurité, l'appréciation des risques de cybersécurité, le plan de traitement des risques de cybersécurité, les objectifs de cybersécurité, les exigences fonctionnelles de cybersécurité du système considéré doivent être mis à jour.

[EX-5.17] Mettre à jour les mesures de cybersécurité applicables au système considéré	
Les mesures de cybersécurité permettant de maintenir ou de réduire les risques de cybersécurité du système considéré à un niveau acceptable, en lien avec les objectifs de cybersécurité, doivent être mises à jour et mises en œuvre.	
Entrées	**Sorties**
EX-0.05 | *EX-0.06* | *EX-3.04* | *EX-5.15*	*EX-5.01* | *EX-0.05*

Les mesures de cybersécurité et l'architecture technique de cybersécurité doivent être mises à jour en lien avec les objectifs de cybersécurité. Les acteurs en charge de l'application des mesures de traitement du risque, quelle que soit la phase du cycle de vie considérée, doivent être formellement identifiés.

Les mesures de cybersécurité doivent être mises en œuvre et être intégrées au plan de maintien en conditions de cybersécurité (EX-5.01) et au système de management de la cybersécurité (EX-0.05), afin d'assurer leur intégration dans une boucle d'amélioration continue.

[EX-5.18] Mettre à jour l'architecture technique de cybersécurité du système considéré	
L'architecture technique de cybersécurité du système considéré doit être mise à jour en prenant en compte les évolutions de l'appréciation des risques de cybersécurité.	
Entrées	**Sorties**
EX-0.06 | *EX-0.10* | *EX-3.07* | *EX-5-17*	*EX-5.11*

Si de nouveaux risques de cybersécurité sont identifiés à partir de l'architecture technique de cybersécurité, l'appréciation des risques de cybersécurité le plan de traitement des risques de cybersécurité, les objectifs de cybersécurité, les exigences fonctionnelles de cybersécurité et les mesures de cybersécurité du système considéré doivent être mis à jour.

4.6 Phase de retrait du service

4.6.1 Objectifs

La phase de retrait du service du système considéré intègre de manière indifférenciée les aspects de dépose ou de démantèlement d'un sous-système ou élément technique du système considéré et les aspects d'arrêt d'un service proposé par le système considéré. Le retrait d'un service fait partie du cycle de vie du système considéré et est pris en compte dans les phases amont du projet.

L'objectif en matière de cybersécurité de cette phase du cycle de vie est de mettre en œuvre les dispositions nécessaires pour assurer que le retrait du service n'a pas d'impact sur la cybersécurité du système considéré.

4.6.2 Activités de cybersécurité

[EX-6.01] Appliquer le plan de contrôle de la cybersécurité du système considéré	
Le plan de contrôle de la cybersécurité du système considéré du système considéré doit être mis en œuvre en phase de retrait du service afin d'en maîtriser les impacts sur la cybersécurité des systèmes connexes conformément au plan qualité cybersécurité.	
Entrées	**Sorties**
EX-0.06 | *EX-0.07*	

Le contrôle de la cybersécurité en phase de retrait du service doit notamment inclure :

- La vérification de l'application du plan qualité cybersécurité (cf. Section 3.2) ;
- La vérification du bon fonctionnement sécurisé des interfaces, des interactions, du comportement et des fonctions système existantes après le retrait du service ;
- La vérification du bon fonctionnement des systèmes connexes supportant des services de cybersécurité après le retrait du service ;
- La vérification du comportement de cybersécurité et les interactions entre le système considéré et l'environnement externe après le retrait du service ;
- La vérification qu'aucun matériel, composant ou équipement remplacé ne puisse être utilisé pour réaliser du renseignement préparatoire à une attaque du système considéré ;
- L'information des parties prenantes concernées par le retrait du service, au titre d'une dépendance ou en tant qu'utilisateurs du service.

Annexes

Annexe A : Index des exigences

Annexe B : Modélisation du système

Processus de modélisation du système

Objectifs

La modélisation fonctionnelle et technique du système considéré est un processus qui vise à faciliter l'appréciation des risques de cybersécurité. Il est d'autant plus important que le système considéré est un système de systèmes, ce qui complexifie l'approche pour l'appréciation des risques de cybersécurité.

Activités

Le processus de modélisation du système considéré inclut les activités suivantes :

- Constituer l'inventaire des éléments du système considéré ;

  L'inventaire des éléments du système considéré découle de la mise en œuvre des principes décrits dans les principes décrits dans les sections descriptives ci-après. Il est également possible de le compléter en s'appuyant sur :

  - Des entretiens ciblés et préparés sur la base des éléments déjà collectés lors de la phase d'étude de l'existant ;
  - Des outils de collecte automatique tels que les outils de gestion de parc ou les logiciels de supervision ;
  - Des données extraites depuis des applications spécifiques (bases de données, tableaux de bord, etc.) ; des documents internes, par exemple les plans de continuité et de reprise d'activité ou les analyses de risques.

- Réaliser des vues et représenter les liens entre elles ;

  Si des sous-systèmes sont modélisés, un mapping entre tous les sous-systèmes et les éléments du système considéré doit être réalisé.

- Constituer l'inventaire des parties prenantes du système considéré ;

  L'inventaire des parties prenantes du système considéré permet de modéliser l'écosystème du système considéré. Il découle de la mise en œuvre des principes décrits dans les sections descriptives ci-après.

- Mettre en œuvre et maintenir à jour la modélisation tout au long du cycle de vue du système considéré avec les exigences suivantes :

  - Les données sensibles de la modélisation fonctionnelle et technique du système considéré doivent être protégées. Il existe différentes mentions de protection (confidentiel entreprise, diffusion restreinte, voire classification et protection au titre du secret de la défense nationale).
  - La modélisation fonctionnelle et technique du système considéré ne doit pas être stockée sur le système d'information qu'elle représente. De plus, son accès doit être limité aux personnes ayant le besoin d'en connaître (par exemple, les métiers pour les vues qui les concernent, la DSI, les membres de la cellule de crise) afin de réduire le risque de fuite.
  - Quelles que soient la taille et la nature de l'organisation, il est important de disposer de ressources suffisantes pour maintenir la modélisation fonctionnelle et technique du système considéré à jour. Ces ressources sont à ajuster selon le niveau de maturité atteint. Il est indispensable de prévoir une fonction spécifique chargée du contrôle des mises à jour, du recueil des besoins d'évolution du modèle et de l'assistance aux équipes contributrices au projet de modélisation fonctionnelle et technique du système considéré.

Principes pour la modélisation du système

Principes de modélisation fonctionnelle d'un système

La modélisation fonctionnelle vise à spécifier, selon un niveau de détail variable, les fonctions et sous-fonctions du système considéré et leurs interactions, ainsi que les interfaces du système considéré et ses limites de responsabilité, en lien avec l'écosystème.

La modélisation fonctionnelle du système considéré peut être facilitée par une approche hiérarchique permettant de raffiner ses missions (cf. Figure 3) ; le niveau de détail attendu est celui qui permet le mieux de caractériser les enjeux du système considéré lors de l'appréciation des risques.

Les raffinements successifs conduisent, à la fin du processus de raffinement, à une modélisation technique détaillée, incluant les objets techniques supportant les fonctions et sous-fonctions, mais aussi les interfaces du système considéré.

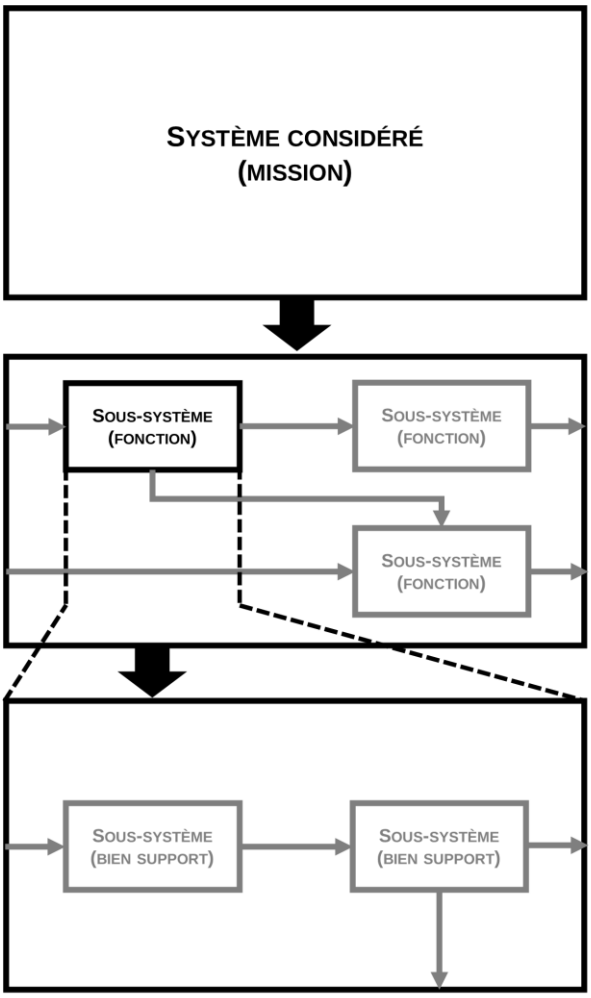


Figure 3 : Approche hiérarchique de la modélisation fonctionnelle

La modélisation fonctionnelle du système peut s'inspirer de modélisations réalisées dans le cadre des analyses de sureté de fonctionnement à condition d'en justifier la pertinence au regard de la cybersécurité.

Modèles de base pour la modélisation fonctionnelle d'un système

Le système considéré est un système complexe composé notamment de nombreux sous-systèmes sous responsabilité de différentes parties prenantes. Ces sous-systèmes interagissent entre eux, et sont vecteurs de risque les uns vis-à-vis des autres.

La modélisation fonctionnelle du système doit permettre de modéliser ces interactions pour mieux appréhender le système considéré dans sa globalité et mieux identifier les scénarios de risques qui concernent plusieurs sous-systèmes.

La présente section propose une approche de modélisation fonctionnelle de certains sous-systèmes du système considéré, et un exemple de mise en application sur un modèle « parfait », c'est-à-dire sans prétention de représenter parfaitement les implémentations réelles, avec les finalités suivantes :

- représenter les sous-systèmes qui composent le système global ;
- faire apparaître une surface d'attaque ;
- faire apparaître les interactions entre les sous-systèmes ;
- faire apparaître les chemins d'attaque ;
- formuler certaines contraintes et hypothèses sur les sous-systèmes ;
- formuler certaines spécificités d'implémentation des sous-systèmes ;
- contribuer à la détermination des scénarios de risques.

La modélisation fonctionnelle fait apparaître des modules de traitement de l'information, représentés par des blocs fonctionnels de différentes nature, qui reçoivent et / ou transmettent des informations avec d'autres modules (cf. Figure 4).

Indépendamment de leur nature, ces modules sont à catégoriser relativement à leur contribution à la cybersécurité du système considéré[2] :

- Module de mise en œuvre de la cybersécurité ;
- Module supportant la cybersécurité ;
- Module sans interférence avec la cybersécurité.

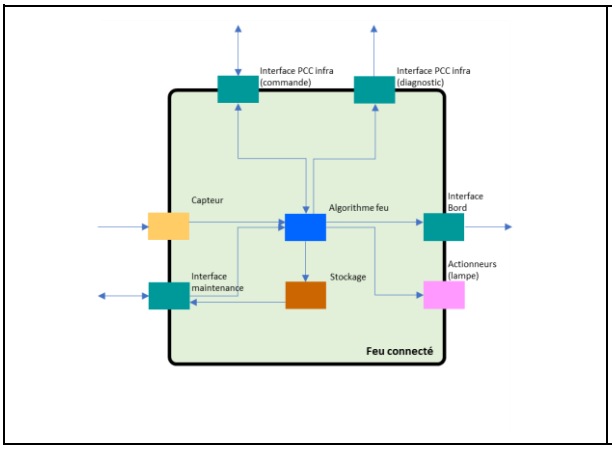
Figure 4 : Typologies des processus de traitement de l'information

La modélisation fonctionnelle ne représente que les processus et les échanges nominaux d'un système ; elle est indépendante des spécificités d'implémentation du système, et ne représente pas les possibles interactions induites par cette implémentation (ex. : connectivité réseau non utile au processus nominal).

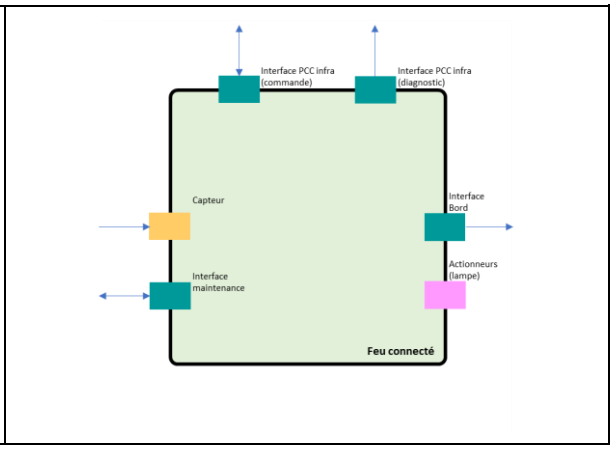
La modélisation fonctionnelle se projette par construction dans le modèle stratifié (cf. Annexe E) ; certains processus de traitement de l'information (cf. Figure 4) n'existent que par les interfaces qu'ils proposent avec les strates physique et anthropique (les processus de génération et de consommation de l'information, notamment).

[2] La notion de « contribution à la cybersécurité » et les différentes catégories associées sont explicitées en annexe K.

Cas d'usage de modélisation de sous-systèmes

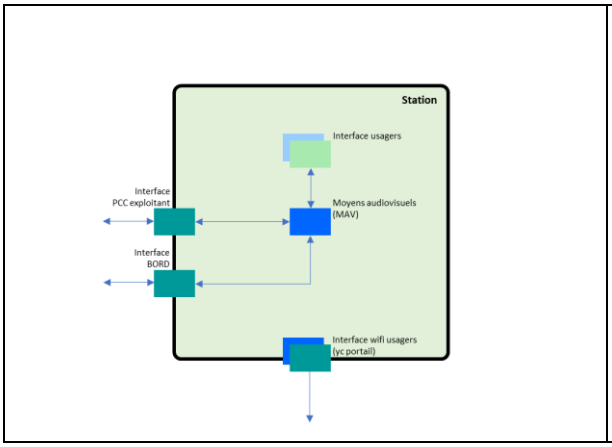


Modélisation fonctionnelle d'un feu connecté

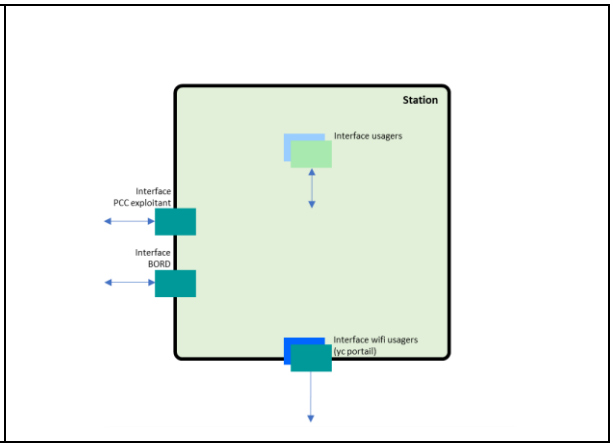


Modélisation de la surface d'attaque d'un feu connecté (hors supply chain)

- Interfaces cybernétiques
- Interfaces physiques (capteurs, actionneurs)

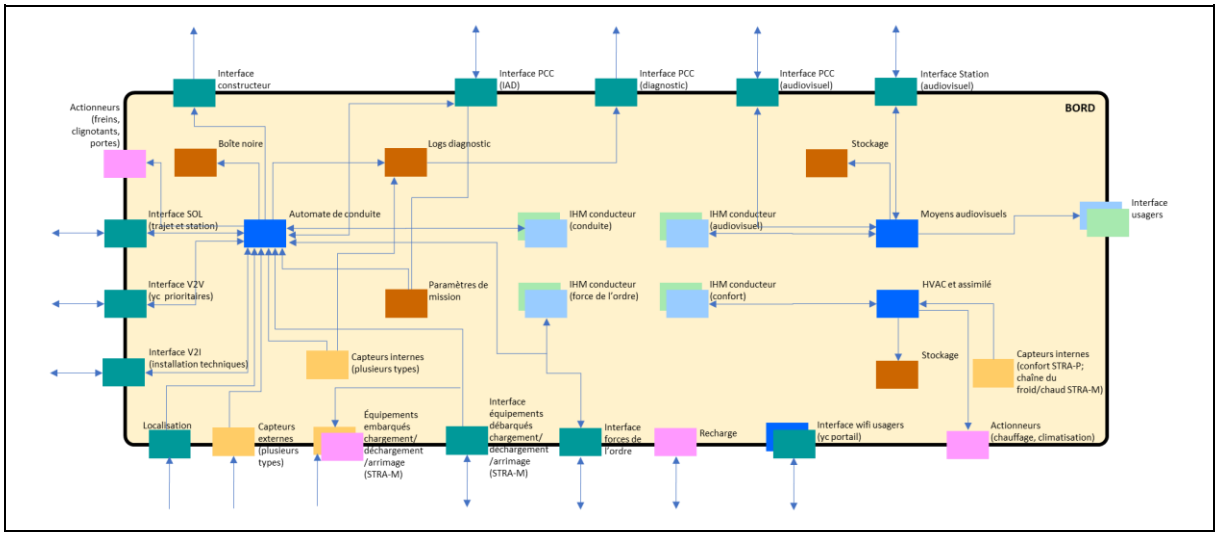


Modélisation fonctionnelle d'une station

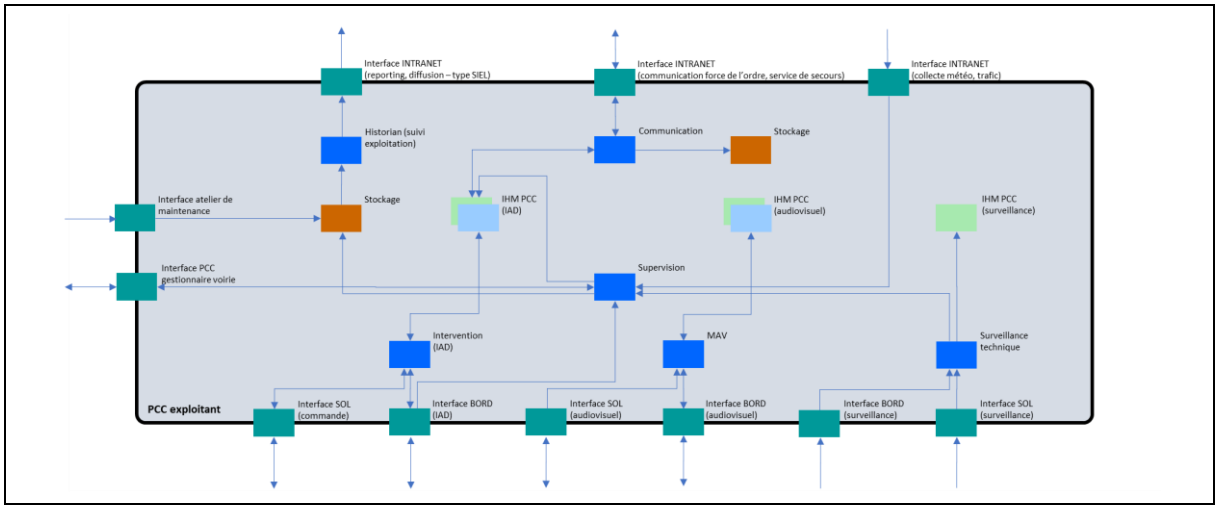


Modélisation de la surface d'attaque d'une station (hors supply chain)

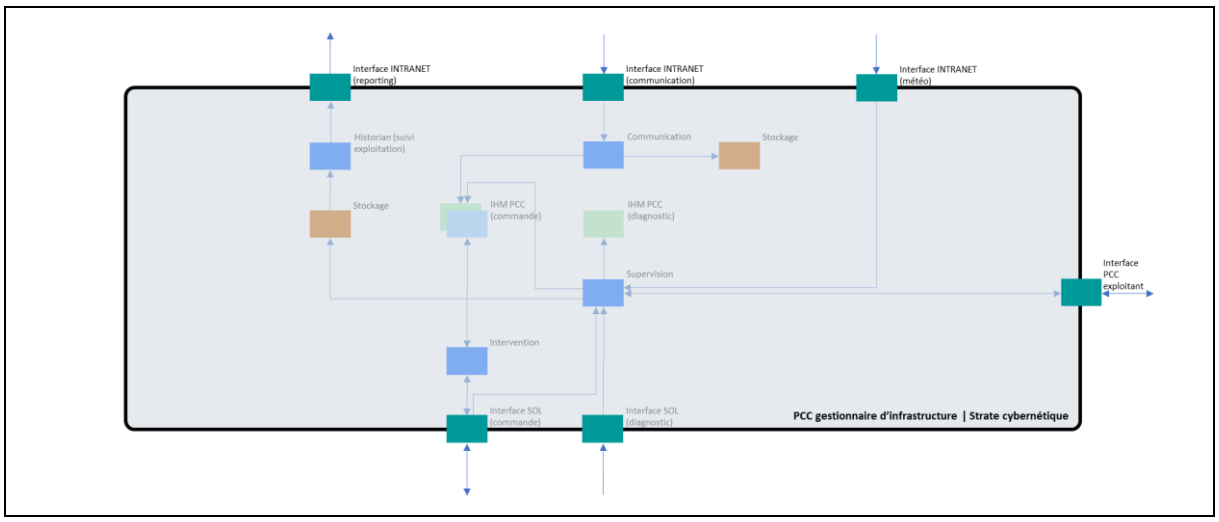
- Interfaces cybernétiques
- Interfaces anthropiques (consommées par les usagers)



Modélisation fonctionnelle d'un véhicule



Modélisation fonctionnelle d'un PCC exploitant



Modélisation fonctionnelle d'un PCC infrastructure – hors périmètre du STRA

Cas d'usage de modélisation fonctionnelle d'un système complexe

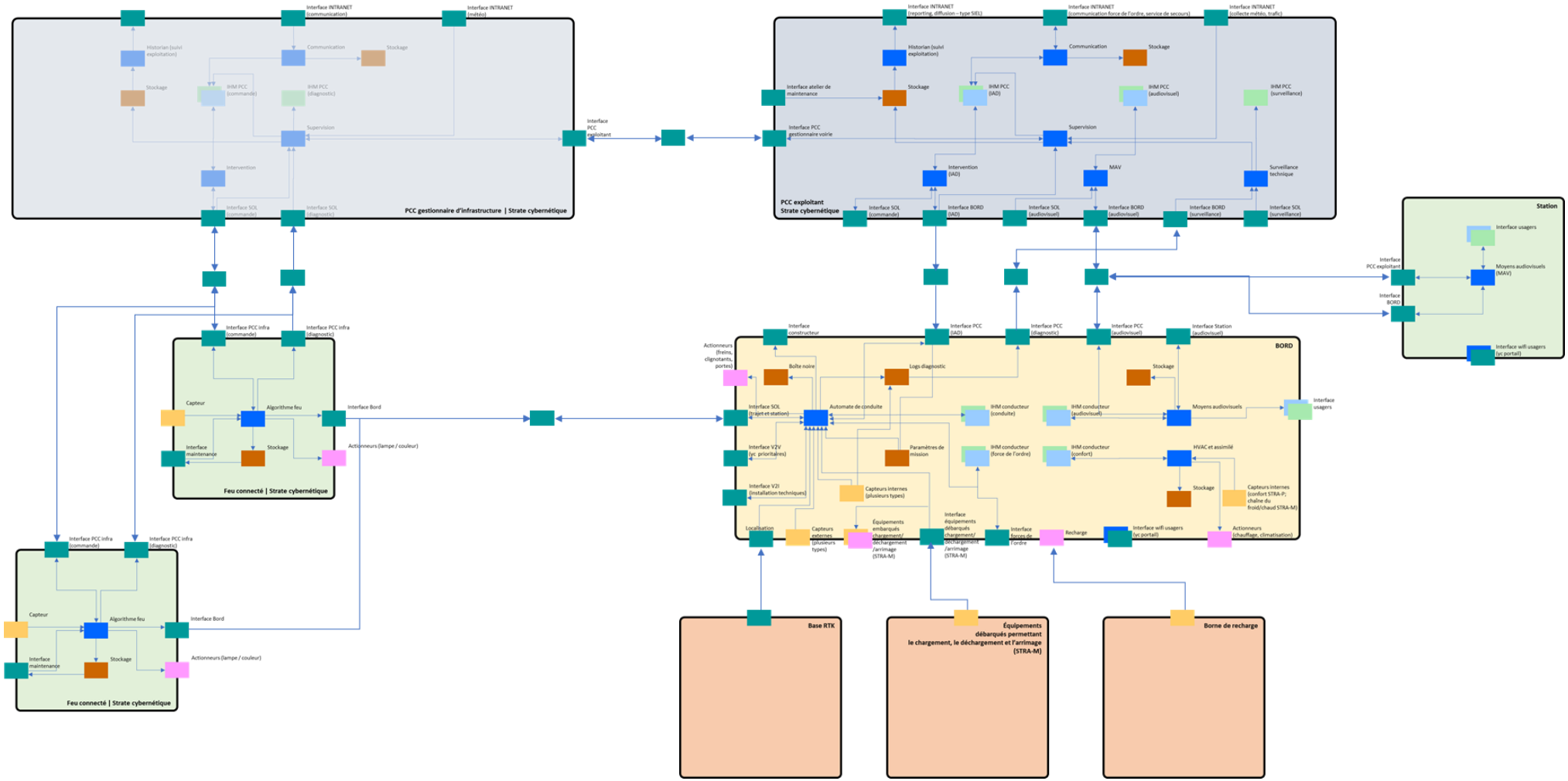


Figure 5 : Modélisation fonctionnelle d'un système complexe

Principes de modélisation technique d'un système

Le système considéré doit être modélisé selon une approche technique pilotée par l'approche fonctionnelle détaillée ci-avant, qui vise à spécifier les biens support du système considéré, parmi l'ensemble des sous-systèmes et éléments qui le constituent.

Les biens support du système considéré peuvent être caractérisés selon leur nature pour permettre de les manipuler plus simplement :

- Biens géographiques :
    - Locaux (bâtiment, installation, etc.) Et zones (zones à accès restreint, etc.)
    - Services essentiels des bâtiments (énergie, etc.) Et moyens généraux
- Biens matériels
    - Plateformes matérielles (serveurs matériels, équipements, etc.)
    - Equipements réseaux et télécom (routeurs, commutateurs, points d'accès wi-fi, etc.)
    - Infrastructures de raccordement (fibre optique, câblage et brassage cuivre, etc.)
    - Médias (support de stockage, etc.)
- Biens cybernétiques :
    - Systèmes numériques complexes (systèmes embarqués, automates, etc.)
    - Systèmes numériques unitaires (système d'exploitation, middleware, application, etc.)
    - Flux de données (flux sans fil, flux en lien avec les infrastructures de raccordement)
    - Environnements utilisateurs (postes de travail, interfaces hommes-systèmes, embarqués et déportés, outils de communication, etc.)
- Biens organisationnels :
    - Entité interne ou externe (personne morale, direction, département, filiale, etc.)
    - Personnes physiques (utilisateurs par fonction, usagers, etc.).

En fonction de la phase du projet, la modélisation technique du système considéré peut relever d'une architecture préliminaire (de haut niveau), d'une spécification détaillée d'architecture, ou d'un dossier d'architecture technique utilisé en production.

La modélisation technique se projette dans le modèle stratifié (cf. Annexe E), afin de représenter la surface d'attaque du système considéré non seulement au niveau de la strate numérique, mais aussi au niveau physique (exposition physique) et au niveau anthropique (interfaces d'utilisation).

Principes de modélisation de l'écosystème d'un système

De plus en plus de modes opératoires de cyberattaque exploitent les maillons les plus vulnérables d'un écosystème pour atteindre leur objectif (ex. : atteinte à la disponibilité d'un service via une cyberattaque sur un fournisseur d'un service support ; piégeage de la chaîne logistique pour introduire des fonctions cachées dans les développements, etc.).

L'écosystème comprend l'ensemble des parties prenantes internes ou externes qui gravitent autour du système considéré et concourent à la réalisation de ses missions, incluant :

- Des parties prenantes externes à l'entité responsable :
    - Partenaires et cotraitants
    - Prestataires et fournisseurs
    - Organismes qualifiés agréés
    - Clients et usagers
    - Services tiers publics ou privés
    - Etc.
- Des parties prenantes internes à l'entité responsable :
    - Services connexes techniques (exemple : services supports proposés par une direction informatique
    - Services connexes métier (exemple : services en charge de la billettique)

- Etc.

Sur le périmètre spécifique des STRA, on peut structurer l'écosystème selon plusieurs approches complémentaires :

- Une approche par les types d'entités responsables rencontrées :
  - Le concepteur du système technique
  - L'organisateur du service
  - L'exploitant du service
- Une approche par la nature des sous-systèmes et éléments qui contribuent aux services fournis par le système considéré, en distinguant :
  - L'écosystème des véhicules automatisés, incluant tous les sous-systèmes et les éléments intégrés aux véhicules automatisés (système de navigation, système V2X, etc.) ;
  - L'écosystème des installations techniques, incluant les équipements installés au sein de l'infrastructure ;
  - L'écosystème des services, incluant les services nominaux gérés par l'organisateur du service ou les services externes (services publics ou privés) ;
  - L'écosystème associés aux parcours / aux zones, incluant les spécificités des parcours et des zones, les infrastructures et leurs entités gestionnaires, les tiers (personnes ou véhicules) et les usagers.
- Une approche par la contribution au cycle de vie, d'un sous-système ou d'un élément, quelle que soit sa nature :
  - Concepteur
  - Constructeur
  - Exploitant
  - Mainteneur
  - Etc.

Chaque partie prenante de l'écosystème est en relation avec le système considéré via une interface tangible (interface technique, interface physique, etc.) et / ou intangible (contrat, délégation de service, etc.) qui doit être spécifié lors de la modélisation de l'écosystème.

Ecosystème-type d'un STRA

L'écosystème-type ci-après est proposé à titre purement indicatif. En particulier, la colonne de droite n'est pas exhaustive et est à spécifier en fonction du projet et de l'activité concernée.

Ecosystème des véhicules		
Concepteur	➡	Système de navigation, Télématiques, Info-divertissement (STRA-P), Radar, Lidar, Caméra embarquée, Système V2X, Plateforme roulante, Équipements embarqués permettant le chargement/déchargement/arrimage (STRA-M)
Constructeur		
Mainteneur		
Ecosystème des infrastructures et des équipements		
Gestionnaire[3]	➡	Equipement sur la voirie : marquage au sol (sur la voie, passages piétons, voies spécifiques type voies de bus / pistes cyclables), trottoirs, etc.
Concepteur	➡	Feu connecté ou non, Panneau de signalisation, Panneau d'affichage, Caméra de surveillance, Radar de contrôle, Signalisations dynamiques, Équipements débarqués permettant le chargement/déchargement/arrimage (STRA-M), etc.
Constructeur		
Mainteneur	➡	Bandes au sol / poteaux, etc.
Ecosystème des services		
Organisateur du service	➡	Personnel de maintenance, Poste de supervision, Logiciel de gestion de la flotte, Site web, Application mobile pour les clients, Gare routière, Zone de parking, Espace d'accueil des clients (boutiques), zone de chargement/déchargement (STRA-M), Personnes en charge du chargement déchargement (STRA-M), etc.
Exploitant du service		
Services publics ou privés	➡	Véhicule de service spécifique (ambulance, police, pompier), Poste de surveillance routier, Station-service (carburant, recharge), Entrepôts, Péages, etc.
Ecosystème des parcours / zones		
Tiers	➡	Véhicules et personnes : Véhicules, Piétons, Riverains, Cyclistes, EDP, Tramways, Etc.
Parcours	➡	Caractéristiques du parcours : Route, Autoroute, Emprise privée, Pont, Tunnel, Etc.
Zones	➡	Zones spécifiques : voie de détresse, voies de stockage, voies réservées (bus, taxi), parking, péage, etc.
Ecosystème transverse		
Sources de veille	➡	Sources internes : Direction juridique, direction technique, etc. Sources ouvertes : Réseau sociaux, etc. Sources gouvernementales : ANSSI, GIP ACYMA, etc. Organismes spécialisés : CERT, éditeurs et mainteneurs de solutions matérielles ou logicielles, universités et pôles de recherche, associations spécialisées en cybersécurité, etc.
Tierces parties cybersécurité	➡	OQA, etc. Organismes de service et de conseil, etc.

Tableau 3 : Ecosystème-type d'un STRA

[3] Désigne le ou les gestionnaire(s) de l'ensemble des équipements, qu'ils soient livrés ou non avec le système technique: feu de circulation, panneau de signalisation, panneau d'affichage, caméra de surveillance, radar de contrôle, signalisation dynamique, etc.

Annexe C : Appréciation et traitement des risques de cybersécurité

Processus d'appréciation et de traitement des risques de cybersécurité

Processus d'identification et d'analyse des risques de cybersécurité

Objectifs

L'identification et l'analyse des risques de cybersécurité est le processus consistant à rechercher, reconnaître et décrire les risques de cybersécurité et d'estimer le niveau de risque. L'objectif est de disposer d'une liste de risques sur la base des événements redoutés de cybersécurité, hiérarchisés selon le niveau de risque.

Activités du processus

Le processus d'identification et d'analyse des risques de cybersécurité est mis en œuvre de manière itérative, tout au long du cycle de vie du système considéré, conformément au processus de gestion des risques de cybersécurité pour le projet (cf. EX-0.10). Il inclut les activités suivantes :

1. Identifier les événements redoutés de cybersécurité
2. Identifier les scénarios de conséquence
3. Estimer la gravité des scénarios de conséquence
4. Identifier et caractériser les sources de menaces
5. Identifier les vulnérabilités
6. Identifier les scénarios de menace
7. Estimer la vraisemblance des scénarios de menace
8. Estimer le niveau des risques de cybersécurité

Processus d'évaluation des risques de cybersécurité

Objectifs

L'évaluation des risques de cybersécurité est le processus consistant à confronter les risques de cybersécurité aux critères d'acceptabilité des risques. L'objectif est d'identifier les risques dont le niveau d'acceptabilité nécessite un plan de traitement des risques de cybersécurité.

Activités du processus

Le processus d'évaluation des risques est mis en œuvre de manière itérative, tout au long du cycle de vie du système considéré, conformément au processus de gestion des risques de cybersécurité pour le projet (cf. EX-0.10). Il inclut les activités suivantes :

1. Identifier les principes d'acceptabilité des risques de cybersécurité
2. Identifier les critères d'acceptabilité des risques de cybersécurité
3. Evaluer les risques de cybersécurité

Processus de traitement des risques de cybersécurité

Objectifs

Le traitement des risques de cybersécurité est le processus consistant à identifier, motiver et tracer les options de traitement des risques de cybersécurité visant à amener les risques de cybersécurité à un niveau acceptable, selon les résultats de l'évaluation des risques de cybersécurité.

Activités du processus

Le processus de traitement des risques de cybersécurité est mis en œuvre après chaque itération de l'appréciation des risques. Il inclut les activités suivantes :

1. Choisir et justifier les options de traitement des risques appropriées
2. Elaborer un plan de traitement des risques de cybersécurité

Principes pour l'appréciation et le traitement des risques de cybersécurité

Un risque de cybersécurité est la combinaison d'un scénario de menace (la cause) et d'un scénario de conséquences (l'effet). La liste des risques de cybersécurité applicables au système considéré est le résultat de l'ensemble des combinaisons possibles des scénarios de menace et des scénarios de conséquences sur le système considéré.

Afin d'éviter l'explosion combinatoire des combinaisons scénarios de menace / scénarios de conséquence, il est recommandé, de considérer l'événement redouté de cybersécurité comme un pivot du risque de cybersécurité (cf. Figure 6) et d'en déduire les causes possibles (les scénarios de menaces) et les conséquences possibles (les scénarios de conséquence). En itérant sur l'ensemble des événements redoutés de cybersécurité, on peut identifier l'ensemble des risques de cybersécurité.

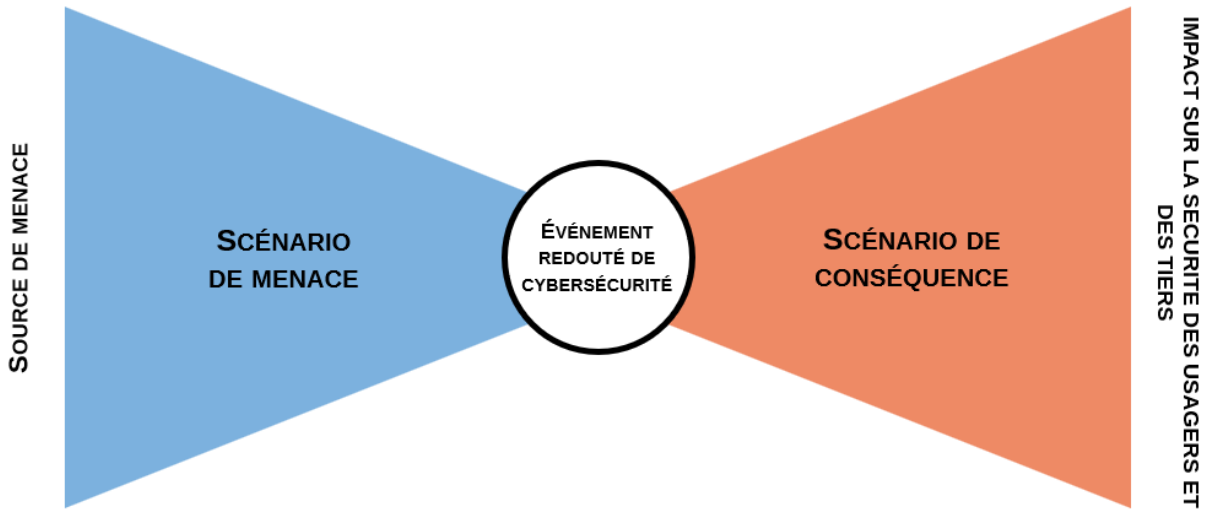


Figure 6 : Construction d'un risque de cybersécurité

En conséquence, le système considéré doit faire l'objet d'une appréciation des risques de cybersécurité, selon les sous-processus suivants :

- Identification des risques de cybersécurité
  - Identification des scénarios de conséquences, par construction de l'arbre des conséquences pour chaque événement redouté ;
  - Identification des scénarios de menace, par construction de l'arbre des causes pour chaque événement redouté.
- Estimation des risques de cybersécurité :
  - Estimation de la gravité des scénarios de conséquences ;
  - Estimation de la vraisemblance des scénarios de menace ;
  - Estimation des risques de cybersécurité.
- Evaluation des risques de cybersécurité :
  - Comparaison des résultats de l'estimation des risques de cybersécurité avec les critères d'acceptabilité des risques ;
  - Classification des risques de cybersécurité par ordre de priorité en vue de leur traitement.

Les risques ainsi identifiés et évalués doivent faire l'objet d'un traitement au titre d'un plan de traitement des risques de cybersécurité.

Principes d'identification et d'estimation des scénarios de conséquence

L'appréciation des risques de cybersécurité, au titre des scénarios de conséquences, doit identifier et estimer la gravité toutes les situations ayant un impact sur la sécurité des usagers et des tiers vis-à-vis du fonctionnement du système en mode délégation de conduite, c'est-à-dire lorsque le contrôle dynamique du véhicule n'est pas assuré par un conducteur humain, sur la voirie ouverte à la circulation publique. Ces situations concernent notamment (cas spécifiés à l'article R.3152-2 du code des transports) :

- Les accidents pouvant résulter de situations raisonnablement prévisibles dans le domaine d'emploi ou le domaine de conception technique (cf. Annexe J) ;
- Les cas de défaillances et les cas de sorties du domaine d'emploi ou du domaine de conception technique.

Les événements redoutés de cybersécurité sont les éléments d'entrée du scénario de conséquences (cf. Figure 7). Ils correspondent à l'ensemble des cas d'atteinte aux fonctions du système considéré[4] (cf. Annexe I). Les scénarios de conséquences ont pour objectif de décrire les scénarios qui, à partir d'un événement redouté de cybersécurité, (cf. Figure 7), ont pour conséquence un accident de niveau système, une défaillance, une sortie du domaine d'emploi ou une sortie du domaine de conception technique.

