CARTOGRAPHIE DU SYSTÈME D'INFORMATION

Guide d'élaboration en 5 étapes

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

TABLE DES MATIÈRES

QU'EST-CE QU'UNE CARTOGRAPHIE ?

Le terme « cartographie » désigne une représentation schématique d'un ensemble d'informations. Les informations représentées sont minutieusement choisies pour répondre efficacement à la ou aux questions posées.

Les cartographies se structurent généralement en plusieurs dimensions. Par exemple, les cartes géographiques intègrent les infrastructures routières et les villes pour répondre aux besoins des usagers.

Les informations représentées peuvent être plus ou moins nombreuses selon les besoins. Par exemple, on peut choisir d'y représenter l'altitude, les stations-service ou encore les péages.

Cartographie du système d'information

Dans un contexte numérique, la cartographie permet de représenter le système d'information (SI) d'une organisation ainsi que ses connexions avec l'extérieur. Cette représentation peut être plus ou moins détaillée et inclure, par exemple, les biens matériels, logiciels, les réseaux de connexion, mais aussi les informations, activités et processus qui reposent sur ces biens.

Concrètement, la cartographie doit permettre de :

- réaliser l'inventaire patrimonial du système d'information, à savoir la liste des composants du SI et leur description détaillée ;
- présenter le système d'information sous forme de vues, à savoir des représentations partielles du SI, de ses liens et de son fonctionnement. Elles visent à rendre lisibles et compréhensibles différents aspects du système d'information.

Composition d'une cartographie

De manière générale, la cartographie est composée de trois visions allant progressivement du métier vers la technique, elles-mêmes déclinées en vues[1] :

1. Vision métier

- La **vue de l'écosystème** présente les différentes entités ou systèmes avec lesquels le SI interagit pour remplir sa fonction.
- La **vue métier du système d'information** représente le SI à travers ses processus et informations principales, qui sont les valeurs métier au sens de la méthode d'appréciation des risques EBIOS Risk Manager.

2. Vision applicative

- La **vue des applications** décrit les composants logiciels du système d'information, les services qu'ils offrent et les flux de données entre eux.
- La **vue de l'administration** répertorie les périmètres et les niveaux de privilèges des utilisateurs et des administrateurs.

3. Vision infrastructure

- La **vue des infrastructures logiques** illustre le cloisonnement logique des réseaux, notamment par la définition des plages d'adresses IP, des VLAN et des fonctions de filtrage et routage ;
- La **vue des infrastructures physiques** décrit les équipements physiques qui composent le système d'information ou utilisés par celui-ci.

Les vues sont composées de différents objets[2], dont des exemples sont proposés en annexe 1. Dans chaque vue, un objet pivot permet de faire le lien avec les vues adjacentes afin d'identifier les dépendances entre les objets du système d'information. ●

1 – Le découpage retenu ici est adapté dans le cadre de la construction d'une cartographie à l'usage de la sécurité. Il est cohérent avec les standards d'architecture ou d'urbanisation des systèmes d'information. En particulier, il est compatible avec le Cadre commun d'urbanisation du SI de l'État proposé par la Direction interministérielle des systèmes d'information et de communication (DINSIC).

2 – Les objets proposés en annexe permettent de répondre à l'usage de la sécurité numérique. Il est également possible de conduire d'autres projets impliquant la réalisation d'une cartographie (par exemple lors de la définition du registre des traitements conformément au règlement européen sur la protection des données personnelles – RGPD) en s'appuyant sur cette méthode et en la complétant par tout autre objet utile.

POURQUOI RÉALISER UNE CARTOGRAPHIE DE SON SYSTÈME D'INFORMATION ?

Dans un contexte de transformation numérique de la société qui nous amène à repenser nos modes de vie et de communication, les attaques informatiques sont de plus en plus nombreuses et complexes. La sécurité des systèmes d'information est donc, plus que jamais, un enjeu essentiel au bon fonctionnement des administrations et des entreprises.

La cartographie est un outil essentiel à la maîtrise du système d'information. Elle permet d'avoir connaissance de l'ensemble des composants du SI et d'obtenir une meilleure lisibilité de celui-ci en le présentant sous différentes vues. L'élaboration d'une cartographie du système d'information s'intègre dans une démarche générale de gestion des risques et répond à quatre enjeux de sécurité numérique :

- **la maîtrise du système d'information :** la cartographie permet de disposer d'une vision commune et partagée du système d'information au sein de l'organisation. C'est un outil indispensable au pilotage de l'évolution du SI, en particulier dans les contextes de mutualisation. Elle facilite également la capitalisation d'expérience et la prise de décision grâce à un langage simple et visuel, ce qui permet de manière générale d'assurer le maintien en condition de sécurité et d'améliorer le niveau de maturité de l'organisme en matière de sécurité numérique ;

- **la protection du système d'information :** la cartographie permet d'identifier les systèmes les plus critiques et les plus exposés, d'anticiper les chemins d'attaque possibles sur ces systèmes et de mettre en place des mesures adéquates pour assurer leur protection[3] ;

3 – La réalisation d'une cartographie facilite et accélère la conduite d'une appréciation de risques selon la méthode EBIOS Risk Manager.

- **la défense du système d'information :** la cartographie permet de réagir plus efficacement en cas d'incident ou d'attaque numérique, de qualifier les impacts et de prévoir les conséquences des actions défensives réalisées ;

- **la résilience du système d'information :** la cartographie permet d'identifier les activités clés de l'organisme afin de définir un plan de continuité d'activité et s'impose comme un outil indispensable à la gestion de crise, qu'elle soit numérique ou non.

Ce guide présente une démarche pour aider les organismes à élaborer des cartographies de leurs systèmes d'information, en vue de répondre aux besoins opérationnels de sécurité numérique. Il propose une approche simple, pratique et progressive du travail de cartographie. Il peut être utilisé par toute organisation, quelles que soient sa nature, sa taille, la complexité de son système d'information ou sa maturité en matière de SSI. Il s'adresse en premier lieu aux opérateurs d'importance vitale (OIV)[4], mais également aux autres organisations des secteurs public et privé.

4 – Tels que définis par l'article L. 1332-1 du Code de la défense. Les OIV pourront en particulier s'appuyer sur le présent guide pour se conformer à la règle « cartographie » (cf. annexe I des arrêtés sectoriels fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale, pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du Code de la défense).

COMMENT CONSTRUIRE UNE CARTOGRAPHIE DU SYSTÈME D'INFORMATION ?

Le succès d'une démarche de cartographie dépend de son caractère **pragmatique, participatif et pérenne**. Il est nécessaire que chacune des parties prenantes s'inscrive dans une démarche de cartographie **incrémentale** (enrichissement par de nouvelles vues) et **itérative** (affinement des vues déjà constituées). Il s'agit donc, selon les objectifs et les besoins de l'organisation, de cartographier au fur et à mesure les différentes vues et d'enrichir les vues déjà décrites en ajoutant des objets, des caractéristiques et des liens de dépendance. Certains détails pourront être temporairement incomplets et affinés lors de l'itération suivante afin de respecter le calendrier du projet.

Afin d'emporter l'adhésion des acteurs, la démarche de construction d'une cartographie doit s'intégrer aux processus de l'organisation et dans le cycle de vie du système d'information. Elle se décompose en cinq étapes, adaptables d'une part à la nature du système d'information à cartographier, et d'autre part aux objectifs visés par l'organisation selon son niveau de maturité et ses enjeux de sécurité numérique.