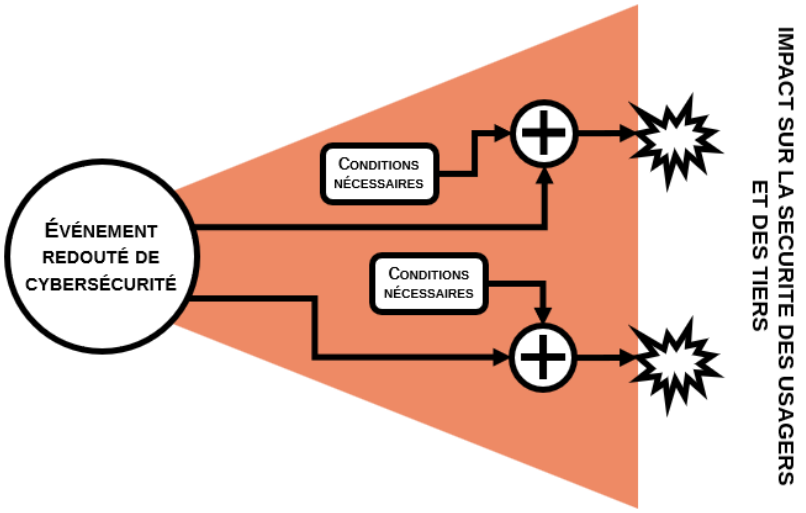


Figure 7 : Schéma-type d'un scénario de conséquences

On trouvera en Annexe H une vision de haut niveau des événements redoutés de cybersécurité, sur la base de scénarios de menace appliqués à la modélisation fonctionnelle-type d'un STRA.

Les scénarios de conséquences doivent être déterminés :

- En liant chaque événement redouté de cybersécurité aux situations ayant un impact sur la sécurité des usagers et des tiers, pour déterminer les conditions nécessaires à la survenance de ces situations ;
- En confrontant les conditions nécessaires déduites ci-avant au domaine de conception technique et / ou au domaine d'emploi pour le système considéré.

[4] À titre d'exemple, on peut caractériser les atteintes aux fonctions du système considéré par les atteintes à la confidentialité, à la disponibilité ou à l'intégrité d'une fonction du système considéré, et plus globalement à la qualité de service et aux performances auxquelles les fonctions du système considéré doivent répondre.

Chaque scénario de conséquences identifié doit faire l'objet d'une estimation de sa gravité, exprimé en termes de niveau d'impact du scénario de conséquences sur la sécurité des usagers et des tiers, selon l'échelle à 4 niveaux (G0 à G3) ci-après issue de la source bibliographique [22] Guide technique relatif à la démonstration GAME pour les STRA.

Niveau de gravité	Description du niveau de dommage(s)
G0	Pas de blessure, dégâts matériels uniquement[5]
G1	Blessures légères et modérées
G2	Blessures graves (survie probable)
G3	Blessures mortelles (survie incertaine) ou décès

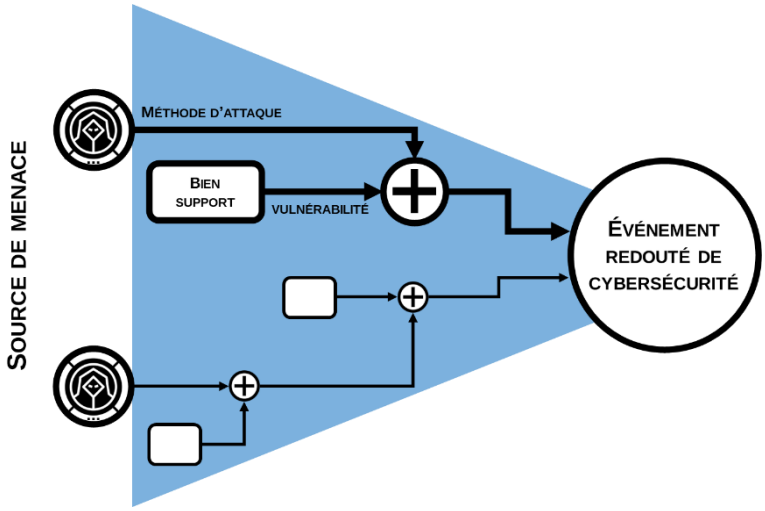
Tableau 4 : Echelle de gravité

L'utilisation de cette échelle devra respecter les conditions et les exigences décrites dans le guide technique relatif à la démonstration « GAME » pour les STRA dans sa dernière version publiée.

Principes d'identification et d'estimation des scénarios de menace

Un scénario de menace est constitué selon la « grammaire » suivante (voir Figure 8) :

Une [source de menace] exploite
une ou plusieurs [vulnérabilité(s)]
d'un ou plusieurs [bien(s) support(s)] du système considéré
pour réaliser un ou plusieurs [mode(s) d'attaque(s)]
induisant un ou plusieurs [événement(s) redouté(s) de cybersécurité]



[5] Si les dégâts concernent le système, des mesures d'exploitation doivent permettre de le traiter de manière à ce qu'il ne conduise pas à un évènement de gravité supérieure.

Figure 8 : Schéma-type d'un scénario de menace

A la différence des scénarios de conséquence, l'identification des scénarios de menace ne se limite pas aux phases de fonctionnement du système en mode délégation de conduite sur la voirie ouverte à la circulation publique, mais couvre bien l'ensemble des phases de vie du système considéré, que ces phases de vie se déroulent ou non sur la voirie ouverte à la circulation publique.[6]

Les scénarios de menace doivent être identifiés en analysant chacune des composantes :

- Les [sources de menace] applicables au système considéré

  La caractérisation fine des sources de menace nécessite de disposer d'informations précises sur l'état de la menace. Elle dépend de nombreux facteurs : secteur d'activité, localisation, contexte de l'activité (géopolitique, conjoncturel, etc.).

  Les sources de menaces sont avant tout caractérisées par leur nature (ex. : groupes criminels ou cybercriminels, groupes d'attaquants assimilables à des états, groupes activistes ou hacktivistes, individus isolés avec des motivations diverses, etc.).

  L'identification des sources de menace (cf. Annexe F) permettra de faciliter leur caractérisation, au travers de leur potentiel d'attaque, basé sur les deux caractères fondamentaux suivants :

  - les motivations de la source de menace : elles sont de natures très diverses (d'ordre politique, économique, etc.), elles dépendent fortement de l'attractivité du système considéré par rapport à la source de menace et sont caractérisées et estimées sur des échelles de motivation, qui sont basées sur un ensemble de marqueurs :

Marqueurs de motivation	Signification
Effort	La part des ressources que la source de menace est prête à mobiliser
Durée	La durée dont la source de menace dispose
Risque	Les risques que la source de menace est prête à prendre

Tableau 5 : Marqueurs de motivation

  - les capacités de la source de menace, qui incluent les ressources disponibles et l'expertise.

    On projette les capacités des sources de menace sur l'espace stratifié, ce qui permet d'identifier des ressources utilisables sur l'espace physique, sur l'espace numérique et sur l'espace anthropique.

    Les capacités des sources de menace sont caractérisées et estimées sur des échelles de capacités, qui sont basées sur un ensemble de marqueurs constitutifs de chaque nature de capacité (physique, numérique, anthropique) :

[6] Par exemple sont à considérer les attaques dites en *supply chain* qui ont pour origine une compromission en phase de développement, les attaques pouvant survenir hors exploitation commerciale, en dépôt de maintenance, sur un banc de test / développement, sur une borne de recharge, etc.

Marqueurs de capacité physique	Marqueurs de capacité numérique	Marqueurs de capacité anthropique
Equipement	Niveau de technicité	Niveau de complexité
Ciblage de l'environnement	Ciblage de l'environnement	Ciblage de groupes sociaux
Ciblage de la victime	Ciblage de la victime	Ciblage de la victime
Niveau de ressources	Niveau de ressources	Niveau de ressources

Tableau 6 : Marqueurs de capacité

- Les [vulnérabilités] des [biens supports] du système considéré

  Les vulnérabilités sont avant tout des propriétés des biens supports qui sont exploitables par une source de menace pour mener à bien une attaque. En ce sens, cette exploitabilité est directement liée aux capacités de la source de menace, sur plusieurs niveaux :

  - Au niveau topologique : certaines vulnérabilités ne sont exploitables que si elles sont « visibles » de la source de menace (ex. : une proximité physique) ;
  - Au niveau temporel : certaines vulnérabilités n'existent et donc ne sont exploitables que dans une fenêtre de temps donnée ;
  - Au niveau capacitaire : certaines vulnérabilités nécessitent des capacités (ressources, savoir-faire, etc.) Importantes.

  Les vulnérabilités des biens supports du système considéré sont de natures très diverses et dépendent de la nature du bien support. A partir de la modélisation technique du système considéré (cf. Annexe B), chaque bien support doit faire l'objet d'une identification et d'une caractérisation de ses vulnérabilités.

  L'absence de mesures de cybersécurité (ex. : absence de règles d'habilitation et d'accès, absence de processus de gestion des correctifs de cybersécurité, etc.) peut constituer une vulnérabilité du système considéré.

- Les [modes d'attaque] applicables

  Les modes d'attaque sont les modes opératoires utilisés par la source de menace pour exploiter les vulnérabilités. Ils sont liés à la capacité de la source de menace et aux vulnérabilités exploitables.

- Les [événements redoutés de cybersécurité]

  Un scénario de menace induit un événement redouté de cybersécurité qui porte atteinte à une fonction du système considéré.

On trouvera en Annexe H une vision de haut niveau des scénarios de menace applicables à un STRA, sur la base de la modélisation fonctionnelle-type d'un STRA. Le contenu de cette annexe constitue un inventaire de haut niveau des scénarios de menace à considérer.

On trouvera en Annexe G une méthodologie pouvant servir à identifier systématiquement les scénarios de menace sur la base de la modélisation du système (cf. Annexe B) et des événements redoutés de cybersécurité.

Chaque scénario de menace identifié doit faire l'objet d'une estimation de sa de vraisemblance. Il s'agit d'une valeur composite (voir Figure 9) intégrant :

- Le potentiel d'attaque de la source de menace, résultant de la motivation de la source de menace et du niveau d'exploitabilité des vulnérabilités (selon les dimensions topologiques, temporelles, capacitaires) en lien avec les capacités de la source de menace ;
- Le niveau de difficulté de réalisation de l'attaque, résultant des mesures de cybersécurité déjà mises en œuvre au sein du système considéré (et, en creux, des vulnérabilités du système).

Figure 9 : Exemple de matrice de vraisemblance

Niveau de vraisemblance	Signification
[1] Invraisemblable	La cible a très peu de chances d'être choisie par la source de menace et / ou d'être atteinte par celle-ci via les modes opératoires envisagés.
[2] Peu vraisemblable	La cible a relativement peu de chances d'être choisie par la source de menace et / ou d'être atteinte par celle-ci via les modes opératoires envisagés.
[3] Assez vraisemblable	La cible a des chances d'être choisie par la source de menace et /ou d'être atteinte par celle-ci via les modes opératoires envisagés.
[4] Vraisemblable	La cible a des chances significatives d'être choisie par la source de menace et d'être atteinte par celle-ci via les modes opératoires envisagés.
[5] Très vraisemblable	La cible risque fortement d'être choisie par la source de menace et d'être atteinte par celle-ci via les modes opératoires envisagés.
[6] Pratiquement certain	La cible risque très fortement d'être choisie par la source de menace et d'être atteinte par celle-ci via les modes opératoires envisagés.

Tableau 7 : Echelle de vraisemblance

Principes d'identification et d'analyse des risques de cybersécurité

Les risques de cybersécurité doivent être identifiés en confrontant de manière systématique des scénarios de menace et des scénarios de conséquences sur le système considéré. On en déduit une liste de risques pertinents à prendre en compte pour le système considéré.

Les risques de cybersécurité doivent être estimés sur la base d'une matrice de risques prenant en compte les valeurs de vraisemblance du scénario de menace et de gravité du scénario de conséquences propres au risque considéré. La matrice de risques est à adapter et à définir en fonction du projet et du système considéré.

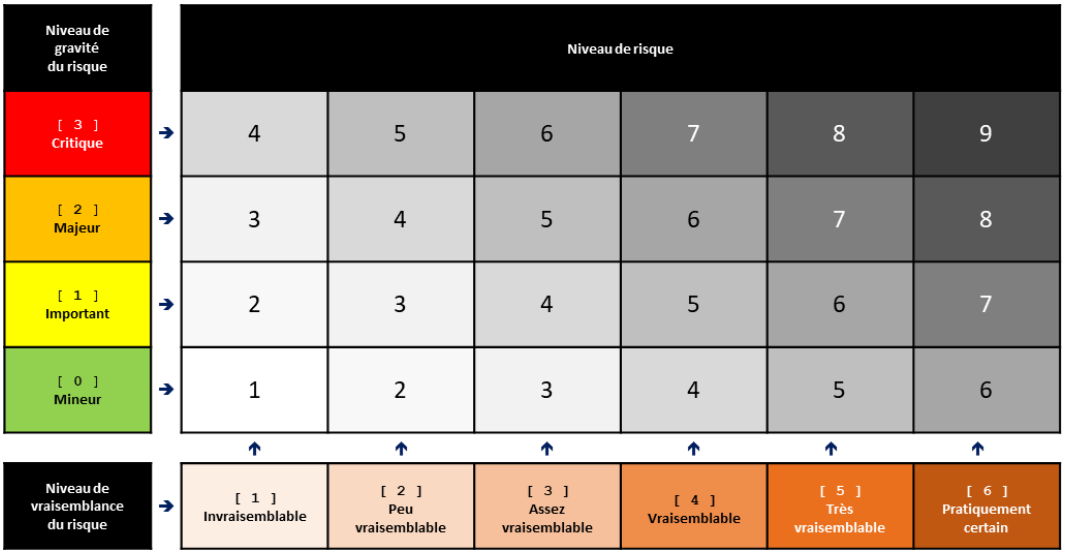


Figure 10 : Exemple de matrice de risque exprimant des niveaux de risques

Le résultat de l'identification et de l'analyse des risques de cybersécurité doit prendre la forme d'une liste de risques hiérarchisée selon le niveau de risque permettant de réaliser le traitement des risques de cybersécurité.

Principes d'évaluation des risques de cybersécurité

L'évaluation des risques de cybersécurité nécessite la spécification préalable :

- Des principes d'acceptation des risques de cybersécurité, parmi les principes suivants :
  - La conformité à un état de l'art ou un code de bonnes pratiques (ex. : instruction interministérielle n°901 relative à la protection des systèmes d'information sensibles) ;
  - La comparaison avec un système de référence ;
  - L'utilisation d'une évaluation explicite du risque sur une matrice gravité / vraisemblance.
- Des critères d'acceptation des risques de cybersécurité dérivés des principes d'acceptation des risques. Ces critères d'acceptation du risque doivent tenir compte, dans l'idéal, de la vraisemblance et de la gravité de manière indépendante, plutôt que d'un simple niveau de risque en tant que combinaison de la vraisemblance et de la gravité.

Les critères d'acceptation des risques de cybersécurité sont définis selon 3 niveaux :

- Risque acceptable : le risque peut être accepté sans mesure de réduction supplémentaire
- Risque tolérable : le risque doit, autant que possible, être ramené à un niveau acceptable
- Risque inacceptable : le risque doit être éliminé ou à minima faire l'objet d'un plan de traitement des risques visant à le ramener à un niveau acceptable ou tolérable

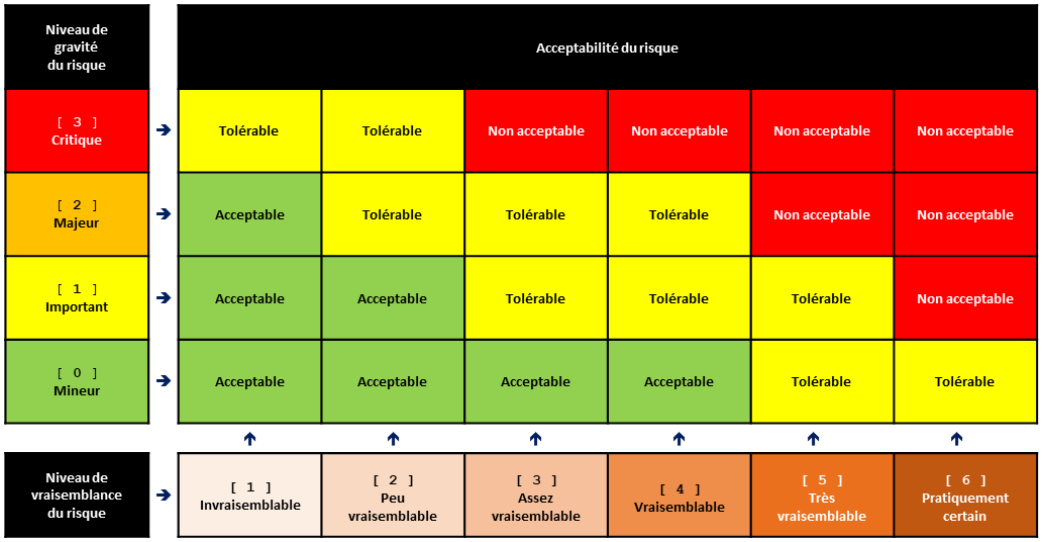


Figure 11 : Exemple de matrice de risque incluant les critères d'acceptation du risque

Principe de traitement des risques de cybersécurité

Les options de traitement des risques, lorsque ces derniers sont déterminés comme non acceptables au titre de l'évaluation des risques de cybersécurité, sont les suivantes :

- le refus des risques de cybersécurité : changer le contexte ou le système de telle sorte qu'on n'y soit plus exposé ;
- la réduction des risques de cybersécurité : appliquer des mesures de cybersécurité au système considéré ou exporter des exigences fonctionnelles de cybersécurité vers une autre partie prenante pour diminuer la gravité et / ou la vraisemblance.

Le choix des options de traitement peut être fait notamment en prenant en compte :

- les constituants du risque de cybersécurité (source de menace, scénario de menace, bien support, événement redouté, etc.) qui permettent de qualifier le fait que le traitement est réalisable ;
- les invariants de l'appréciation des risques de cybersécurité : contraintes, hypothèses et éléments identifiés ;
- les critères de gestion des risques définis par ailleurs ou induits (ex. : difficulté d'agir sur la vraisemblance d'un risque très peu vraisemblable).

Le choix des options de traitement, pour chaque risque de cybersécurité, doit être motivé et tracé. Plusieurs options peuvent être choisies pour traiter un même risque de cybersécurité.

Annexe D : Définition et attribution des NICS

L'assurance cybersécurité du système considéré est sous-tendue par les Niveaux d'Intégrité Cybersécurité Système (NICS). Ceux-ci constituent un système de classification décrivant les exigences à respecter pour assurer que les activités relatives aux exigences applicables à la cybersécurité sont réalisées, à chaque étape du cycle de vie du système considéré, proportionnellement aux risques de cybersécurité sur le système considéré. Une fois déterminé, un NICS caractérise la rigueur attendue dans la réalisation des activités de cybersécurité constitutives du cycle de vie du système considéré.

Processus de définition des NICS

Généralités

Le NICS est globalement utilisé pour garantir que les exigences applicables à la cybersécurité sont satisfaites avec le niveau de confiance requis sur un système donné (le système considéré, un de ses sous-systèmes, ou un de ses éléments).

Le NICS vise notamment à garantir qu'un objectif de cybersécurité est atteint avec le niveau de confiance requis, et par conséquent que le risque de cybersécurité qui a fait l'objet d'un traitement au titre de cet objectif de cybersécurité est à un niveau acceptable (cf. Annexe C).

Dans le cadre de ce guide :

- Le niveau de confiance est caractérisé par le niveau de rigueur dans la réalisation des activités liées aux exigences applicables à la cybersécurité sur le système considéré ;
- Le niveau de confiance requis est proportionnel au niveau de risque estimé, sans tenir compte des mesures de cybersécurité existantes.

En conséquence, les NICS sont déterminés sur la base d'une matrice prenant en compte les valeurs de potentiel d'attaque de la (ou des) source(s) de menace et de gravité du (ou des) scénario(s) de conséquences sur ce périmètre.

La matrice de NICS est à adapter et à définir par projet et en fonction du système considéré. La présente annexe propose un exemple de matrice de NICS.

Niveau de gravité du risque	Niveau d'Intégrité Cybersécurité Système (NICS)					
[3] Critique	[NICS 3]	[NICS 4]	[NICS 4]	[NICS 4]	[NICS 4]	[NICS 4]
[2] Majeur	[NICS 3]	[NICS 3]	[NICS 3]	[NICS 3]	[NICS 4]	[NICS 4]
[1] Important	[NICS 2]	[NICS 2]	[NICS 2]	[NICS 2]	[NICS 3]	[NICS 3]
[0] Mineur	[NICS 1]	[NICS 1]	[NICS 1]	[NICS 2]	[NICS 2]	[NICS 2]
Potentiel d'attaque de la source de menace	[1] Très faible	[2] Faible	[3] Modéré	[4] Significatif	[5] Élevé	[6] Très élevé

Figure 12 : Exemple de matrice de NICS en fonction de la gravité et du potentiel d'attaque

L'assertion de NICS est la traduction formelle de la définition des NICS en une assertion assumée par l'entité responsable et le cas échéant, les autres entités responsables en interface, devant servir de base à :

- L'établissement de la matrice de NICS ;
- L'association des exigences de NICS à chaque NICS.

et permettre d'en justifier la pertinence. L'assertion de NICS associée à l'exemple ci-dessus pourrait être, concernant le NICS 4 :

- Lorsque celui-ci est utilisé globalement : « le NICS 4 représente l'assurance que les exigences applicables à la cybersécurité sont satisfaites avec un niveau de rigueur approprié aux risques de gravité 3 quel que soit le potentiel d'attaque, et aux risques de gravité supérieure à 2 et de potentiel d'attaque élevé ou très élevé ».
- Lorsque celui-ci est notamment utilisé en lien avec un objectif de cybersécurité : « le NICS 4 représente l'assurance d'une protection vis-à-vis des risques de gravité 3 quel que soit le potentiel d'attaque, et des risques de gravité supérieure à 2 et de potentiel d'attaque élevé ou très élevé ».

Objectifs

Le processus de définition des NICS a pour but de se fixer et justifier une échelle de NICS afin de partager une compréhension du niveau de rigueur attendu entre l'entité responsable et les parties prenantes concernées, notamment les autres entités responsables en interface.

Activités du processus

Le processus de définition des NICS inclut les activités suivantes :

1. Identifier les parties prenantes qui doivent partager une compréhension du niveau de rigueur attendu relatif au système considéré avec l'entité responsable, notamment les autres entités responsables en interface.
2. Elaborer le référentiel contenant la définition des NICS
3. Définir l'assertion de NICS conformément aux exigences des parties prenantes du système considéré.
4. Etablir la matrice de NICS
5. Définir les échelles d'exigences de NICS pour le projet, couvrant l'ensemble des exigences applicables du présent guide.

Processus de détermination et de réévaluation des NICS

Généralités

Un NICS est déterminé pour le système considéré, y compris quand le risque est jugé acceptable en l'état (cf. Annexe C), et donc quelle que soit l'option de traitement des risques choisie.

Des NICS peuvent être alloués à différents éléments du système considéré avec un niveau de raffinement variable, hérité de l'appréciation des risques de cybersécurité. En effet, en cas de NICS élevé pour un système donné (le système considéré ou un de ses éléments), il est recommandé de décomposer ce périmètre en éléments permettant de séparer les éléments présentant les enjeux les plus forts, et donc nécessitant des NICS élevés, des éléments à moindre enjeu. Cette décomposition hérite notamment :

- De la décomposition fonctionnelle du système considéré, qui est une approche naturelle de raffinement du système (cf. Annexe I) ;
- De l'applicabilité d'un ou plusieurs scénarios de risque à un système donné (le système considéré, un sous-système ou un élément du système considéré) ;
- Le cas échéant, de l'architecture fonctionnelle de cybersécurité et de l'architecture technique de cybersécurité.

Les NICS étant liés aux niveaux de risques de cybersécurité, un élément du système considéré peut hériter d'un NICS différent d'un autre élément, dès lors qu'il est soumis à des risques de cybersécurité qui lui sont propres.

Le système considéré ou tout élément du système considéré hérite du niveau de risque maximal des scénarios qui lui sont applicables, et donc du NICS associé.

Le ou les NICS ainsi déterminés sont le(s) NICS requis, permettant de déterminer les exigences de NICS qui s'appliquent au système considéré et, le cas échéant, à ses éléments.

NOTA : le NICS déterminé pour le système considéré est toujours requis, y compris dans le cas où l'ensemble de ses éléments se voient allouer un NICS. En effet, certaines exigences applicables à la cybersécurité, et par conséquent certaines exigences de NICS, s'appliquent toujours à l'ensemble du système considéré et de ses interfaces.

Principes de détermination initiale et de réévaluation d'un NICS

La détermination initiale d'un NICS est effectuée en début de cycle de vie du système considéré, car les exigences de NICS doivent être intégrées dans le processus de planification du projet. La détermination d'un NICS doit se faire dans le cadre de la définition des exigences des parties prenantes concernées, notamment les autres entités responsables en interface. Un NICS est déterminé sur la base des résultats de l'appréciation des risques.

Un NICS doit être réévalué après chaque itération de l'appréciation des risques. Si le NICS évolue, deux cas sont à distinguer :

1. Le risque auquel est lié le NICS reste acceptable : dans ce cas, le NICS réévalué devient le NICS requis pour toutes les activités relatives aux exigences applicables à la cybersécurité en cours ou à venir.
2. Le risque auquel est lié le NICS devient inacceptable : dans ce cas, le NICS réévalué devient le NICS requis pour toutes les activités relatives aux exigences applicables à la cybersécurité de l'ensemble du cycle de vie. Le système considéré fait l'objet d'une modification substantielle.

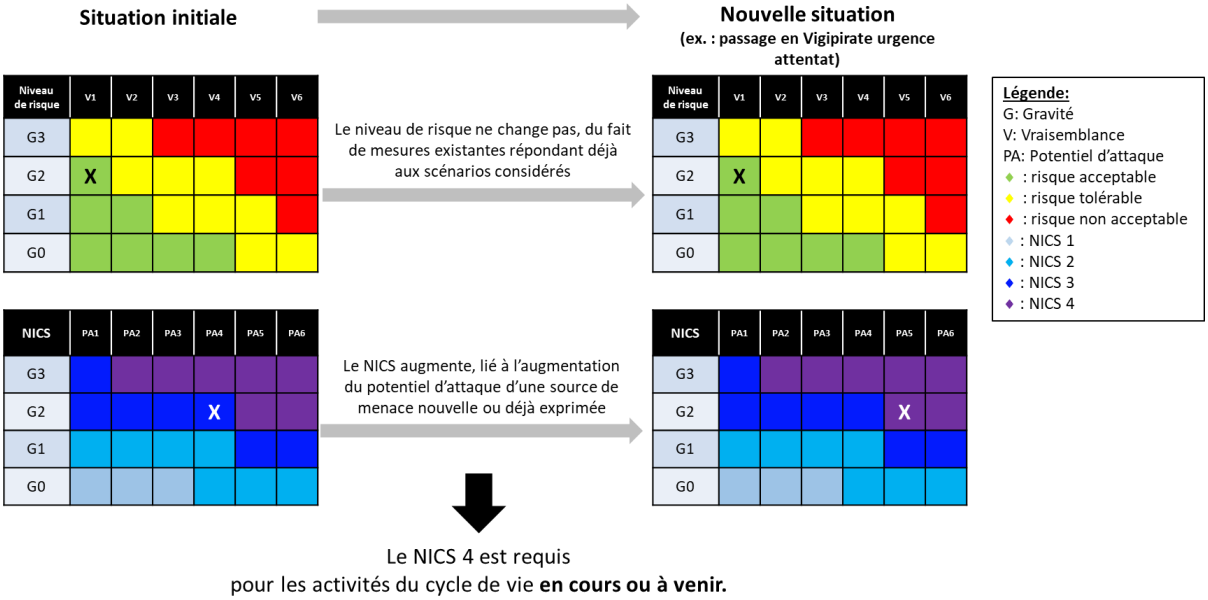


Figure 13 : Exemple de réévaluation d'un NICS (risque résiduel non modifié, niveau acceptable)

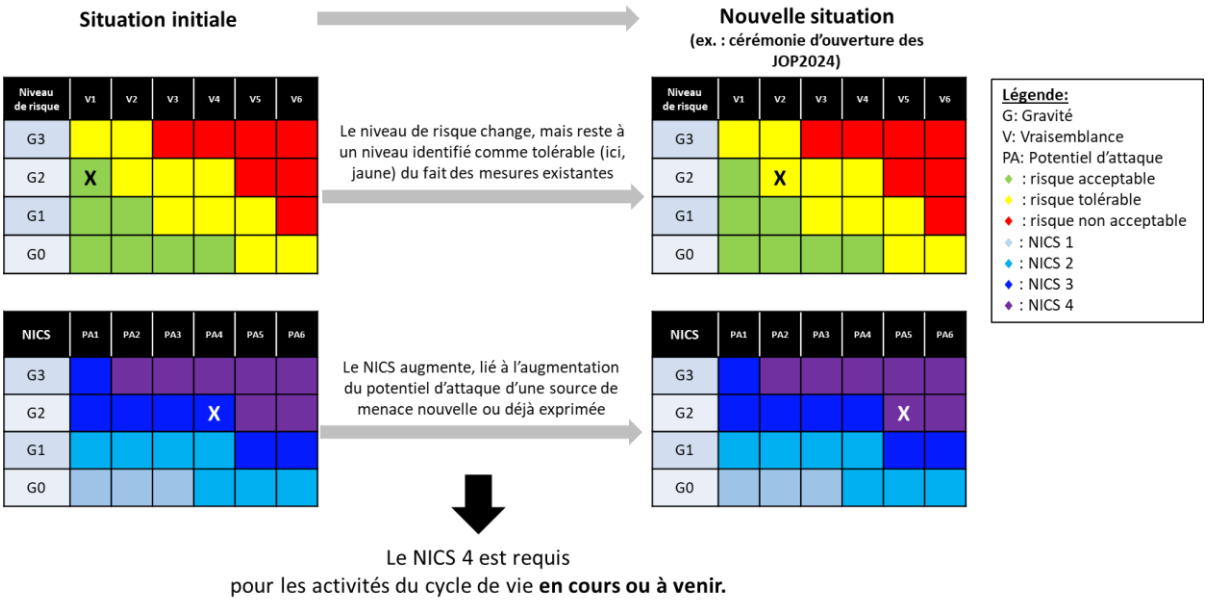


Figure 14 : Exemple de réévaluation d'un NICS (risque résiduel modifié, niveau tolérable)

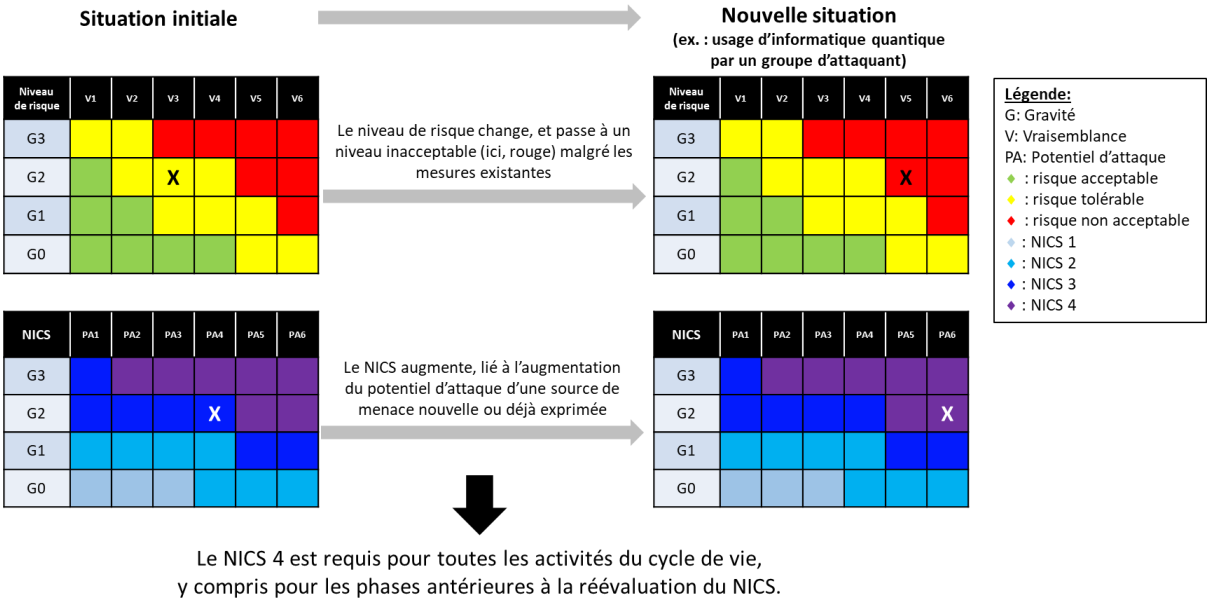


Figure 15 : Exemple de réévaluation d'un NICS (risque résiduel modifié, niveau inacceptable)

Objectifs

Le processus de détermination et de réévaluation d'un NICS a pour but d'établir le NICS garantissant que les exigences applicables à la cybersécurité sont satisfaites avec le niveau de confiance requis sur le système considéré, un sous-système ou un élément (et notamment qu'un objectif de cybersécurité est atteint avec le niveau de confiance requis), et par conséquent que les activités relatives aux exigences applicables à la cybersécurité sont réalisées avec le niveau de rigueur requis, proportionnellement aux risques de cybersécurité sur le système considéré.

Activités du processus

Le processus de détermination et de réévaluation du ou des NICS est mis en œuvre après chaque itération de l'appréciation des risques. Il inclut les activités suivantes en fonction des informations disponibles :

1. Identifier les scénarios de risques de cybersécurité pour le système considéré ;
2. Evaluer le potentiel d'attaque et la gravité de chacun de ces scénarios ;
3. Calculer le NICS de chaque scénario selon la matrice de NICS ;
4. Déterminer le NICS requis pour le système considéré : il s'agit de la valeur maximale des NICS de tous les scénarios de risques pour le système considéré ;
5. Allouer les NICS :

   5.1 Allouer globalement des NICS aux sous-systèmes ou éléments du système considéré :

   a. Identifier et définir les sous-systèmes ou éléments du système considéré pour lesquels une allocation de NICS est souhaitée ;
   b. Pour chaque sous-système ou élément identifié ci-avant :
      i. Identifier et convenir des parties prenantes concernées ;
      ii. Identifier le ou les scénarios de risque de cybersécurité qui le concerne ;
      iii. Déterminer son NICS requis, qui correspond à la valeur maximale des NICS de tous les scénarios de risque qui le concernent ;

   5.2 Allouer successivement les NICS des scénarios de risques du système considéré :

   c. Aux objectifs de cybersécurité du système considéré : le NICS requis d'un objectif de cybersécurité correspond au NICS du scénario auquel il est associé ;
   d. Aux exigences fonctionnelles de cybersécurité du système considéré : le NICS requis d'une exigence fonctionnelle de cybersécurité correspond à la valeur maximale des NICS des objectifs de cybersécurité qu'elle décline ;
   e. Aux sous-systèmes du système considéré appartenant à l'architecture fonctionnelle de cybersécurité : le NICS requis d'un sous-système de l'architecture fonctionnelle de cybersécurité correspond à la valeur maximale des NICS des exigences fonctionnelles qui lui sont attribuées.
   f. Aux mesures de cybersécurité du système considéré : le NICS requis d'une mesure de cybersécurité correspond à la valeur maximale des NICS des exigences fonctionnelles de cybersécurité auxquelles elle est associée.
   g. Aux éléments du système considéré appartenant à l'architecture technique de cybersécurité : le NICS requis d'un élément de l'architecture technique de cybersécurité correspond à la valeur maximale des NICS des mesures de cybersécurité auxquelles il est lié ;

6. Identifier les exigences de NICS associées au(x) NICS requis.

Processus de respect des exigences de NICS

Généralités

Une exigence applicable à la cybersécurité est réputée respectée pour le système considéré si les exigences de NICS associées au NICS déterminé pour le système considéré sont respectées.

Le respect des exigences de NICS est un processus qui permet de s'assurer que les exigences de NICS associées au NICS déterminé pour le système considéré et aux NICS alloués aux éléments du système considéré sont satisfaites. Ce processus repose sur un ensemble de preuves obtenues au cours des processus du cycle de vie du système considéré. La confirmation qu'un niveau de risque acceptable est atteint ou maintenu faisant partie des activités de validation de la cybersécurité, le processus de respect des exigences de NICS fait partie de la validation de la cybersécurité.

Objectifs

L'objectif du processus de respect des exigences en matière de niveau d'intégrité est de parvenir à un accord entre l'entité responsable et les parties prenantes concernées, notamment les autres entités responsables, sur le fait que les exigences applicables à la cybersécurité sont respectées, et donc que le niveau de risque résiduel pesant sur le système considéré demeure acceptable.

Cas particulier du véhicule

L'entité responsable doit :

- S'assurer que tous les risques identifiés au niveau du système considéré et impliquant le véhicule ou ses serveurs dorsaux ont bien été identifiés par le constructeur du véhicule dans le cadre de sa réception au titre du code de la route (homologation) ;
- S'assurer que l'appréciation de chaque risque ainsi identifié tient compte de toutes les composantes du risque (cf. Annexe C) ;
- Prendre en compte les mesures d'atténuation mises en place au niveau du véhicule dans son appréciation des risques au niveau du système considéré.

Dans ces conditions, les exigences de NICS qui pourraient concerner le véhicule ou ses serveurs dorsaux sont réputées respectées par l'homologation du véhicule, et notamment par la conformité du constructeur et du véhicule au règlement UNR 155.

Activités du processus

Le processus de respect des exigences de NICS est mis en œuvre dans les phases de cycle de vie suivants du système considéré :

a. Phase de spécification/conception, phase de développement, phase de fabrication, phase d'exploitation/ maintenance en référence au processus de gestion des risques de cybersécurité :
    1. Pour chaque élément concerné du système considéré, recueillir les preuves démontrant la conformité aux exigences de NICS associées au NICS de cet élément du système considéré ;
    2. Concernant le véhicule, recueillir la preuve que tous les risques identifiés au niveau du système considéré et impliquant le véhicule ou ses serveurs dorsaux ont bien été identifiés par le constructeur du véhicule dans le cadre de sa réception au titre du code de la route ;
    3. Recueillir les preuves nécessaires pour démontrer la conformité aux exigences de NICS associées au NICS du système considéré.
b. Phase d'intégration / installation :
    1. Pour chaque élément concerné du système considéré, recueillir les preuves démontrant la conformité aux exigences de NICS associées au NICS de cet élément du système considéré ;
    2. Recueillir les preuves démontrant la conformité aux exigences de NICS associées au NICS du système considéré ;
    3. Pour chaque élément concerné du système considéré, vérifier que les preuves obtenues satisfont aux exigences de NICS associées au NICS de cet élément du système considéré ;
    4. Vérifier que les preuves obtenues satisfont aux exigences de NICS du système considéré ;
    5. Valider que les preuves obtenues montrent que le NICS requis du système considéré est atteint.

Annexe E : Outils de modélisation via le modèle stratifié

La modélisation du système considéré se projette dans un espace stratifié pour l'élaboration des scénarios de menace. Les éléments exposés ci-après proviennent pour partie du Guide AFNOR – Normes volontaires et approches innovantes pour la cybersécurité.

Modèle de base pour la projection dans un espace stratifié

Des moyens innovants de représentation d'un espace de confrontation sont abordés, notamment, dans la doctrine militaire française de lutte informatique offensive. Il s'agit de rendre en compte de la complexité des composantes humaines, numériques et physiques et de leurs interdépendances.

L'un de ces moyens consiste à modéliser l'espace, et par extension le système considéré, en introduisant un modèle de représentation stratifié en trois strates fondamentales :

- La strate ANTHROPIQUE qui représente les acteurs humains et les groupes d'acteurs humains organisés en réseaux sociaux ;
- La strate NUMERIQUE qui représente les processus logiques et les données informatiques, incluant les avatars des acteurs humains ;
- La strate PHYSIQUE qui représente les composants physiques et la localisation géographique des composants et des personnes.

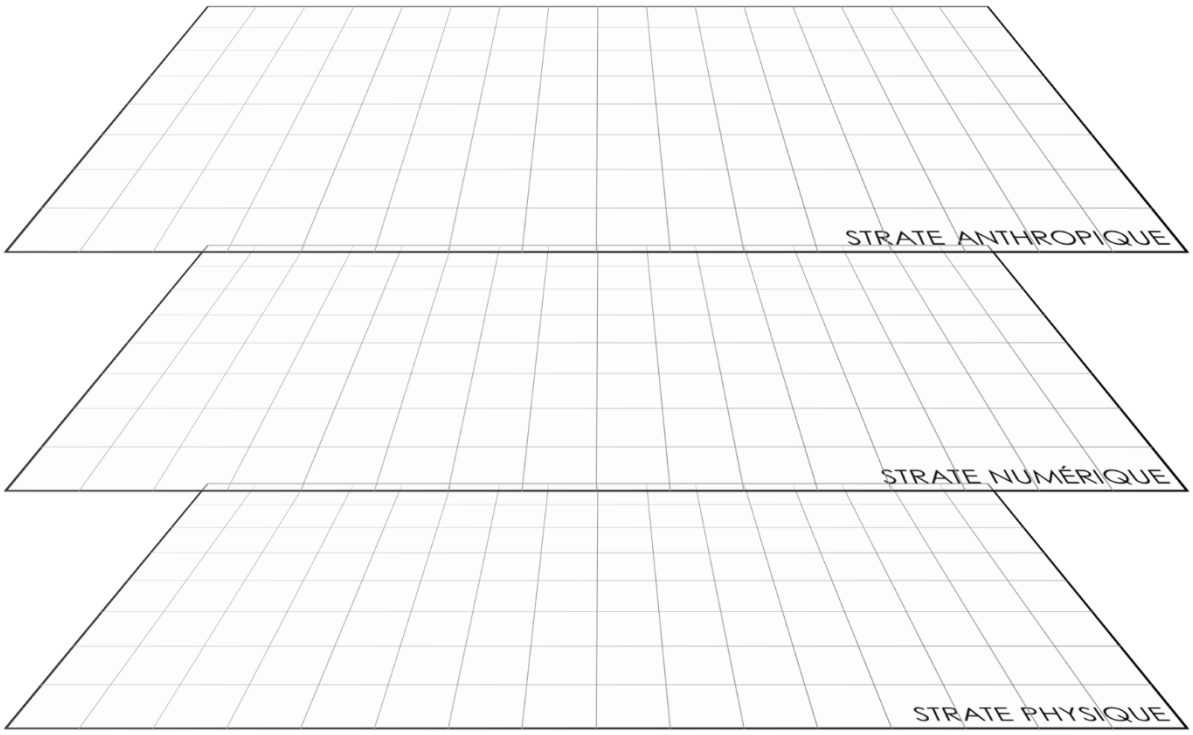


Figure 16 : Projection de l'espace de confrontation sur un modèle de l'espace stratifié

Le modèle de représentation stratifié permet en particulier d'y projeter la modélisation du système considéré et son écosystème, avec un niveau de détail à la discrétion de l'analyste en fonction de la profondeur d'analyse requise, mais en gardant le modèle invariant.

Les projections sont facilitées par l'usage de bases de connaissance. Chaque strate est composée d'objets qui lui sont propres :

- Des nœuds et des liens intra-strates parcourus par des flux, de natures très différentes en fonction de la strate concernée (voir Tableau 8) ;

- Des liens inter-strates parcourus par des flux, dont la nature est propre aux strates concernées par l'échange (voir Tableau 9).

Strate	Caractéristiques
Strate anthropique	Modèle fractal : l'unité est la personne qui peut former des groupes ou des réseaux sociaux imbriqués • Nœuds : individus et groupes d'individus • Liens : diverses formes de liens sociaux (autorité, partenariat, antagonisme, etc.) • Flux : flux associés aux liens sociaux (subornation, collaboration, confrontation, etc.)
Strate numérique	Modèle fractal : chaque système logique peut être constitué de sous-systèmes logiques et peut être le constituant de systèmes plus volumineux : • Nœud : processus informatique • Lien : protocole de communication • Flux : flux d'informations
Strate physique	Modèle fractal : niveau de détail variable (plan d'occupation des sols, structure d'un bâtiment, carte topographique, etc.). La strate est soumise aux lois de la physique. • Nœud : biens meubles • Lien : canalisation [matière], câble électrique [énergie], câble ethernet [information] • Flux : flux de matière, flux d'énergie, flux d'informations

Tableau 8 : Typologie des composants par strate

Strates concernées	Nature des liens inter-strates
anthropique ↔ numérique	Lien d'identité : identités numériques d'un acteur humain (adresse mail, compte utilisateur, avatar sur un réseau social, etc.) Lien de connaissance : connaissance par l'acteur humain d'une identité numérique (ex. : un avatar de réseau social) Lien d'accès : accès d'un acteur humain à un composant numérique (au sens contrôle / commande du terme)
anthropique ↔ physique	Lien de localisation : localisation géographique (dans une zone, un bâtiment, etc.) d'un acteur humain Lien de connaissance : connaissance par l'acteur humain d'une information de localisation physique ou géographique Lien d'accès : capacité d'un acteur humain à accéder à un composant physique et / ou à une zone géographique
numérique ↔ physique	Lien de localisation : localisation des composants physiques qui hébergent une donnée (possiblement très distribués) Lien d'implémentation : localisation des composants physiques qui exécutent un programme (possiblement très distribués) Lien de contrôle / commande : capacité d'un programme à interagir avec un composant physique (ex. : capteur / actionneur)

Tableau 9 : Typologies des liens inter-strates

Projection du STRA dans le modèle stratifié

La représentation résultante offre une vision topologique du système considéré, facilitant la construction des scénarios de menace. L'application de ce modèle au STRA s'effectue en deux étapes :

- Identifier et expliciter les composants propres au système considéré sur chacune des strates de représentation (cf. Figure 17, Figure 18, Figure 19) ;
- Identifier et caractériser les liens entre les différents composants sur chacune des strates (cf. Figure 20).

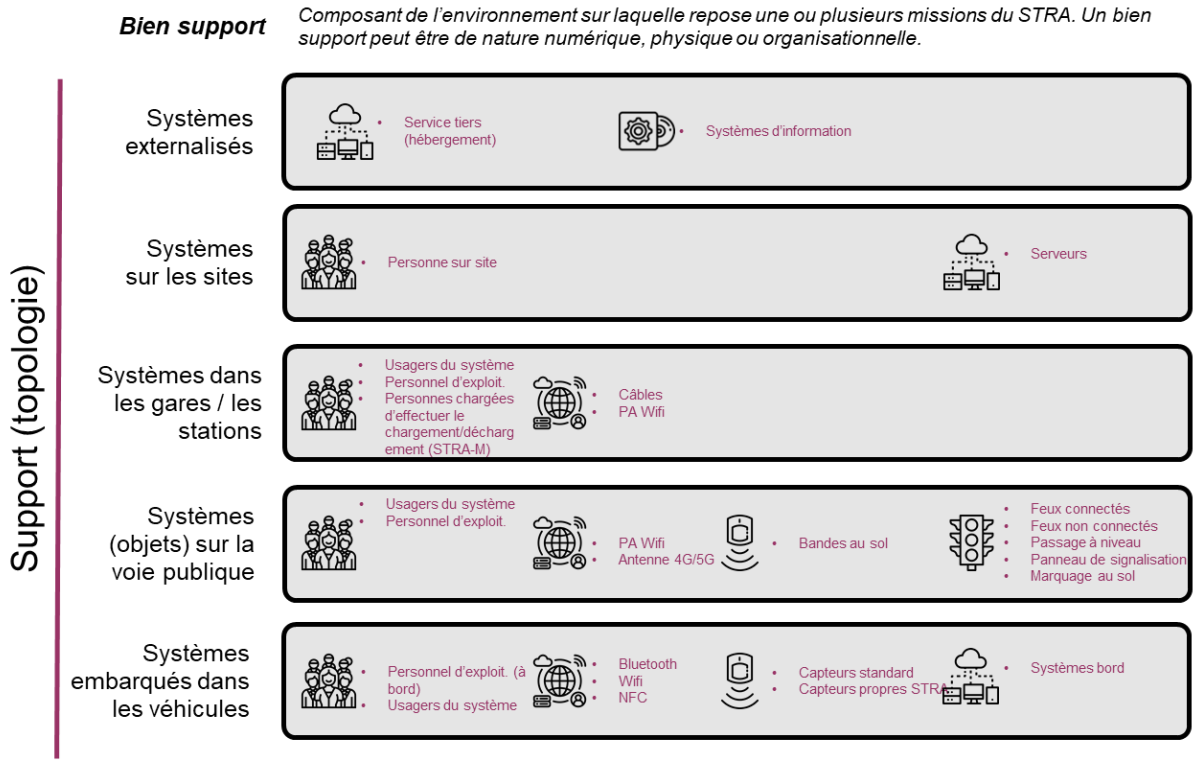


Figure 17 : Approche topologique pour la modélisation du système considéré (espace physique)

Figure 18 : Approche topologique pour la modélisation du système considéré (espace numérique)

Figure 19 : Approche topologique pour la modélisation du système considéré (espace anthropique)

Ces trois couches fondamentales peuvent aussi être subdivisées pour des analyses particulières ; le caractère fractal du modèle de représentation stratifié permet de modéliser des interactions fines entre deux strates distinctes.

En d'autres termes, autant de strates que nécessaires peuvent être introduites, dès lors qu'elles servent à mieux représenter la réalité. Les subdivisions les plus rencontrées sont les suivantes :

- Subdivision de la strate physique (voir Figure 20) en une strate « géographique » (topologie physique de l'espace et localisation géographique des composants et des personnes) et une

strate « composant » (composants physiques de l'espace, incluant les matériels constitutifs des STRA) ;

- Subdivision de la strate numérique en une strate « cybernétique » (processus et données informatiques, qui peut-être elle-même subdivisée si nécessaire en couches du modèle OSI - voir Figure 20) et une strate « cyber-persona » (identités numériques nécessaires pour les échanges).

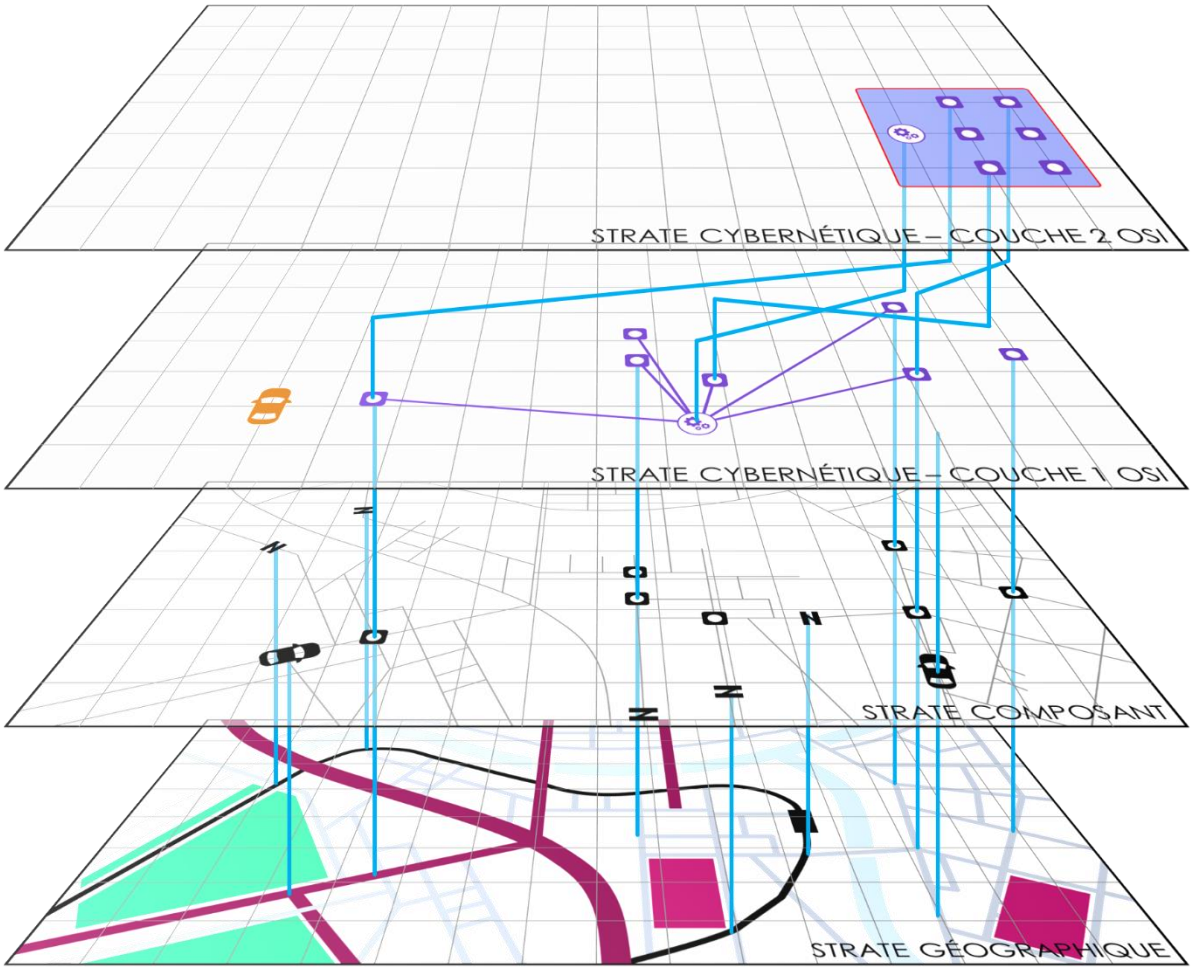


Figure 20 : Projection (partielle) d'un STRA dans la modélisation stratifiée de l'espace

Annexe F : Outils de caractérisation des sources de menaces

La caractérisation des sources de menace est une étape indispensable de l'élaboration des scénarios de menace. Les éléments exposés ci-après proviennent pour partie de la source bibliographique [24] Guide AFNOR – Normes volontaires et approches innovantes pour la cybersécurité.

Identification des sources de menaces

L'identification des sources de menaces est directement issue des activités de veille menace réalisée lors du cycle de vie du système considéré (en phase de spécification / conception et en phase d'exploitation / maintenance).

A des fins d'identification systématique des sources de menace relativement au système considéré, elles peuvent être structurées :

- En catégories générales d'acteurs naturellement à l'origine de menace (ex. : états agressifs, crime organisé, groupes terroristes, mouvements sectaires, etc.) ;
- En catégories reflétant une relation particulière avec un acteur de l'écosystème pouvant développer un antagonisme (ex. : concurrents, fournisseurs, employés, etc.).

Additionnellement, les sources de menaces peuvent être positionnées dans des zones caractérisant leur activité en fonction du contexte global (ce zonage peut évoluer dans le temps : cas d'une source de menace étatique en situation de paix vs en situation de guerre, d'une source de menace interne en période nominale ou en période de tension sociale, etc.) :

- Zone de veille : la source de menace est pertinente pour le système considéré et son activité peut simplement être suivie au titre de la veille menace usuelle ;
- Zone de vigilance : la source de menace est pertinente pour le système considéré et son activité doit faire l'objet d'une vigilance accrue au titre de la veille menace usuelle ;
- Zone de surveillance : la source de menace est pertinente pour le système considéré et son activité doit faire l'objet d'une surveillance particulière au titre de la veille menace.

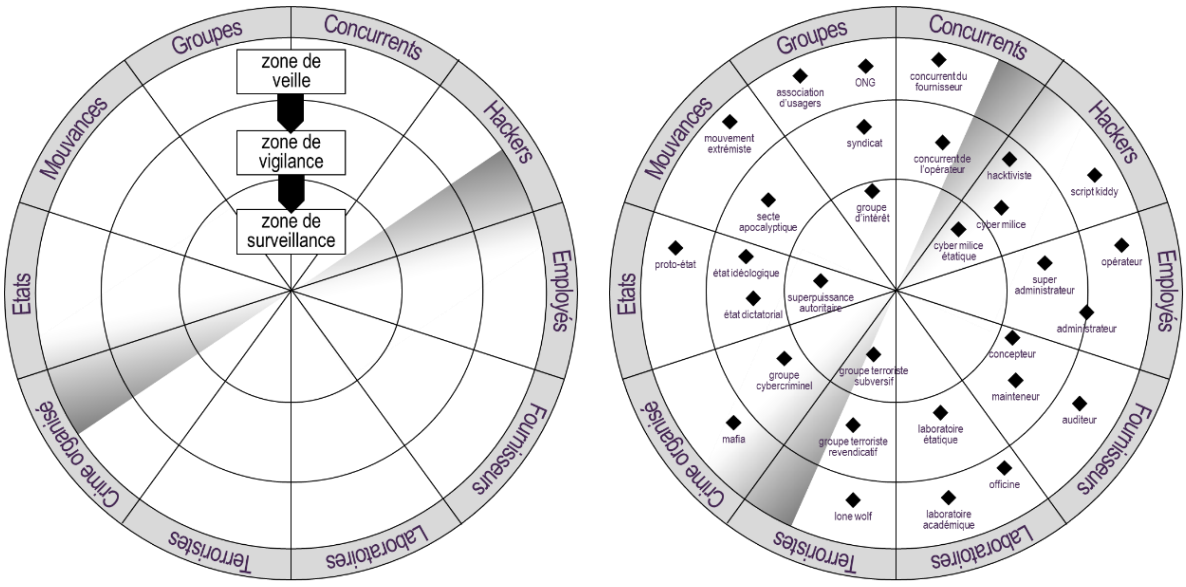


Figure 21 : Caractérisation des sources de menaces en catégories générales

Caractérisation et évaluation des motivations des sources de menaces

Les sources de menace identifiées sont caractérisées – entre autres caractéristiques – par leurs motivations. Les différentes typologies de motivation peuvent s'exprimer comme suit :

- Motivation politique (induit des notions de pouvoir, prestige, puissance, etc.) ;
- Motivation économique (induit des notions de richesse, possession, influence, etc.) ;
- Motivation idéologique (induit des notions de culture, religion, éthique, etc.) ;
- Motivation sociale (induit des notions de reconnaissance, influence, etc.) ;
- Motivation idiosyncrasique (propre à chaque individu et par conséquent peu prédictible).

La motivation est directement liée à l'attractivité du système considéré pour la source de menace. En conséquence, on peut matérialiser la motivation d'une source de menace au travers du projet de la source de menace et l'exprimer sous la forme d'un Etat Final Recherché (EFR) : la situation globale que veut atteindre l'attaquant à l'issue de la confrontation.

Les EFR sont ainsi structurés selon deux axes :

- La typologie de la motivation de la source de menace (voir ci-avant) ;
- Les buts de la source de menace, dépendant notamment de l'attractivité de la cible pour la source de menace :
    - Conquérir : obtenir la suprématie (supériorité totale)
    - Evincer : obtenir la supériorité en neutralisant l'adversaire
    - Acquérir : obtenir la supériorité en s'appropriant de nouvelles ressources
    - Repousser : préserver la parité en contenant le développement adverse
    - Maintenir : préserver la parité en conservant sa situation
    - Empêcher : préserver la parité en entravant les actions d'un tiers
    - Défendre : limiter la situation d'infériorité (à l'extrême : assurer la survie)

La combinaison des deux facteurs permet :

- De déterminer des EFR qui dépendent à la fois d'éléments de contexte et de la catégorie de la source de menace (cf. Tableau 10) ;
- D'identifier les sources de menaces les plus pertinentes et une première approche des types d'attaque sans passer par une étape de gradation de la motivation (cf. Tableau 11).

EFR	Politique	Economique	Idéologique	Sociale	Idiosyncrasique
Conquérir	Gagner le pouvoir absolu	Dominer un marché	Imposer ses valeurs	Contrôler les autres groupes sociaux	Agir par fanatisme, mégalomanie ou orgueil
Evincer	Interdire le pouvoir	Eliminer l'acteur économique	Interdire les valeurs	Mettre au ban Déchoir	Agir par haine ou désir de vengeance
Acquérir	Participer au pouvoir	Obtenir des parts de marché	Faire reconnaître ses valeurs	Acquérir un capital social ou des droits	Agir par ambition ou cupidité
Repousser (infériorité)	Chasser du pouvoir	Faire perdre des parts de marché	Faire reculer les valeurs	Compromettre la réputation	Agir par jalousie ou par envie
Maintenir (statu quo)	Garder le pouvoir	Conserver ses parts de marché	Protéger ses valeurs	Conserver sa réputation	Agir par fierté ou par devoir
Empêcher (statu quo)	Interdire l'accès au pouvoir	Confiner une position de marché	Interdire la progression	Entraver la notoriété	Agir par aversion ou par mépris
Défendre (survie)	Limiter la perte de pouvoir	Limiter la perte de marché	Limiter le recul de ses valeurs	Limiter la perte de capital social	Agir par peur ou instinct de survie

Tableau 10 : Confrontation des facteurs de motivation et des buts de la source de menace

Source de menace	Objectif visé Etat Final Recherché	Type d'attaque Objectifs stratégiques	Scénario d'attaque Niveau Opérationnel
Etat autoritaire	Acquisition d'un vecteur d'attaque stratégique [motivation : politique] [but : acquérir]	Subversion des infrastructures critiques	Déploiement d'un malware furtif et persistant dans la chaîne logistique
Entreprise agressive	Obtention d'un monopole sur un marché [motivation : économique] [but : conquérir]	Influence du régulateur	Corruption d'un décideur
Mafia	Développement d'activités illicites [motivation : économique] [but : acquérir]	Extorsion	Diffusion de ransomware

Tableau 11 : Exemple d'identification de sources de menaces pour un STRA basée sur les EFR

Les motivations des sources de menace sont évaluées à l'aide d'une échelle de motivation (cf. Tableau 13), chacun des niveaux de l'échelle étant lui-même associé à une ou plusieurs combinaison(s) de marqueurs de motivation (cf. Tableau 12), tous dépendant de la typologie de la source de menace et de l'attractivité de la cible vis-à-vis de la source de menace :

- Marqueur « effort » : la part de ses ressources que la source de menace est prête à mobiliser ou à mettre en œuvre ;
- Marqueur « durée » : le temps que la source de menace est prête à passer (ou dont elle dispose) pour atteindre un but ;
- Marqueur « risque » : le risque que la source de menace est prête à prendre pour atteindre son but.

Les marqueurs d'effort, de durée et de risque seront à considérer au regard du prisme de cette notion d'attractivité. A titre d'illustration de la notion d'attractivité de la cible, on peut considérer l'exemple d'une opération de blocage du trafic (motivation diverse ; but : repousser / évincer) : elle présentera un grand intérêt dans une gare routière parisienne compte tenu de son impact sociétal et médiatique potentiel mais aucun dans une gare routière de province faiblement desservie.

Effort	
E1	La part de ses ressources que la source de menace est prête à mobiliser est minimale
E2	La part de ses ressources que la source de menace est prête à mobiliser est faible
E3	La part de ses ressources que la source de menace est prête à mobiliser est significative
E4	La part de ses ressources que la source de menace est prête à mobiliser est substantielle
E5	La source de menace est prête à mettre en œuvre la quasi-intégralité de ses ressources
E6	La source de menace est prête à mettre en œuvre l'intégralité de ses ressources

Durée	
D1	La source de menace n'est en capacité que de réaliser des actes opportunistes
D2	La durée dont la source de menace dispose s'évalue en jours
D3	La durée dont la source de menace dispose s'évalue en semaines
D4	La durée dont la source de menace dispose s'évalue en mois
D5	La durée dont la source de menace dispose s'évalue en semestres
D6	La durée dont la source de menace dispose s'évalue en années

Risque	
R1	La source de menace n'est pas prête à prendre des risques
R2	La source de menace est prête à prendre des risques mais a un fort sentiment d'impunité
R3	La source de menace est prête à engager sa réputation
R4	Niveau R3 + La source de menace est capable d'actes illégaux
R5	Niveau R4 + La source de menace est prête à engager sa liberté
R6	Niveau R5 + La source de menace est prête à engager son intégrité physique

Tableau 12 : Echelle de marqueurs de motivation

Les marqueurs de motivation sont à combiner pour estimer la motivation. Il n'existe pas de formule stabilisée pour évaluer le niveau de motivation d'une source de menace en fonction de ces marqueurs ; une source de menace peut combiner des marqueurs de valeurs très différentes (ex. : E2, D1, R5).

	Echelle de motivation
1	**Niveau 1 : Indifférent** Le système considéré a une valeur quasi-nulle pour la source de menace. La source de menace ne réalisera que des actes opportunistes sur le système considéré.
2	**Niveau 2 : Curieux** Le système considéré a une valeur minime pour la source de menace. La source de menace ne réalisera que des actes opportunistes ou exploratoires, éventuellement pour vérifier si des actes plus élaborés sont simplement réalisables, sans s'exposer à des risques trop important (réputation, riposte judiciaire, etc.).
3	**Niveau 3 : Explorateur** Le système considéré a une valeur modérée pour la source de menace. La source de menace pourra tenter de porter atteinte au système considéré pour des bénéfices ciblés sans s'exposer à des risques trop importants (réputation, riposte judiciaire, etc.).
4	**Niveau 4 : Intéressé** Le système considéré a une valeur significative pour la source de menace. La source de menace pourra tenter de porter atteinte au système considéré pour des bénéficies ciblés, de manière persistante et / ou fréquente, en s'exposant à des risques modérés (réputation, riposte judiciaire, etc.).
5	**Niveau 5 : Engagé** Le système considéré a une valeur importante pour la source de menace. La source de menace pourra tenter de porter atteinte au système considéré pour des bénéficies ciblés, de manière persistante et / ou fréquente, sans prise en compte des risques encourus, notamment en termes de riposte judiciaire.
6	**Niveau 6 : Déterminé** Le système considéré a une valeur fondamentale pour la source de menace. La source de menace ciblera le système considéré systématiquement, de manière persistante et / ou fréquente, avec l'ensemble de ses moyens et sans prise en compte des risques encourus, notamment en termes de riposte judiciaire.

Tableau 13 : Exemple d'échelle de motivation

A partir de cette taxonomie, il est possible d'établir un graphe de motivation pour chaque source de menace (voir Figure 22). Ce graphe est contextuel au système considéré, puisque la motivation dépend du couple source de menace / système considéré.

Ces graphes de motivation sont construits sur la base des concepts et étapes décrits précédemment :

- Chaque source de menace identifiées dans la phase d'identification des sources de menace peut faire l'objet d'un graphe de motivation ;
- Pour une source de menace donnée, la caractérisation des EFR permet une première évaluation de l'attractivité de la cible relativement à la source de menace ;
- Pour une source de menace donnée, les marqueurs de motivation contribuent à évaluer une valeur de motivation à reporter dans le graphe de motivation.

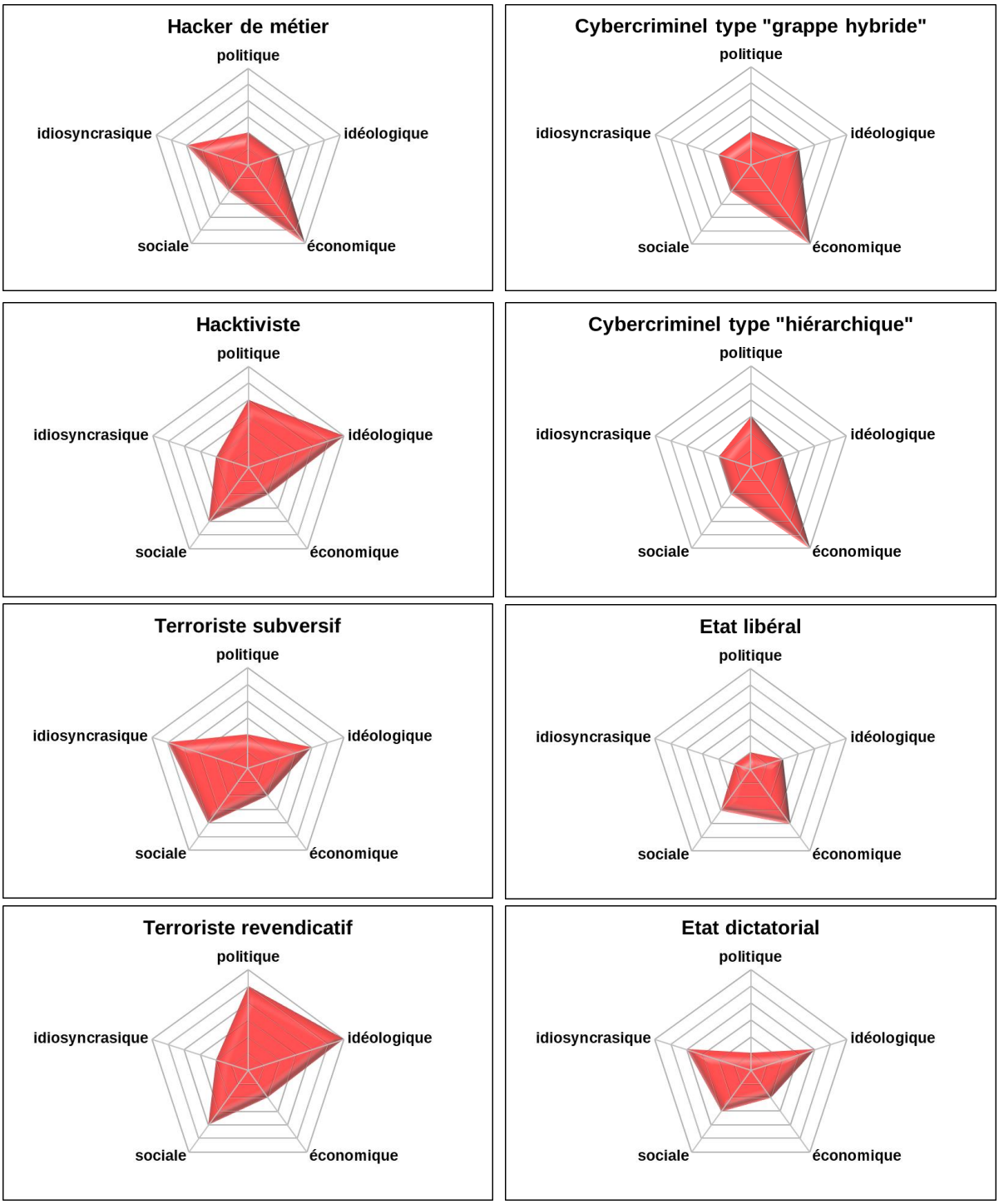


Figure 22 : Exemples de graphes de motivation pour un système considéré

Caractérisation et évaluation des capacités des sources de menaces

Les sources de menace identifiées sont caractérisées – entre autres caractéristiques – par leurs capacités : les moyens (préexistants, développés spécifiquement ou mis à disposition par un soutien) qu'elle peut mobiliser et combiner pour produire des effets sur les ressources ciblées.

Pour affiner la caractérisation des sources de menace, on peut subdiviser les capacités selon les axes suivants, en les projetant dans le modèle stratifié de l'espace :

- En plusieurs catégories opérationnelles, sur chacune des strates (physique, anthropique, numérique), notamment :
    - Les capacités logistiques qui gèrent la mise à disposition et la coordination des ressources nécessaires ;
    - Les capacités de renseignement qui fournissent les informations indispensables à la préparation et à la conduite des opérations ;
    - Les capacités défensives nécessaires à la protection des ressources engagées par l'attaquant dans la confrontation ;
    - Les capacités offensives qui exécutent l'attaque.
- En types de ressources à activer, sur chacune des strates (physique anthropique, numérique), notamment (modèle DORESE augmenté avec les moyens financiers) :
    - Doctrine : collection de principes et de bonnes pratiques permettant de guider les activités de la source de menace
    - Organisation : manière dont les ressources humaines sont agencées pour exécuter l'ensemble des activités (logistique, conduite des opérations, renseignement, etc.)
    - Ressources : quantité et qualité (connaissances et compétences), des individus appartenant à la source de menace
    - Equipements : ressources matérielles et installations mises à disposition de la source de menace pour mener ses activités
    - Soutiens : catégories de soutiens externes, financiers, matériels, intellectuels ou moraux dont bénéficie la source de menace
    - Entraînement : modalité d'acquisition et de maintien des connaissances des ressources humaines de la source de menace (exercices, simulations, etc.)
    - Finance : moyens financiers que peut mobiliser la source de menace

Les capacités des sources de menace sont évaluées à l'aide d'une échelle de capacité, chacun des niveaux de l'échelle étant lui-même associé à une combinaison de marqueurs de capacité (voir exemples proposés Tableau 14, Tableau 15 et Tableau 16).

A partir de ces éléments (la taxonomie des capacités, les marqueurs constitutifs des capacités, et les échelles de capacité), il est possible d'établir un graphe de capacités contextuel au système considéré, pour chaque source de menace.

	Echelle de capacités cinétiques	Marqueurs			
		Equipement (in DORESE)	Ciblage de l'environnement	Ciblage de la victime	Ressources (DORESE)
1	Acteurs ou groupes d'acteurs disposant de moyens limités et grand public destinés au renseignement et / ou aux actions de terrain et capables de mener des opérations physiques (infiltration, pénétration) de manière opportuniste sur des cibles vulnérables ou présentant des vulnérabilités évidentes.	initial	-	opportuniste	connaissances
2	Acteurs ou groupes d'acteurs disposant de moyens limités destinés au renseignement et / ou aux actions de terrain et capables de les combiner pour mener des opérations physiques (infiltration, pénétration) de manière opportuniste sur tous types de cibles.	élaboré	opportuniste	opportuniste	compétences
3	Acteurs ou groupes d'acteurs organisés disposant de moyens légers destinés au renseignement et / ou aux actions de terrain, capables de les combiner et de les utiliser pour mener des opérations physiques (infiltration, pénétration, etc.) dans un objectif opportuniste ou ciblé.	moyens légers	opportuniste	opportuniste ou ciblé	niveau 2 + organisation
4	Acteurs organisés (type groupe cybercriminel, groupe hacktiviste ou assimilé, affiliés à un état ou non) disposant de moyens légers destinés au renseignement et / ou aux actions de terrain et d'une organisation professionnelle, de moyens financiers importants et de personnel compétent dans le domaine, travaillant en équipe pour planifier et mener des opérations physiques (infiltration, pénétration, etc.) dans un environnement et pour un objectif ciblé.	moyens légers	ciblé	ciblé	niveau 3 + financement
5	Acteurs organisés (groupe cybercriminel, groupe hacktiviste ou assimilé, affiliés à un état ou non) disposant de moyens lourds et sophistiqués destinés au renseignement et / ou aux actions de terrain, et capables de les utiliser pour mener des opérations physiques (infiltration, pénétration, etc.) dans un environnement et pour un objectif ciblé.	moyens lourds	ciblé	ciblé	niveau 4 + doctrine
6	Acteurs de niveau étatique ayant la capacité de combiner des capacités cinétiques avec l'ensemble de leurs capacités militaires et de leurs capacités de renseignement pour obtenir un résultat spécifique dans les domaines identifiés (politique, militaire, économique, etc.) et pour l'appliquer à grande échelle.	moyens lourds	ciblé	ciblé	toutes ressources combinées

Tableau 14 : Exemple d'une échelle de capacités cinétiques

	Echelle de capacités numériques	Marqueurs			
		Niveau de technicité	Ciblage de l'environnement	Ciblage de la victime	Ressources (DORESE)
1	Praticiens ou groupes de praticiens qui comptent sur les autres pour développer des codes malveillants, des mécanismes de diffusion et des stratégies d'exécution sur des vulnérabilités connues pour les utiliser de manière opportuniste.	initial	-	opportuniste	connaissances
2	Praticiens ou groupes de praticiens ayant une expérience plus approfondie, avec la capacité de développer leurs propres codes malveillants, mécanismes de diffusion et stratégies d'exécution à partir de vulnérabilités connues du public pour les utiliser de manière opportuniste.	élaboré	opportuniste	opportuniste	compétences
3	Praticiens ou groupes de praticiens organisés ayant la capacité de découvrir de nouvelles vulnérabilités et de développer des exploits de manière opportuniste (sans ciblage d'un environnement donné), et capables de les utiliser pour un objectif opportuniste ou ciblé.	complexe	opportuniste	opportuniste ou ciblé	niveau 2 + organisation
4	Acteurs organisés (type groupe cybercriminel, groupe hacktiviste ou assimilé, affiliés à un état ou non) disposant d'une organisation professionnelle, de moyens financiers importants et de personnel compétent dans le domaine, travaillant en équipe pour découvrir de nouvelles vulnérabilités et de développer des exploits sur un environnement donné, et capables de les utiliser pour un objectif ciblé.	complexe	ciblé	ciblé	niveau 3 + financement
5	Acteurs organisés (groupe cybercriminel, groupe hacktiviste ou assimilé, affiliés à un état ou non) créant des vulnérabilités et les exploits associés par le biais d'un programme actif visant à cibler des produits et services lors de tout leur cycle de vie, et capables de les utiliser dans un objectif ciblé.	complexe	ciblé	ciblé	niveau 4 + doctrine
6	Acteurs de niveau étatique ayant la capacité de combiner des capacités cybernétiques avec l'ensemble de leurs capacités militaires et de leurs capacités de renseignement pour obtenir un résultat spécifique dans les domaines identifiés (politique, militaire, économique, etc.) et pour l'appliquer à grande échelle.	complexe	ciblé	ciblé	toutes ressources combinées

Tableau 15 : Exemple d'une échelle de capacités numériques

	Echelle de capacités anthropiques	Marqueurs			
		Niveau de complexité	Ciblage de groupes sociaux	Ciblage de la victime	Ressources (DORESE)
1	Praticiens ou groupes de praticiens ayant la capacité de mener des opérations d'influence sur des personnes vulnérables (influençables, crédules, en situation de dépendance, etc.) pour les utiliser de manière opportuniste.	initial	-	opportuniste	connaissances
2	Praticiens ou groupes de praticiens ayant une expérience plus approfondie, avec la capacité de mener des opérations d'influence, de subversion ou d'infiltration élaborées sur des personnes ou des groupes de personnes vulnérables (influençables, crédules, en situation de dépendance, etc.) pour les utiliser de manière opportuniste.	élaboré	opportuniste	opportuniste	compétences
3	Praticiens ou groupes de praticiens organisés ayant la capacité de mener des opérations d'influence, de subversion ou d'infiltration élaborées, et capables de les utiliser pour un objectif opportuniste ou ciblé sur tous types de personnes ou de groupes de personnes.	élaboré	opportuniste	opportuniste ou ciblé	niveau 2 + organisation
4	Acteurs organisés (type organisation criminelle, organisation activiste ou assimilé, affiliées à un état ou non) disposant d'une organisation professionnelle, de moyens financiers importants et de personnel compétent dans le domaine, travaillant en équipe pour réaliser des opérations d'influence, de subversion ou d'infiltration adaptées à un contexte donné, afin de les utiliser dans un objectif ciblé sur tous types de personnes ou de groupes de personnes.	complexe	ciblé	ciblé	niveau 3 + financement
5	Acteurs organisés (groupe cybercriminel, groupe hacktiviste ou assimilé, affiliés à un état ou non) ayant la capacité de réaliser des opérations d'influence ciblées ou de masse, des opérations de subversion ciblées ou de masse ou des opérations d'infiltration ciblées ou de masse, afin de les utiliser dans un objectif ciblé.	complexe	ciblé	ciblé	niveau 4 + doctrine
6	Acteurs de niveau étatique ayant la capacité de combiner des capacités anthropiques avec l'ensemble de leurs capacités militaires et de leurs capacités de renseignement pour obtenir un résultat spécifique dans les domaines identifiés (politique, militaire, économique, etc.) et capables de l'appliquer à grande échelle.	complexe	ciblé	ciblé	toutes ressources combinées

Tableau 16 : Exemple d'une échelle de capacités anthropiques

Annexe G : Outils d'élaboration des scénarios de menace

Les scénarios de menace, objet de la présente section, visent à maîtriser les risques sur la sécurité des usagers et des tiers, ce qui légitimise une approche de modélisation selon une sémantique complexe inspirée des sémantiques utilisées dans le domaine de la *safety* (ex. : AMDEC).

Principe d'élaboration des scénarios de menace et de risque

Un scénario de risque est un enchaînement d'actions unitaires qui transforme un système d'un état initial à un état final défini par une situation ayant un impact sur la sécurité des usagers et des tiers, via des états intermédiaires qui caractérisent la transformation du système (cf. Figure 23).

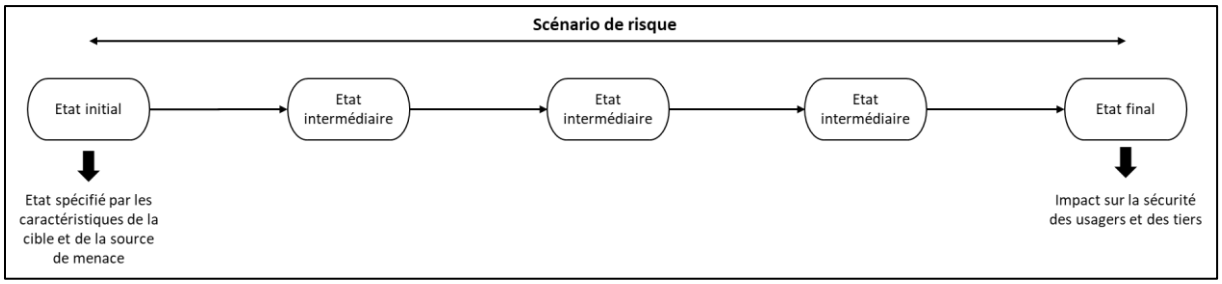


Figure 23 : Scénario de risque vu comme un enchaînement d'états

Un scénario de risque est par ailleurs la combinaison d'un scénario de menace, qui induit un événement redouté de cybersécurité, et un scénario de conséquence qui combine l'événement redouté de cybersécurité à des conditions nécessaires pour arriver à l'état final (cf. Figure 24).

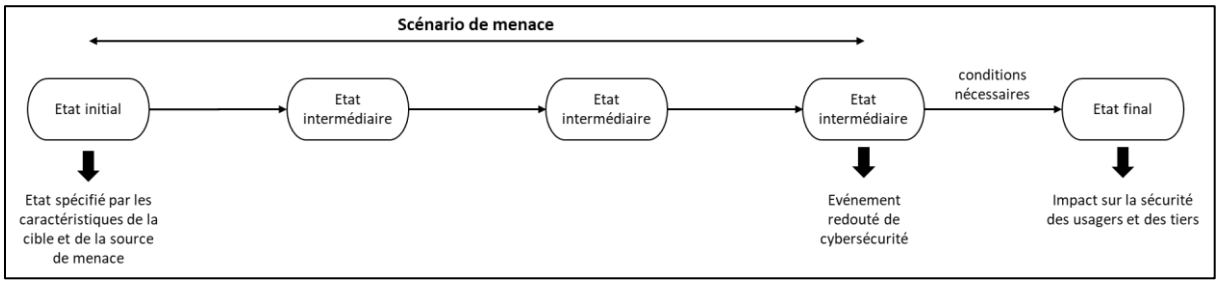


Figure 24 : Scénario de menace vu comme un enchaînement d'états

L'élaboration des scénarios de menace consiste à identifier l'ensemble des chemins possibles pour transformer le système d'un état initial à un état final, et par extension l'ensemble des états intermédiaires et des actions unitaires qui permettent de les atteindre (cf. Figure 25).