Étape n°1

Comment initier la démarche de cartographie ?

Définir les enjeux de la cartographie, les acteurs à mobiliser, le périmètre du système d'information à représenter, le niveau de granularité de l'inventaire et les types de vues à réaliser, les différentes itérations et le calendrier associé.

Étape n°2

Quel modèle dois-je adopter ?

Recenser toutes les informations disponibles en rassemblant les inventaires et schémas de représentation du système d'information déjà constitués. Définir le modèle de représentation de l'inventaire et des différentes vues ainsi qu'une nomenclature pour les différents objets.

Étape n°3

Quel outillage dois-je utiliser ?

Identifier les outils utiles à la construction de la cartographie et à son maintien à jour.

Étape n°4

Comment construire ma cartographie pas à pas ?

Construire l'inventaire en mettant à jour, le cas échéant, les informations recensées. Représenter les différentes vues de la cartographie selon le modèle.

Étape n°5

Comment pérenniser ma cartographie ?

Diffuser et promouvoir la cartographie au sein de l'organisation. Mettre en place un processus de mise à jour de la cartographie et la gouvernance[5] associée.

5 – On entend ici par « gouvernance » l'identification des rôles et responsabilités de chacun sur la pérennisation de la cartographie et la comitologie permettant de piloter et suivre sa mise à jour.

Étape n°

1

COMMENT INITIER LA DÉMARCHE DE CARTOGRAPHIE ?

Au cours de cette première étape, vous allez définir avec l'ensemble des parties prenantes tous les éléments nécessaires à l'initialisation et au bon déroulement du projet de cartographie.

1 Identifier les enjeux et parties prenantes de la construction de la cartographie

En premier lieu, il est nécessaire de **définir clairement les objectifs et les enjeux du projet** de cartographie pour répondre aux besoins de l'organisation.

Les objectifs du projet de cartographie doivent être partagés par toutes les parties prenantes et validés par un **« sponsor »**. Le sponsor du projet est un **membre de la direction de l'organisation** et prend une part active dans la gouvernance du projet de cartographie.

Dans le cas où la démarche de cartographie du système d'information est orientée sur la sécurité numérique, elle implique un nombre limité de parties prenantes. **Le Responsable de la sécurité des systèmes d'information (RSSI)** doit jouer le rôle de coordinateur et se positionner comme responsable de la mise en place et du suivi de la démarche.

Dans le cas où l'organisme a l'ambition d'engager une démarche plus globale et complète de cartographie de son système d'information, intégrant les besoins de sécurité numérique, le **Directeur des systèmes d'information (DSI)** peut être responsable du projet. Il coordonne une équipe comprenant un plus grand nombre de parties prenantes dont il est indispensable de définir clairement les rôles et responsabilités. Parmi les parties prenantes potentielles du projet de cartographie, on peut citer le RSSI, les architectes, les urbanistes, les métiers, le DPO[6], les responsables sûreté, les équipes d'audit et de conformité, etc. La mise en place de cette équipe projet doit être accompagnée et soutenue par les directions.

6 – *Data protection officer* ou Délégué à la protection des données.

Note

Il est primordial que les équipes SI et SSI travaillent ensemble pour que la cartographie obtenue couvre les besoins des deux équipes, et ce, en particulier si le RSSI n'est pas positionné au sein de la DSI. Une cartographie orientée sur la sécurité numérique ne pourra pas être maintenue au fil des évolutions du système d'information. Une cartographie uniquement SI ne sera pas adaptée à l'usage de la sécurité numérique.

La cartographie ne doit pas être portée exclusivement par les équipes SI et SSI. Elle doit aussi impliquer les métiers, en tant que propriétaires de leurs processus et de leurs données. Cette implication des parties prenantes facilitera l'adoption de la cartographie, qui pourra leur être utile, par exemple, pour avoir une vision d'ensemble des parties prenantes de leur écosystème.

2 Définir le périmètre à cartographier

Dans un deuxième temps, il est indispensable de **formaliser le périmètre à cartographier** afin de s'assurer que toutes les parties prenantes de la démarche partagent la même vision.

Quels que soient les objectifs fixés, il est recommandé de cartographier dans un premier temps les systèmes les plus exposés ou les plus critiques (pour les opérations, pour l'économie de l'entreprise, pour la nation). Ces systèmes sont les plus sensibles au regard de leurs besoins de sécurité et les plus vulnérables par rapport à leur exposition aux menaces.

3 Définir la cartographie cible et la trajectoire de construction

La définition de la **cible** consiste à **identifier l'ensemble des vues** à réaliser ainsi que leur **niveau de granularité**. La granularité des différentes vues de la cartographie est à adapter au contexte et aux objectifs recherchés. Elle peut donc varier d'un système d'information à l'autre selon sa criticité ou l'importance accordée à celui-ci.

La **trajectoire** de construction de la cartographie permet de **prévoir les différentes itérations** et les grands **jalons dans l'avancement de la cartographie.** Il est recommandé d'adopter une trajectoire progressive basée sur l'atteinte échelonnée de niveaux de maturité croissants.

La définition de la cible et de la trajectoire permet de **déterminer les responsabilités des différentes parties prenantes, d'estimer les ressources à prévoir et de définir le calendrier**. Une méthode de construction de la cartographie respectant les différents stades de maturité est détaillée en annexe 2.

Pour un système d'information de taille importante, il est recommandé de commencer par une cartographie limitée à certaines vues et centrée sur les systèmes critiques ou exposés, qui sera complétée avec d'autres vues par la suite.

Pour un SI de petite taille, il est possible de réaliser une cartographie cumulant plusieurs vues dès le départ. ●

Étape n°

2

QUEL MODÈLE DOIS-JE ADOPTER ?

Durant la deuxième étape, vous rassemblerez l'ensemble des inventaires et schémas de représentation du système d'information déjà constitués. Ensuite, vous définirez le modèle de représentation de l'inventaire et des différentes vues.
En pratique, la définition du modèle s'effectue en parallèle de la collecte afin de l'ajuster en fonction des retours obtenus.

1 Collecter et analyser les éléments de cartographie existants

L'étude de l'existant contribue à accélérer la démarche de cartographie puisqu'elle permet de **rassembler l'ensemble du travail déjà effectué** pour constituer une base de départ.

La conduite d'entretiens avec les acteurs de la sécurité numérique au sein de l'organisation, la conception et l'exploitation du système d'information sont l'occasion de **présenter la démarche de réalisation d'une cartographie, de recueillir les informations existantes et d'identifier les premiers manques** (par rapport au modèle de cartographie construit en parallèle).

Il est recommandé de prêter une attention particulière aux actions suivantes :

- recueillir et analyser l'ensemble des documents relatifs à la description du système d'information, aux normes utilisées et à l'inventaire des ressources et des actifs ;
- identifier les outils de cartographie actuellement en place ;
- identifier les processus existants concernant l'alimentation et la mise à jour des informations patrimoniales ;
- identifier les difficultés rencontrées dans la constitution et l'utilisation des cartographies précédentes.

2 Définir le modèle de cartographie

La définition d'un modèle de cartographie permet à l'organisation de **disposer d'un référentiel commun** qui assurera le succès de la communication et du partage d'information entre tous les acteurs de l'organisation. Le contenu du modèle varie selon les vues à développer, choisies dans l'étape n°1.

Pour chacune des vues de la cartographie, il convient de **choisir les objets et attributs** à représenter ainsi que leur format. **Les objets** sont un ensemble d'éléments référencés dans la cartographie, qui sont les **valeurs métier** et les **biens supports** au sens de la méthode d'appréciation des risques EBIOS Risk Manager. Les relations entre objets peuvent également être représentées (objets pivots présents dans différentes vues, importance de la dépendance entre les objets, etc.). Des listes d'objets sont présentées pour chaque vue en annexe 1. Elles contiennent à la fois des objets retrouvés habituellement dans les modèles d'urbanisation, mais aussi des objets répondant spécifiquement aux besoins de sécurité numérique. **Les attributs** sont des informations essentielles aux futures analyses, dont certaines ont trait à la sécurité numérique. Par exemple, on peut distinguer pour une application **son type** (développement interne, logiciel, progiciel, etc.), **ses besoins** de sécurité ou encore **son exposition vis-à-vis de l'extérieur**. Le modèle de cartographie doit définir la liste des attributs correspondant à chaque objet choisi, avec une priorité pour ceux qui sont liés à la sécurité numérique. Des listes d'attributs sont présentées pour chaque objet en annexe 1.

Enfin, la définition du modèle de cartographie inclut la définition de la **représentation graphique attendue** pour chaque objet et attribut ainsi que le respect d'une **nomenclature** permettant de disposer d'informations homogènes. La fonction des objets et attributs doit se traduire dans leur représentation afin de faciliter leur exploitation et le passage d'une vue à l'autre (ex. : mêmes formes, couleurs, nomenclature, etc.). ●

Étape n°

3

QUELS OUTILS DOIS-JE UTILISER ?

Dans cette troisième étape, vous allez définir le ou les outils logiciels que vous utiliserez pour mener à bien votre projet de cartographie. Le choix d'outils plus ou moins spécialisés dépend du niveau de maturité visé et du contexte.

L'utilisation d'un **logiciel spécifique** (logiciel de modélisation du système d'information ou logiciel d'architecture d'entreprise) s'avère rapidement indispensable dès lors que le volume de données et/ou le nombre de contributeurs deviennent importants.

Les outils choisis doivent satisfaire les besoins suivants[7] :

- 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.

Il est possible que des outils d'inventaire, de gestion de mouvements matériels ou de modélisation d'infrastructure soient déjà en place dans l'organisme ou que certains systèmes proposent des cartographies sur certains périmètres. L'objectif du projet de cartographie n'est pas de remplacer les outils existants. Il convient, cependant, de **s'assurer que les outils en place correspondent toujours aux usages et d'identifier dans quelle mesure ils peuvent être utiles à la réalisation du projet de cartographie**. Si les outils en place ne conviennent pas, le choix d'un nouvel outil pourra être proposé.

Note

La simplicité de l'outil est un atout majeur pour mener à bien le projet de cartographie et éviter la réalisation ou la découverte de cartographies « parallèles ».

7 – L'outillage pourra également permettre de répondre à des besoins complémentaires comme l'association de documentation aux objets de la cartographie, la visualisation graphique de dépendances entre objets, la création de relations entre les objets et leurs propriétaires, la création de cartographies selon le modèle de l'organisation (par directions, par filiales, par pays…), etc.

Les **outils de modélisation du système d'information** permettent, en plus de la réalisation de schémas et d'inventaires, de **simplifier les actions de mise à jour et le partage des informations**. Par exemple, certains répercutent automatiquement les changements effectués sur les vues dans l'inventaire (et inversement) afin de garantir une cohérence d'ensemble et des interdépendances entre les éléments du SI. Les fonctions d'automatisation des processus proposées dans certains logiciels permettent de réaliser des étapes de validation et des relances auprès des acteurs responsables des mises à jour sur un périmètre.

Peu de logiciels permettent de réaliser directement la collecte des informations. Néanmoins, les plus flexibles peuvent **s'interfacer avec des outils de collecte informatique** (outil de gestion de parc, gestion d'adresses IP, etc.).

Ainsi, les outils de modélisation du système d'information facilitent cette collecte et permettent un gain de temps important. Ils garantissent la cohérence du contenu et de la représentation des systèmes, tant sur le fond que sur la forme, et facilitent leur lecture. Les cartographies sont également centralisées au sein d'un référentiel unique avec un accès facilité pour les acteurs concernés.

Dans tous les cas, et pour un partage de l'information réussi, il est fortement recommandé[8] de rendre la cartographie exportable sur un support électronique et dans un format qui puisse être lu par les principaux logiciels bureautiques, en vue d'une utilisation en lecture seule.

8 – Pour les Opérateurs d'importance vitale (OIV), cette recommandation devient obligatoire dans le cadre de la règle « cartographie ».

Étape n°

4

COMMENT CONSTRUIRE MA CARTOGRAPHIE PAS À PAS ?

Dans cette quatrième étape, vous réaliserez l'inventaire et construirez les vues cartographiques à l'aide de l'outillage choisi lors de l'étape précédente et selon la trajectoire définie lors du cadrage.

La réussite d'un projet de cartographie passe notamment par le caractère progressif de la démarche. La construction de l'inventaire et des différentes vues doit être réalisée pas à pas, de manière :

- **incrémentale** (enrichissement par de nouvelles vues) ;
- **itérative** (affinement des vues déjà constituées).

Il convient de porter une attention particulière à la **sensibilité des informations** comprises dans l'inventaire et dans les vues de la cartographie. Si le besoin de protection le justifie, le chef de projet ou le RSSI peut décider de faire porter à la cartographie une mention de protection[9] (confidentiel entreprise, diffusion restreinte[10], voire classification et protection au titre du secret de la défense nationale[11]).

1 Réaliser l'inventaire du système d'information

La réalisation de l'**inventaire du système d'information** se base sur les éléments recueillis durant l'étude de l'existant. L'objectif est de compléter ces informations avec celles définies dans le modèle, au cours de l'étape 2.

Pour construire l'inventaire exhaustif des éléments d'une vue, il est par exemple possible d'explorer progressivement les éléments **en partant d'une liste d'objets et en parcourant les liens de dépendance**.

9 – Pour les Systèmes d'information d'importance vitale (SIIV), il est spécifié dans la règle « cartographie » que la cartographie dans son ensemble est marquée « diffusion restreinte » et peut, le cas échéant, être classée « confidentiel défense ».

10 – Au sens de l'Instruction interministérielle n°901 relative à la protection des systèmes d'information sensibles (n°901/SGDSN/ANSSI).

11 – Au sens de l'Instruction générale interministérielle n°1300 sur la protection du secret de la défense nationale (n°1300/SGDSN/PSE/PSD).

Il est également possible de compléter l'inventaire 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, comme par exemple les plans de continuité et de reprise d'activité ou les analyses de risques.

2 Construire les vues de la cartographie

Tous les objets et attributs de l'inventaire ne doivent pas forcément être représentés sur les vues de la cartographie : les vues peuvent avoir différents niveaux de granularité.

Toutefois, **l'exhaustivité des liens entre les objets pivots est importante** pour l'analyse des impacts de sécurité numérique. Ces schémas sont généralement les premiers éléments à être exploités lors d'audits ou d'analyses post-incidents, car ils permettent une compréhension rapide du système d'information.

Les vues de la cartographie sont générées par des outils dédiés. Il est important de **considérer chaque schéma comme un extrait à un instant T** et non comme un schéma définitif ou un état final. Dans le cas où une vue non définie par l'outillage serait nécessaire, il n'est pas recommandé que celle-ci soit réalisée manuellement à partir d'extractions. La plupart des outils possèdent des modules complémentaires ou des extensions : cette voie est à privilégier.