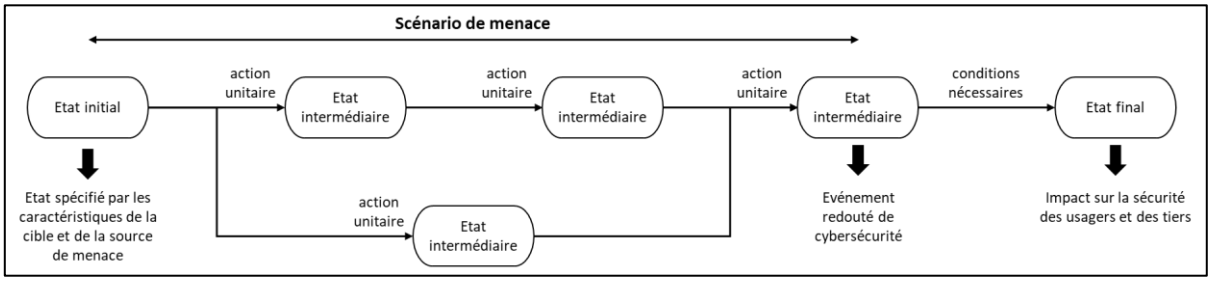


Figure 25 : Scénario de menace vu comme un enchaînement d'états et d'actions unitaires

Modèle de base pour les actions unitaires

On considère 4 types d'actions unitaires pour compromettre un processus donné (cf. Figure 26) :

- **[K] Prise de contrôle**

  Cette action unitaire caractérise la capacité à contrôler ou commander illégitimement le processus pour lui faire réaliser ses tâches nominales.

  Cette action se comprend facilement pour un objet numérique (ex : exécution d'un programme malveillant) mais ne s'y limite pas : la corruption d'une personne ou le fait de réaliser des actions physiques sur une interface analogique sont des cas de prise de contrôle.

- **[A] Corruption de l'état interne**

  Cette action unitaire caractérise une modification du processus pour qu'il produise des résultats illégitimes dans son fonctionnement nominal.

  Cette action se comprend facilement pour un objet numérique (ex. : modification d'un code ou d'un paramètre d'un programme) mais ne s'y limite pas : l'endoctrinement d'une personne physique ou l'altération d'un composant physique sont des cas de corruption de l'état interne.

- **[T] Envoi de données non conformes**

  Cette action unitaire caractérise l'envoi de données à un processus pour qu'il produise des résultats illégitimes dans son fonctionnement nominal.

  Cette action se comprend facilement pour un objet numérique ou pour une personne physique (ex. : envoi de données falsifiées ou incomplètes dans le processus décisionnel) mais ne s'y limite pas : le brouillage électromagnétique est un cas d'envoi de données non conformes.

- **[S] Attaque de la supply chain**

  Cette action unitaire caractérise une modification d'un composant d'un processus avant son intégration dans le système considéré, dans le but de permettre une action de type [K] ou [A].

  Cette action se comprend facilement pour un objet numérique (ex. : modification du code source d'un progiciel) mais ne s'y limite pas : la modification de la composition d'un matériau ou l'infiltration d'une personne dans une équipe sont des cas d'attaque de la supply chain.

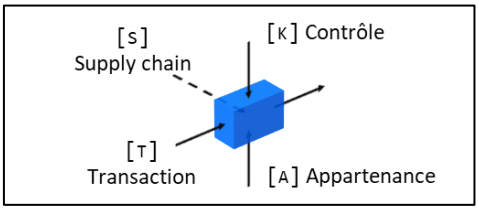


Figure 26 : Modèle de base pour les actions unitaires de compromission d'un processus

Par ailleurs, ces actions unitaires peuvent se combiner entre elles (cf. Figure 27) ; l'enchaînement de deux actions unitaires sur un même processus est vu comme un changement d'état du système, et donc comme une étape à part entière du scénario de menace.

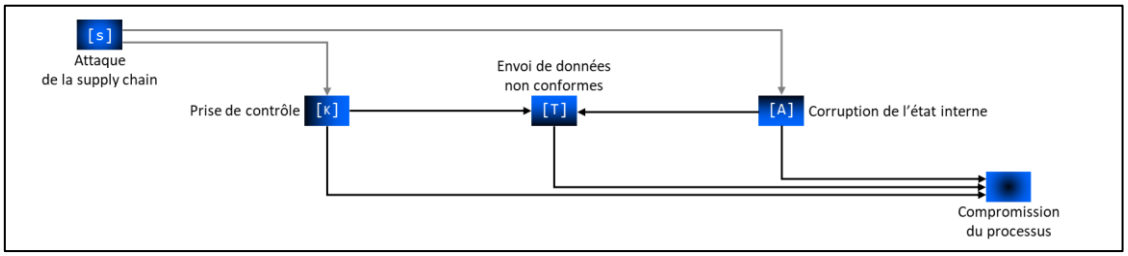
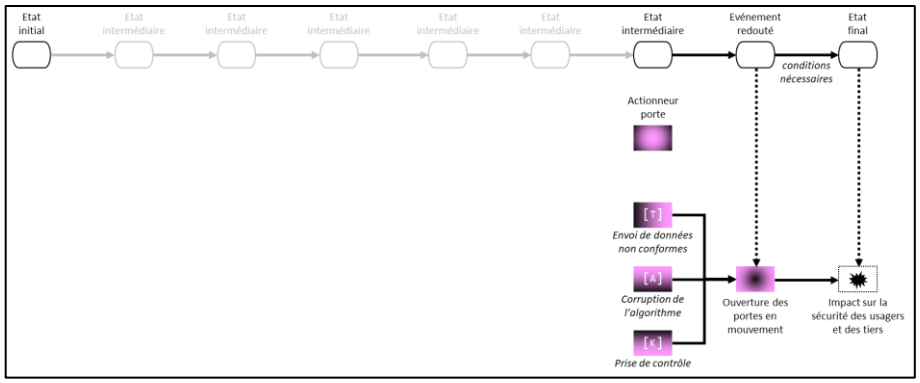
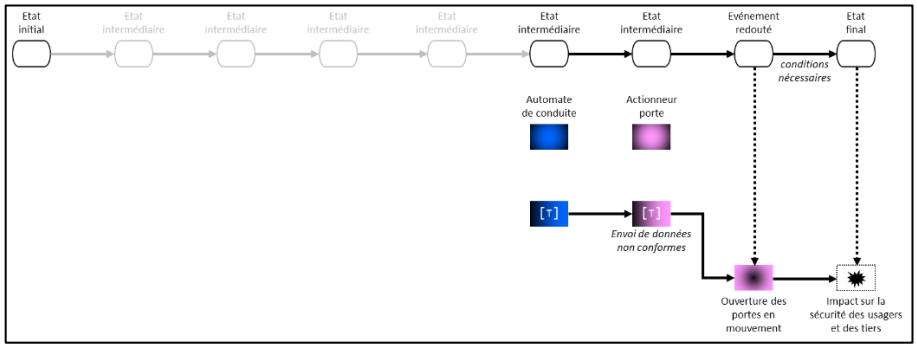
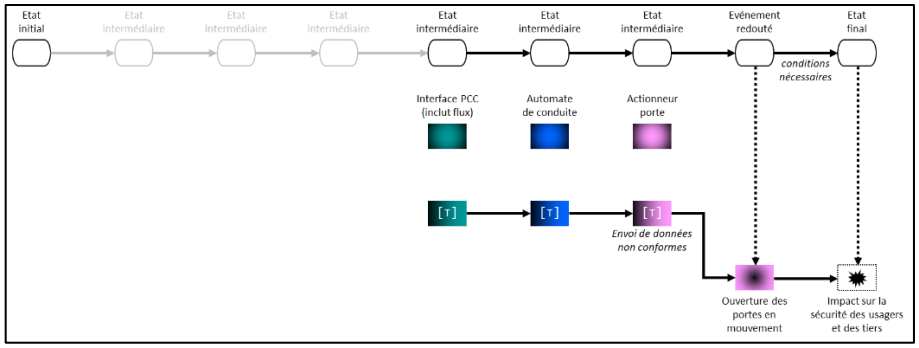
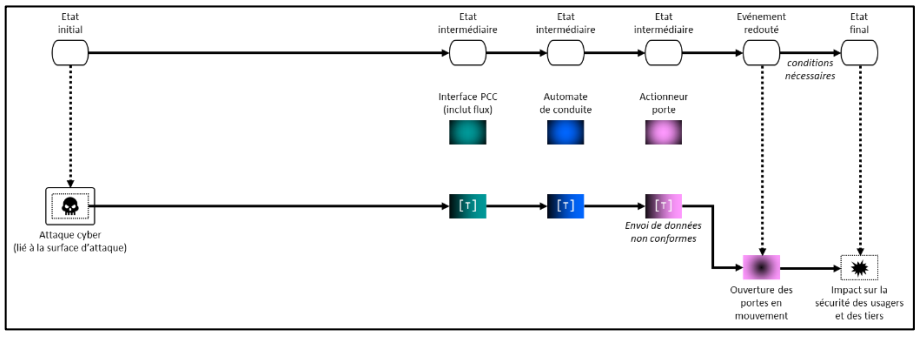
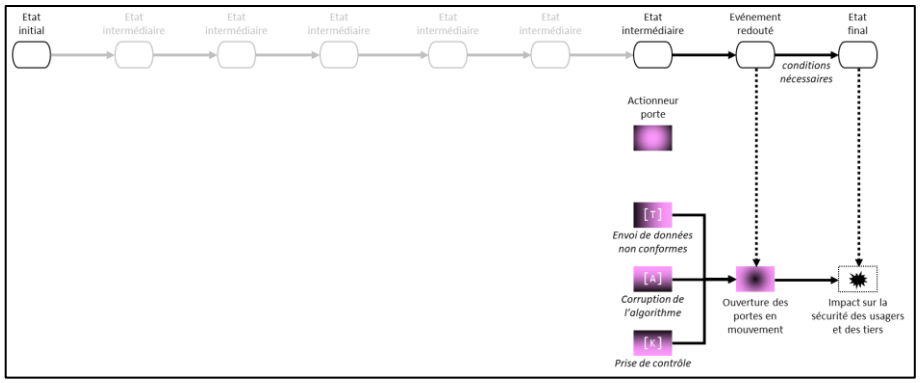
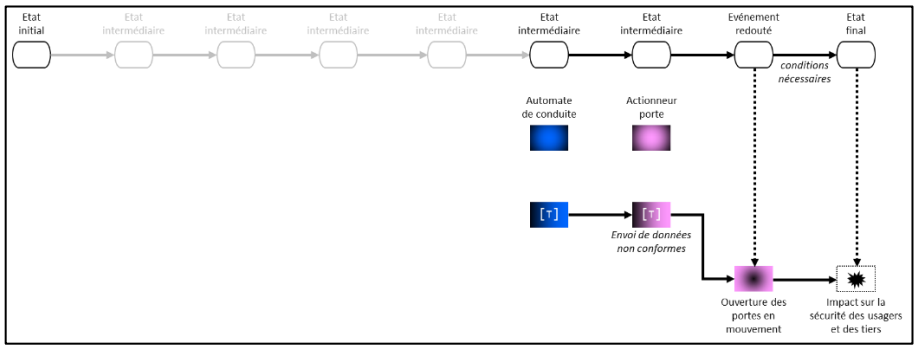
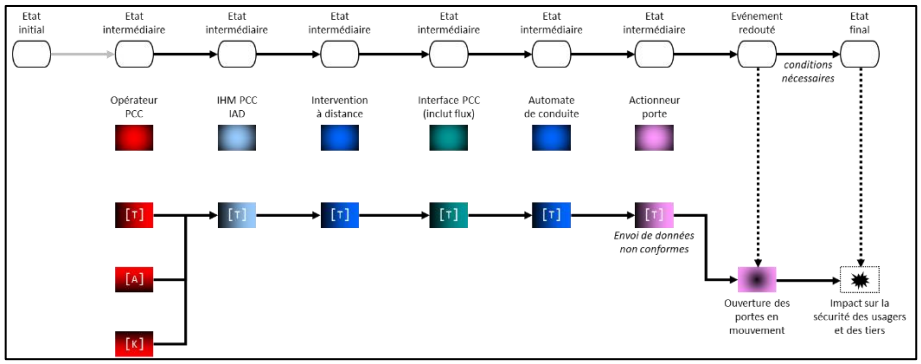
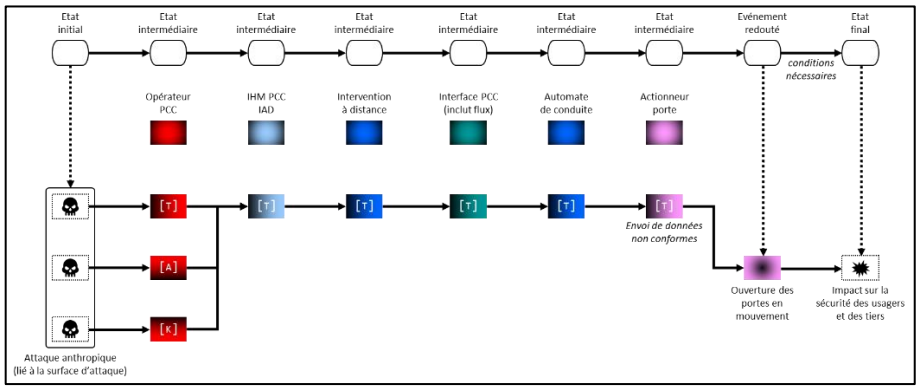


Figure 27 : Combinaisons possibles d'actions unitaires sur une processus donné

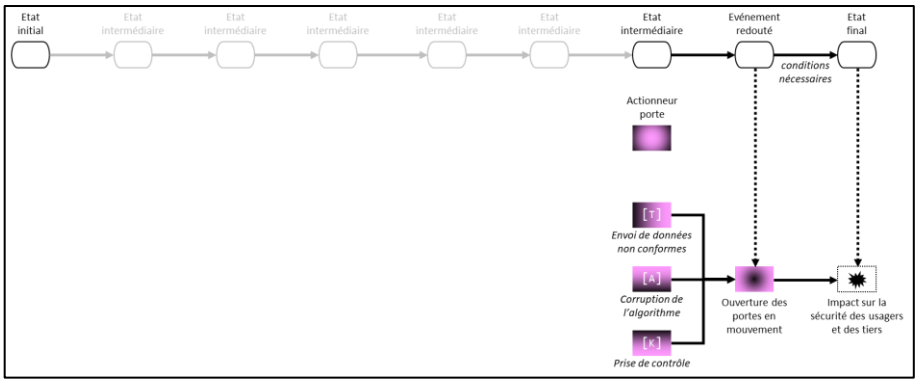
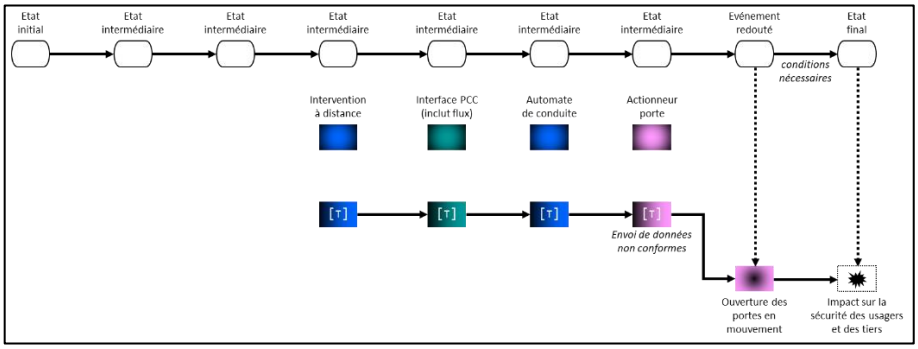
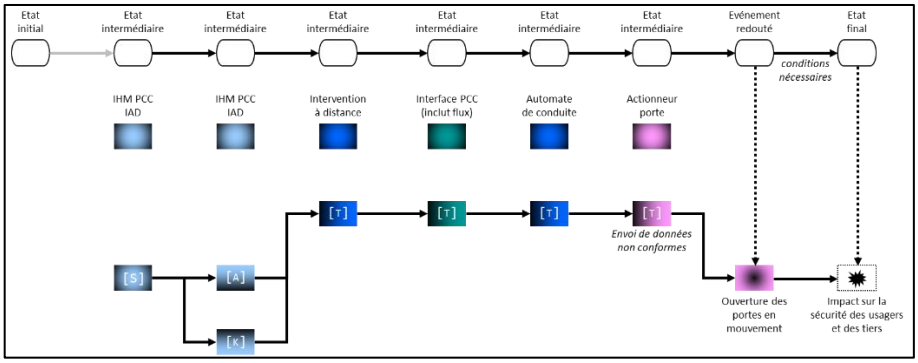
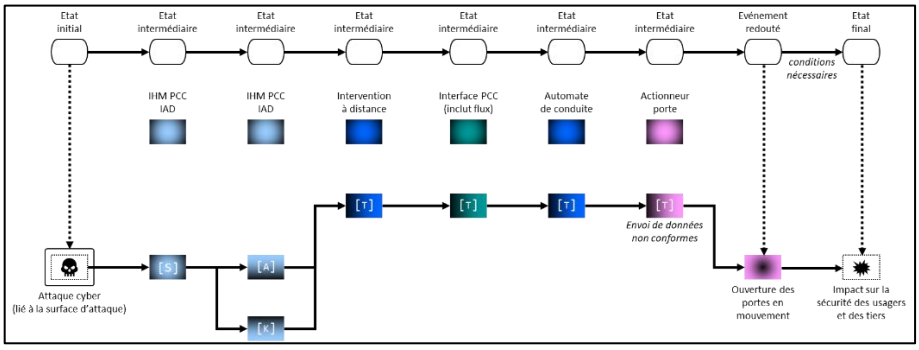
Cas d'usage 1 : élaboration d'un scénario unitaire (parmi d'autres)

Modélisation de toutes les actions unitaires `[T]` `[A]` `[K]` permettant de mener à l'état correspondant à l'événement redouté de cybersécurité « ouverture des portes en mouvement ».	
Modélisation de la seule action unitaire `[T]` permettant de mener à l'état intermédiaire identifié (les actions unitaires `[A]` `[K]` et les actions unitaires possibles au regard de la surface d'attaque ne sont pas considérés ici).	
Modélisation d'une action unitaire `[T]` parmi d'autres permettant de mener à l'état intermédiaire identifié (les autres actions unitaires `[T]` `[A]` `[K]` et les actions unitaires possibles au regard de la surface d'attaque ne sont pas considérés ici).	
Modélisation de l'action unitaire possible au regard de la surface d'attaque (exclusivement numérique, dans ce cas) sur le processus porteur de l'état intermédiaire antérieur). La nature de l'attaque ne peut pas être détaillée sans la spécification de l'implémentation technique du système considéré.	

Cas d'usage 2 : élaboration d'un scénario introduisant une surface d'attaque anthropique

Modélisation de toutes les actions unitaires `[T]` `[A]` `[K]` permettant de mener à l'état correspondant à l'événement redouté de cybersécurité « ouverture des portes en mouvement ».	
Modélisation de la seule action unitaire `[T]` permettant de mener à l'état intermédiaire identifié (les actions unitaires `[A]` `[K]` et les actions unitaires possibles au regard de la surface d'attaque ne sont pas considérés ici).	
Modélisation d'un enchaînement d'actions unitaires `[T]` permettant de mener à l'état intermédiaire identifié (les autres enchaînements d'actions unitaires ne sont pas considérés ici).	
Modélisation de toutes les actions unitaires possibles au regard de la surface d'attaque (exclusivement anthropique, dans ce cas) sur le processus porteur de l'état intermédiaire antérieur). La nature de l'attaque ne peut pas être détaillée sans la connaissance des capacités des sources de menace.	

Cas d'usage 3 : élaboration d'un scénario introduisant une action sur la supply chain

Modélisation de toutes les actions unitaires `[T]` `[A]` `[K]` permettant de mener à l'état correspondant à l'événement redouté de cybersécurité « ouverture des portes en mouvement ».	
Modélisation d'un enchaînement d'actions unitaires `[T]` permettant de mener à l'état intermédiaire identifié (les autres enchaînements d'actions unitaires ne sont pas considérés ici).	
Modélisation d'actions unitaires `[A]` `[K]` parmi d'autres permettant de mener à l'état intermédiaire identifié (les autres actions unitaires `[T]` `[A]` `[K]` et les actions unitaires possibles au regard de la surface d'attaque ne sont pas considérées ici).	
Modélisation d'un enchaînement d'actions unitaires introduisant une action de type `[S]` et les actions unitaires possibles au regard de la surface d'attaque permettant de mener à l'état intermédiaire identifié. La nature de l'attaque ne peut pas être détaillée sans la spécification de l'implémentation technique du système considéré.	

Algorithme générique pour l'élaboration des scénarios de menace

L'application systématique d'un algorithme d'élaboration des scénarios de menace à un état donné du système considéré permet d'identifier l'ensemble des scénarios de menace possibles permettant d'atteindre cet état.

En appliquant de manière systématique cet algorithme à l'ensemble des états du système considéré caractérisant un événement redouté de cybersécurité, on peut identifier l'ensemble des scénarios de menace sur le système considéré.

```
ER = Evénement Redouté de cybersécurité
EI = Etat intermédiaire

Pour chaque ER du système considéré
    EI = ER
    Exécuter Fonction_Algorithme (EI)

Fonction_Algorithme (EI)
    Pour chaque AU (Action Unitaire) [K] permettant d'atteindre l'EI
        Pour chaque attaque permettant de réaliser l'AU au regard de la surface d'attaque
            Modéliser Le scénario de menace
        EI = Etat caractérisé par l'AU
        Exécuter Fonction_Algorithme (EI)
    Pour chaque AU (Action Unitaire) [A] permettant d'atteindre l'EI
        Pour chaque attaque permettant de réaliser l'AU au regard de la surface d'attaque
            Modéliser Le scénario de menace
        EI = Etat caractérisé par l'AU
        Exécuter Fonction_Algorithme (EI)
    Pour chaque AU (Action Unitaire) [S] permettant d'atteindre l'EI
        Pour chaque attaque permettant de réaliser l'AU au regard de la surface d'attaque
            Modéliser Le scénario de menace
        EI = Etat caractérisé par l'AU
        Exécuter Fonction_Algorithme (EI)
    Pour chaque AU (Action Unitaire) [T] permettant d'atteindre l'EI
        Pour chaque attaque permettant de réaliser l'AU au regard de la surface d'attaque
            Modéliser Le scénario de menace
        Pour chaque source de données permettant de réaliser l'AU [T]
            EI = état caractérisé par la compromission de la source de données
            Exécuter Fonction_Algorithme (EI)
```

On note que l'algorithme décrit précédemment peut être appliqué à tout moment du cycle de vie du système considéré, mais que ses conclusions diffèrent :

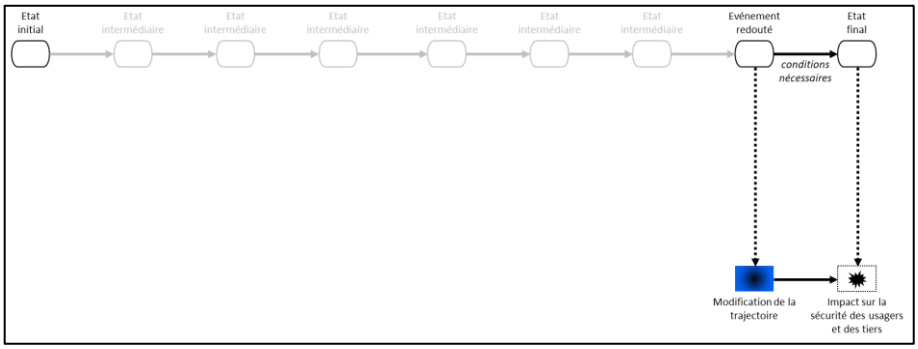
- Lorsqu'il est appliqué dans les phases amont du cycle de vie, notamment lorsque les spécifications d'implémentation ne sont pas connues, les scénarios de menace peuvent être projetés sur la modélisation fonctionnelle, et les scénarios mettant en jeu la surface d'attaque peuvent être identifiés mais pas être modélisés en détail ;
- Lorsqu'il est appliqué dans les phases aval du cycle de vie, notamment lorsque l'implémentation est spécifiée ou mise en œuvre, les scénarios de menace mettant en jeu la surface d'attaque peuvent être modélisés de manière de plus en plus détaillée, selon le niveau de connaissances de l'implémentation des éléments du système considéré.

Cas d'usage d'application de l'algorithme générique pour l'élaboration des scénarios de menace

Situation initiale

On considère un événement redouté de cybersécurité donné parmi l'ensemble des événements redoutés de cybersécurité (ici, la modification de la trajectoire).

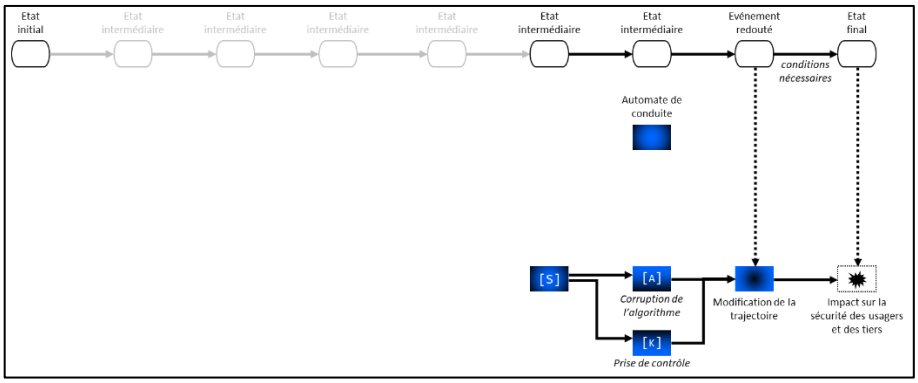
L'algorithme étant récursif, on pourra considérer par la suite un état intermédiaire comme une situation initiale.



Etape 1

On étudie de manière systématique toutes les actions unitaires `[A]` `[K]` `[S]` possibles au regard de la modélisation fonctionnelle des processus du système considéré

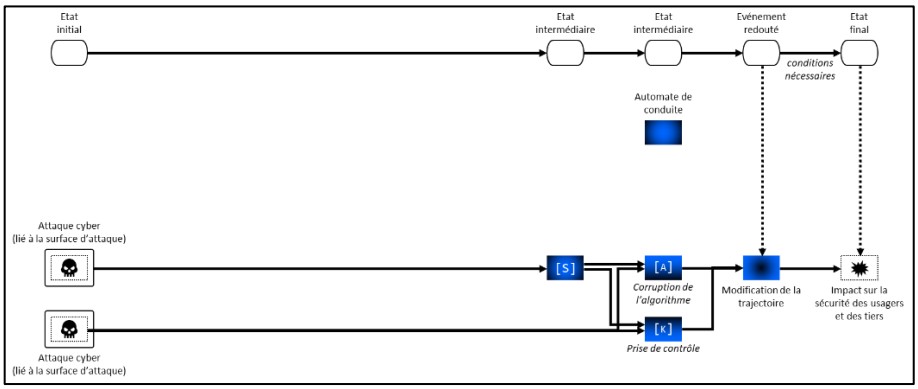
Ici, seul l'automate de conduite est éligible au regard de la modélisation fonctionnelle, mais c'est un cas particulier.



Etape 2

On étudie l'ensemble des actions unitaires possibles au regard de la surface d'attaque(physique, numérique, anthropique) sur le processus porteur de l'état.

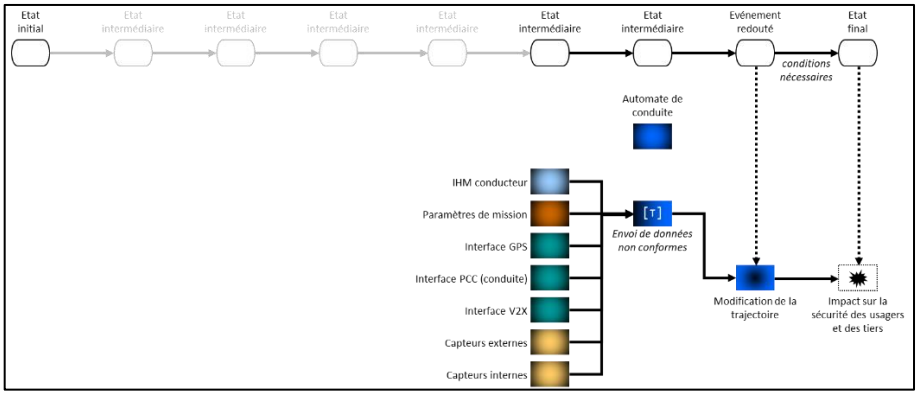
La nature de l'attaque ne peut pas être détaillée sans la spécification de l'implémentation technique du système considéré.



A l'issue de cette étape 2, une partie des scénarios de menace propres à l'événement de cybersécurité considéré en situation initiale sont modélisés et utilisables au titre de l'appréciation des risques.

Etape 3

On étudie l'ensemble des sources de données permettant de réaliser des actions unitaires `[T]` permettant de mener à l'état intermédiaire identifié.



A l'issue de l'étape 3, de nouveaux états intermédiaires sont identifiés ; l'algorithme spécifié peut être appliqué de manière récursive en considérant les résultats de l'étape 3 comme de nouvelles situations initiales.

Projection d'un scénario de menace sur la modélisation fonctionnelle du système complexe STRA

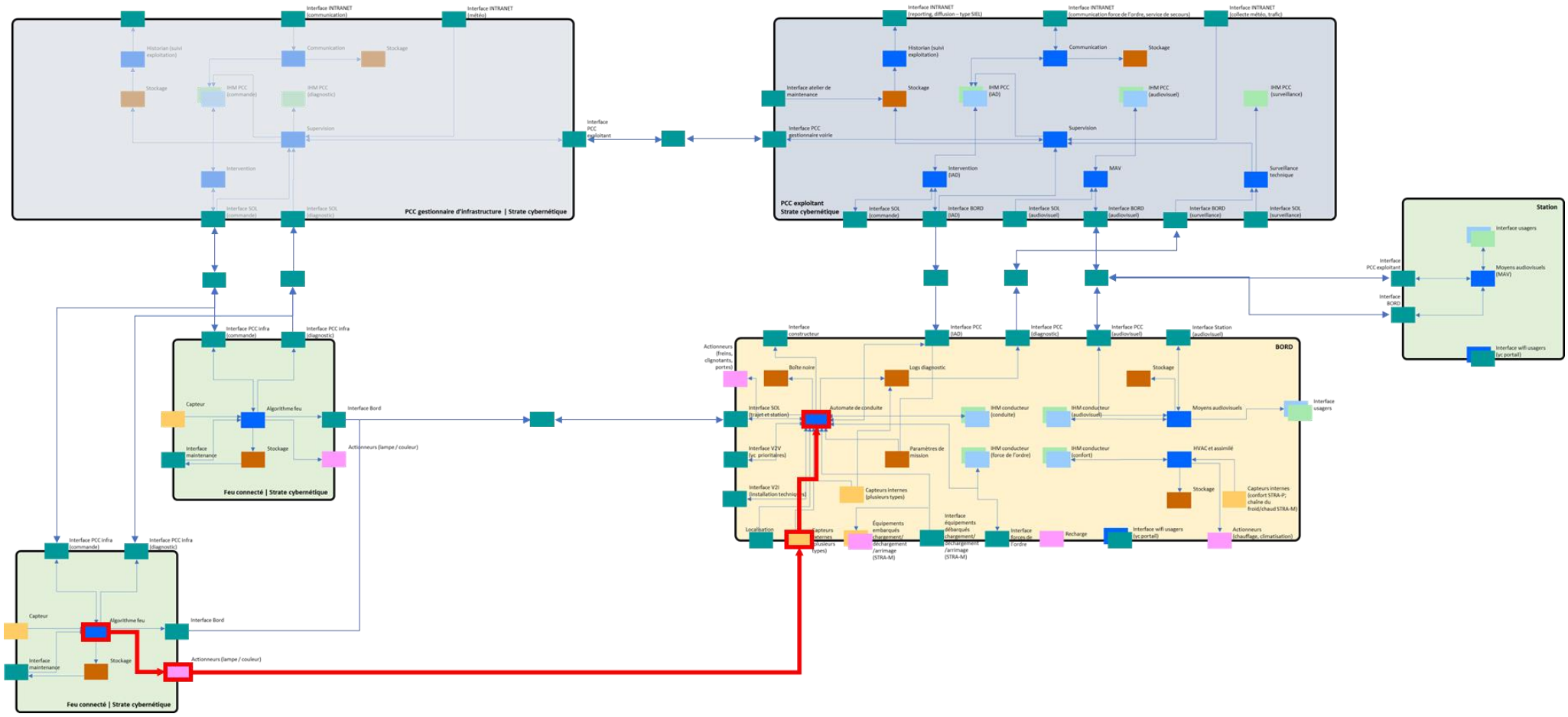


Figure 28 : Projection d'un scénario de menace dans la modélisation d'un STRA (exemple d'une attaque en supply chain)

Annexe H : Liste des scénarios de menace de haut niveau

Les scénarios de menace de haut niveau déclinent les scénarios de menace à considérer, avec un niveau d'abstraction élevé, sur les différentes fonctions du STRA (cf. Annexe I). Déclinés sur les fonctions de rang 2 sous la forme de vignettes, ils constituent une topologie réputée complète de scénarios de menace. Ils sont toutefois à adapter au système considéré.

Parmi ces scénarios, en considérant la liste des fonctions du STRA (cf. Tableau 17) :

- Certaines fonctions ne relèvent pas du périmètre des risques considérés limité aux impacts sur sécurité des usagers et des tiers (ex. : fonction 4) ;
- Certaines fonctions de rang 2 nécessitent une déclinaison au rang 3, voire au rang 4 pour caractériser un événement redouté de cybersécurité (ex. : fonction 7.4) ;
- Certaines fonctions sont des combinaisons de fonctions existantes et sont, par conséquent, modélisées via une combinaison de vignettes (ex : fonctions 9.1. à 9.5).

Fonction de rang 2	Vignette
1.1-Percevoir l'environnement (sense)	1.1a + 1.1b
1.2-Localiser le véhicule sur le parcours / zone par rapport à l'itinéraire défini	1.2
1.3-Prendre la décision concernant le contrôle dynamique (plan)	1.3
1.4-Assurer le contrôle dynamique (act)	1.4
2.1-Signaler le mode délégation de conduite	2a 2b
2.2-Signaler les intentions de manœuvre du véhicule	
2.3-Signaler une décélération importante du véhicule	
2.4-Signaler la position du véhicule	
2.5-Signaler la situation du véhicule	
2.6-Signaler un danger imminent	
3.1-Gérer le transfert des personnes aux points autorisés (STRA-P)	Modélisation rang 2 non pertinente
3.2-Maintenir le véhicule automatisé fermé hors transfert personnes/évacuation (STRA-P)	
3.3-Permettre l'évacuation et l'accès des secours (STRA-P)	
3.4-Gérer les interfaces avec les opérations de chargement/déchargement (STRA-M)	
3.5 -Maintenir le véhicule automatisé fermé hors des phases de chargement/déchargement (STRA-M)	
4- Assurer des conditions de transport satisfaisantes pour les passagers (STRA-P, pas de fonction de rang 2)	Modélisation rang 2 non pertinente

Fonction de rang 2	Vignette
5.1-Permettre la communication des usagers vers le personnel d'exploitation (COM)	5.1
5-2 Permettre aux passagers de demander l'arrêt du véhicule (STRA-P)	5.2
5.3-Permettre aux usagers l'accès à des services	5.3ab
6-1 Commander la signalisation dynamique	6
6-2-Commander les équipements dynamiques mobiles	
7.1-Définir la mission de chaque véhicule	7.1 / 7.2
7.2 Intervenir à distance sur des composants techniques du système	
7.3-Permettre la communication entre les personnels d'exploitation	7.3
7.4-Permettre la communication entre le système et des intervenants extérieurs	7.4
7.5-Enregistrer les données	7.5
7.6-Informer sur l'état des composants du système	7.6
7.7-Permettre à l'opérateur de percevoir la situation dans le véhicule	7.7
7.8-Permettre à l'opérateur de percevoir la situation à l'extérieur du véhicule	7.8
7.9-Permettre la transmission de l'information voyageurs (STRA-P)	7.9
7.10-Permettre l'intervention en sécurité des services de secours	Non pertinent
8.1-Détecter et gérer les départs de feu	8a + 8b
8.2-Détecter les chocs contre le véhicule	
9.1-Adapter les consignes d'exploitation aux conditions de circulation	Cas particuliers de combinaisons des fonctions 1.1 à 1.4
9.2-Détecter la sortie du système de son domaine d'emploi	
9.3-Exécuter une MRM adaptée à la situation	
9.4-Exécuter une manœuvre d'urgence adaptée à la situation	
9.5-Exécuter un arrêt "ultime"	

Tableau 17 : Identification des vignettes applicables aux fonction de rang 2 d'un STRA

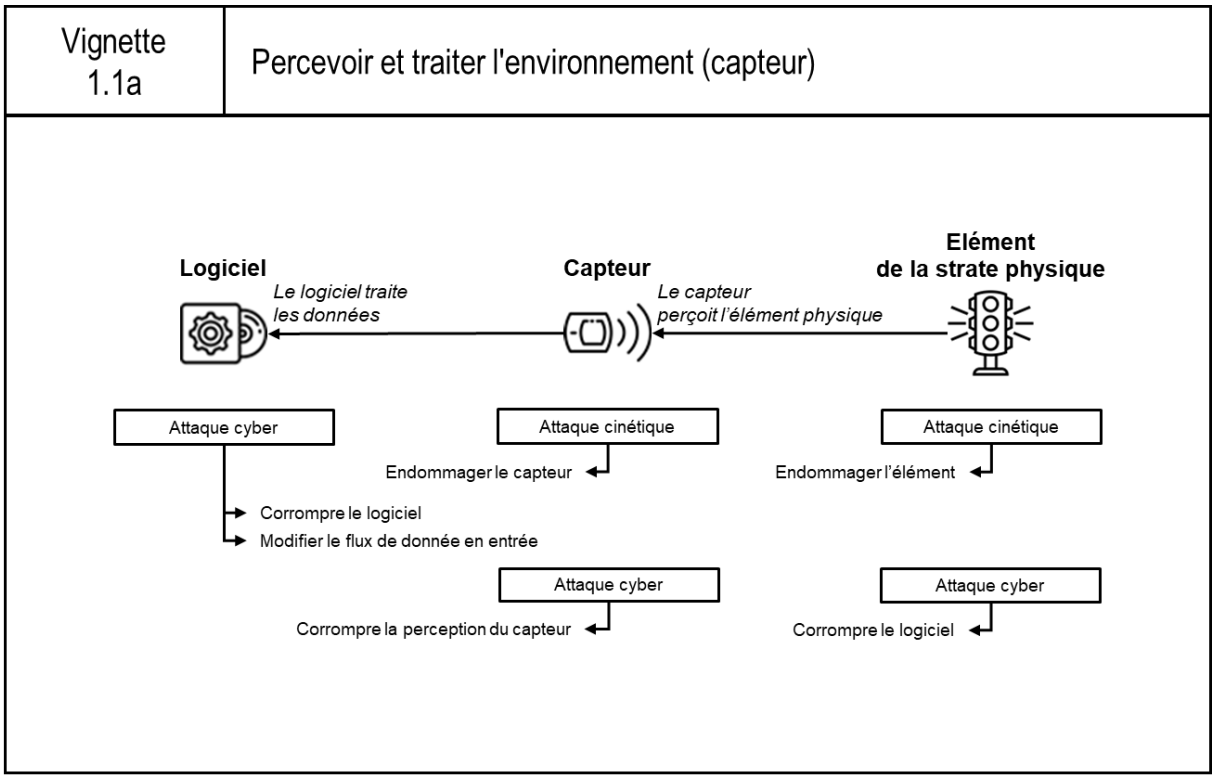


Figure 29 : Vignette 1.1a – Percevoir et traiter l'environnement (capteur)