Note

Chaque schéma doit comporter un titre, une date, un numéro de version et une légende.

Pour représenter l'ensemble des éléments qui composent chaque vue, il est possible, comme lors de la construction de l'inventaire, de procéder pas à pas. Un élément ajouté est ainsi immédiatement relié aux éléments déjà représentés. Il est rappelé que la représentation des différents éléments doit respecter le formalisme défini au cours de l'étape 2. ●

Étape n°

5

COMMENT PÉRENNISER MA CARTOGRAPHIE ?

Les quatre étapes précédentes ont permis de constituer une première vision du patrimoine de l'organisme. Or, une cartographie n'est utile que si elle est communiquée au plus grand nombre et si les informations qu'elle contient sont fiables et à jour. Ainsi, pour être pérenne et conserver sa valeur, la cartographie doit être partagée et revue régulièrement. C'est l'objet de cette cinquième étape.

1 Communiquer sur la cartographie

Pour être la plus efficace possible, la **communication doit faire partie intégrante du processus de mise à jour de la cartographie.** Toutefois, il est indispensable de prêter attention à la sensibilité voire au caractère confidentiel de certaines informations. Il est donc recommandé de limiter les accès aux différentes vues de la cartographie, pour que seules les personnes concernées puissent y accéder. Par exemple, les vues d'infrastructure seront accessibles à la seule DSI, alors que la vue métier pourra être partagée plus largement.

La cartographie doit notamment être tenue à disposition du RSSI et du CERT[12] de l'entité (ou dispositif équivalent). Les opérateurs d'importance vitale doivent également la communiquer à l'ANSSI[13] à sa demande, notamment en cas de besoin de coordination opérationnelle suite à une attaque informatique d'ampleur.

12 – *Computer Emergency Response Team* ou Équipe de réponse à incidents.
13 – Agence nationale de la sécurité des systèmes d'information.

Note

La cartographie du système d'information constitue un élément essentiel de l'organisation. Aussi, des mesures doivent être prises pour garantir sa disponibilité et sa confidentialité :

- *une sauvegarde de la cartographie doit être réalisée régulièrement sur un support de stockage sécurisé. Elle doit notamment être accessible en cas de coupure du réseau. La conservation d'une version papier la plus à jour possible permet de répondre à cet impératif. Cette conservation devra être sécurisée conformément au niveau de classification de la cartographie ;*
- *la cartographie ne doit pas être stockée sur le système d'information qu'elle représente. En effet, un attaquant qui se serait infiltré dans le SI aurait alors accès à toutes les informations concernant l'architecture du système. De plus, les accès à la cartographie doivent être limités 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.*

2 Maintenir la cartographie à jour

Quelles que soient la taille et la nature de l'organisation, il est important de disposer de ressources suffisantes pour **maintenir la cartographie 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 cartographie.

Les actions de revue de la cartographie doivent être structurées via **un processus d'amélioration continue et une gouvernance bien définis** afin d'éviter, entre autres, l'apparition de versions multiples. Une bonne pratique

consiste à **instaurer des campagnes de mises à jour régulières** nécessitant l'implication des acteurs concernés afin qu'ils vérifient et actualisent les informations de leur périmètre.

Dans le cadre de la revue de la cartographie, les parties prenantes pourront répondre aux questions suivantes :

- Faut-il étendre le périmètre de la cartographie ?
- Faut-il viser le niveau de maturité supérieur ?
- Faut-il affiner certaines vues déjà représentées ?
- Quel est le délai souhaité pour réaliser les prochaines actions ?

Une autre bonne pratique consiste à **intégrer une étape de mise à jour de la cartographie** dans les projets d'évolution du système d'information.

FACTEURS CLÉS DE RÉUSSITE

La construction d'une cartographie peut se révéler complexe et se heurter à des difficultés organisationnelles, humaines, techniques ou calendaires. Les conseils développés dans cette partie vous permettront d'accéder plus facilement aux résultats attendus.

Suivre une démarche projet et pérenniser le résultat

La construction de la cartographie doit s'appuyer sur une stratégie de développement fixant des priorités et objectifs réalistes en termes de contenus et de calendrier, dont la mise en œuvre doit être pilotée en mode projet et impliquer le plus haut niveau hiérarchique de l'organisation. Afin de favoriser la pérennité de la cartographie, il convient de privilégier une information macroscopique et à jour, par rapport à une information détaillée, entretenue de manière épisodique et au prix d'efforts trop lourds.

Construire la cartographie par itérations

Cartographier à court terme l'ensemble d'un système d'information avec l'exhaustivité des informations utiles et des vues afférentes est souvent très difficile, voire irréalisable. La cartographie doit s'inscrire dans une démarche d'amélioration continue à la fois incrémentale et itérative. Cette démarche permet d'élargir le périmètre de représentation de la cartographie, d'augmenter son niveau de maturité et d'industrialiser toujours davantage les processus engagés afin de répondre aux nouvelles exigences de sécurité numérique.

Adopter un modèle de cartographie comme langage commun

Afin de faciliter le partage d'informations, les parties prenantes doivent s'appuyer sur un langage commun. La définition du modèle de cartographie est une étape structurante de la démarche, qui permet de créer des concepts partagés entre les différents acteurs. Il est essentiel que ces concepts soient clairement définis et adaptés au contexte d'utilisation. Ainsi, chaque partie prenante doit s'être approprié ces définitions sans ambigüité et de manière concrète.

Communiquer à toutes les étapes du projet

La communication au sein d'un projet de cartographie est essentielle, quel que soit l'état d'avancement de la démarche. En particulier, il est important de communiquer sur la démarche en début de projet en rappelant son utilité et ses objectifs (par exemple, amélioration significative de la maîtrise du système d'information, de la réactivité en cas de panne, de la gestion des évolutions du système, etc.). Cette communication doit permettre de fédérer les acteurs autour de la démarche. Une fois celle-ci aboutie, il est également indispensable de diffuser la cartographie et de la rendre disponible auprès des équipes qui pourraient en avoir l'utilité (selon son niveau de confidentialité).

Entretenir la cartographie

La mise à jour de la cartographie est une étape indispensable de la démarche afin de pouvoir garantir une synchronisation entre les évolutions du système d'information et leur représentation dans l'inventaire et les vues. Le choix de l'outil est primordial afin de simplifier le travail de réalisation et d'entretien de la cartographie. Il est également nécessaire de définir et mettre en place un processus de mise à jour de la cartographie et sa gouvernance afférente. Les actions de revue de la cartographie doivent être réalisées de manière régulière et structurée. ●

ANNEXES

ANNEXE 1
DÉFINITION ET PROPOSITION DE CONTENU DES DIFFÉRENTES VUES

Cette annexe **définit les différentes vues présentées lors de l'étape 1** et propose des éléments de contenu pour chacune d'elles. Il convient de **sélectionner, parmi ces propositions, les éléments à inventorier et éventuellement de les compléter** selon le besoin de l'organisation et le contexte. Les éléments proposés pour les différentes vues n'ont pas forcément vocation à tous être représentés sur des schémas.

À chaque élément son niveau de granularité. Trois niveaux croissants sont répertoriés dans ce guide :

- **granularité minimale de niveau 1 :** informations indispensables ;
- **granularité intermédiaire de niveau 2 :** informations importantes ;
- **granularité fine de niveau 3 :** informations utiles.

Les objets et attributs mentionnés dans les différents tableaux de cette annexe, ainsi que les niveaux de granularité associés, forment des propositions cohérentes avec la trajectoire proposée en annexe 2. Chaque organisation, lors de la définition de sa cible de cartographie et de sa trajectoire, est libre de définir de nouveaux objets ou attributs et d'adapter, au besoin, le niveau de granularité de chaque élément.

Note

Les attributs mentionnés en bleu sont orientés sur la sécurité numérique.

1 Vue de l'écosystème

La vue de l'écosystème décrit **l'ensemble des entités ou systèmes qui gravitent autour du système d'information** considéré dans le cadre de la cartographie. Cette vue permet à la fois de délimiter le **périmètre de la cartographie,** mais aussi de disposer d'une **vision d'ensemble de l'écosystème** sans se limiter à l'étude individuelle de chaque entité.

Objet	Attribut	Granularité	Objet pivot
Entité ou système	Identification et description	1	
	Type d'entité ou de système (ex. : interne, externe, fournisseur, client, etc.)		
	Niveau de sécurité (ex. : maturité, mesures de sécurité en place ou définies au niveau contractuel, degré de confiance, homologation)		
	Liste des processus soutenus		Vue 2
	Point de contact sécurité de l'entité (ex. : RSSI)		
Relation	Nature (ex. : fourniture de biens, de services, partenariat commercial, etc.)	1	
	Lien contractuel ou règlementaire	2	
	Niveau d'importance fonctionnelle de la relation		

2 Vue métier du système d'information

La vue métier du système d'information décrit **l'ensemble des processus métiers de l'organisme avec les acteurs qui y participent,** indépendamment des choix technologiques faits par l'organisme et des ressources mises à sa disposition. La vue métier est essentielle, car **elle permet de repositionner les éléments techniques dans leur environnement métier et ainsi de comprendre leur contexte d'emploi.**

Un processus est décrit de bout en bout, depuis l'événement déclencheur jusqu'au résultat final fourni, indépendamment du cloisonnement qui existe dans l'organisme. Pour les processus transverses sous gouvernance de plusieurs entités, une organisation doit être prévue pour les décrire dans leur entièreté en conservant une perception partagée par tous les acteurs.

Dans cette vue sont également recensées les informations de l'organisme, dont certaines peuvent avoir un caractère critique et représenter des cibles de choix lors d'attaques.

Objet	Attribut	Granularité	Objet pivot
Macro-processus	Identification et description	2	
	Éléments entrants et sortants		
	Liste des processus qui le composent		
	Besoins de sécurité (DICT)		
	Propriétaire	3	
Processus	Identification et description	1	
	Éléments entrants et sortants		
	Liste des activités qui le composent (ou des opérations qui le composent, si les niveaux de maturité 1 ou 2[14] sont ciblés)		
	Liste des entités ou systèmes associés		Vue 1
	Liste des applications qui le soutiennent		Vue 3
	Besoins de sécurité (DICT)		
	Propriétaire		
Activité	Identification et description	3	
	Liste des opérations qui la composent		
Opération	Identification et description	1	
	Liste des tâches qui la composent	3	
	Liste des acteurs qui interviennent	2	
Tâche	Identification et description	3	
Acteur	Nom et moyens de contact	2	
	Nature : personne, groupe, entité, etc.		
	Type : interne ou externe à l'organisme		

14 – Tel que défini dans l'annexe 2.

Objet	Attribut	Granularité	Objet pivot
Information	Identification et description	1	
	Propriétaire		
	Administrateur		
	Stockage (type, localisation)		
	Processus lié		
	Besoins de sécurité (DICT)		
	Sensibilité : donnée à caractère personnel, donnée médicale, donnée classifiée, etc.		
	Contraintes règlementaires et normatives	3	

3 Vue des applications

La vue des applications permet de décrire une partie de ce qui est classiquement appelé le « système informatique ». Cette vue décrit **les solutions technologiques qui supportent les processus métiers,** principalement les applications.

Dans le cadre de la vision sécurité numérique, une importance forte est donnée aux flux applicatifs. Cette vue est particulièrement intéressante pour visualiser les échanges d'informations d'un point de vue logiciel. Les modalités d'échange sont ici caractérisées en détail.

Objet	Attribut	Granularité	Objet pivot
Bloc applicatif	Identification et description	2	
	Responsable		
	Liste des applications qui le composent		
Application	Identification et description	1	
	Liste de la (des) entité(s) utilisatrice(s)	2	Vue 1
	Entité responsable de l'exploitation		
	Responsable SSI	1	
	Type de technologie : client lourd, web, etc.		

Objet	Attribut	Granularité	Objet pivot
Application	Type d'application : développement interne, logiciel, progiciel, script, plateforme EAI/ESB, etc.	1	
	Volume d'utilisateurs et profils	2	
	Flux associés	1	
	Besoins de sécurité (DICT)		
	Exposition à l'externe (ex. : solution de type Software as a Service – SaaS)		
	Liste des processus utilisant l'application		Vue 2
	Liste des services applicatifs délivrés par l'application	2	
	Liste des bases de données utilisées par l'application	1	
	Liste des serveurs logiques soutenant l'application		Vue 5
Service applicatif	Identification et description	2	
	Liste des modules qui le composent		
	Flux associés		
	Exposition à l'externe (ex. : service dans le nuage - *Cloud*)		
Module	Identification et description	2	
	Flux associés		
Base de données	Identification et description	1	
	Liste de la (des) entité(s) utilisatrice(s)	2	Vue 1
	Entité responsable de l'exploitation		
	Responsable SSI	1	
	Type de technologie		
	Flux associés		
	Liste des informations contenues		Vue 1
	Besoins de sécurité (DICT)		
	Exposition à l'externe		
Flux	Identification et description	1	
	Émetteur : application, module, base de données, etc.		
	Récepteur : application, module, base de données, etc.		
	Chiffrement		

4 Vue de l'administration

La vue de l'administration est un cas particulier de la vue des applications. Elle répertorie les **périmètres et les niveaux de privilèges des administrateurs**.

La représentation schématique de cette vue n'est utile que s'il existe une gestion centralisée des droits d'administration sur les équipements comportant plusieurs périmètres d'administration. Dans le cas où les droits sur les équipements sont gérés par des comptes locaux, elle est réduite à la constitution d'une liste des comptes et droits associés pour chaque équipement.

Objet	Attribut	Granularité
Zone d'administration	Identification et description	1
	Groupe d'administrateurs et niveaux de privilèges	
	Liste des éléments contenus dans la zone	
	Liste des secrets associés à l'administration des ressources	
Service d'annuaire d'administration	Identification et description	1
	Solution : Active Directory, Novell, NT4, Samba, etc.	
Forêt Active Directory/ Arborescence LDAP	Identification et description	1
	Domaines appartenant à la forêt/l'arborescence	
	Relations inter-forêts/inter-arbres : domaines, bidirectionnelle, filtrée, transitive, etc.	
Domaine Active Directory/LDAP	Identification et description	1
	Nombre de contrôleurs de domaines	
	Nombre de comptes utilisateurs rattachés	
	Nombre de machines rattachées	
	Relations inter-domaines : domaines, bidirectionnelle, filtrée, etc.	

5 Vue des infrastructures logiques

Cette vue correspond à la **répartition logique du réseau.** Elle illustre **le cloisonnement des réseaux et les liens logiques entre eux**. En outre, elle répertorie les équipements réseau en charge du trafic.