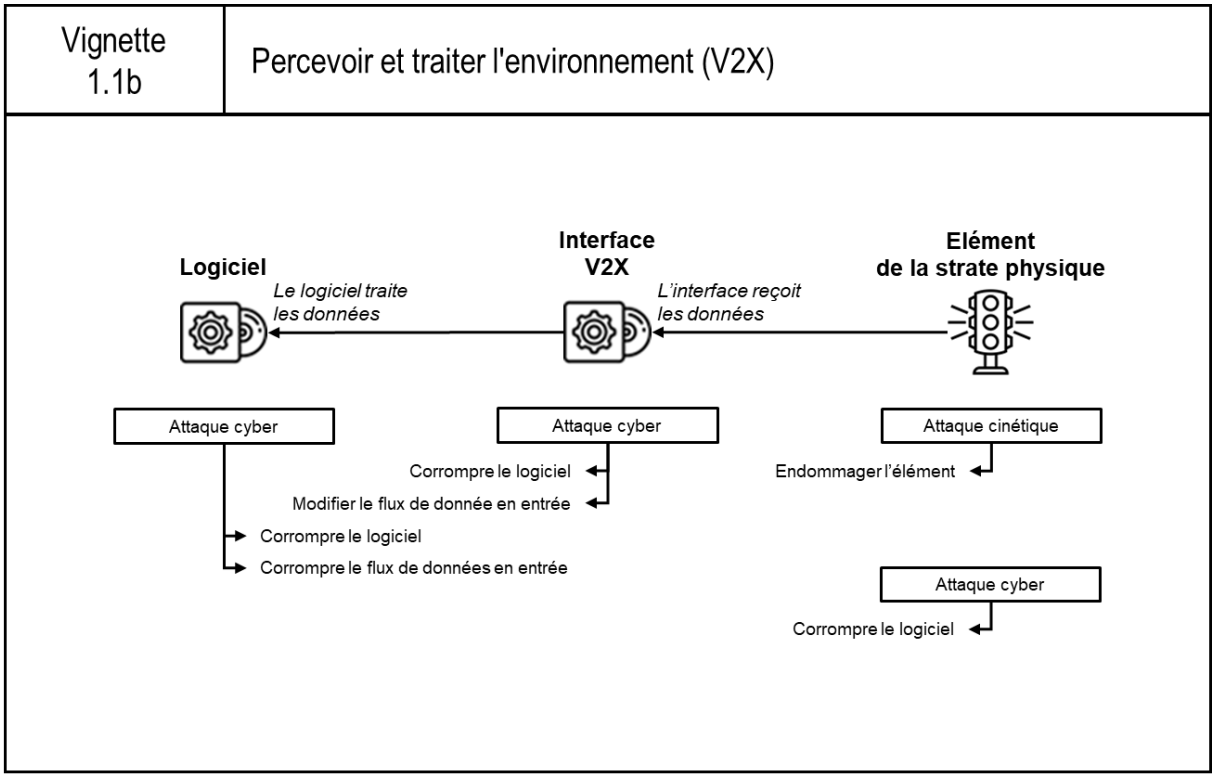


Figure 30 : Vignette 1.1a – Percevoir et traiter l'environnement (V2X)

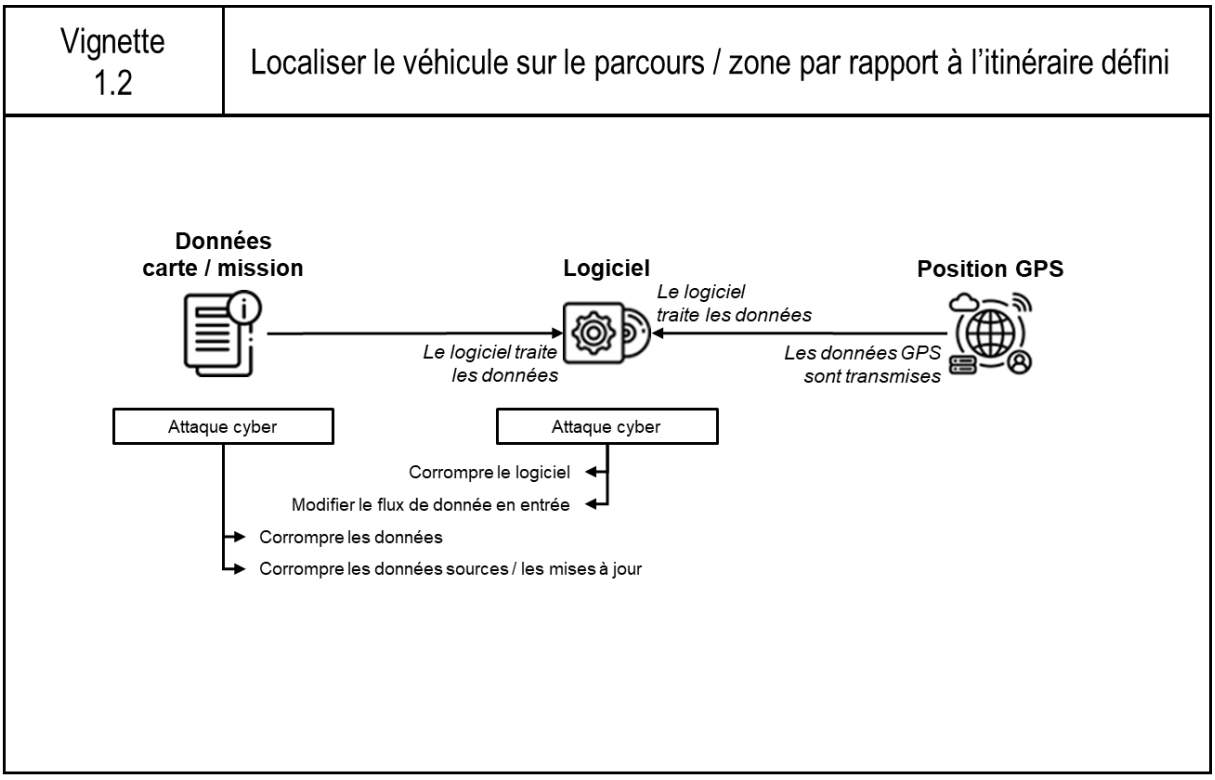


Figure 31 : Vignette 1.2 – Localiser le véhicule sur le parcours / zone par rapport à l'itinéraire défini

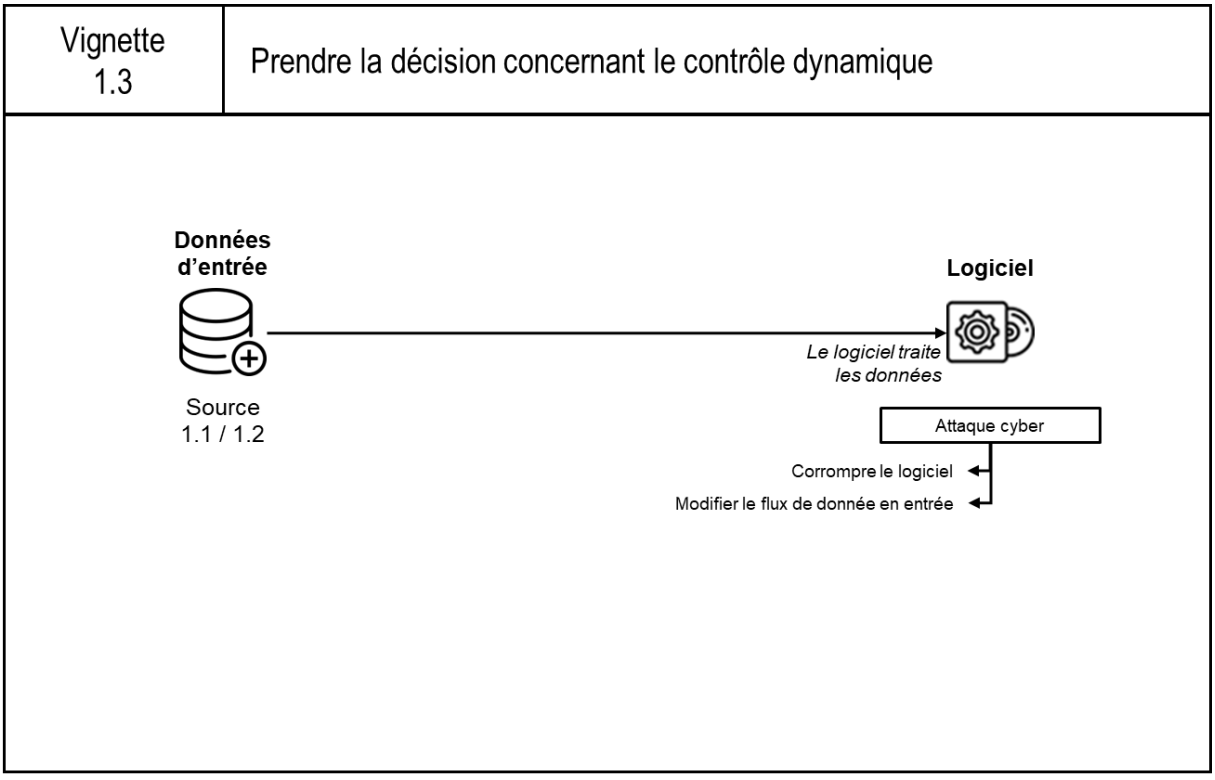


Figure 32 : Vignette 1.3 – Prendre la décision concernant le contrôle dynamique

Vignette 1.4	Assurer le contrôle dynamique

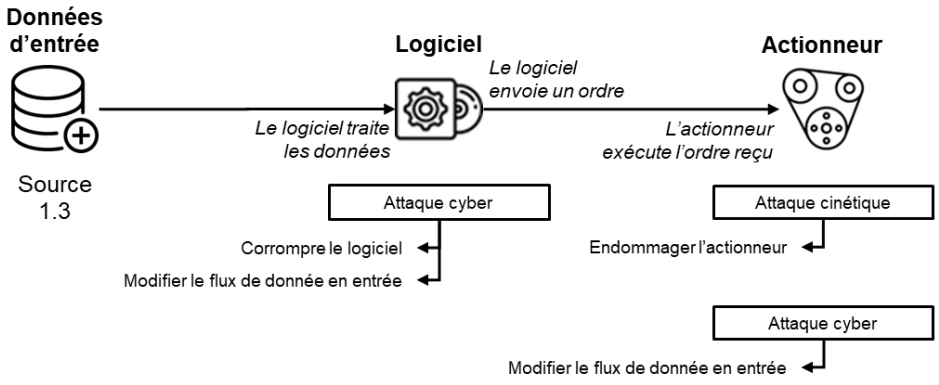


Figure 33 : Vignette 1.4 – Assurer le contrôle dynamique

Vignette 2a	Signaler le véhicule vis-à-vis des autres usagers de la route (dispositif lumineux ou sonore)

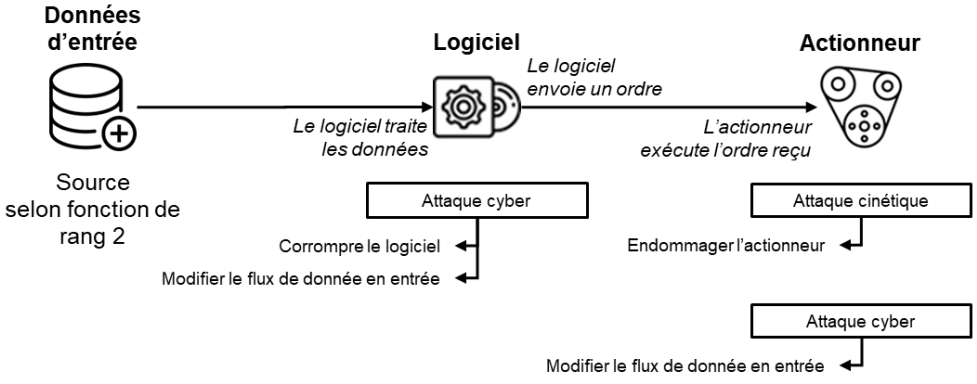


Figure 34 : Vignette 2a – Signaler le véhicule vis-à-vis des autres usagers (lumineux / sonore)

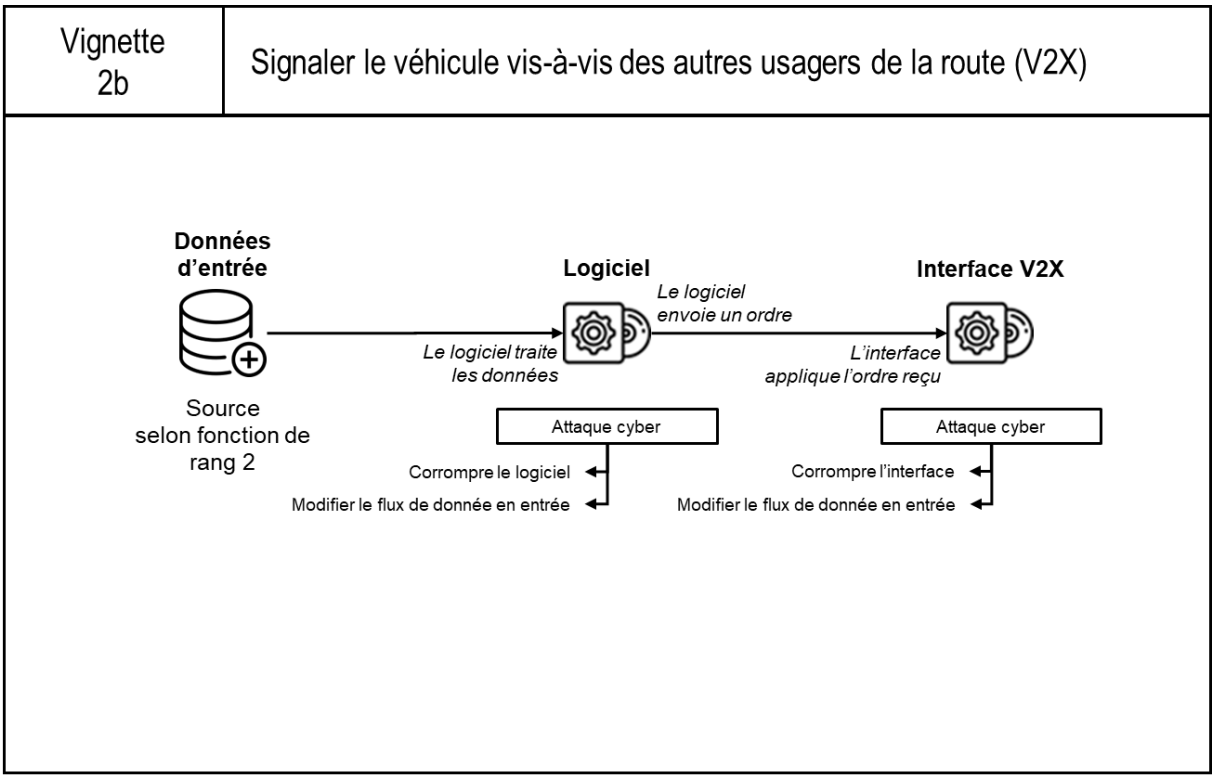


Figure 35 : Vignette 2b – Signaler le véhicule vis-à-vis des autres usagers (V2X)

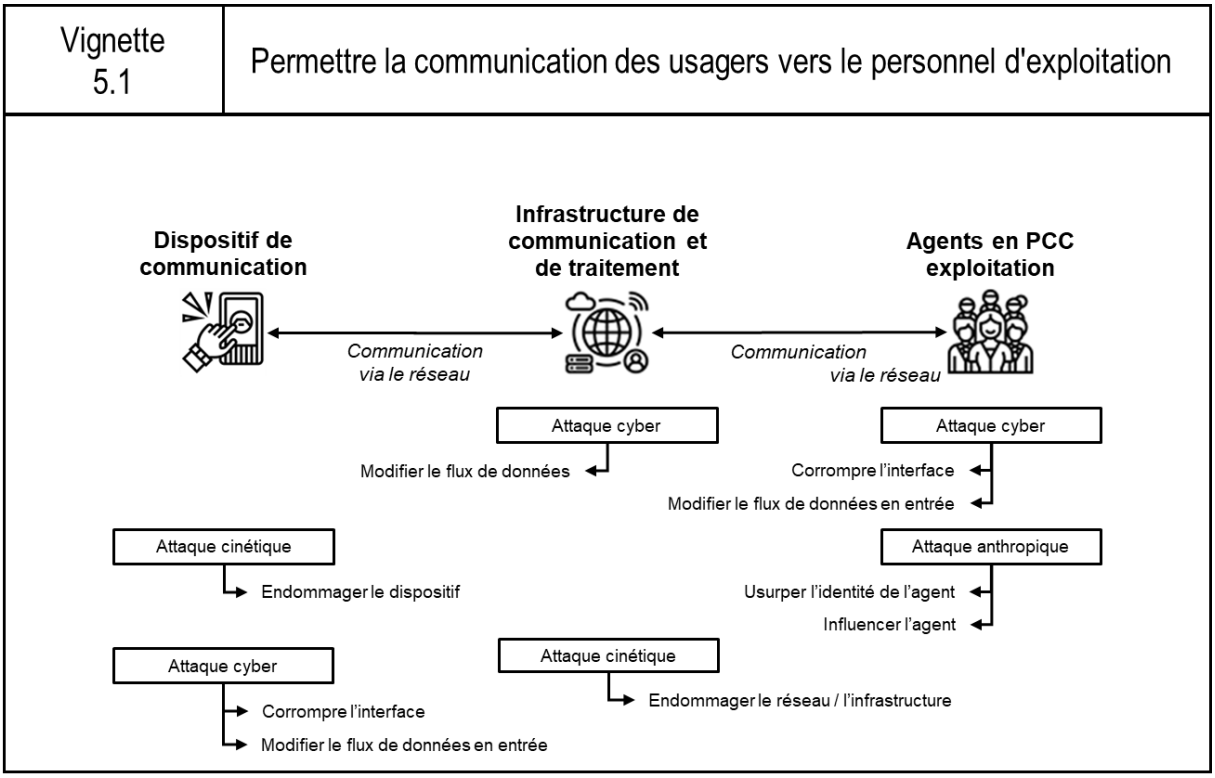


Figure 36 : Vignette 5.1 – Permettre la communication des usagers vers le personnel d'exploitation

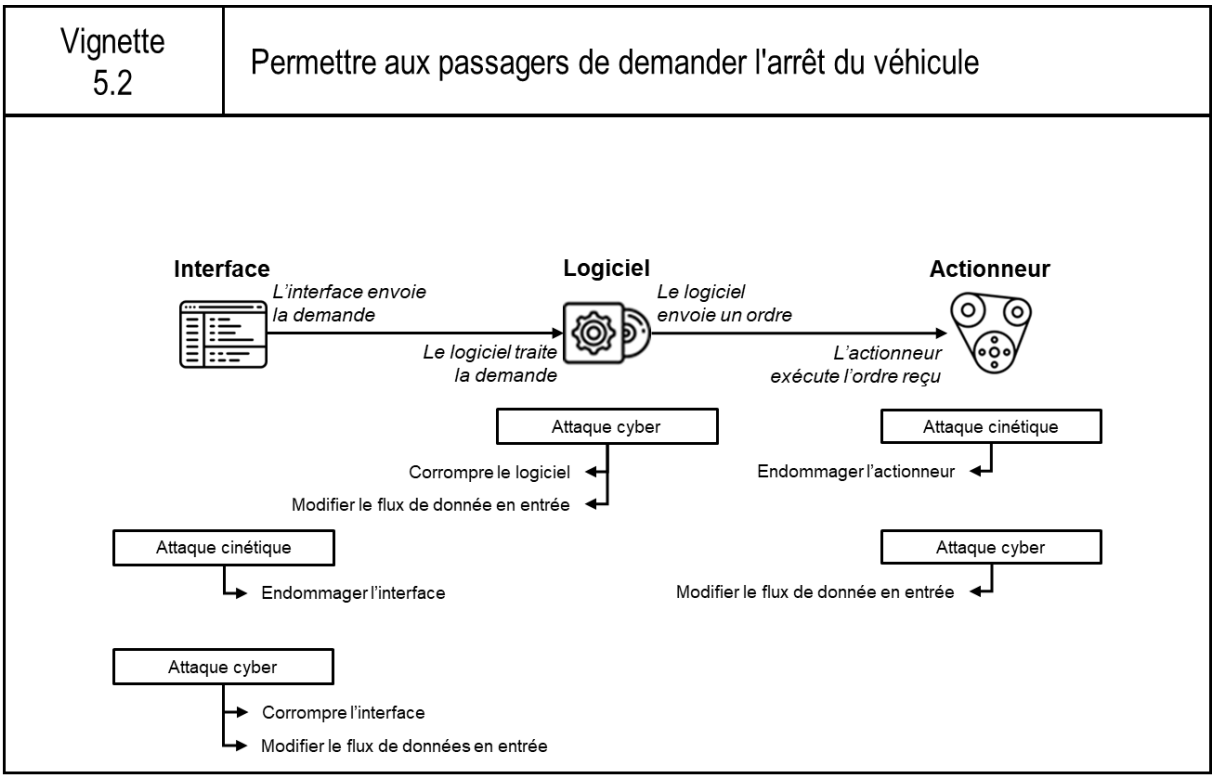


Figure 37 : Vignette 5.2 – Permettre aux passagers de demander l'arrêt du véhicule (STRA-P)

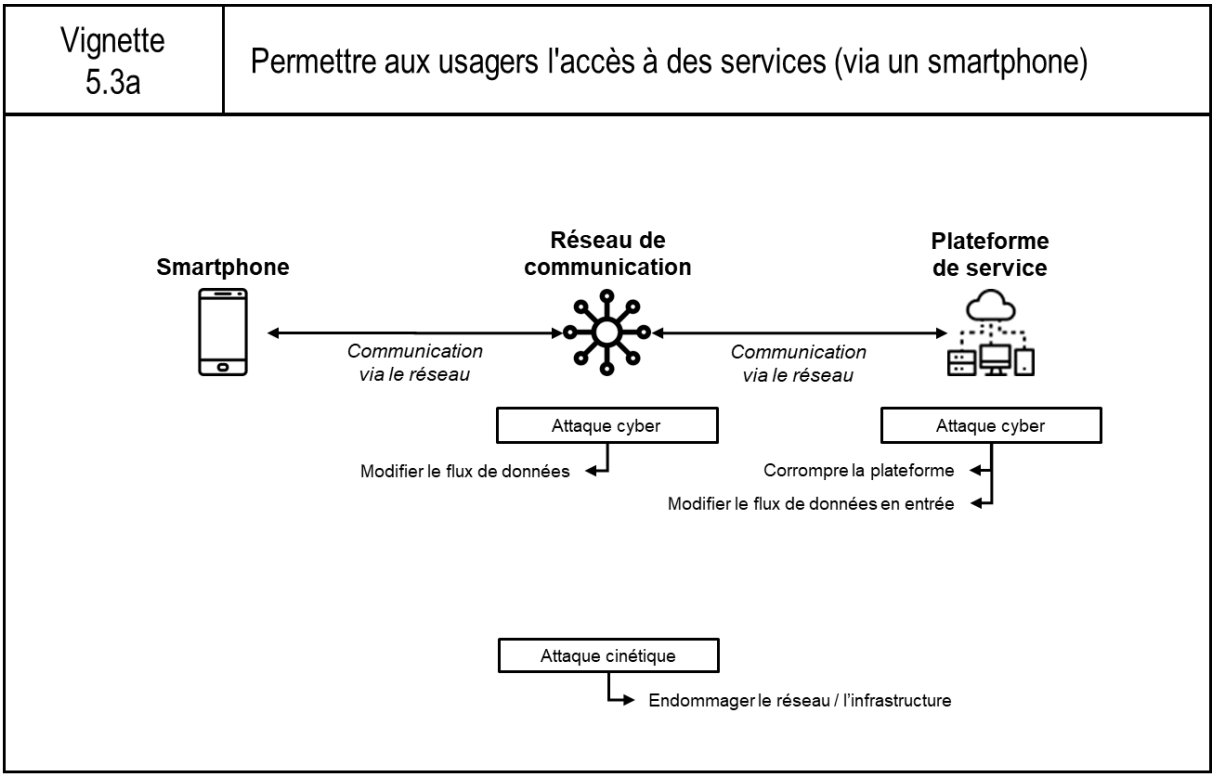


Figure 38 : Vignette 5.2 – Permettre aux passagers l'accès à des services (via un smartphone)

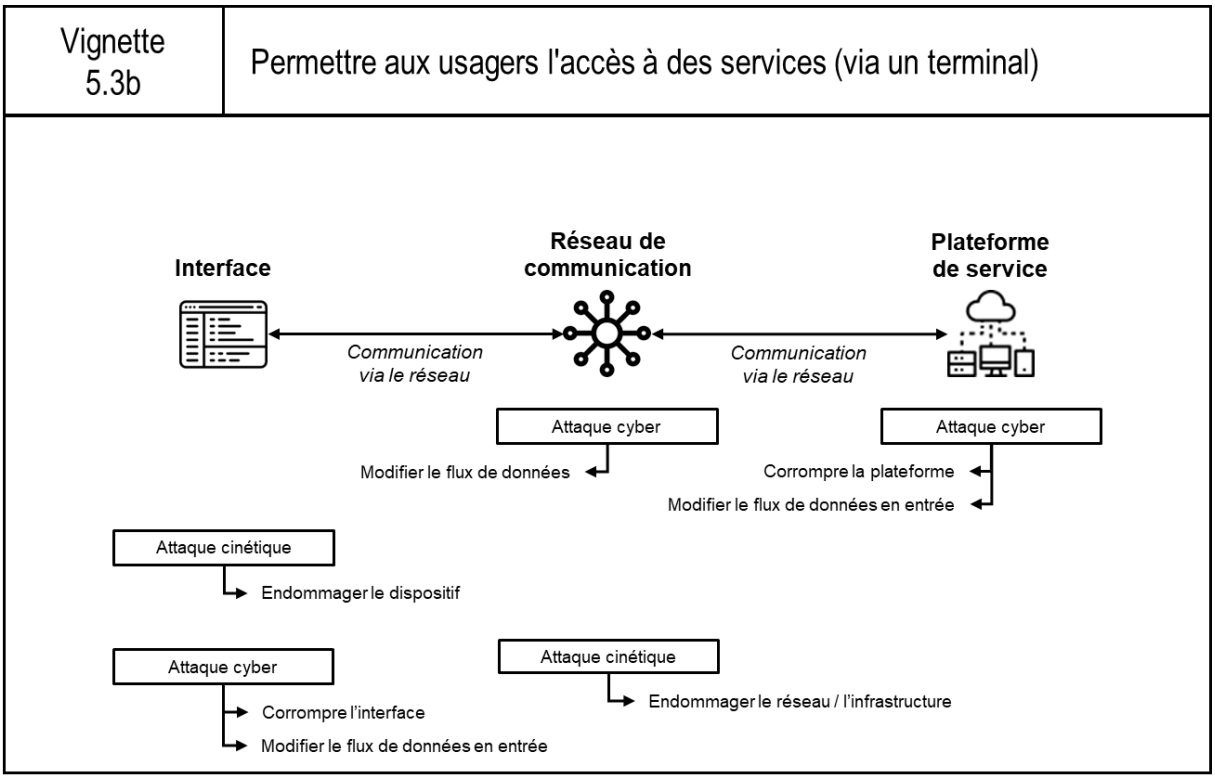


Figure 39 : Vignette 5.2 – Permettre aux passagers l'accès à des services (via un terminal)

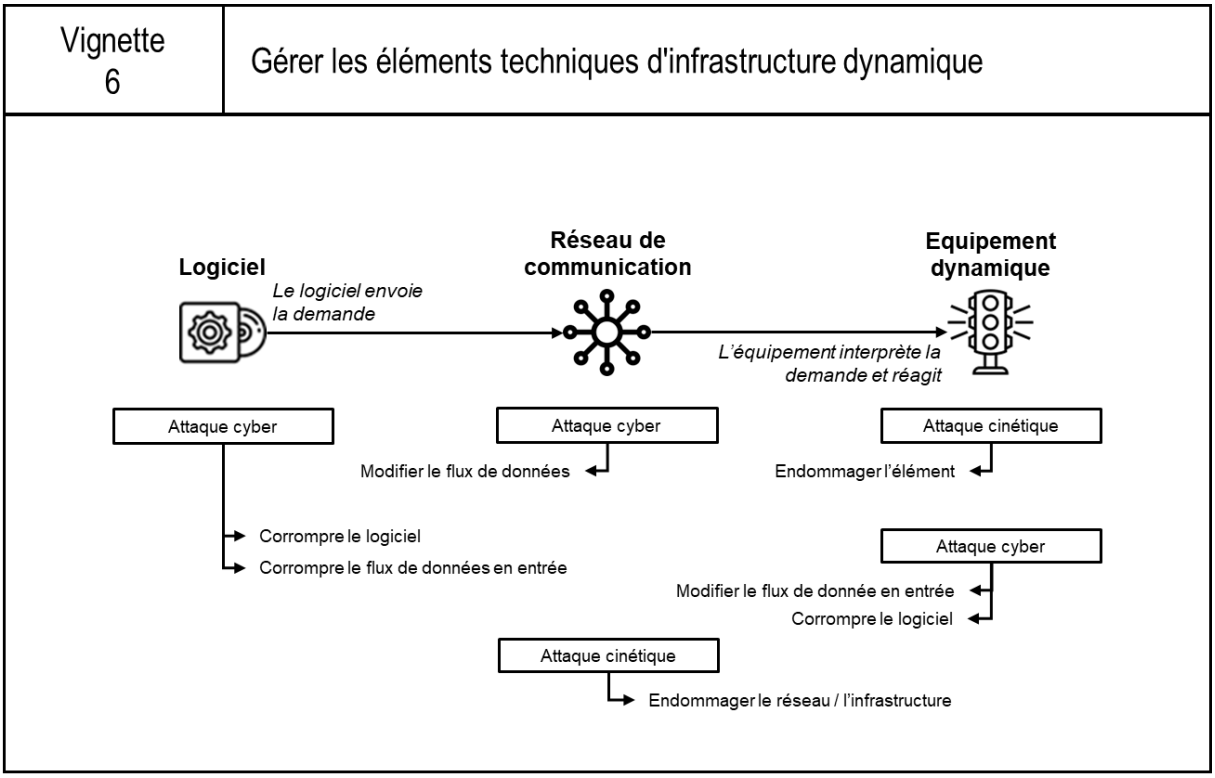


Figure 40 : Vignette 6 – Gérer les éléments techniques d'infrastructure dynamique

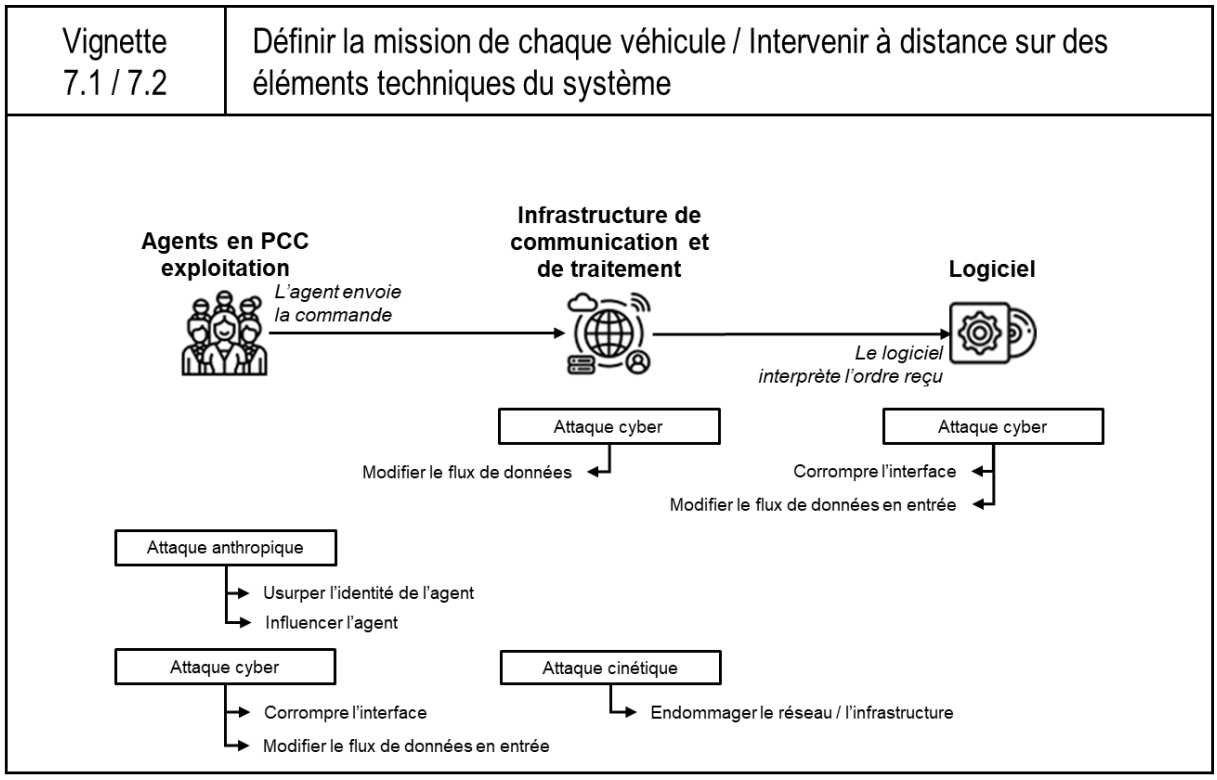


Figure 41 : Vignette 7.1 / 7.2 – Définir la mission du véhicule / Intervenir sur des composants

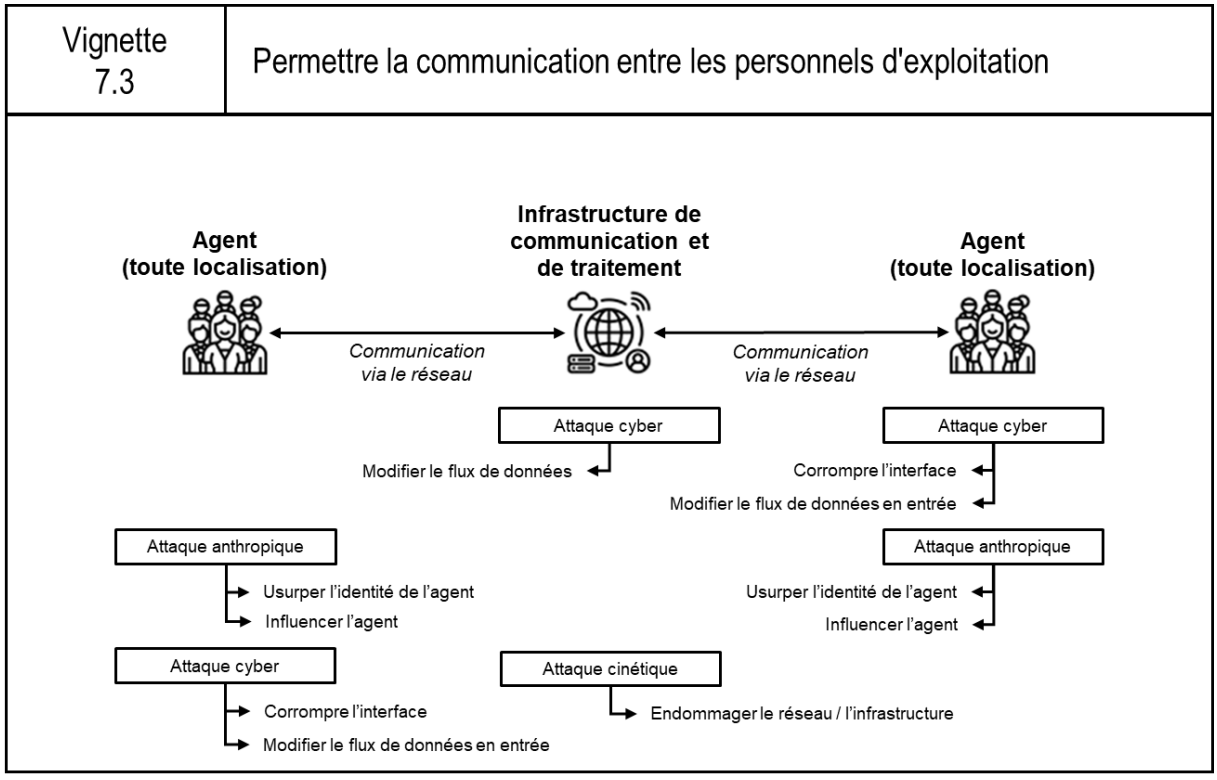


Figure 42 : Vignette 7.3 – Permettre la communication usagers / le personnel d'exploitation

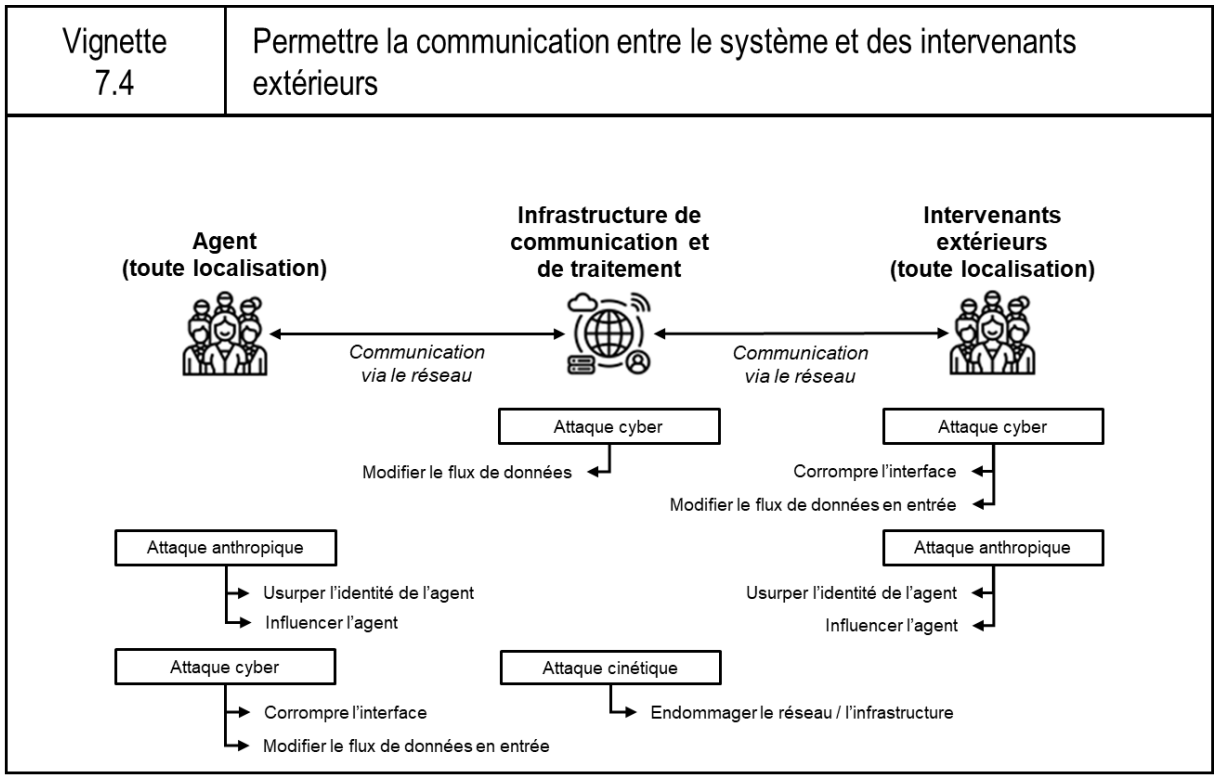


Figure 43 : Vignette 7.4 – Permettre la communication entre système / intervenants extérieurs

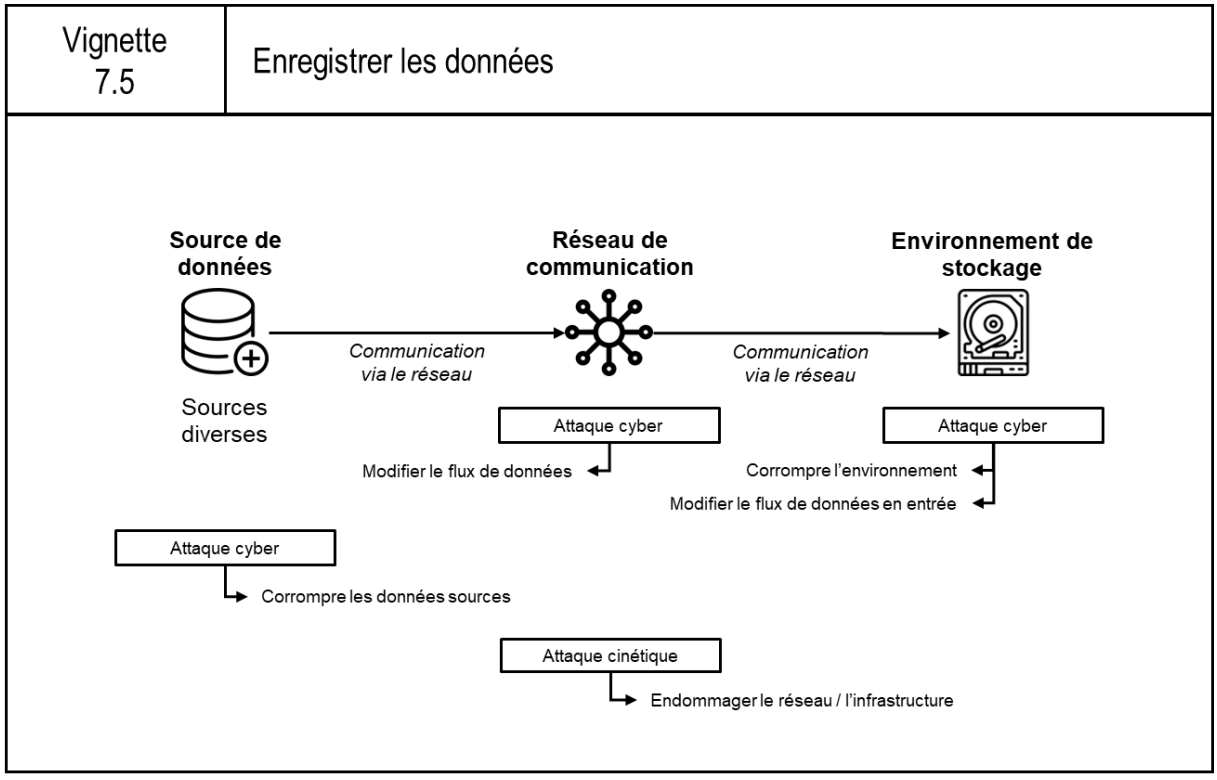


Figure 44 : Vignette 7.5 – Enregistrer les données

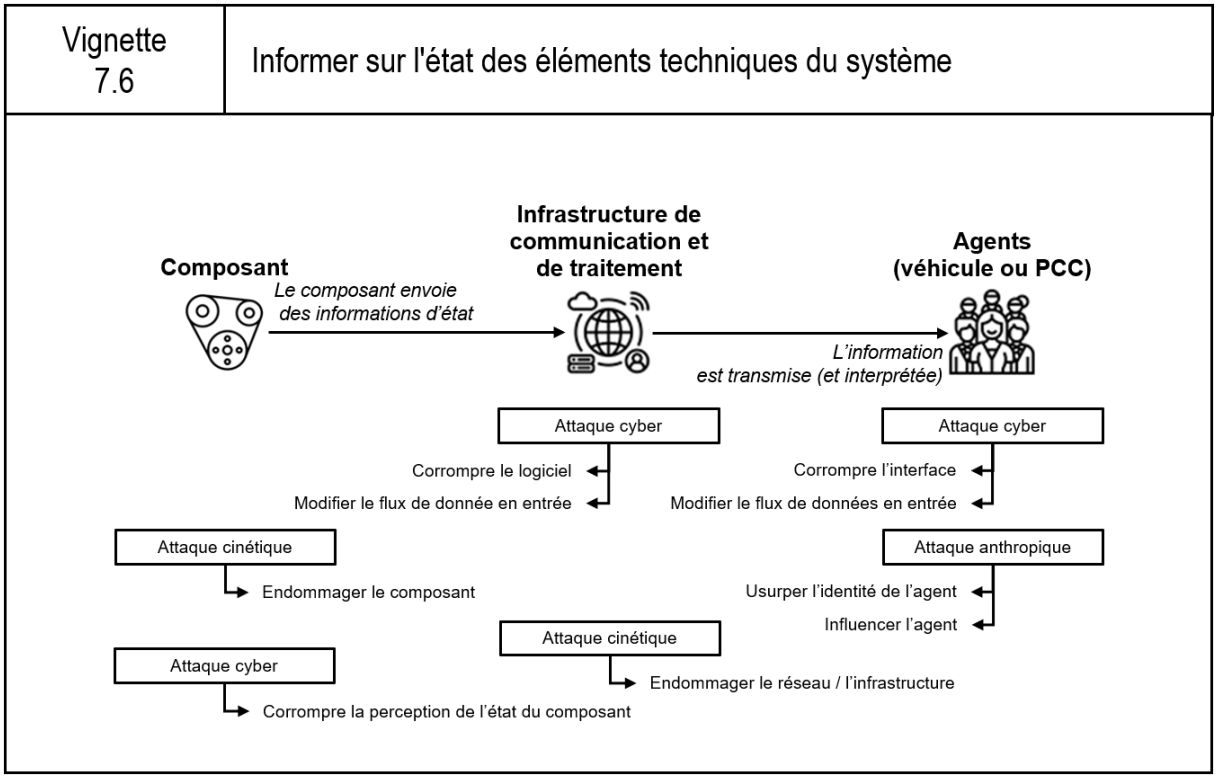


Figure 45 : Vignette 7.6 – Informer sur l'état des éléments techniques du système

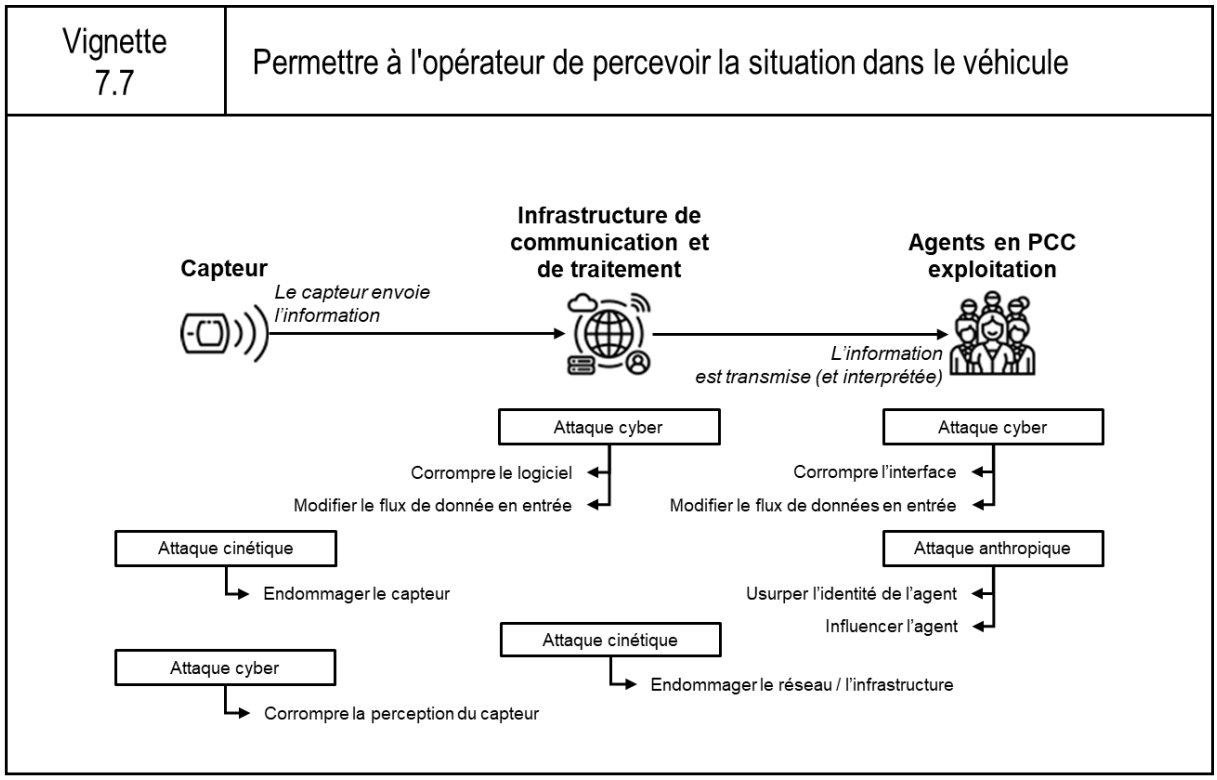


Figure 46 : Vignette 7.7 – Permettre à l'opérateur de percevoir la situation dans le véhicule

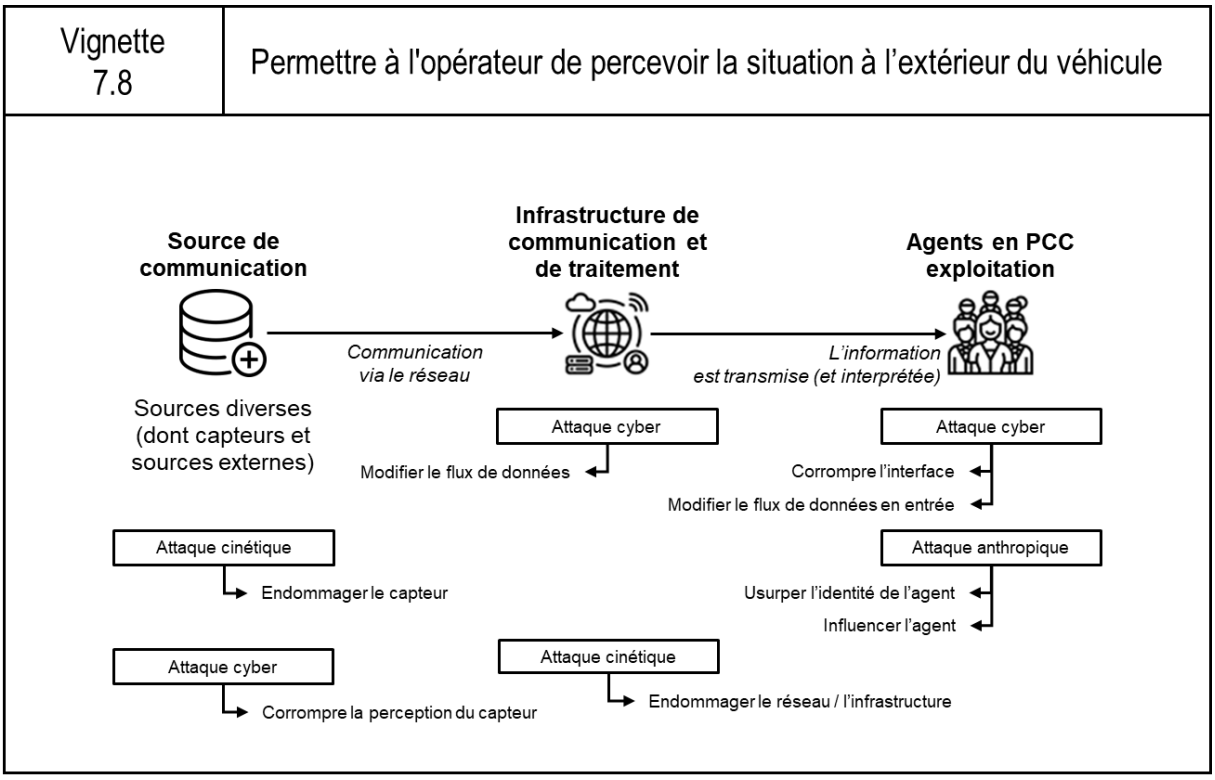


Figure 47 : Vignette 7.8 – Permettre à l'opérateur de percevoir la situation à l'extérieur du véhicule

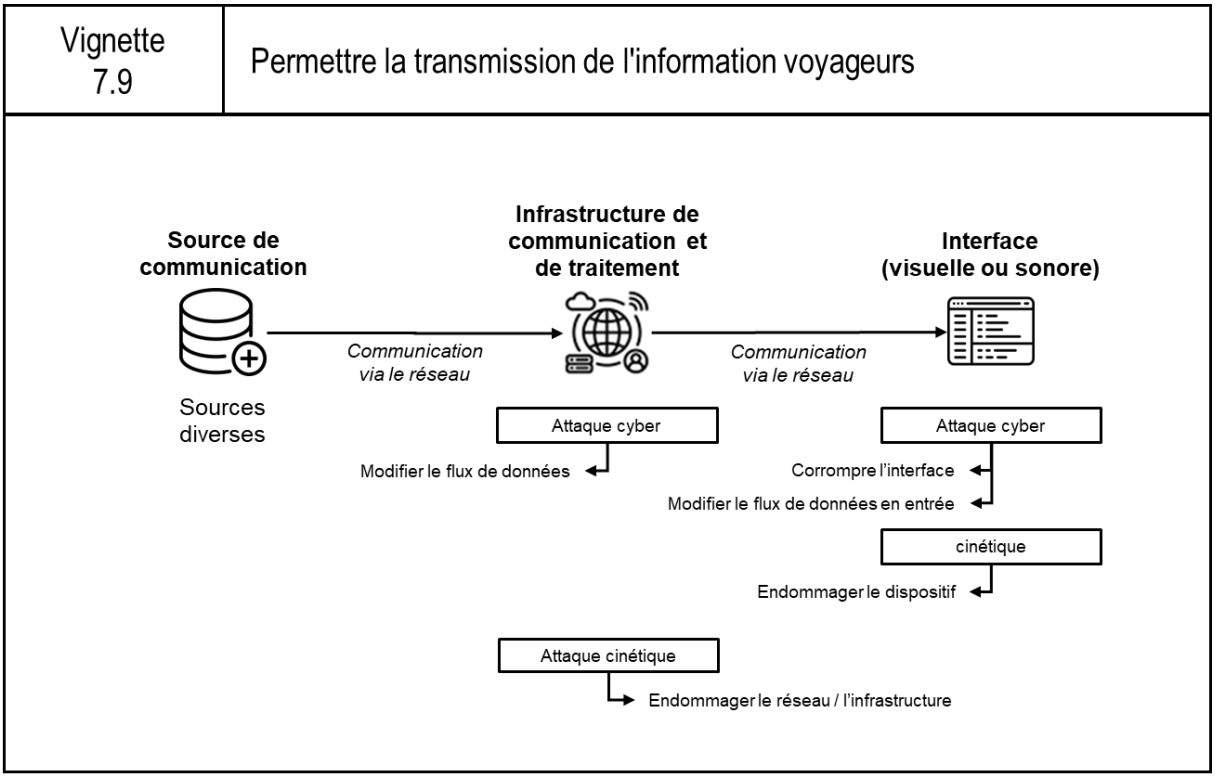


Figure 48 : Vignette 7.9 – Permettre la transmission de l'information voyageurs (STRA-P)

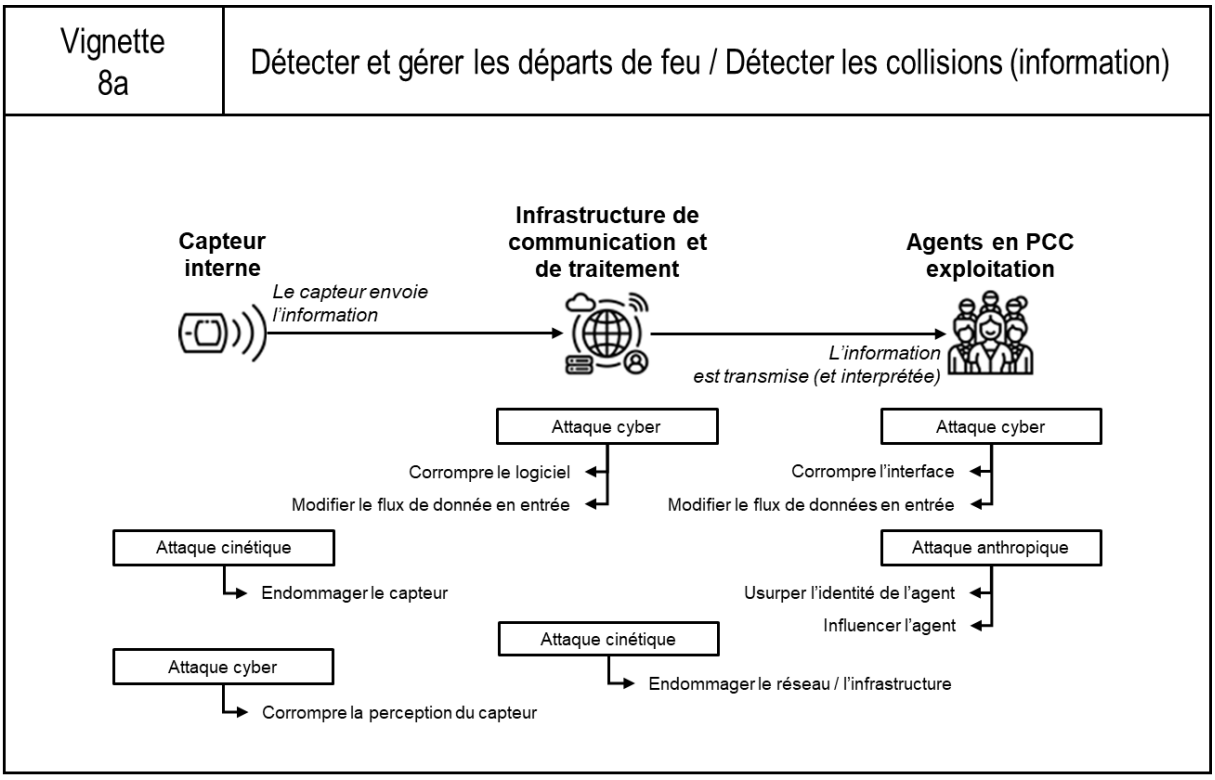


Figure 49 : Vignette 8a – Détecter et gérer les départs de feu / Détecter les collisions (information)

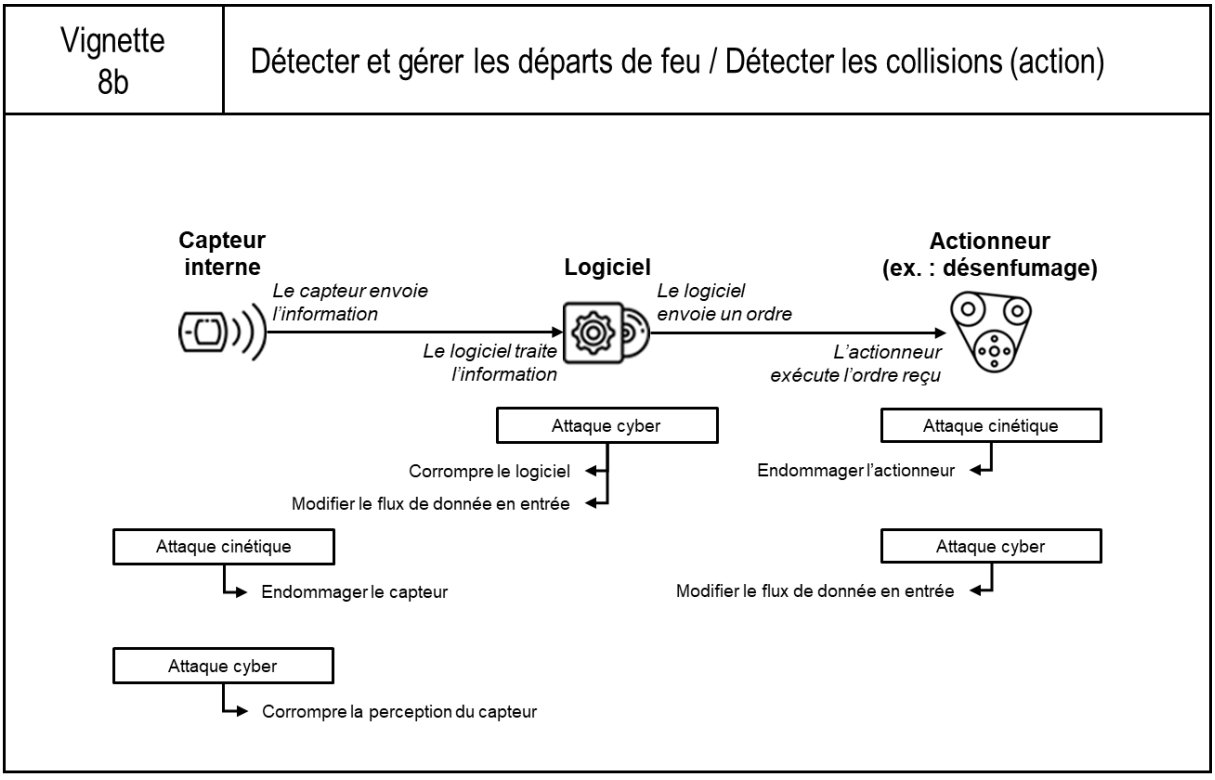


Figure 50 : Vignette 8b – Détecter et gérer les départs de feu / Détecter les collisions (action)

Annexe I : Liste des fonctions d'un STRA

Les éléments exposés ci-après proviennent du Guide technique relatif à la démonstration GAME pour les STRA.

La décomposition fonctionnelle se veut indépendante des technologies mises en œuvre dans le système et des types de parcours de circulation. Ce tableau doit être adapté et complété par les porteurs de projet au vu des spécificités de chaque système.

Les règles suivantes sont à prendre en compte lors de l'utilisation de ce tableau :

- La liste des fonctions ne saurait être exhaustive et a vocation à être enrichie dans le cadre du déroulement d'un projet ;
- A l'inverse, même si les fonctions présentées se veulent génériques, certaines peuvent ne pas être présentes sur un projet spécifique ; il conviendra dans ce cas de le tracer et de le justifier ;
- La décomposition des fonctions suit une arborescence purement fonctionnelle. Le rang de la fonction ne préjuge aucunement de son poids vis-à-vis des enjeux de sécurité ou des obligations réglementaires ;
- Une fonction (quel que soit son rang) peut contribuer par la transmission du flux (ex. Données, matière, énergie, etc.) A plusieurs fonctions de rang équivalent ou supérieur (ex. : la fonction 1.1 « percevoir l'environnement » peut transmettre des données utiles aux fonctions : 1.2, 1.3, 2, etc.) ;
- Les fonctions listées dans le tableau ne comportent pas les fonctions "techniques" telles que l'alimentation électrique, les liaisons de communication, etc. Celles-ci doivent être prises en compte au stade de l'analyse de chaque fonction auxquelles elles contribuent.

Rang 1		Rang 2		Rang 3		Rang 4	
Fonctions	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**
1-Assurer la définition, le suivi et le contrôle de la trajectoire du véhicule	**-**	1.1-Percevoir l'environnement (sense)	La fonction 1.1 permet d'assurer la perception des données, par exemple : la détection d'objets (statiques, dynamiques, êtres vivants…), des événements de circulation, de conditions (météo…) et les éléments de l'infrastructure Peut être assurée par des capteurs : ex. caméras, lidars, radars, par exemple (embarqué/débarqué)	1.1.1-Percevoir/traiter les objets	Obstacles statiques/mobiles et/ou autres usagers de la route	1.1.1.1-Détecter les objets	Savoir détecter un objet sur la trajectoire ou proche
						1.1.1.2-Caractériser les objets	Savoir identifier un objet (vélo, moto, camion, animal, obstacle, piéton, agent des FO, véhicule prioritaire...)
						1.1.1.3-Prédire/interpréter le comportement des objets	Anticiper la vitesse et la trajectoire des objets identifiés (en amont de la prise de décision : je double, je m'arrête) Interpréter les gestes et injonctions des forces de l'ordre
				1.1.2-Percevoir/traiter les infrastructures	Connectées ou non (feux, panneau STOP, passage piéton, marquage au sol, …), peut aussi être assurée par la localisation (a priori perception)	1.1.2.1-Détecter les infrastructures	Savoir détecter une infrastructure
						1.1.2.2-Caractériser les infrastructures	Savoir identifier une infrastructure statique ou dynamique (feu rouge, vert, STOP, marquage au sol…)
						1.1.2.3-Traiter le statut d'une infrastructure	Respecter la signalétique dynamique ou non (s'arrêter au feu rouge, avancer au feu vert, s'arrêter au STOP…)

Rang 1		Rang 2		Rang 3		Rang 4	
Fonctions	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**
1-Assurer la définition, le suivi et le contrôle de la trajectoire du véhicule				1.1.3-Percevoir/traiter les VP et AFO	-	1.1.3.1-Détecter les VP et les agents des FO	Détecter les véhicules d'intérêt général à caractère prioritaire ou bénéficiant de facilités de passages (VP) et les agents des forces de l'ordre (AFO)
						1.1.3.2-Caractériser les VP et les AFO	Identifier les types de VP en présence, et la nature des agents
						1.1.3.3-Interpréter les injonctions des AFO et intentions des VP	-
		1.2-Localiser le véhicule sur le parcours / zone par rapport à l'itinéraire défini	La fonction 1.2 permet d'assurer la localisation du véhicule sur un parcours/une zone L'itinéraire peut être défini à différents niveaux : - en amont de la mission (cas d'un STRA déployé sur un parcours prédéfini) - pendant la mission : cas d'un itinéraire calculé et remis à jour pendant la mission, par le système en fonction d'éléments extérieurs (trafic, informations supervision,	1.2.1 Connaître la mission (itinéraire défini)	Connaître l'itinéraire à suivre, relatif au service de transport alloué au véhicule, y compris les stations, les points d'arrêt à la demande, les points d'évacuation possibles, ... par exemple, dans le cas d'un itinéraire prédéfini en amont, en flashant et mettant à jour la map et la mission (temps) dans le PC du système.	-	-

Rang 1		Rang 2		Rang 3		Rang 4	
Fonctions	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**
1-Assurer la définition, le suivi et le contrôle de la trajectoire du véhicule			etc.) (cas d'un STRA de type robot-taxi par exemple) -etc.	1.2.2 - Localiser le véhicule	Positionner le véhicule (coordonnées)	1.2.2.1-Charger la carte	Surveiller à distance la position et le déplacement du véhicule, et connaitre à priori l'environnement dans lequel va circuler le véhicule. Prendre des mesures si la position ou le déplacement s'écarte de certaines valeurs fixées d'avance. => 1.3
						1.2.2.2-Localiser le véhicule sur la carte	La localisation peut être assurée par des signaux GPS et/ou des capteurs embarqués, : ex. IMU/odométrie, accompagnés ou non d'équipements déployés sur l'infrastructure.
		1.3-Prendre la décision concernant le contrôle dynamique (plan)	En fonction de la perception (1.1) et la localisation (1.2), décider des mouvements et de la dynamique du véhicule, en tenant compte de la mission, des manœuvres et des contraintes réglementaires.	1.3.1- Décider des actions opérationnelles pour le déplacement longitudinal et latéral du véhicule.	Décider de la prochaine séquence de manœuvres "nominales" (avec ses composantes longitudinale et latérale) à réaliser à court terme (par exemple tourner à gauche et changer de file, en ralentissant à x km/h etc.	-	-

Rang 1		Rang 2		Rang 3		Rang 4	
Fonctions	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**
1-Assurer la définition, le suivi et le contrôle de la trajectoire du véhicule				1.3.2- Décider des actions tactiques pour le déplacement longitudinal et latéral du véhicule.	Décider de la manœuvre en temps réel (avec ses composantes longitudinale et latérale) à réaliser immédiatement (par exemple décélérer, freiner et tourner à gauche d'un angle de 10°)	-	-
		1.4-Assurer le contrôle dynamique (act)	La fonction 1.4 permet d'assurer les commandes du mouvement latéral (direction) et longitudinal (freinage et accélération) en tenant compte l'énergie servant à la traction/freinage.	1.4.1-Assurer le contrôle longitudinal	Va permettre de répondre aux exigences de niveau service de type "respecter la limitation de vitesse", "respecter l'inter distance"…	1.4.1.1- Gérer l'accélération	- inclut les actions sur la traction et le frein - inclut la prise en compte des valeurs du gamma + et du jerk
						1.4.1.2-Gérer la décélération	- inclut les actions sur la traction et le frein - inclut la prise en compte des valeurs du gamma - et du jerk
						1.4.1.3- Immobiliser	- arrêt prolongé - assurer l'immobilisation du véhicule
				1.4.2-Assurer le contrôle latéral (direction)	Fonction élémentaire permettant de se positionner sur la voie en Y (se centrer sur la voie, prendre un virage, changer de voie…)	-	-

Rang 1		Rang 2		Rang 3		Rang 4	
Fonctions	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**
2-Signaler le véhicule vis-à-vis des autres usagers de la route (signalisation sonore, visuel, etc.)	En fonction de la fonction 1, se signaler aux autres usagers de la route via des avertisseurs sonores (klaxon, cloche…), via des avertisseurs visuels (les feux de croisement, de route, bouillard, clignotant…), ou via des communications V2X. Cette fonction peut être supportée par le véhicule et/ou des équipements d'infrastructure (intentions de manœuvre à l'arrivée/départ de station par ex)	2.1 - signaler le mode délégation de conduite	-	-	-	-	-
		2.2 - signaler les intentions de manœuvre du véhicule	- vers les autres véhicules - vers les piétons - vers les VRU - lors de phases spécifiques (entrées/sorties de station)	-	-	-	-
		2.3 - signaler une décélération importante du véhicule	cf. homologation: signalisation si gamma > seuil	-	-	-	-
		2.4 - signaler la position du véhicule	- situations nominales - situations avec manque de visibilité	-	-	-	-
		2.5 - signaler la situation du véhicule	- signalisation suite à MRM - signalisation suite à incident (feux de détresse)	-	-	-	-
		2.6 - signaler un danger imminent	- en cas de danger imminent détecté par le véhicule ego (feux de détresse, avertisseur sonore, appel de phares, etc.)	-	-	-	-

Rang 1		Rang 2		Rang 3		Rang 4	
Fonctions	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**
3-Gérer les accès aux véhicules automatisés	**-**	3.1-Gérer le transfert des personnes aux points autorisés (STRA-P)	La fonction 3.1 permet d'assurer le transfert des personnes (montée/descente des passagers/personnel d'urgence/employés du service…) aux points autorisés (station, point d'arrêt à la demande...)	3.1.1-Assurer un accostage avec espacement limité véhicule/trottoir	- cas de TC : lacune horizontale et verticale < 50 mm (cf. Arrêté accessibilité 13/07/2009) - A traiter le cas du point d'arrêt à la demande / robot-taxi Déployer les dispositifs dédiés en station ou dans le véhicule (emmarchements mobiles, baraquage…)	3.1.1.1 - Respecter une lacune verticale limitée	-
						3.1.1.2 - Respecter une lacune horizontale limitée	-
				3.1.2- Gérer l'ouverture et la fermeture des portes pour faire entrer/sortir les personnes	- ouverture des portes aux points autorisés - non-ouverture des portes hors des points autorisés et des cas d'évacuation - …	-	-
				3.1.3-Gérer l'E/S des PMR	Déployer les dispositifs dédiés en station ou dans le véhicule (emmarchements mobiles, rampe PMR, baraquage…)	-	-
				3.1.4- Surveillance du dépassement de la capacité maxi du véhicule	-	3.1.4 .1 - surveiller le nombre de passagers debout et/ou assis	-
						3.1.4.2 - surveiller le PTAC	-

Rang 1		Rang 2		Rang 3		Rang 4	
Fonctions	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**
3-Gérer les accès aux véhicules automatisés				3.1.5- surveiller les conditions de redémarrage du véhicule en ce qui concerne les dispositifs mobiles d'accès et d'embarquement	- position des dispositifs portes, élévateur, rampe, système de baraquage, - absence de coincement - absence d'entrainement d'un usager	-	-
		3.2-Maintenir le véhicule automatisé fermé hors transfert personnes/évacuation (STRA-P)	En dehors des points autorisés, la fonction 3.2 permet d'assurer le maintien des portes en position fermée.	3.2.1 - Empêcher l'autorisation d'ouverture de portes hors des phases de transfert ou d'évacuation	-	-	-
				3.2.2 - Surveiller l'état des portes	Surveillance du verrouillage et de la position fermée des portes hors des phases de transfert ou d'évacuation	-	-

Rang 1		Rang 2		Rang 3		Rang 4	
Fonctions	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**
3-Gérer les accès aux véhicules automatisés		3.3-Permettre l'évacuation et l'accès des secours (STRA-P)	En complément des fonctions 3.1 et 3.2, la fonction 3.3 permet l'évacuation des passagers et l'accès de secours en cas d'urgence.	3.3.1- Donner moyen aux passagers d'évacuer l'habitacle du véhicule	Issues de secours suffisantes et accessibles. Moyens d'ouverture accessibles et adaptés. Cas des PMR à prendre en compte Pour les cat M2 et M3, l'homologation fixe le nb d'issues de secours présentes (cf. UNR 107). Cas de commande automatique d'ouverture des portes automatiques dans les situations d'urgence.	-	-
				3.3.2 - Donner moyen au personnel technique et aux services de secours d'accéder à l'habitacle du véhicule	-	-	-
				3.3.3 - Informer l'opérateur distant en cas d'actionnement des systèmes d'ouverture prévus des issues de secours pour l'évacuation	-	-	-

Rang 1		Rang 2		Rang 3		Rang 4	
Fonctions	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**
3-Gérer les accès aux véhicules automatisés		3.4-Gérer les interfaces avec les opérations de chargement/déchargement (STRA-M)	La fonction 3.4 permet d'assurer les interfaces entre les opérations de chargement et de déchargement, y compris d'arrimage des marchandises, et les fonctions de conduite automatisée.	-	-	-	-
		3.5 -Maintenir le véhicule automatisé fermé hors des phases de chargement/déchargement (STRA-M)	En dehors des points autorisés, la fonction 3.5 permet d'assurer le maintien des portes en position fermée.	-	-	-	-
4-Assurer des conditions de transport satisfaisantes pour les passagers (STRA-P)	Ces fonctions permettent d'assurer le confort des passagers (thermique, acoustique, vibratoire, maintien, luminosité et visibilité...) Néanmoins, certaines de ces fonctions peuvent présenter un enjeu en termes de sécurité, et doivent alors être prises en compte dans la démonstration de sécurité. Par exemple, l'éclairage de l'habitacle du véhicule peut être nécessaire pour prévenir le risque de chute des passagers ; le désembuage des vitres permettant la perception de l'environnement par les passagers peut être important dans le contexte d'une évacuation.						
5-Permettre aux usagers d'interagir avec des éléments techniques du système	**-**	5.1-Permettre la communication des usagers vers le personnel d'exploitation (COM)	La fonction 5.1 permet d'assurer la communication sonore et visuelle entre les usagers (à bords du véhicule et en station) et le personnel d'exploitation.	5.1.1 - Permettre aux usagers du système de dialoguer avec le personnel d'exploitation	Interphonie véhicule, interphonie station, etc.	-	-

Rang 1		Rang 2		Rang 3		Rang 4	
Fonctions	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**
				5.1.2 - Permettre aux usagers du système d'alerter le personnel d'exploitation	Par ex. : Système de demande d'assistance passagers (projet NAVURBAUT)	-	-
		5-2 Permettre aux passagers de demander l'arrêt du véhicule (STRA-P)	Système de demande d'arrêt sécurité passagers (projet NAVURBAUT)	-	-	-	-
		5.3-Permettre aux usagers l'accès à des services	La fonction 5.3 permet d'assurer l'accès à des services pour les usagers en station/ sur smartphone/ dans les véhicules, ... (ex. Horaire, tickets, réservation, ...). Certaines de ces fonctions peuvent éventuellement présenter des risques liés à la sécurité	-	-	-	-
6-Gérer les éléments techniques d'infrastructure dynamiques pilotés par le système	La fonction 7 permet de gérer la signalisation dynamique (gestion des priorités avec feux de signalisation, vitesse, …), les composants de ségrégation dynamique (barrières, potelets, etc.), etc.	6-1 commander la signalisation dynamique	Par exemple, pilotage des feux connectés	-	-	-	-

Rang 1		Rang 2		Rang 3		Rang 4	
Fonctions	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**
		6-2 commander les équipements dynamiques mobiles	Par exemple, pilotage des barrières mobiles, bornes escamotables, etc.	-	-	-	-

Rang 1		Rang 2		Rang 3		Rang 4	
Fonctions	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**
7-Assurer l'exploitation du système	Gestion de la flotte et des missions, du service dans son ensemble, surveillance de l'environnement des éléments techniques du système sur parcours/zone, changer/planifier la mission, enclencher un mode dégradé (refuge)…	7.1 - définir la mission de chaque véhicule	- Définir les contraintes d'itinéraire , relatif au service de transport alloué au véhicule, y compris les stations voyageurs, les points d'arrêt à la demande, les points d'évacuation possibles - Définir les contraintes temporelles (date, heure de départ, heure d'arrivée, heures de passage, fréquence, ...) La mission peut être définie au préalable en fonction des conditions prévues sur le parcours, ou être éventuellement modifiée en cours d'exploitation au vu des évènements rencontrés ou connus (nécessite une communication avec les services extérieurs).	-	-	-	-

Rang 1		Rang 2		Rang 3		Rang 4	
Fonctions	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**
7-Assurer l'exploitation du système		7.2- Intervenir à distance sur des éléments techniques du système	La fonction 9.1 permet d'assurer les différents types d'intervention à distance prévus par le système. Intervention à distance : Action exercée par une personne habilitée située à l'extérieur d'un système de transport routier automatisé, aux fins : • d'activer ou de désactiver le système, ou de donner l'instruction d'effectuer, modifier, interrompre une manœuvre, d'acquitter des manœuvres proposées par le système, • de donner instruction au système de choisir ou de modifier la planification d'un itinéraire ou des points d'arrêt pour les usagers (notamment en réponse à des aléas ou des défaillances).	7.2.1 - arrêter le(s) véhicules	Immédiat en zone station, next stop, ASAP, etc.	-	-
				7.2.2 - activer/désactiver le mode délégation de conduite		-	-
				7.2.3 - donner une consigne au(x) véhicule(s)	Réduction de vitesse, consigne de vitesse maximale	-	-
				7.2.4 - acquitter une manœuvre proposée		-	-
				7.2.5 – donner l'instruction d'effectuer une manœuvre		-	-
				7.2.6 – donner l'instruction d'interrompre une manœuvre	Définir l'état suite à interruption manœuvre	-	-
				7.2.7 – donner l'instruction de modifier une manœuvre		-	-
				7.2.8 - commander des équipements du véhicule	essuie-glaces, éclairage, etc. rampes portes etc.	-	-

Rang 1		Rang 2		Rang 3		Rang 4	
Fonctions	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**
7-Assurer l'exploitation du système				7.2.9 - percevoir l'environnement de l'équipement commandé, pour donner les autorisations de manœuvre ou de démarrage	Environnement des portes si commande des portes à distance ou en cas de défaut, environnement de la rampe PMR si commandée à distance	-	-
		7.3-Permettre la communication entre les personnels d'exploitation	La fonction 9.2 permet d'assurer la communication entre les personnels d'exploitation. Par exemple, communication entre le personnel d'exploitation situé au poste de supervision et le personnel d'exploitation sur site ou dans le véhicule	-	-	-	-
		7.4-Permettre la communication entre le système et des intervenants extérieurs	La fonction 9.3 permet d'assurer la communication entre les personnels d'exploitation et les intervenants extérieurs (ex. Force de l'Ordre, les opérateurs PCC, Préfet dans le cas d'un plan ORSEC ou équivalemment service de secours comme les pompiers, SAMU, les fournisseurs de service (EDF, télécom), la ville et les acteurs intervenant sur la voirie (Gaz, DDE, EDF…)).	7.4.1 - permettre l'initiation de la communication avec le système à la demande de l'intervenant extérieur	Moyen pour l'intervenant d'établir la communication	-	-
				7.4.2 - permettre la communication entre le personnel d'exploitation et les intervenants extérieurs	Communication à l'initiative du personnel ou à l'initiative de l'intervenant extérieur (agent des forces de l'ordre, services de secours par exemple)	-	-

Rang 1		Rang 2		Rang 3		Rang 4	
Fonctions	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**
7-Assurer l'exploitation du système				7.4.3 - permettre la communication des informations nécessaires à l'intervenant extérieur	Par exemple, documents du véhicule à destination des agents des forces de l'ordre	-	-
		7.5-Enregistrer les données	La fonction 7.5 permet d'enregistrer les données pour répondre aux besoins de l'exploitation.	7.5.1 - Enregistrer les données des différents sous-systèmes pour l'amélioration continue du système	-	-	-
				7.5.2 - Enregistrer les données des différents sous-systèmes pour l'analyse des accidents	Cf. code des transports art R3152-22	-	-

Rang 1		Rang 2		Rang 3		Rang 4	
Fonctions	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**
7- Assurer l'exploitation du système		7.6- informer sur l'état des éléments techniques du système	La fonction 7.6 permet la supervision / l'exploitation (afficher les états des éléments techniques, des alertes, des évènements, des conditions (météo, etc.), etc.)	7.6.1 - informer sur l'état du véhicule	Y compris niveau de charge batterie Y compris ceintures de sécurité Y compris état des portes Y compris état des issues de secours Y compris vitesse instantanée, etc.	-	-
				7.6.2 - informer sur les conditions de fonctionnement du véhicule	Par exemple véhicule en situation d'évacuation, véhicule en attente, état de délégation de conduite du véhicule, arrêt suite manœuvre d'urgence, arrêt suite à MRM, arrêt suite à collision, évènement	-	-
				7.6.3 - Informer sur l'état des équipements du système, ou participant à la sécurité du système.	Y compris la supervision Y compris les équipements du système préexistants et participant à la sécurité	-	-

Rang 1		Rang 2		Rang 3		Rang 4	
Fonctions	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**
7-Assurer l'exploitation du système		7.7- permettre à l'opérateur de percevoir la situation dans le véhicule	Écoute passive visio sur passagers	7.7.1 - Percevoir l'ambiance sonore dans l'habitacle du véhicule	-	-	-
				7.7.2 - Pouvoir avoir une vision de l'intérieur véhicule	-	7.7.2 - Pouvoir avoir une vision générale de l'habitacle du véhicule	Par ex gérer les demandes d'arrêt passagers
					-	7.7.3 - Pouvoir avoir une vision sur des points particuliers de l'habitacle	Par exemple pour réaliser des identifications ou des levées de doute (zones de coincement portes, incendie…)
		7.8 - permettre à l'opérateur de percevoir la situation à l'extérieur du véhicule	-	7.8.1 - percevoir le voisinage du véhicule		7.8.1.1 - percevoir l'environnement de circulation au voisinage du véhicule	Perception des conditions d'une évacuation ou d'une manœuvre, y compris des conditions météo
						7.8.1.2 - Pouvoir avoir une vision sur des points particuliers situés hors de l'habitacle	Par exemple pour réaliser des identifications ou des levées de doute : zones portes côté quai, zone rampe, incendie Vérification d'absence de coincement, d'absence d'entrainement d'un passager, etc.