Les emplacements logiques des équipements de sécurité (sonde, pare-feu, SIEM, etc.) sont également recensés dans cette vue.

Objet	Attribut	Granularité	Objet pivot
Réseau	Identification et description	1	
	Type de protocole		
	Responsable d'exploitation		
	Responsable SSI		
	Sous-réseaux rattachés		
	Niveau de sensibilité ou de classification		
Sous-réseau	Identification et description	1	
	Adresse/Masque		
	Passerelle		
	Plage d'adresses IP : adresse de début, de fin		
	Méthode d'attribution des IP : fixe ou dynamique		
	Responsable d'exploitation		
	DMZ ou non		
	Liste des sous-réseaux interconnectés		
	Possibilité d'accès sans fil		
Passerelle d'entrée depuis l'extérieur	Caractéristiques techniques	1	
	IP publique et privée		
	Type d'authentification		
Entité extérieure connectée	Nom, Responsable SSI, contacts SI	2	
	Réseaux internes interconnectés à l'entité		

Objet	Attribut	Granularité	Objet pivot
Commutateur (*switch*)	Identification : identifiant et adresse IP	1	
	Caractéristiques techniques : modèle, version du logiciel embarqué		
	Règles de filtrage des flux réseaux	2	
	Équipement physique de support (si virtualisé)		Vue 6
Routeur	Identification : identifiant et adresse IP	1	
	Caractéristiques techniques : modèle, version du logiciel embarqué		
	Règles de filtrage des flux réseaux	2	
	Équipement physique de support (si virtualisé)		Vue 6
Équipement de sécurité	Identification (identifiant, adresse IP, adresse MAC) et description	1	
	Caractéristiques techniques : type d'équipement (sonde, pare-feu, SIEM, etc.), modèle, OS et version, version du logiciel embarqué		
	Équipement physique de support (si virtualisé)	2	Vue 6
Serveur DHCP	Identification (identifiant, adresse IP si fixe, adresse MAC) et description	2	
	Caractéristiques techniques : modèle, OS et version		
	Serveur physique de support (si machine virtuelle)		Vue 6
Serveur DNS	Identification (identifiant, adresse IP si fixe, adresse MAC) et description	2	
	Caractéristiques techniques : modèle, OS et version		
	Serveur physique de support (si machine virtuelle)		Vue 6
Serveur logique	Identification (identifiant, adresse IP, adresse MAC) et description	1	
	Caractéristiques techniques : modèle, OS et version		
	Services réseaux actifs		
	Serveur physique de support	2	Vue 6
	Applications liées	1	Vue 3

6 Vue des infrastructures physiques

La vue des infrastructures physiques permet de **décrire les équipements physiques** qui composent le système d'information ou qui sont utilisés par celui-ci. Cette vue correspond à la **répartition géographique des équipements réseaux au sein des différents sites de l'organisme**. Elle offre une vision d'ensemble des actifs connectés au réseau de télécommunication de l'entreprise.

Objet	Attribut	Granularité	Objet pivot
Site	Identification et description	1	
	Bâtiments rattachés		
Bâtiment/Salle	Identification et description	1	
	Baies rattachées		
Baie	Identification et description	1	
	Liste des machines hébergées		
Serveur physique	Identification : identifiant, adresse IP, nom DNS	1	
	Caractéristiques techniques : type, modèle, OS et version		
	Emplacement physique : site, bâtiment, salle, baie		
	Serveur(s) logique(s) rattaché(s)		Vue 5
	Liste des commutateurs reliés		
	Responsable d'exploitation		
Poste de travail	Identification	2	
	Caractéristiques techniques : type (fixe ou portable), modèle, OS et version		
	Emplacement physique : site, bâtiment, salle		
Infrastructure de stockage	Identification	2	
	Caractéristiques techniques : type (NAS, SAN, disque dur, etc.), modèle		
	Emplacement physique : site, bâtiment, salle, baie		

Objet	Attribut	Granularité	Objet pivot
Périphérique	Identification	2	
	Caractéristiques techniques : type (imprimante, scanner, etc.), modèle		
	Responsable d'exploitation		
Téléphone	Identification	2	
	Caractéristiques techniques : type (fixe ou portable), modèle		
	Emplacement physique : site, bâtiment, salle		
Commutateur physique	Identification	1	
	Commutateur(s) logique(s) rattaché(s)		Vue 5
	Caractéristiques techniques : niveau (L1, L2, L3, etc.), modèle, version du logiciel embarqué		
	Emplacement physique : site, bâtiment, salle, baie		
	VLAN associé		
Routeur physique	Identification	1	
	Routeur logique associé		Vue 5
	Caractéristiques techniques : modèle, version du logiciel embarqué		
	Emplacement physique : site, bâtiment, salle, baie		
	VLAN associé		
Borne wifi	Identification	2	
	Caractéristiques techniques : modèle		
	Emplacement physique : site, bâtiment, salle, baie		
Équipement de sécurité physique	Identification (identifiant, adresse IP, adresse MAC) et description	1	
	Équipement(s) de sécurité logique(s) rattaché(s)		Vue 5
	Caractéristiques techniques : type d'équipement (sonde, pare-feu, SIEM, etc.), modèle, OS et version, version du logiciel embarqué		
	Emplacement physique : site, bâtiment, salle		
WAN	Identification	1	
	MAN ou LAN rattachés		
MAN	Identification	1	
	LAN rattachés		
LAN	Identification	1	
VLAN	Identification et description	1	
	Commutateurs associés		

ANNEXE 2
PROPOSITION DE CIBLE ET DE TRAJECTOIRE DE CONSTRUCTION DE LA CARTOGRAPHIE

Cette annexe propose **un exemple de cible et de trajectoire pour construire la cartographie au fil des stades de maturité atteints**.

Lors de la définition des objectifs de la cartographie, il est possible de s'orienter vers une démarche axée sur la sécurité numérique, pilotée par le RSSI, ou une démarche plus globale pilotée par le DSI qui répond à l'ensemble des besoins liés à la cartographie. Les besoins du projet de cartographie doivent être validés par un sponsor, membre de la direction de l'organisation.

Le niveau de maturité cible est ensuite défini en adéquation avec le choix de démarche projet :

- **maturité de niveau 1 :** la démarche vise à élaborer une cartographie comprenant les **premiers éléments indispensables** aux opérations de sécurité numérique. Ce niveau est considéré comme une **étape intermédiaire**, centrée sur un nombre limité de vues, pour aboutir de manière progressive au niveau de maturité 2 ;
- **maturité de niveau 2 :** la démarche vise à élaborer une cartographie orientée sur la sécurité numérique dans laquelle **l'ensemble des vues sont représentées**. Les **systèmes d'information d'importance vitale (SIIV)** doivent disposer d'une cartographie ayant ce niveau de maturité *a minima* ;
- **maturité de niveau 3 :** la démarche vise à élaborer une cartographie **exhaustive et détaillée, qui intègre les besoins de sécurité numérique.** Le niveau de granularité des différentes vues est plus fin de manière à obtenir une vision complète du système d'information.

Le tableau ci-dessous présente les informations collectées pour chaque niveau de maturité.