Rang 1		Rang 2		Rang 3		Rang 4	
Fonctions	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**
7-Assurer l'exploitation du système				7.8.2 - permettre à l'opérateur de connaître la situation sur le parcours		7.8.2.1 -connaître les conditions de circulation prévisibles sur le parcours	Conditions trafic et météo afin d'adapter les consignes d'exploitation
						7.8.2.2 -connaître les conditions de circulation en des points particuliers du parcours	Par exemple, vision déportée sur un PN ou zone accidentogène
		7.9 -Permettre la transmission de l'information voyageurs (STRA-P)	La fonction 5.2 permet d'assurer la transmission d'informations sonores ou visuelles aux usagers (à bord du véhicule et en station).	7.9.1- Donner des informations aux usagers en station	Messages audio ou affichage	-	-
				7.9.2 - Donner des informations aux passagers du véhicules	Messages audio ou affichage	-	-
		7.10 - permettre l'intervention en sécurité des services de secours	Existence de moyens d'immobilisation du véhicule, protection / risque électrique, etc. existants, connus et accessibles pour secours	-	-	-	-

Rang 1		Rang 2		Rang 3		Rang 4	
Fonctions	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**
8- Détecter et gérer certaines situations particulières	**-**	8.1 - détecter et gérer les départs de feu	-	8.1.1 - détecter et gérer les départs de feu dans les véhicules	-	-	-
				8.1.2 - détecter et gérer les départs de feu dans les stations	-	-	-
				8.1.3 -détecter et gérer les départs de feu dans les équipements du parcours	Y compris équipements dédiés à la supervision	-	-
				8.1.4 -détecter et gérer les départs de feu dans les équipements de la supervision	-	-	-
		8.2- détecter les chocs contre le véhicule	Cas de collision impactant la sécurité des passagers ou des tiers (tiers, obstacles fixes, etc..)	-	-	-	-

Rang 1		Rang 2		Rang 3		Rang 4	
Fonctions	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**	**Fonctions**	**Commentaires**
9 - Assurer le maintien du système dans ses conditions de sécurité	**-**	9.1 - Adapter les consignes d'exploitation aux conditions de circulation	Réduction de vitesse, arrêt préventif du service en cas de conditions de circulation dégradées > seuil (trafic et/ou météo)	-	-	-	-
		9.2 - Détecter la sortie du système de son domaine d'emploi	Y compris dysfonctionnement équipements extérieurs participant à la sécurité	-	-	-	-
		9.3 - Exécuter une MRM adaptée à la situation	Adaptée au contexte, à la situation de parcours, etc. (y compris en cas de défaut d'acquittement de la part de l'opérateur)	-	-	-	-
		9.4 - Exécuter une manœuvre d'urgence adaptée à la situation	-	-	-	-	-
		9.5 - Exécuter un arrêt "ultime"	Fonction(s) liée(s) à la réponse à l'exigence de conserver la capacité d'arrêter le véhicule même en cas de défaillance profonde du système entrainant l'incapacité du système à effectuer une MRM (FAILURE MITIGATION STRATEGY cf. SAE J3016_202104 3.11)	-	-	-	-

Tableau 18 : Liste des fonctions d'un STRA

Annexe J : Liste des accidents de niveau système

Les éléments exposés ci-après proviennent du Guide technique relatif à la démonstration GAME pour les STRA.

Certains points d'attention sont à noter sur ce tableau :

- La liste n'est pas exhaustive et a vocation à être enrichie ;
- Un type d'accident peut être la conséquence d'un autre type d'accident dans le cadre d'un scénario : par exemple, une collision peut survenir suite à une sortie de route du véhicule ou un incendie peut survenir suite à une collision, etc. L'analyse peut alors prioriser le traitement de l'accident initial de manière à mettre en place les mesures de réduction du risque visant à s'en prémunir ;
- Une cyberattaque peut être à l'origine de ces accidents ;
- Certains accidents présentés pourront faire l'objet d'un regroupement si l'analyse montre que leurs traitements sont identiques.

Type	ID	Accidents potentiels
Collision[7]	1.1	Collision avec usager vulnérable de la voirie (cycliste, piéton, etc.)
	1.2	Collision (latérale / frontale) contre un obstacle massif (containers, animaux, chute d'arbres, etc.)
	1.3	Collision avec un autre véhicule routier
	1.4	Collision avec le véhicule d'un système de transport guidé (tramways, etc.) ou ferré (ferroviaire lourd)
	1.5	Collision avec un autre type de véhicule
Chute de personnes	2.1	Chute de personne à l'intérieur du véhicule
	2.2	Chute de personne depuis le véhicule du système vers l'extérieur en station
	2.3	Chute de personne depuis le véhicule du système vers l'extérieur en ligne (STRA-P)
Renversement	3.1	Renversement véhicule
Electrisation / Électrocution	4.1	Electrisation / électrocution dans le véhicule
	4.2	Electrisation / électrocution dans une station
	4.3	Electrisation / électrocution sur le parcours au niveau d'un équipement du système
Feu / Fumée / Explosion	5.1	Feu / fumée dans le véhicule
	5.2	Feu / fumée au niveau d'une station

[7] La collision peut concerner également la collision avec un élément dépassant du gabarit du véhicule : collision avecla partie mobile du véhicule dont l'immobilisation serait inopérante ou collision avec un objet entraîné par le véhicule.

Type	ID	Accidents potentiels
Feu / Fumée / Explosion	5.3	Feu / fumée sur le parcours au niveau d'un équipement du système
	5.4	Explosion dans le véhicule
Feu / Fumée / Explosion	5.5	Explosion au niveau d'une station
	5.6	Explosion sur le parcours au niveau d'un équipement du système
Autres accidents de personnes	6.1	Personnes coincées / pincées par les ouvrants (fenêtres, portes, etc.) d'un élément technique du système
	6.2	Personnes coincées / pincées / heurtées par une partie mobile d'un élément technique du système
	6.3	Entrainement de personne par le véhicule (en particulier entrainement de personnes lors de la sortie de la station ou suite à un coincement de vêtement)
	6.4	Contact avec un élément agressif d'un élément technique du système (blessure suite à contact avec / par les parties saillantes, coupantes, pointues, etc.)
	6.5	Contact avec une partie chaude ou froide d'un des éléments techniques du système
	6.6	Contact avec un liquide dangereux (toxique, corrosive, etc.) d'un des éléments techniques du système
	6.7	Contact avec un gaz dangereux (toxique, etc.) d'un des éléments techniques du système
Chute / Projection ou perte d'objet	7.1	Chute / projection / perte d'éléments d'un véhicule du système vers la voirie
	7.2	Personnes heurtées suite à la chute / projection / perte d'élément d'un véhicule dans son habitacle
	7.3	Personnes heurtées suite à la chute d'objets transportés dans l'habitacle d'un véhicule du système d'un objet transporté (ex. : bagages, colis, etc.)
	7.4	Chute d'objets de l'infrastructure du système (feux de trafic, panneaux ou éclairage en station, etc.)

Tableau 19 : Liste des accidents de niveau système

Annexe K : Liste d'exigences de NICS

Cette annexe fournit des exemples d'exigences de NICS pour chaque exigence applicable à la cybersécurité pouvant faire l'objet d'une application des NICS. Elle donne également un aperçu du NICS qui pourrait être associé à chaque exigence de NICS, à titre purement indicatif.

Elle constitue une aide informative à la définition des exigences de NICS.

Ces exemples d'exigences de NICS ne se substituent pas au contenu des exigences applicables à la cybersécurité décrites dans le corps de texte du guide, qui doivent être respectées quel que soit le NICS.

Pour simplifier la présentation, les exemples d'exigences de NICS ne sont pas répétés quand ils concernent la mise à jour d'une exigence applicable à la cybersécurité déjà traitée auparavant. Ainsi, toutes les exigences applicables à la cybersécurité relatives à des mises à jour d'autres exigences sont implicitement censées reprendre les exemples d'exigences de NICS de ces dernières.

Certains exemples d'exigences de NICS renvoient à des notions qui sont précisées à la fin de la présente annexe.

Certains exemples d'exigences de NICS renvoient à des compétences de cybersécurité (cf. Annexe L pour la description de ces compétences).

Exemples d'exigences de NICS : phase de spécification / conception

[EX-1.02] Identifier l'existant à prendre en compte pour le système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
L'identification des facteurs à prendre en compte pour le système considéré est réalisée par un spécialiste en ingénierie système ou un spécialiste en gestion des risques[8] OU a minima, un spécialiste en ingénierie système ou un spécialiste en gestion des risques est consulté pour l'identification du référentiel de cybersécurité du système considéré.	X	X	X	X
Le spécialiste en ingénierie système ou le spécialiste en gestion des risques sollicité pour l'identification du référentiel de cybersécurité du système considéré est indépendant de l'équipe projet.				X
…				

[EX-1.03] Réaliser l'appréciation des risques de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Activité : Identifier les événements redoutés de cybersécurité				
Les événements redoutés de cybersécurité sont identifiés sur la base des fonctions de rang 1 et 2 de la décomposition fonctionnelle. (Voir Annexe I – Liste des fonctions d'un STRA)	X	X	X	X
Les événements redoutés de cybersécurité sont identifiés sur la base des fonctions de rang 3 de la décomposition fonctionnelle. (Voir Annexe I – Liste des fonctions d'un STRA)			X	X
Les événements redoutés de cybersécurité sont identifiés sur la base des fonctions de rang 4 de la décomposition fonctionnelle. (Voir Annexe I – Liste des fonctions d'un STRA)				X
…				

[8] Les compétences de cybersécurité sont détaillées dans l'annexe L – Nomenclature des compétences de cybersécurité.

[EX-1.03] Réaliser l'appréciation des risques de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Activité : Identifier et estimer les scénarios de conséquence				
Les scénarios de conséquence sont identifiés avec l'aide d'un spécialiste en sûreté de fonctionnement et en sécurité fonctionnelle.		X	X	X
Les scénarios de conséquence sont identifiés en cohérence avec la démonstration de sécurité de la partie sûreté de fonctionnement et sécurité fonctionnelle.	X	X	X	X
…				
Activité : Identifier et caractériser les sources de menace				
L'identification des sources de menaces est réalisée sur la base d'un rapport d'état de la menace en vigueur établi par un organisme reconnu de type CSIRT, non ciblé sur un secteur.		X	X	X
L'identification des sources de menaces est réalisée sur la base d'un rapport d'état de la menace en vigueur établi par un organisme reconnu de type CSIRT sur le secteur des transports publics ou concernant des systèmes à enjeux de sécurité équivalents.			X	X
L'identification des sources de menaces est réalisée en collaboration avec un spécialiste en analyse de la menace.			X	X
…				
Activité : Identifier les vulnérabilités				
L'identification des vulnérabilités est réalisée par un architecte cybersécurité et un expert cybersécurité réseaux et systèmes d'exploitation.			X	X
…				
Activité : Identifier les modes d'attaque				
…				
Activité : Identifier et estimer les scénarios de menace				
Les parties prenantes dans la zone pour laquelle le niveau de menace est considéré comme faible et acceptable en l'état sont prises en compte pour l'identification des scénarios de menace.				X
Les parties prenantes dans la zone pour laquelle le niveau de menace est considéré comme tolérable sous contrôle sont prises en compte pour l'identification des scénarios de menace.			X	X
Les parties prenantes dans la zone pour laquelle le niveau de menace est considéré comme très élevé et difficilement acceptable sont prises en compte pour l'identification des scénarios de menace.	X	X	X	X
La vraisemblance du risque de cybersécurité est cotée à l'aide d'un algorithme qui est défini et qui détermine la vraisemblance à chaque état intermédiaire des scénarios de menace possibles. (Voir Annexe G – Outils d'élaboration des scénarios de menaces)				X
…				

[EX-1.03] Réaliser l'appréciation des risques de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Activité : Identifier et estimer les risques de cybersécurité				
L'identification et l'estimation des risques de cybersécurité est réalisée par un spécialiste en gestion des risques de cybersécurité indépendant du projet.			X	X
…				
Activité : Evaluer les risques de cybersécurité				
…				
Ensemble du processus (toutes les activités)				
L'appréciation des risques de cybersécurité est réalisée en collaboration avec un prestataire qualifié.				X
L'appréciation des risques du système considéré est réalisée par un spécialiste en gestion des risques et en conformité OU a minima, un spécialiste en gestion des risques et en conformité est consulté pour l'appréciation des risques du système considéré.	X	X	X	X
Le spécialiste en gestion des risques et en conformité sollicité pour l'appréciation des risques du système considéré est indépendant de l'équipe projet.				X
…				

[EX-1.04] Elaborer un plan de traitement des risques de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Le plan de traitement des risques de cybersécurité est élaboré par un spécialiste en gestion des risques et en conformité OU a minima, un spécialiste en gestion des risques et en conformité est consulté pour l'élaboration du plan de traitement des risques de cybersécurité.	X	X	X	X
Le spécialiste en gestion des risques et en conformité sollicité pour l'élaboration du plan de traitement des risques de cybersécurité est indépendant de l'équipe projet.				X
…				

[EX-1.05] Définir les objectifs de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Les objectifs de cybersécurité sont formulés de la manière suivante : • En spécifiant le ou les élément(s) du système considéré visé(s) par l'objectif ; • Sous formes de souhait avec des verbes au conditionnel ; • En détaillant le but derrière l'objectif.			X	X

[EX-1.05] Définir les objectifs de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Chaque objectif de cybersécurité fait l'objet d'une justification qui doit permettre de tracer les risques de cybersécurité auxquels cet objectif répond, les politiques organisationnelles de cybersécurité mises en œuvre par cet objectif de cybersécurité, et les hypothèses soutenues par cet objectif de cybersécurité.	X	X	X	X
La justification des objectifs de cybersécurité doit démontrer que l'ensemble des objectifs de cybersécurité respectent toutes les politiques organisationnelles de cybersécurité.			X	X
La justification des objectifs de cybersécurité doit démontrer que l'ensemble des objectifs de cybersécurité tiennent compte de toutes les hypothèses et de toutes les contraintes.			X	X
La justification des objectifs de cybersécurité de cybersécurité doit inclure un argumentaire permettant de démontrer la pertinence et la cohérence des objectifs de cybersécurité avec les risques de cybersécurité.				X
La définition des objectifs du système considéré est réalisée par un spécialiste en gestion des risques et en conformité OU a minima, un spécialiste en gestion des risques et en conformité est consulté pour la définition des objectifs du système considéré.	X	X	X	X
Le spécialiste en gestion des risques et en conformité sollicité pour la définition des objectifs du système considéré est indépendant de l'équipe projet.				X
…				

[EX-1.06] Décliner les objectifs de cybersécurité du système considéré en exigences fonctionnelles de cybersécurité				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Les exigences fonctionnelles de cybersécurité sont formulées avec : • Une précondition optionnelle qui indique les circonstances ou le contexte requis pour que l'exigence prenne sens ; • Un stimulus définissant l'action qui amène le système de sécurité à déclencher une réponse visible (mesurable) ; • Une réponse définissant le comportement de la mise en œuvre de l'exigence fonctionnelle à la réception du stimulus défini.			X	X
Tous les termes utilisés pour la définition des exigences fonctionnelles de cybersécurité doivent être définis.		X	X	X
Chaque exigence fonctionnelle de cybersécurité fait l'objet d'une justification qui doit permettre de tracer le ou les objectif(s) de cybersécurité qu'elle décline.	X	X	X	X
Dans la justification des exigences fonctionnelles de cybersécurité, les liens de filiation entre les objectifs de cybersécurité et les exigences fonctionnelles sont représentés avec des outils graphiques.				X
La justification des exigences fonctionnelles de cybersécurité doit démontrer qu'elles couvrent l'ensemble des objectifs de cybersécurité du système considéré.	X	X	X	X
La justification des exigences fonctionnelles de cybersécurité doit inclure un argumentaire permettant de démontrer la pertinence et la cohérence des exigences fonctionnelles de cybersécurité avec les objectifs de cybersécurité.				X
Chaque dépendance des exigences fonctionnelles de cybersécurité entre elles doit être satisfaite, ou la justification des exigences fonctionnelles de cybersécurité doit expliquer pourquoi la dépendance n'est pas satisfaite.			X	X
La justification des exigences fonctionnelles de cybersécurité doit démontrer qu'elles mettent en œuvre toutes les politiques organisationnelles de cybersécurité.				X
La déclinaison des objectifs de cybersécurité en exigences fonctionnelles de cybersécurité est réalisée par un spécialiste en gestion des risques et en ingénierie système OU a	X	X	X	X

[EX-1.06] Décliner les objectifs de cybersécurité du système considéré en exigences fonctionnelles de cybersécurité				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
minima, un spécialiste en gestion des risques et en ingénierie système est consulté pour la déclinaison des objectifs de cybersécurité en exigences fonctionnelles de cybersécurité.				
Les spécialistes en gestion des risques et en ingénierie système sollicités pour la déclinaison des objectifs de cybersécurité en exigences fonctionnelles sont indépendants de l'équipe projet.				X
…				

[EX-1.07] Spécifier l'architecture fonctionnelle de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Chaque sous-système, élément et interface identifiés lors de la modélisation du système et de son écosystème (EX-1.01) en lien avec un ou plusieurs risque(s) de cybersécurité doit se voir attribuer une ou plusieurs exigence(s) fonctionnelle(s) de cybersécurité.	X	X	X	X
La spécification de l'architecture fonctionnelle de cybersécurité du système considéré est réalisée par un spécialiste en gestion des risques et en ingénierie système OU a minima, un spécialiste en gestion des risques et en ingénierie système est consulté pour la spécification de l'architecture fonctionnelle de cybersécurité.	X	X	X	X
Les spécialistes en gestion des risques et en ingénierie système sollicités pour la spécification de l'architecture fonctionnelle de cybersécurité du système considéré sont indépendants de l'équipe projet.				X
…				

[EX-1.08] Spécifier les mesures de cybersécurité applicables au système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Les mesures de cybersécurité doivent être formulées de manière : • Non ambigüe et compréhensible dans la syntaxe et la sémantique utilisée ; • A être modulable et englobante ; • A prendre en compte la complexité du système ; • A soutenir l'utilisation de techniques de conception et de mise en œuvre sûres ; • A avoir la capacité d'intégrer des composants déjà existants ; • A apporter une résilience du langage contre les vulnérabilités liées à une mauvaise utilisation.	X	X	X	X
La spécification fonctionnelle est rédigée par un spécialiste en gestion des risques, un spécialiste en gouvernance et un spécialiste en compétences techniques de cybersécurité OU a minima, un spécialiste en gestion des risques, un spécialiste en gouvernance et un spécialiste en compétences techniques de cybersécurité sont consultés pour la rédaction de la spécification fonctionnelle.	X	X	X	X
Le spécialiste en gestion des risques, le spécialiste en gouvernance et le spécialiste en compétences techniques de cybersécurité sollicités pour la spécification des mesures de cybersécurité sur le système considéré sont indépendants de l'équipe projet.				X
…				

[EX-1.08] Spécifier les mesures de cybersécurité applicables au système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Spécification fonctionnelle basique				
Pour chaque mesure de cybersécurité sur le système considéré : • • une spécification fonctionnelle et la correspondance aux exigences fonctionnelles de cybersécurité auxquelles elle répond doivent être fournies. • • Les éléments liés à la mesure de cybersécurité et les interfaces de cybersécurité correspondantes doivent être identifiés et leur contribution à la cybersécurité doit être catégorisée (« mettant en œuvre », « supportant », ou « sans interférence »)[9].	X	X	X	X
Pour chaque interface de mise en œuvre de la cybersécurité et chaque interface supportant la cybersécurité, la spécification fonctionnelle doit : • • Décrire l'objectif et la méthode d'utilisation[10] • • Identifier tous les paramètres associés.	X	X	X	X
Pour chaque interface sans interférence avec la cybersécurité, la spécification fonctionnelle doit intégrer une justification de cette catégorisation.	X	X	X	X
…				
Spécification fonctionnelle avancée				
La spécification fonctionnelle doit représenter complètement la mesure de cybersécurité.		X	X	X
La spécification fonctionnelle doit identifier et décrire tous les paramètres associés à chaque interface de cybersécurité.		X	X	X
Pour chaque interface de mise en œuvre de la cybersécurité, la spécification fonctionnelle doit décrire : • Les actions qui mettent en œuvre la cybersécurité • Les messages d'erreur directe résultant du traitement associé à ces actions		X	X	X
…				
Spécification fonctionnelle complète				
Pour chaque interface de mise en œuvre de la cybersécurité, la spécification fonctionnelle doit décrire : • les messages d'erreur directe qui résultent des actions qui mettent en œuvre la cybersécurité • les exceptions associées à l'invocation de cette interface			X	X
La spécification fonctionnelle doit résumer les actions supportant la cybersécurité et les actions sans interférence avec la cybersécurité associée à chaque interface de cybersécurité afin de justifier qu'elles ne mettent pas en œuvre la cybersécurité.			X	X
…				

[9] La notion de « contribution à la cybersécurité » et les différentes catégories associées sont précisées à la fin de la présente annexe

[10] La terminologie utilisée pour la spécification des interfaces de cybersécurité est explicitée à la fin de la présente annexe

[EX-1.08] Spécifier les mesures de cybersécurité applicables au système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Spécification fonctionnelle semi-formelle complète				
La spécification fonctionnelle doit décrire les interfaces de cybersécurité en utilisant un style semi-formel.				X
Pour chaque interface de cybersécurité, la spécification fonctionnelle doit décrire toutes les actions associées ainsi que tous les messages d'erreur directe qui pourrait résulter de l'invocation de cette interface.				X
Pour chaque mesure de cybersécurité sur le système considéré, la spécification fonctionnelle doit décrire tous les messages d'erreur indirectes et restantes.				X
La spécification fonctionnelle doit intégrer une justification pour chaque message d'erreur contenue dans l'implémentation de la mesure de cybersécurité mais qui ne résulte pas d'une invocation d'une interface de cybersécurité.				X
La spécification fonctionnelle doit être rédigée sous la responsabilité d'un gestionnaire des exigences.				X
…				

[EX-1.09] Spécifier l'architecture technique de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
L'architecture technique de cybersécurité est spécifiée par un spécialiste en gestion des risques, un spécialiste en gouvernance et un spécialiste en compétences techniques de cybersécurité OU a minima, un spécialiste en gestion des risques, un spécialiste en gouvernance et un spécialiste en compétences techniques de cybersécurité sont consultés pour la spécification de l'architecture technique de cybersécurité.	X	X	X	X
Le spécialiste en gestion des risques, le spécialiste en gouvernance et le spécialiste en compétences techniques de cybersécurité sollicités pour la spécification de l'architecture technique de cybersécurité sur le système considéré sont indépendants de l'équipe projet.				X
Une justification montrant la correspondance entre l'architecture de cybersécurité et les exigences d'architecture doit être fournie.	X	X	X	X
La justification doit inclure un argumentaire permettant de démontrer la pertinence et la cohérence de l'architecture technique de cybersécurité avec les exigences d'architecture auxquelles elles répondent.			X	X
Les spécifications de l'architecture technique de cybersécurité portent sur les sous-systèmes, éléments et interfaces de mise en œuvre de la cybersécurité.	X	X	X	X
Les spécifications de l'architecture technique de cybersécurité portent sur les sous-systèmes, éléments et interfaces supportant la cybersécurité.			X	X
Les spécifications de l'architecture technique de cybersécurité portent sur les sous-systèmes, éléments et interfaces sans interférence avec la cybersécurité.				X
Les caractéristiques techniques de l'architecture technique de cybersécurité doivent être décrites		X	X	X
…				

Exemples d'exigences de NICS : phase de développement

[EX-2.01] Mettre à jour la modélisation du système considéré et de son écosystème				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Fournisseurs/sous-traitants : la modélisation de l'écosystème inclut les parties prenantes de rang 1.	X	X	X	X
Fournisseurs/sous-traitants : la modélisation de l'écosystème inclut les parties prenantes de rang 2.			X	X
La mise à jour de la modélisation du système considéré et de l'écosystème est réalisée par un spécialiste en ingénierie système ou un spécialiste en gestion des risques OU a minima, un spécialiste en ingénierie système ou un spécialiste en gestion des risques est consulté pour la modélisation.	X	X	X	X
Le spécialiste en ingénierie système ou le spécialiste en gestion des risques sollicité pour la mise à jour du système considéré et de l'écosystème est indépendant de l'équipe projet.				X
…				
Modélisation basique				
Une modélisation qui décrit le système considéré en termes de sous-systèmes doit être fournie. Cette modélisation doit identifier tous les sous-systèmes liés à des mesures de cybersécurité et les catégoriser (« mettant en œuvre », « supportant », ou « sans interférence »).	X	X	X	X
Une correspondance entre les interfaces de cybersécurité et le plus bas niveau de décomposition disponible pour la modélisation du système considéré doit être fournie.	X	X	X	X
La modélisation doit décrire le comportement de cybersécurité de chaque sous-système lié à des mesures de cybersécurité.	X	X	X	X
Pour chaque sous-système de mise en œuvre de la cybersécurité, la modélisation doit intégrer une description des interactions entre eux, et de leurs interactions avec les autres sous-systèmes liés à des mesures de cybersécurité.	X	X	X	X
…				
Modélisation de l'architecture				
Pour chaque sous-système lié à des mesures de cybersécurité, la modélisation doit intégrer une description des interactions entre eux.		X	X	X
…				
Modélisation modulaire basique				
La modélisation doit décrire le système considéré en termes de modules[11]. Ces modules doivent être catégorisés (« mettant en œuvre », « supportant », ou « sans interférence »).			X	X
La modélisation doit intégrer la correspondance entre les sous-systèmes liés à des mesures de cybersécurité et les modules.			X	X

[11] Une approche de la description sous forme de module est présentée en annexe B

[EX-2.01] Mettre à jour la modélisation du système considéré et de son écosystème				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
La modélisation doit décrire chaque module de mise en œuvre de la cybersécurité en termes : • D'objectifs et d'interactions avec les autres modules ; • D'interfaces de cybersécurité, en identifiant celles qui sont appelées par les autres modules de mise en œuvre de la cybersécurité ; • De valeurs retournées par ces interfaces.			X	X
La modélisation doit décrire chaque module supportant la cybersécurité et chaque module sans interférence avec la cybersécurité en termes d'objectifs et d'interactions avec les autres modules			X	X
…				
Modélisation modulaire semi-formelle				
La modélisation doit intégrer une description semi-formelle de chaque sous-système lié à des mesures de cybersécurité, complétée par un texte informel et explicatif si approprié.				X
La modélisation doit décrire chaque module supportant la cybersécurité en termes : • D'objectifs et d'interactions avec les autres modules ; • D'interfaces de cybersécurité, en identifiant celles qui sont appelées par les autres modules de mise en œuvre de la cybersécurité ; • De valeurs retournées par ces interfaces.				X
La modélisation fonctionnelle et technique est réalisée à l'aide d'un logiciel spécifique (logiciel de modélisation du système d'informations ou logiciel d'architecture d'entreprise) permettant de : • Constituer l'inventaire ; • Réaliser les vues et représenter les liens entre elles ; • Mettre en œuvre et contrôler le processus de maintien à jour de la cartographie.				X
…				

[EX-2.02] Mettre à jour l'appréciation des risques de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Voir les exigences de NICS de l'[EX-1.03] en cas de mise à jour.	X	X	X	X
…				

[EX-2.03] Mettre à jour le plan de traitement des risques de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Voir les exigences de NICS de l'[EX-1.04] en cas de mise à jour	X	X	X	X
…				

[EX-2.04] Mettre à jour les exigences fonctionnelles de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Voir les exigences de NICS de l'[EX-1.06] en cas de mise à jour	X	X	X	X
…				

[EX-2.05] Mettre à jour l'architecture fonctionnelle de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Voir les exigences de NICS de l'[EX-1.07] en cas de mise à jour	X	X	X	X
…				

[EX-2.06] Mettre à jour les mesures de cybersécurité applicables au système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Voir les exigences de NICS de l'[EX-1.08] en cas de mise à jour	X	X	X	X
La documentation sur la cybersécurité du développement doit être produite et fournie.	X	X	X	X
La documentation sur la cybersécurité du développement doit décrire toutes les mesures de cybersécurité (physiques, logiques, procéduraux, personnels et autres) qui sont nécessaires pour protéger la confidentialité et l'intégrité de la conception et de l'implémentation de l'architecture de cybersécurité du système considéré dans son environnement de développement.	X	X	X	X
La documentation sur la cybersécurité du développement doit justifier que les mesures de cybersécurité fournissent le niveau de protection nécessaire pour maintenir la confidentialité et l'intégrité de l'architecture de cybersécurité du système considéré.	X	X	X	X
…				

[EX-2.07] Mettre à jour l'architecture technique de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Voir les exigences de NICS de l'[EX-1.09] en cas de mise à jour	X	X	X	X
…				

[EX-2.08] Mener à bien le développement du système considéré conformément aux spécifications de cybersécurité				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Le système considéré doit être testable.	X	X	X	X
Les mesures de cybersécurité doivent être développées en vue d'obtenir, de la testabilité et une capacité de modification sans dégrader la cybersécurité.	X	X	X	X
Pour chaque élément identifié dans l'architecture, un affinement supplémentaire des spécifications doit être basé sur la partition en modules. La conception de chaque module et la vérification à réaliser sur chaque module doivent être spécifiées.			X	X
La représentation du développement (code source, document qualité, consignes d'exploitation/maintenance…) doit être rendue disponible à des fins d'évaluation pour l'ensemble des mesures de cybersécurité.	X	X	X	X
La correspondance entre les spécifications de cybersécurité (spécifications des mesures de cybersécurité et de l'architecture de cybersécurité) et la représentation du développement doit être démontrée.			X	X
Le niveau de détail utilisé pour la représentation du développement est tel qu'aucune décision complémentaire de conception n'est nécessaire pour le développement du système considéré.	X	X	X	X
Le développement du système considéré conformément aux spécifications de cybersécurité est réalisé par un spécialiste en compétences techniques de cybersécurité, OU a minima, un spécialiste en compétences techniques de cybersécurité est consulté pour la réalisation du développement du système considéré conformément aux spécifications de cybersécurité.	X	X	X	X
Le spécialiste en compétences techniques de cybersécurité consulté pour la réalisation du développement du système considéré est indépendant de l'équipe projet.				X
…				

[EX-2.09] Appliquer le plan de contrôle de la cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Une justification de la couverture de tests doit être fournie. Elle doit montrer la correspondance entre les tests prévus dans la documentation de tests et les interfaces de cybersécurité identifiées dans les spécifications fonctionnelles des mesures de cybersécurité.	X	X	X	X
Une analyse de la couverture de tests doit démontrer que toutes les interfaces de cybersécurité ont été complètement testées.			X	X
L'analyse de la profondeur des tests doit démontrer : • La correspondance entre les tests prévus dans la documentation de test et les sous-systèmes liés à des mesures de cybersécurité • Que tous les sous-systèmes liés à des mesures de cybersécurité ont été testés.		X	X	X
L'analyse de la profondeur des tests doit démontrer : • La correspondance entre les tests prévus dans la documentation de test, les sous-systèmes liés à des mesures de sécurité et les modules de mise en œuvre de la cybersécurité. • Que les modules de mise en œuvre de la cybersécurité ont été testés.			X	X
L'analyse de la profondeur des tests doit démontrer : • La correspondance entre les tests prévus dans la documentation de test, les sous-systèmes liés à des mesures de cybersécurité, et les modules du système considéré. • Que tous les modules du système considéré ont été testés.				X

[EX-2.09] Appliquer le plan de contrôle de la cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Le plan de contrôle de la cybersécurité est mis en œuvre sous la responsabilité d'un spécialiste en pilotage ou gestion de projet ainsi que par un spécialiste en compétences techniques de cybersécurité OU a minima, un spécialiste en pilotage ou gestion de projet et un spécialiste en compétences techniques de cybersécurité sont consultés pour la mise en œuvre du plan.	X	X	X	X
Le spécialiste en pilotage ou gestion de projet et le spécialiste en compétences techniques de cybersécurité consultés pour la mise en œuvre du plan de contrôle de la cybersécurité sont indépendants de l'équipe projet.				X
…				

Exemples d'exigences de NICS : phase de fabrication / intégration / installation

[EX-3.01] Mettre à jour la modélisation du système considéré et de son écosystème				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Voir les exigences de NICS de l'[EX-2.01] en cas de mise à jour	X	X	X	X
…				

[EX-3.02] Mettre à jour l'appréciation des risques de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Voir les exigences de NICS de l'[EX-1.03] en cas de mise à jour	X	X	X	X
…				

[EX-3.03] Mettre à jour le plan de traitement des risques de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Voir les exigences de NICS de l'[EX-1.04] en cas de mise à jour	X	X	X	X
…				

[EX-3.04] Mettre à jour les exigences fonctionnelles de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Voir les exigences de NICS de l'[EX-1.06] en cas de mise à jour	X	X	X	X
…				

[EX-3.05] Mettre à jour l'architecture fonctionnelle de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Voir les exigences de NICS de l'[EX-1.07] en cas de mise à jour	X	X	X	X
…				

[EX-3.06] Mettre à jour les mesures de cybersécurité applicables au système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Voir les exigences de NICS de l'[EX-1.08] en cas de mise à jour	X	X	X	X
…				

[EX-3.07] Mettre à jour l'architecture technique de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Voir les exigences de NICS de l'[EX-1.09] en cas de mise à jour	X	X	X	X
…				

[EX-3.08] Mener à bien la phase de fabrication / intégration / installation conformément aux spécifications de cybersécurité				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Composants du système considéré				
Les composants liés à des mesures de cybersécurité doivent être testables.	X	X	X	X
Le système considéré intégré et assemblé doit être testable et livrable à des fins de test.	X	X	X	X
Une liste des composants du système considéré doit être fournie, avec une information sur le fournisseur le cas échéant.	X	X	X	X
Pour chaque composant lié à des mesures de cybersécurité, une information sur le développement doit être fournie. Celle-ci doit décrire l'objectif de chaque interface de ce composant utilisée dans le système considéré. Elle doit également montrer la correspondance entre ces interfaces et le système considéré dans la mise en œuvre des mesures de cybersécurité.	X	X	X	X
L'information sur le développement doit inclure un haut niveau de description du comportement du composant qui supporte la mise en œuvre des exigences de cybersécurité du système considéré.			X	X
L'information sur le développement doit identifier les sous-systèmes du composant qui fournissent des interfaces utilisées dans le système considéré, et doit inclure un mapping entre ces interfaces et les sous-systèmes de ce composant.				X

[EX-3.08] Mener à bien la phase de fabrication / intégration / installation conformément aux spécifications de cybersécurité				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Une information sur la confiance à accorder aux composants doit être fournie pour le système considéré. Pour chaque composant intégré au système considéré et lié à des mesures de cybersécurité, elle doit décrire : • Les fonctionnalités du matériel, du logiciel et/ou du programme sur lequel s'appuient les mesures de cybersécurité liées • Toutes les interactions à travers lesquelles les mesures de cybersécurité requièrent des services auprès du composant • Comment les mesures de cybersécurité se protègent elles-mêmes contre la corruption du composant et les interférences créées par le composant		X	X	X
L'information sur la confiance à accorder aux composants doit décrire chaque interaction en termes d'interface utilisée et de valeurs retournées par ces interfaces				X
La documentation de test d'intégration des composants liés à des mesures de cybersécurité doit être fournie.	X	X	X	X
La documentation de test d'interfaces des composants liés à des mesures de cybersécurité doit être fournie.	X	X	X	X
Un ensemble de ressources équivalent à celles qui ont été utilisées lors des tests fonctionnels des composants liés à des mesures de cybersécurité doit être fourni.	X	X	X	X
Un ensemble de tests d'intégration entre les éléments composites du système considéré, en rapport avec les spécifications de cybersécurité, doit être réalisé.	X	X	X	X
…				
Gestion de la configuration du système considéré				
La documentation liée à la gestion de la configuration du système considéré doit être fournie.	X	X	X	X
Un système de gestion des configurations doit être défini et mis en œuvre.	X	X	X	X
La documentation sur la gestion des configurations du système doit décrire la méthode utilisée pour identifier de manière unique les éléments du système servant à le configurer. Le système de gestion des configurations doit identifier de manière unique les éléments du système servant à le configurer.	X	X	X	X
Le système de gestion des configurations doit fournir des moyens de contrôle de telle sorte que seuls les changements autorisés sont mis en œuvre sur les éléments du système servant à le configurer.	X	X	X	X
Le système de gestion des configurations doit fournir des moyens de contrôle automatique de telle sorte que seuls les changements autorisés sont mis en œuvre sur les éléments du système servant à le configurer.			X	X
La documentation sur la gestion des configurations doit inclure un plan. Ce plan doit décrire comment le système de gestion des configurations doit être utilisé pour développer le système considéré.	X	X	X	X
Les preuves apportées doivent démontrer que tous les éléments de configuration sont maintenus dans le cadre du système de gestion des configurations. Les preuves apportées doivent démontrer que le système de gestion des configurations est appliqué conformément au plan de gestion des configurations.	X	X	X	X
Le système de gestion des configurations doit permettre la configuration des éléments du système considéré de manière automatique.			X	X
Le plan de gestion des configurations doit décrire les procédures utilisées pour accepter les éléments nouveaux ou modifiés du système considéré servant à le configurer			X	X
…				

[EX-3.09] Appliquer le plan de contrôle de la cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Le plan de contrôle de la cybersécurité est mis en œuvre sous la responsabilité d'un spécialiste en pilotage ou gestion de projet ainsi que par un spécialiste en compétences techniques de cybersécurité OU a minima, un spécialiste en pilotage ou gestion de projet et un spécialiste en compétences techniques de cybersécurité sont consultés pour la mise en œuvre du plan.	X	X	X	X
Le spécialiste en pilotage ou gestion de projet et le spécialiste en compétences techniques de cybersécurité consultés pour la mise en œuvre du plan de contrôle de la cybersécurité sont indépendants de l'équipe projet.				X
Tests fonctionnels des mesures de cybersécurité				
Les mesures de cybersécurité et l'architecture de cybersécurité doivent être fonctionnellement testées selon les spécifications de cybersécurité et les résultats doivent être documentés. La documentation de test doit être fournie. Elle doit comprendre les plans de test, les résultats attendus et les résultats réellement obtenus.	X	X	X	X
Les plans de tests doivent identifier les tests fonctionnels à effectuer et décrire les scénarios d'exécution de chaque test. Ces scénarios doivent inclure toute dépendance d'ordonnancement par rapport aux résultats d'autres tests.	X	X	X	X
Les résultats attendus des tests fonctionnels doivent indiquer les résultats attendus d'une exécution réussie des tests fonctionnels.	X	X	X	X
Les résultats réels des tests fonctionnels doivent être conformes aux résultats de tests attendus.	X	X	X	X
La documentation de tests fonctionnels doit comprendre une analyse des dépendances relatives à l'ordonnancement des procédures de test.			X	X
Un évaluateur premier regard doit effectuer des tests fonctionnels sur la mesure de cybersécurité pour confirmer qu'elle peut être mise en œuvre conformément à ses spécifications.	X	X	X	X
Un ensemble de ressources équivalent à celles qui ont été utilisées lors des tests fonctionnels de la mesure doit être utilisé pour l'évaluation premier regard.			X	X
Un échantillon de tests fonctionnels de la documentation de test doit être exécuté par un évaluateur premier regard pour vérifier les résultats de tests réalisés lors du développement.			X	X
L'évaluateur premier regard ne doit pas avoir participé au développement.		X	X	X
L'évaluateur premier regard doit être indépendant de l'équipe projet.			X	X
…				
Tests d'intégration et d'interfaces des composants liés à des mesures de cybersécurité				
La documentation de tests d'intégration et d'interfaces des composants liés à des mesures de cybersécurité doit comprendre les plans de test, les résultats attendus et les résultats réellement obtenus. Elle doit démontrer : • Que les mesures de cybersécurité sont développées conformément à leur spécification. • Que les interfaces des composants liés à des mesures de cybersécurité se comportent conformément à leur spécification	X	X	X	X
La documentation de tests d'intégration et d'interfaces des composants liés à des mesures de cybersécurité doit démontrer : • Que les mesures de cybersécurité sont complètes • Que les interfaces des composants liés à des mesures de cybersécurité sont complètes			X	X

[EX-3.09] Appliquer le plan de contrôle de la cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Un évaluateur premier regard doit effectuer des tests d'interface sur le système considéré intégré pour confirmer que les mesures de cybersécurité peuvent être mises en œuvre conformément à leurs spécifications.	X	X	X	X
Un échantillon de tests d'intégration et d'interfaces de la documentation de test doit être exécuté par un évaluateur premier regard pour vérifier les résultats de tests réalisés lors du développement.	X	X	X	X
L'évaluateur premier regard ne doit pas avoir participé au développement		X	X	X
L'évaluateur premier regard doit être indépendant de l'équipe projet			X	X
…				

Exemples d'exigences de NICS : phase de livraison

[EX-4.01] Valider la cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Une recherche dans les sources du domaine public doit être effectuée afin d'identifier les vulnérabilités potentielles du système considéré, incluant notamment celles liées à des produits informatiques spécifiques dont les éléments techniques du système considéré dépendent.	X	X	X	X
Une recherche dans les sources du domaine public doit être effectuée afin d'identifier les vulnérabilités potentielles découlant de l'utilisation de composants liés à des mesures de cybersécurité dans l'environnement opérationnel du système considéré intégré et assemblé.	X	X	X	X
Une analyse indépendante de vulnérabilités du système considéré doit être réalisée en utilisant la documentation technique, la spécification fonctionnelle, la conception du système considéré et la description de l'architecture technique de cybersécurité afin d'identifier les vulnérabilités potentielles du système considéré.	X	X	X	X
Une analyse indépendante de vulnérabilités du système considéré doit être réalisée en utilisant la représentation du développement afin d'identifier les vulnérabilités potentielles du système considéré.		X	X	X
Une analyse indépendante de vulnérabilités du système considéré assemblé et intégré doit être réalisée en utilisant les informations sur la confiance à accorder aux composants et la justification de l'assemblage afin d'identifier les vulnérabilités potentielles du système considéré intégré et assemblé.			X	X
Des tests de pénétration basés sur les vulnérabilités potentielles identifiées doivent être effectués sur le système considéré, pour déterminer que celui-ci est résistant aux attaques réalisées par un attaquant ayant un potentiel d'attaque équivalent au maximum des potentiels d'attaque du système considéré.	X	X	X	X
Une analyse permettant de déterminer que toutes les vulnérabilités résiduelles identifiées pour les composants liés à des mesures de cybersécurité ne sont pas exploitables dans le système considéré intégré et assemblé dans son environnement opérationnel doit être effectuée.		X	X	X
Les éléments techniques du système considéré préexistants doivent être inclus dans le processus de validation du système considéré.	X	X	X	X
Le processus de validation doit assurer : 1) Que les éléments préexistants du système considéré satisfont aux exigences allouées, 2) Que les défaillances sur les éléments préexistants sont détectées et le système considéré est protégé de ces défaillances, 3) Que les hypothèses relatives à l'environnement des éléments préexistants du système considéré sont respectées.			X	X

[EX-4.01] Valider la cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
La validation de la cybersécurité du système considéré est réalisée par un spécialiste en gouvernance, un spécialiste en conformité ainsi que par un spécialiste en compétences techniques de cybersécurité OU a minima, un spécialiste en gouvernance, un spécialiste en conformité et un spécialiste en compétences techniques de cybersécurité sont consultés pour la validation.	X	X	X	X
Le spécialiste en gouvernance, le spécialiste en conformité et le spécialiste en compétences techniques de cybersécurité consultés pour la validation de la cybersécurité du système considéré sont indépendants de l'équipe projet.				X
…				

[EX-4.02] Accepter le système considéré sur le domaine cybersécurité				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
L'acceptation de la cybersécurité du système considéré est réalisée par un spécialiste en gouvernance et par un spécialiste en compétences techniques de cybersécurité OU a minima, un spécialiste en gouvernance et un spécialiste en compétences techniques de cybersécurité sont consultés pour l'acceptation de la cybersécurité du système considéré.	X	X	X	X
Le spécialiste en gouvernance et le spécialiste en compétences techniques de cybersécurité consultés pour l'acceptation de la cybersécurité du système considéré sont indépendants de l'équipe projet.				X
Le rapport d'acceptation de la cybersécurité comprend une confirmation selon laquelle le système considéré est apte à la mise en service.		X	X	X
…				

[EX-4.03] Intégrer la cybersécurité dans les actions de transfert vers l'entité responsable				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
L'intégration de la cybersécurité dans les actions de transfert vers l'entité responsable est réalisée par un spécialiste en pilotage ou gestion de projet OU a minima, un spécialiste en pilotage ou gestion de projet est consulté pour l'intégration de la cybersécurité dans les actions de transfert vers l'entité responsable.	X	X	X	X
Le spécialiste en pilotage ou gestion de projet consultés pour l'intégration de la cybersécurité dans les actions de transfert vers l'entité responsable est indépendant de l'équipe projet.				X
…				

[EX-4.04] Intégrer la cybersécurité dans la période de Vérification de Service Régulier				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
L'intégration de la cybersécurité dans la période de Vérification de Service Régulier est réalisée par un spécialiste en pilotage ou gestion de projet OU a minima, un spécialiste en pilotage ou gestion de projet est consulté pour l'intégration de la cybersécurité dans la période de Vérification de Service Régulier.	X	X	X	X
Le spécialiste en pilotage ou gestion de projet consultés pour l'intégration de la cybersécurité dans la période de Vérification de Service Régulier est indépendant de l'équipe projet.				X
…				

Exemples d'exigences de NICS : phase d'exploitation / maintenance

[EX-5.01] Etablir le plan de maintien en conditions de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Le plan de maintien conditions de cybersécurité est élaboré par un spécialiste en gouvernance OU a minima, un spécialiste en gouvernance est consulté pour l'élaboration du plan.	X	X	X	X
Le spécialiste en gouvernance consulté pour l'élaboration du plan de maintien en conditions de cybersécurité est indépendant de l'équipe projet.				X
…				

[EX-5.02] Réaliser les opérations courantes concourant à la cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Les opérations courantes de cybersécurité sont réalisées par un spécialiste en système d'information OU a minima, un spécialiste en système d'information est consulté pour les opérations courantes de cybersécurité.	X	X	X	X
Le spécialiste en système d'information consulté pour les opérations courantes de cybersécurité est indépendant de l'équipe projet.				X
Les activités de gestion des configurations sont réalisées à l'aide d'un outil de gestion de parc informatique (CMDB)		X	X	X
Le workflow de gestion des habilitations d'accès est outillé		X	X	X
…				

[EX-5.03] S'assurer que les risques pesant sur le système considéré sont maintenus à un niveau acceptable lors des opérations de maintenance et à la suite de celles-ci				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Le maintien des risques à un niveau acceptable est assuré par un spécialiste en gestion des risques OU a minima, un spécialiste en gestion des risques est consulté pour le maintien des risques à un niveau acceptable.	X	X	X	X
Le spécialiste en gestion des risques consulté pour le maintien des risques à un niveau acceptable est indépendant de l'équipe projet.				X
…				

[EX-5.04] Assurer la compétence en matière de cybersécurité des personnels intervenants sur le système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Les attendus en matière de compétence, qualification et expérience dans le domaine de la cybersécurité des personnels intervenants sont identifiés	X	X	X	X
Les compétences, qualification et expérience des personnels intervenants sont cohérents avec les attendus en matière de compétences dans le domaine de la cybersécurité	X	X	X	X
La compétence du personnel, y compris les connaissances techniques, les qualifications, l'expérience adéquate et la formation appropriée, doit être documentée afin de démontrer une organisation de sécurité appropriée.		X	X	X
L'organisation doit maintenir les procédures de gestion des compétences du personnel à être apte aux rôles appropriés en conformité à des normes de qualité existantes.		X	X	X

[EX-5.04] Assurer la compétence en matière de cybersécurité des personnels intervenants sur le système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Un maintien et un développement continu des compétences doit être démontré pour chaque individu, par exemple par la tenue d'un journal de bord montrant que l'activité est effectuée correctement sur une base régulière et qu'une formation complémentaire est dispensée conformément à l'EN ISO 9001 et à 6.2.2 « Compétence, sensibilisation et formation ») de la CEI 90003:2004.			X	X
La compétence en cybersécurité des personnels intervenants est assurée par un spécialiste en gouvernance OU a minima, un spécialiste en gouvernance est consulté pour la compétence en cybersécurité des personnels intervenant.	X	X	X	X
Le spécialiste en gouvernance consulté pour la compétence en cybersécurité des personnels intervenant est indépendant de l'équipe projet.				X
Un audit interne exploitant est réalisé tous les ans.			X	X
Un audit interne exploitant est réalisé tous les semestres.				X
…				

[EX-5.05] Surveiller les performances de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
La surveillance des performances de cybersécurité est réalisée par un spécialiste en gouvernance, un spécialiste en architecture cybersécurité ainsi que par un analyste SOC OU a minima, un spécialiste en gouvernance, un spécialiste en architecture cybersécurité et un analyste SOC sont consultés pour la surveillance des performances de cybersécurité.	X	X	X	X
Le spécialiste en gouvernance, le spécialiste en architecture cybersécurité et l'analyste SOC consultés pour la surveillance des performances de cybersécurité sont indépendants de l'équipe projet.				X
La revue des indicateurs et des tableaux de bord permettant de mesurer des tendances et de détecter des signaux faibles est réalisée tous les ans.	X	X	X	X
La revue des indicateurs et des tableaux de bord permettant de mesurer des tendances et de détecter des signaux faibles est réalisée tous les trimestres.		X	X	X
La revue des indicateurs et des tableaux de bord permettant de mesurer des tendances et de détecter des signaux faibles est réalisée tous les mois.			X	X
La revue des indicateurs et des tableaux de bord permettant de mesurer des tendances et de détecter des signaux faibles est réalisée toutes les semaines.				X
La surveillance des incidents de sécurité doit se baser sur une stratégie d'analyse intégrant la liste des incidents redoutés de cybersécurité issus de l'analyse de risque		X	X	X
La surveillance des incidents de cybersécurité doit de baser sur une stratégie de collecte répondant aux attendus de la stratégie d'analyse		X	X	X
…				

[EX-5.06] Assurer la gestion des incidents de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
La gestion des incidents de cybersécurité est assurée par un spécialiste en gouvernance OU a minima, un spécialiste en gouvernance est consulté pour la gestion des incidents de cybersécurité.	X	X	X	X
Le spécialiste en gouvernance consulté pour la gestion des incidents de cybersécurité est indépendant de l'équipe projet.				X
…				

[EX-5.07] Assurer la gestion des crises de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
La gestion des crises de cybersécurité est assurée par un spécialiste en gouvernance OU a minima, un spécialiste en gouvernance est consulté pour l'élaboration du plan.	X	X	X	X
Le spécialiste en gouvernance consulté pour la gestion des crises de cybersécurité est indépendant de l'équipe projet.				X
…				

[EX-5.08] Assurer une veille continue sur les vulnérabilités et correctifs de ces vulnérabilités du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
La veille continue sur les vulnérabilités et correctifs de ces vulnérabilités est assurée par un spécialiste en système d'information OU a minima, un spécialiste en système d'information est consulté pour la veille continue sur les vulnérabilités et correctifs de ces vulnérabilités.	X	X	X	X
La veille vulnérabilités et correctifs est effectuée par un CERT			X	X
La qualification de l'applicabilité des vulnérabilités sur le système est réalisée sur la base de la CMDB du système			X	X
La qualification de la criticité intrinsèque des vulnérabilités doit être scorée et sourcée			X	X
La qualification de la criticité des vulnérabilités dans le contexte d'utilisation du système doit être évaluée et justifiée			X	X
…				

[EX-5.09] Assurer les mises à jour des éléments du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Les correctifs ou les solutions de contournement en cas de vulnérabilités de criticité importante dans le contexte d'utilisation du système doivent être identifiés et appliqués sans délais				X
Les correctifs ou les solutions de contournement en cas de vulnérabilités de criticité importante dans le contexte d'utilisation du système doivent être identifiés et appliqués en moins de 24 heures			X	X
Les correctifs ou les solutions de contournement en cas de vulnérabilités de criticité importante dans le contexte d'utilisation du système doivent être identifiés et appliqués en moins de 48 heures		X	X	X
Les correctifs ou les solutions de contournement en cas de vulnérabilités de criticité importante dans le contexte d'utilisation du système doivent être identifiés et appliqués en moins de 7 jours	X	X	X	X
…				

[EX-5.10] Assurer une veille continue sur les évolutions du système considéré et de son environnement				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
La veille continue sur les évolutions du système et de son environnement est élaborée par un spécialiste en système d'information OU a minima, un spécialiste en système d'information est consulté pour la veille continue sur les évolutions du système et de son environnement.	X	X	X	X
Le spécialiste en système d'information consulté pour la veille continue sur les évolutions du système et de son environnement est indépendant de l'équipe projet.				X
Les évolutions de l'environnement sont à revoir périodiquement tous les ans.	X	X	X	X
Les évolutions de l'environnement sont à revoir périodiquement tous les trimestres.		X	X	X
Les évolutions de l'environnement sont à revoir périodiquement tous les mois.			X	X
Les évolutions de l'environnement sont à revoir périodiquement toutes les semaines.				X
…				

[EX-5.11] Mettre à jour la modélisation du système considéré et de son écosystème				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Voir les exigences de NICS de l'[EX-2.01] en cas de mise à jour	X	X	X	X
…				

[EX-5.12] Réapprécier les risques de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Voir les exigences de NICS de l'[EX-1.03] en cas de mise à jour	X	X	X	X
…				

[EX-5.13] Mettre à jour le plan de traitement des risques de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Voir les exigences de NICS de l'[EX-1.04] en cas de mise à jour	X	X	X	X
…				

[EX-5.14] Mettre à jour les objectifs de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Voir les exigences de NICS de l'[EX-1.05] en cas de mise à jour	X	X	X	X
…				

[EX-5.15] Mettre à jour les exigences fonctionnelles de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Voir les exigences de NICS de l'[EX-1.06] en cas de mise à jour	X	X	X	X
…				

[EX-5.16] Mettre à jour l'architecture fonctionnelle de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Voir les exigences de NICS de l'[EX-1.07] en cas de mise à jour	X	X	X	X
…				

[EX-5.17] Mettre à jour les mesures de cybersécurité applicables au système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Voir les exigences de NICS de l'[EX-1.08] en cas de mise à jour	X	X	X	X
…				

[EX-5.18] Mettre à jour l'architecture technique de cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Voir les exigences de NICS de l'[EX-1.09] en cas de mise à jour	X	X	X	X
…				

Exemples d'exigences de NICS : phase de retrait du service

[EX-6.01] Appliquer le plan de contrôle de la cybersécurité du système considéré				
Détail exigence de NICS	**NICS 1**	**NICS 2**	**NICS 3**	**NICS 4**
Le plan de contrôle de la cybersécurité est élaboré par un spécialiste en pilotage ou gestion de projet OU a minima, un spécialiste en pilotage ou gestion de projet est consulté pour l'élaboration du plan.	X	X	X	X
Le spécialiste en pilotage ou gestion de projet consulté pour l'élaboration du plan de maintien en conditions de cybersécurité est indépendant de l'équipe projet.				X
…				

Précisions concernant les éléments liés à des mesures de cybersécurité du système considéré et leurs interfaces

Pour les besoins de l'exemple, on introduit la notion de contribution à la cybersécurité des éléments du système considéré liés à des mesures de cybersécurité et de leurs interfaces (appelées dans la suite « interfaces de cybersécurité »). Elle représente en quelque sorte leur degré d'implication dans la mise en œuvre des exigences fonctionnelles de cybersécurité. Trois degrés de contribution sont ainsi proposés, selon trois catégories :

- **Elément ou interface de « mise en œuvre de la cybersécurité »** : l'élément lié à une mesure de cybersécurité ou les services concernés par l'interface de cybersécurité jouent un rôle direct dans la mise en œuvre des exigences fonctionnelles de cybersécurité.
- **Elément ou interface « supportant la cybersécurité »** : l'élément lié à une mesure de cybersécurité ou les services concernés par l'interface de cybersécurité jouent un rôle de soutien aux exigences fonctionnelles de cybersécurité. Leur mauvais fonctionnement seul ne suffit pas à altérer significativement la cybersécurité du système.
- **Elément ou interface « sans interférence avec la cybersécurité »** : l'élément lié à une mesure de cybersécurité ou les services concernés par l'interface de cybersécurité ne jouent aucun rôle dans la mise en œuvre des exigences fonctionnelles de cybersécurité. Ils ne sont liés à des mesures de cybersécurité qu'en raison de leur environnement.

Cette catégorisation peut être extrapolée aux sous-systèmes du système considéré en lien avec des mesures de cybersécurité, ainsi qu'à leur comportement.

Exemples

Au niveau le plus haut de contribution à la cybersécurité se trouvent les éléments de « mise en œuvre de la cybersécurité ». Par exemple :

- Mesure de cybersécurité qui consiste à mettre en œuvre un mécanisme de contrôle d'accès discrétionnaire (DAC) : les quelques lignes de code qui effectuent effectivement la vérification des attributs d'un sujet par rapport aux attributs de l'objet sont une vision possible, à un niveau très fin, de l'élément de mise en œuvre de la cybersécurité. Une vision plus large pourrait inclure l'entité logicielle (par exemple, une fonction C) qui contient ces lignes de code. Une vision encore plus large pourrait inclure les appelants de la fonction C, puisqu'ils seraient responsables de l'application de la décision renvoyée par la vérification des attributs. Une vision encore plus large pourrait inclure tout code dans l'arbre d'appel (ou l'équivalent de programmation pour le langage de mise en œuvre utilisé) de cette fonction C, comme par exemple, une fonction de tri qui trie les entrées de la liste de contrôle d'accès dans une mise en œuvre de l'algorithme de première correspondance.
- Mesure de cybersécurité qui consiste à mettre en œuvre une consigne d'exploitation et de maintenance sur un composant du système : les quelques phrases qui décrivent la consigne sont une vision possible, à un niveau très fin, de l'élément de mise en œuvre de la cybersécurité. Une vision plus large pourrait inclure l'ensemble des consignes d'exploitation et de maintenance sur ce composant. Une vision encore plus large pourrait inclure le processus global dans lequel s'inscrivent ces consignes (par exemple le processus de maintien en conditions de cybersécurité). Une vision encore plus large pourrait inclure le système de gestion de la sécurité (SGS) du STRA.

En élargissant la vision, à un moment donné l'élément visualisé ne met plus vraiment en œuvre les exigences fonctionnelles de cybersécurité mais joue plutôt un rôle de soutien à celles-ci et rentre donc dans la catégorie des « éléments supportant la cybersécurité ». Cet élément peut être dépendant de l'élément de mise en œuvre de la cybersécurité, mais la dépendance se situe généralement à un niveau fonctionnel, par exemple :

- la gestion de la mémoire vive,
- la gestion de la mémoire tampon,
- la gestion des ressources humaines liées à la maintenance du système considéré…

En allant encore plus bas dans le niveau de contribution à la cybersécurité se trouvent les éléments **«** sans interférence avec la cybersécurité ». Par exemple :

- Tout code s'exécutant dans un mode matériel privilégié sur le système d'exploitation, comme par exemple un ensemble d'opérations mathématiques en virgule flottante traitées en mode

kernel pour des raisons de rapidité. Cet élément doit être considéré comme lié aux mesures de cybersécurité car, s'il est compromis (ou remplacé par un code malveillant), il peut compromettre le bon fonctionnement d'une exigence fonctionnelle de cybersécurité.

- La gestion des moyens logistiques et d'intervention des personnels d'exploitation et de maintenance du système considéré. Cet élément doit être considéré comme lié aux mesures de cybersécurité car, s'il est compromis ou saboté, il peut compromettre le bon fonctionnement d'une exigence fonctionnelle de cybersécurité.

Précisions concernant la spécification des interfaces de cybersécurité

Les interfaces de cybersécurité peuvent être spécifiées (à divers degrés de détail) en termes d'objectif, de méthode d'utilisation, de paramètres, de descriptions de paramètres et de messages d'erreur.

L'objectif d'une interface de cybersécurité est une description de haut niveau de l'objectif général de l'interface (par exemple, traiter les commandes de l'interface graphique, recevoir des paquets de réseau, fournir des sorties d'imprimante, etc.).

La méthode d'utilisation de l'interface de cybersécurité décrit comment celle-ci est censée être utilisée. Cette description doit s'articuler autour des différentes interactions disponibles au niveau de l'interface. Par exemple, si l'interface est un shell de commande Unix, ls, mv et cp seraient des interactions pour cette interface. Pour chaque interaction, la méthode d'utilisation décrit ce que fait l'interaction, tant pour le comportement observé au niveau de l'interface (par exemple, le programmeur qui appelle l'API, les utilisateurs de Windows qui modifient un paramètre dans le registre, etc.) que le comportement à d'autres interfaces (par exemple, la génération d'un enregistrement d'audit).

Les paramètres sont des entrées et des sorties explicites d'une interface de cybersécurité qui contrôlent le comportement de cette interface. Par exemple, les paramètres sont les arguments fournis à une API, les différents champs d'un paquet pour un protocole réseau donné, les valeurs des clés individuelles dans le registre Windows, les signaux à travers un ensemble de broches sur une puce, les drapeaux qui peuvent être définis pour le ls, etc. Les paramètres sont "identifiés" par une simple liste de ce qu'ils sont.

Une description de paramètre indique ce qu'est le paramètre de manière explicite. Par exemple, une description de paramètre acceptable pour l'interface foo(i) serait "le paramètre i est un nombre entier qui indique le nombre d'utilisateurs actuellement connectés au système". Une description telle que "le paramètre i est un entier" n'est pas acceptable.

La description des actions d'une interface de cybersécurité décrit ce que fait cette interface. Cette description est plus détaillée que celle de l'objectif en ce sens que, si l'objectif indique les raisons pour lesquelles on pourrait vouloir l'utiliser, les actions révèlent tout ce qu'elle fait. Ces actions peuvent être liées ou non aux exigences fonctionnelles de cybersécurité. Dans les cas où l'action de l'interface n'est pas liée aux exigences fonctionnelles de cybersécurité, sa description est dite « résumée », ce qui signifie que la description indique simplement qu'elle n'est pas liée aux exigences fonctionnelles de cybersécurité.

La description du message d'erreur identifie la condition qui l'a généré, la nature du message et la signification des codes d'erreur. Un message d'erreur est généré par un élément lié à une mesure de cybersécurité pour signifier qu'un problème ou une irrégularité d'un certain degré ont été rencontrés. Il y a différents types de messages d'erreur :

- Un message d'erreur "direct" est une réponse en rapport avec la cybersécurité par le biais d'une invocation spécifique d'une interface de cybersécurité.
- Une erreur "indirecte" ne peut pas être liée à une invocation spécifique d'une interface de cybersécurité car elle résulte de conditions générales (par exemple, épuisement des ressources, interruptions de connectivité, etc.). Les messages d'erreur qui ne sont pas en rapport avec la cybersécurité sont également considérés comme "indirects".
- Les erreurs "restantes" sont toutes les autres erreurs, telles que celles qui peuvent être référencées dans le code. Par exemple, l'utilisation d'un code de vérification des conditions qui ne devraient pas se produire logiquement (par exemple, un "else" final après une liste d'instructions "case"), permettrait de générer un message d'erreur fourre-tout ; dans un système considéré opérationnel, ces messages d'erreur ne devraient jamais être vus.

Annexe L : Nomenclature des compétences de cybersécurité

La présente annexe propose 14 fiches correspondant aux compétences attendues au titre de la mise en œuvre et / ou de l'évaluation des exigences applicables à la cybersécurité formulées dans le présent guide. Ces compétences sont structurées et référencées comme présenté dans l'infographie ci-après.

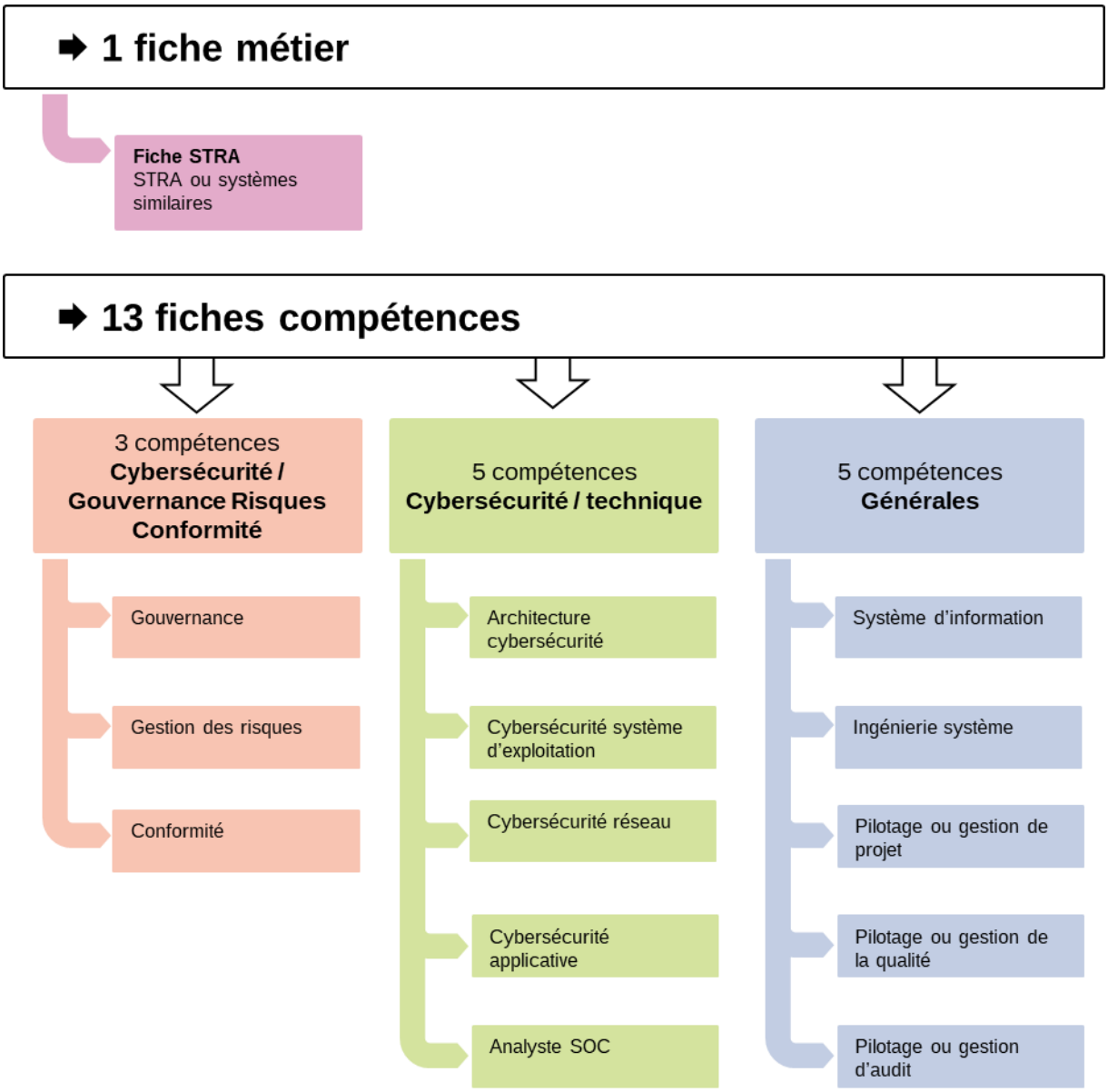


Figure 51 : Infographie des compétences de cybersécurité

Ces compétences sont utilisées dans la formulation d'exemples d'exigences de NICS (cf. Annexe K). Voici une description des différentes compétences identifiées :

Fiche métier

Fiche :	**STRA**
Description du champ de compétences	
Le champ de compétences couvre les domaines des STRA ou des systèmes similaires à enjeux de sécurité équivalents (acteurs, filière, état de l'art, etc.). Il couvre notamment le contexte réglementaire et les référentiels suivants : - Règlement ONU n°155 - Règlement ONU n°156 - Règlement UE 2022/1426 (UE ADS) - Règlement UE 2018/858 (réception des véhicules à moteur) - Décret n°2021-873 du 29 juin 2021 / Décret STRA - Décret n° 2017-440 du 30 mars 2017 / Décret STPG - Guides STRMTG dont : o Guide d'application relatif à la cybersécurité des STRA o Guides GAME o Guides missions de l'OQA	

Fiches compétences cybersécurité / Gouvernance Risques Conformité

Fiche :	**Gouvernance**
Description du champ de compétences	
Le champ de compétences couvre les domaines suivants : - Politique de cybersécurité - Principes de chaines de responsabilités en cybersécurité - Gestion des incidents liés à la cybersécurité - Gestion du plan de continuité de l'activité	

Fiche :	**Gestion des risques**
Description du champ de compétences	
Ce champ de compétence recouvre les domaines suivants : - Menaces et vulnérabilités - Méthodes et techniques d'appréciation et de réduction des risques Ce champ de compétence recouvre les domaines connexes suivants : - Organisation de la cybersécurité - Réglementations et normes - Outils de sécurité usuels (IDS/IPS, EDR/XDR, pare-feu et assimilé, scanners de vulnérabilité et assimilé, etc.)	

Fiche :	**Conformité**
Description du champ de compétences	
Le champ de compétences couvre les domaines suivants : - Normes relatives à la cybersécurité, aux audits et aux sujets connexes[12], dont ISO 27001, ISO 27002, ISO 27005, ISO 21434, IEC 62443 - Référentiels relatifs à la cybersécurité, aux audits et aux sujets connexes, dont Guide d'hygiène SSI, NIST SP-800-53, CIS Controls, SANS Critical Security Controls, ISF Standard of Good Practice for Information Security - Textes relatifs à la cybersécurité, aux audits et aux sujets connexes, dont : o Loi de Programmation Militaire (LPM) o Directive NIS o Directive UE 2022/2555 (NIS2) o Référentiel Général de Sécurité (RGS) o Instruction Interministérielle n°901 (II901) - Instruction Générale Interministérielle n°1300 (IGI 1300)	

Fiches compétences cybersécurité technique

Fiche :	**Architecture cybersécurité**
Description du champ de compétences	
Le champ de compétences couvre les domaines suivants : - Réseaux et protocoles (protocoles réseau et infrastructures, protocoles applicatifs courants et service d'infrastructure) et grands principes de sécurisation - Equipements de sécurité (pare-feu, bastion, dispositif de chiffrement, équipement de détection et prévention d'intrusion) - Architectures applicatives de type « n-tiers » et les grands principes de sécurisation des applications - Connaissance des propriétés de sécurité d'une architecture et de ses modules, ainsi que des exigences auxquelles ils répondent (notion de résilience / contribution au plan de traitement du risque) - Connaissances spécifiques des spécificités des systèmes d'information selon leur nature ainsi que les principes de sécurisation associés (ex. systèmes de virtualisation et les environnements cloud) - Le champ de compétences inclut la capacité à comprendre l'intégralité d'un rapport d'audit d'architecture (constats d'audit et recommandations).	

12 Les sujets connexes peuvent recouvrir dans cette compétence la conformité et la continuité.

Fiche :	**Cybersécurité systèmes d'exploitation**
Description du champ de compétences	
Le champ de compétences couvre les domaines suivants : - Architectures et systèmes Microsoft et grands principes de sécurisation - Systèmes UNIX/Linux et grands principes de sécurisation - Solution de virtualisation et grands principes de sécurisation - Le champ de compétences inclut la capacité à comprendre l'intégralité d'un rapport d'audit de configuration (constats d'audit et recommandations) sur des périmètres composés de systèmes d'exploitation.	

Fiche :	**Cybersécurité réseau**
Description du champ de compétences	
Le champ de compétences couvre les domaines suivants : - Protocoles réseau et infrastructures et grands principes de sécurisation - Protocoles applicatifs courants et services d'infrastructure et grands principes de sécurisation - Configuration/Sécurisation des équipements réseau du marché - Réseaux de télécommunication et grands principes de sécurisation - Technologie sans fil et grands principes de sécurisation - Le champ de compétences inclut la capacité à comprendre l'intégralité d'un rapport d'audit de configuration (constats d'audit et recommandations) sur des périmètres réseau.	

Fiche :	**Cybersécurité environnements et interfaces applicatives**
Description du champ de compétences	
Le champ de compétences couvre les domaines suivants : - Applications Web et grands principes de sécurisation - Applications mobiles et grands principes de sécurisation - Applications desktop et grands principes de sécurisation - Web Services / API et grands principes de sécurisation - Le champ de compétences inclut la capacité à comprendre l'intégralité d'un rapport de test d'intrusion (constats d'audit et recommandations).	

Fiche :	**Analyste SOC**
Description du champ de compétences	
Le champ de compétences couvre les domaines suivants : - Protocoles et architectures réseau - Analyse de journaux (systèmes ou applicatifs) - Analyse de flux réseaux - Vulnérabilités - Modes opératoires d'attaque et des codes malveillants	

Fiches compétences générales

Fiche :	**Système d'information**
Description du champ de compétences	
Le champ de compétences couvre les domaines suivants : - Gestion de l'exploitation et de l'administration du système d'information - Contrôle d'accès logique au système d'information - Maintien en conditions opérationnelles d'un système d'information - Maintien en conditions de sécurité d'un système d'information - Administration des outils d'exploitation du système d'information	

Fiche :	**Ingénierie système**
Description du champ de compétences	
Le champ de compétences couvre les domaines suivants : - Analyse des besoins - Analyse de systèmes - Formulation des exigences / Spécification des exigences - Conception de systèmes - Programmation - Ordonnancement / Planification / Coordination - Outils de modélisation utilisés en ingénierie système - Outils de simulation utilisés en ingénierie système - Outils de gestion de projet	

Fiche :	**Pilotage ou gestion de projet**
Description du champ de compétences	
Le champ de compétences couvre les domaines suivants : - Analyse des besoins - Planification - Gestion de budget - Gestion des délais - Gestion de risques projet - Coordination d'équipe - Gestion de la qualité - Reporting	

Fiche :	**Pilotage ou gestion de la qualité**
Description du champ de compétences	
Le champ de compétences couvre les domaines suivants : - Normes relatives à la qualité - Amélioration continue - Analyse de données - Résolution de problèmes - Audit qualité - Outils de gestion de la qualité (diagramme de Pareto, analyse des causes racines, cartographie de processus, etc.)	

Fiche :	**Pilotage ou gestion d'audit**
Description du champ de compétences	
Le champ de compétences couvre les domaines suivants : - Conduite d'entretien - Visite sur site - Analyse documentaire - Référentiels d'audit.	

Annexe M : Bibliographie

Références réglementaires

- articles R. 3151-1 à R. 3153-1 (STRA de personnes) et R. 3251-1 à R. 3253-1 (STRA de marchandises) du code des transports
- Règlement ONU n°155 — Prescriptions uniformes relatives à l'homologation des véhicules en ce qui concerne la cybersécurité et de leurs systèmes de gestion de la cybersécurité [2021/387]
- Règlement ONU n°156 — Prescriptions uniformes relatives à l'homologation des véhicules en ce qui concerne les mises à jour logicielles et le système de gestion des mises à jour logicielles [2021/388]
- Arrêté du 11 août 2016, 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'activités d'importance vitale « Transports terrestres » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense
- IGI n° 1300/SGDSN/PSE/PSD sur la protection du secret de la défense nationale

Références normatives

- ISO/SAE 21434:2021 - Road vehicles — Cybersecurity engineering
- ISO/IEC 27005:2022 Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information
- CLC/TS 50701:2021 - Cybersécurité pour les applications ferroviaires
- NF EN 50126-1 octobre 2017 - Applications ferroviaires Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) – Partie 1 : processus FMDS générique
- NF EN 50126-2 octobre 2017 - Applications ferroviaires Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) – Partie 2 : Approche système pour la sécurité
- ISO/IEC 15408:2022 - Sécurité de l'information, cybersécurité et protection de la vie privée - Critères d'évaluation pour la sécurité des technologies de l'information - Parties 1 à 5
- IEC 62443-1-1:2009 - Industrial communication networks – Network and system security
- Part 1-1: Terminology, concepts and models
- IEC 62443-3-3:2009 - Industrial communication networks – Network and system security
- Part 3-3: System security requirements and security levels
- SAE J3016 2021-04-30 – Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles
- ETSI TR 102 893 – Intelligent Transport Systems (ITS) – Security – Threat, Vulnerability and Risk Analysis (TVRA)
- NF EN 50159 août 2021 - Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement - Communication de sécurité sur des systèmes de transmission
- ISO/IEC/IEEE 15026-1:2010 - Ingénierie du logiciel et des systèmes — Assurance du logiciel et des systèmes - Concepts et vocabulaire
- ISO/IEC/IEEE 15026-2:2022 - Ingénierie du logiciel et des systèmes — Assurance du logiciel et des systèmes – Cas d'assurance
- ISO/IEC/IEEE 15026-3:2015 - Ingénierie du logiciel et des systèmes — Assurance du logiciel et des systèmes – Niveaux d'intégrité système
- ISO/TR 4804:2020 - Road vehicles - Safety and cybersecurity for automated driving systems - Design, verification and validation
- ISO 9001:2015 Systèmes de management de la qualité — Exigences

Guides et bonnes pratiques

- Guide d'application relatif au principe GAME pour les STRA
- Guide technique relatif à la démonstration GAME pour les STRA
- Méthode EBIOS Risk Manager
- Guide AFNOR - Normes volontaires et approches innovantes pour la cybersécurité
- ENISA - Good practices for security of Smart Cars
- Guide d'application relatif à la mission de l'organisme qualifié agréé pour l'évaluation de la sécurité et pour l'audit de sécurité en exploitation des STRA
- ANSSI - Référentiel d'exigences pour les Prestataires de détection des incidents de sécurité Version 2.0 du 21 décembre 2017

Conformément au décret n° 2010-1580 du 17 décembre 2010, portant création du Service technique des remontées mécaniques et des transports guidés, le STRMTG est chargé de produire des guides et référentiels.

Le présent document a été élaboré par le groupe de travail national CYBERSECURITE STRA mis en place par le STRMTG, assisté de la société NEOSOFT.

Pilote : M. François Brun - STRMTG – Département transports publics automatisés
Secrétaire : M. Léo Maisonobe - STRMTG – Département transports publics automatisés
Assistance projet : M. Sylvain Conchon – NEOSOFT, M. Samaad Alladin – NEOSOFT

Pour les versions 1 et 2 (transport de personnes) :

SADIO BA	ANSSI
BRICE GILBERT	AFNOR
HEND HOUIMEL	AFNOR
PASCAL THOMAS	AFNOR
JEAN-MARC PAGLIERO	ALSTOM
JEAN-BAPTISTE RENAULT	ALSTOM
NICOLAS BONIAKOWSKI	BUREAU VERITAS
HAKIM NYAMPA	BUREAU VERITAS
DAMIEN DUCHASSIN	CEREMA
PIERRE-YVES TANNIOU	CEREMA
THIBAUT TOILLIEZ	CERTIFER
LIONEL AUBERT	CETU
SEVERINE BESSON	CETU
ERIC CHARLES	CETU
ELSA LANAUD	DGITM
ROMAIN DUPONT	EASYMILE
ARNAUD MOTTE	EASYMILE
JULIEN BURLET	GENDARMERIE
STEPHANE MILET	GENDARMERIE
ARYLDO RUSSO	GESTE
ARNAUD KAISER	IRT SYSTEMX
SAMUEL BELLANCA	KEOLIS
JULIEN TIN	KEOLIS
MARINE BRAULT	LSTI
ARMELLE TROTIN	LSTI
SAMMY HADDAD	OPPIDA
JEAN CAIRE	RATP
MBAYE SANKHE	RATP
ALEXANDRE AUBRY	STELLANTIS
STEPHANE GERONIMI	STELLANTIS
FREDERIC LENTI	STELLANTIS
MICHAEL BAKADAL	TRANSDEV
MICHEL DELHOM	TRANSDEV
NICOLAS DESMOINEAUX	TRANSDEV
JEAN CASSOU-MOUNAT	TRANSPOLIS
GUILLAUME MARTIN	TWINSWHEEL
VINCENT TALON	TWINSWHEEL
VIRGINIE DENIAU	UGE
LEO MENDIBOURE	UGE
RAFAEL DE SOUSA FERNANDES	UTAC
FABRICE HERVELEU	UTAC
YACINE LADJICI	UTAC
VERONIQUE DELEBARRE	SAFERIVER
ELENA TUSHKANOVA	SAFERIVER
BRICE GOMBAULT	SECTOR
PIERRE JOUVE	STRMTG
JEAN-MICHEL PASSELAIGUE	STRMTG
YVES SCHNEIDER	STRMTG
FLORENT SOVIGNET	STRMTG
ANISS ZIAD	STRMTG
BRICE GOMBAULT	SECTOR

Pour la version 3 (transport de marchandises) :

THOMAS SANJULLIAN	AFNOR
BRICE GOMBAULT	SECTOR
MERYEM MOUSTAHI	GESTE
MARINE THOMASSON	CARA
VINCENT TALON	TWINSWHEEL
CHRISTOPHE WILLMANN	CETU
JULIEN BONNETON	TRANSPOLIS
DAVID CROENNE	EASYMILE
LUC BARTHELEMY	EASYMILE
JOËLLE ENSMINGER	MILLA
SYLVAIN CONCHON	NEOSOFT
FLORENCE GALLAY	DGITM
CHRISTOPHE CELISSE	LSTI
FRANÇOIS BRUN	STRMTG
PIERRE JOUVE	STRMTG
LEO MAISONOBE	STRMTG
FLORENT SOVIGNET	STRMTG
YVES SCHNEIDER	STRMTG

Ont également contribué à la relecture du guide :

Mme Peggy Azam, STRMTG,
M. Ludovic Brun, STRMTG.