Objets/Attributs concernés	Démarche de cartographie orientée sur la sécurité numérique		Démarche globale de cartographie
	Maturité de niveau 1	Maturité de niveau 2	Maturité de niveau 3
Vue de l'écosystème			
Granularité 1	●	●	●
Granularité 2			●
Vue métier du système			
Granularité 1	●	●	●
Granularité 2		●	●
Granularité 3			●
Vue des applications			
Granularité 1	●	●	●
Granularité 2			●
Vue de l'administration			
Granularité 1		●	●
Vue des infrastructures logiques			
Granularité 1	●	●	●
Granularité 2		●	●
Vue des infrastructures physiques			
Granularité 1		●	●
Granularité 2			●

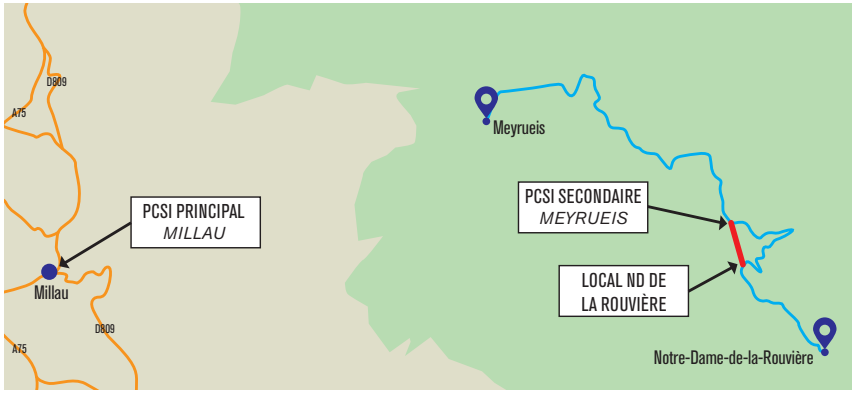
ANNEXE 3
EXEMPLE DE CARTOGRAPHIE

Cette annexe propose un exemple d'application s'appuyant sur une étude de cas sur un tunnel routier réalisée par l'**ANSSI**[15].

La cartographie de ce cas pratique est de niveau de maturité 1 et s'articule autour de trois vues de granularité 1 : une vue métier, une vue applicative et une vue architecture technique. La vue métier de l'écosystème n'est pas représentée puisque seul le tunnelier est présent dans l'écosystème.

L'exemple de cartographie porte sur le système d'information industriel d'un tunnel routier fictif situé sous le mont Aigoual, sur la route reliant Meyrueis à Notre-Dame-de-la-Rouvière.

Figure 1 – Carte de situation



Il s'agit d'un tunnel routier de type monotube à circulation bidirectionnelle d'une longueur de 2 550 mètres. Le tunnel est supervisé depuis un poste de contrôle et de commande distant localisé à Millau. Un poste de contrôle et de commande secondaire utilisé en secours est localisé sur site côté Meyrueis.

15 – ANSSI, « La cybersécurité des systèmes industriels : étude de cas sur un tunnel routier » [en ligne], https://www.ssi.gouv.fr/etude-tunnel/

À l'intérieur du tunnel, des niches sont installées tous les 200 mètres environ. On y trouve des piquages pour les divers fluides, des alimentations électriques ou des commutateurs pour les réseaux informatiques présents.

Les missions du tunnel sont les suivantes :

- permettre le transit de véhicules de l'entrée à la sortie du tunnel ;
- assurer la sécurité des usagers et du personnel en fonctionnement nominal ;
- assurer la sécurité des usagers et du personnel en cas d'incendie ou d'émanation de gaz.

Les fonctions principales mises en œuvre pour assurer un niveau de sûreté de fonctionnement satisfaisant du tunnel sont les suivantes :

- l'alimentation et la distribution électrique ;
- l'indication des sorties de secours ;
- la ventilation ;
- la signalisation ;
- la détection de véhicules hors gabarit ;
- la vidéo-surveillance ;
- la détection incendie ;
- le réseau d'appel d'urgence ;
- le contrôle de la qualité de l'air ;
- l'acquisition et le traitement des données en provenance du tunnel (télémesures, téléalarmes, télésignalisation) : la supervision ;
- le contrôle des équipements par envoi de télécommandes et de téléréglages : le pilotage.

D'après la méthode formalisée dans le guide *La Cybersécurité des systèmes industriels*[16], une classification des fonctions principales a été définie en fonction de la vraisemblance et de l'impact d'une attaque sur chaque fonction.

16 – ANSSI, *La Cybersécurité des systèmes industriels – Méthode de classification et mesures principales*, 2014

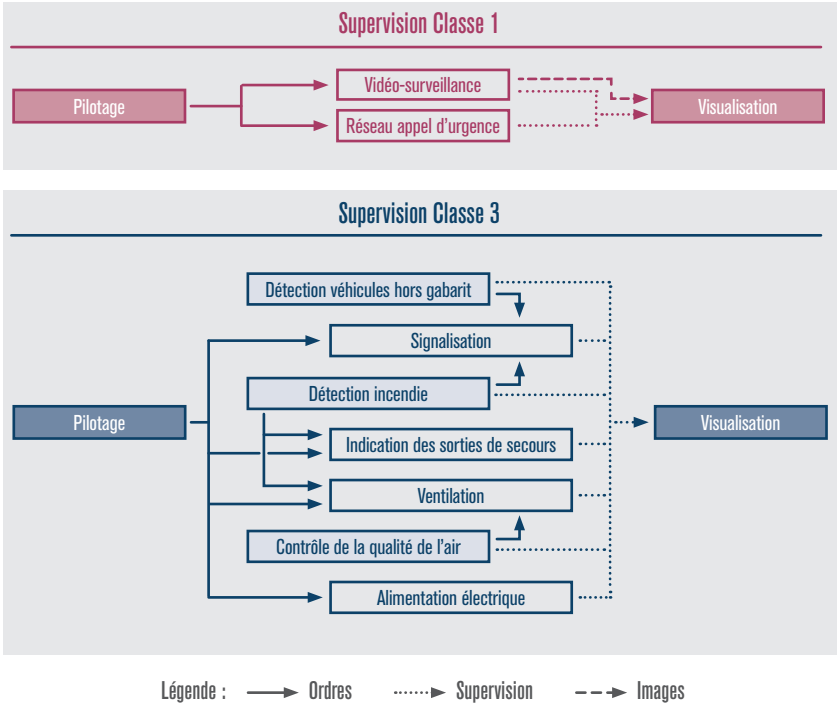
Pour les systèmes industriels, la méthode formalisée dans le guide propose trois classes numérotées de 1 à 3, par ordre croissant de criticité et dont les couvertures sont :

- **classe 1 :** le risque et l'impact d'une attaque sont faibles ;
- **classe 2 :** le risque ou l'impact d'une attaque est significatif ;
- **classe 3 :** le risque ou l'impact d'une attaque est critique.

Afin de limiter les contraintes sur les équipements de classe 2 tout en réduisant la complexité technique et opérationnelle de l'ensemble, il a été décidé de regrouper les éléments de classe 2 avec ceux de classe 3.

Le résultat de l'analyse est illustré par la vue métier, reproduite dans la figure 2.

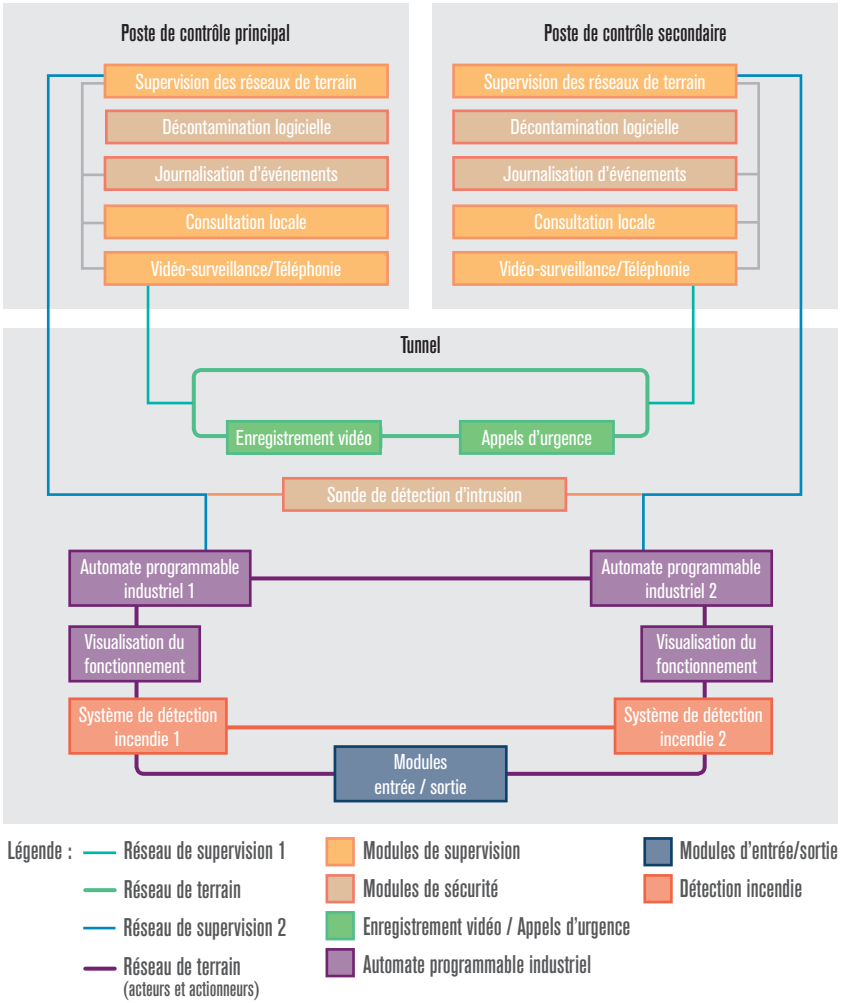
Figure 2 – Vue métier du système d'information



À partir de cette analyse et de l'organisation métier qui en découle, une déclinaison plus complète de l'ensemble des mesures principales présentées dans *La Cybersécurité des systèmes industriels* dont sont issus les schémas d'architecture a été effectuée.

La vue applicative reproduite sur la figure 3 fait apparaître les différents modules applicatifs qui contribuent à la sécurisation du système industriel.

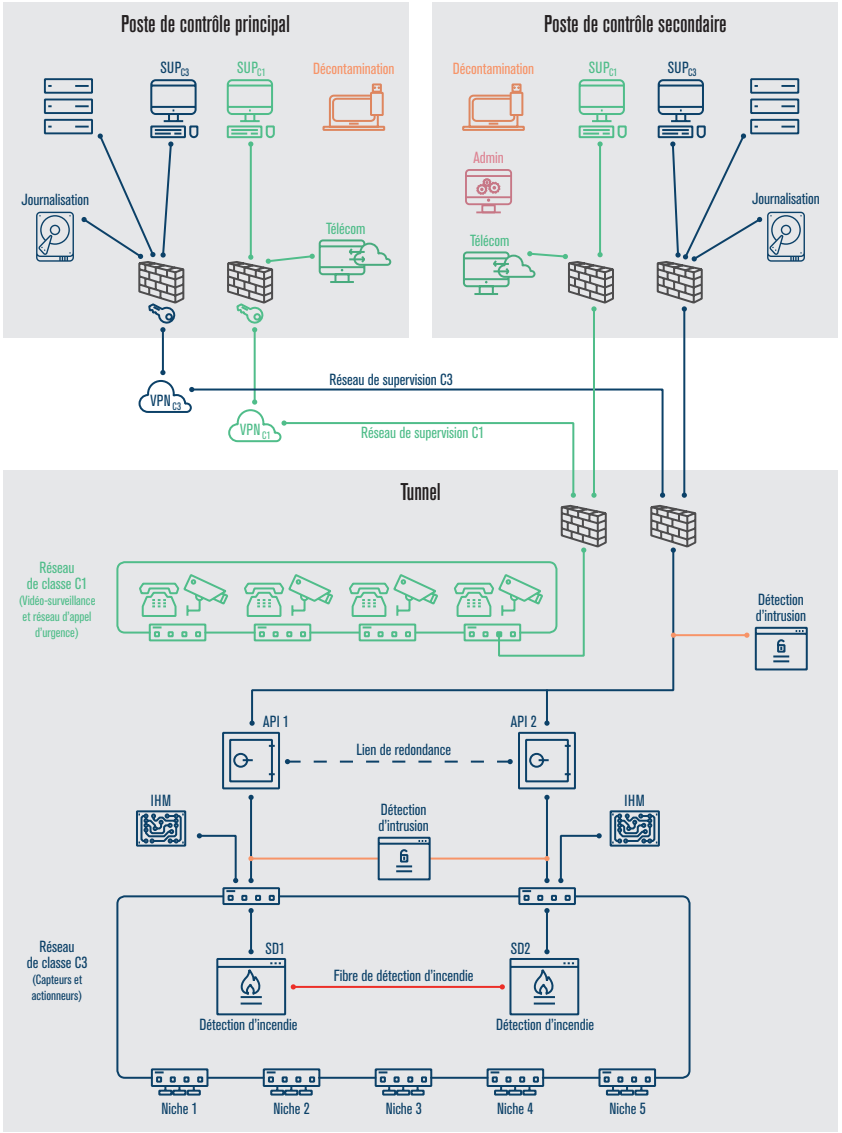
Figure 3 – Vue applicative du système d'information



La vue de l'architecture technique du système d'information est reproduite quant à elle sur la figure 4.

Cette vue permet de constater que les réseaux de terrain des classes 1 et 3 sont disjoints. Les équipements qui y sont raccordés sont pilotés depuis un poste de supervision dédié. Sur chaque site, on trouve également un poste de décontamination qui n'est relié à aucun réseau. À l'entrée du tunnel sur le site secondaire, un poste d'administration est placé dans un coffre. Il est dédié aux interventions sur les équipements ne pouvant être administrés que localement.

Figure 4 – Vue de l'infrastructure technique du système d'information



ANNEXE 4
GLOSSAIRE

Acteur	Représentant d'un rôle métier qui exécute des opérations, utilise des applications et prend des décisions dans le cadre des processus. Ce rôle peut être porté par une personne, un groupe de personnes ou une entité.
Activité	Étape nécessaire à la réalisation d'un processus. Elle correspond à un savoir-faire spécifique et pas forcément à une structure organisationnelle de l'entreprise.
Application	Ensemble cohérent d'objets informatiques (exécutables, programmes, données…). Elle constitue un regroupement de services applicatifs.
Baie	Armoire technique rassemblant des équipements de réseau informatique ou de téléphonie.
Base de données	Ensemble structuré et ordonné d'informations destinées à être exploitées informatiquement.
Bâtiment / Salle	Localisation des personnes ou ressources à l'intérieur d'un site.
Bloc applicatif	Ensemble d'applications.
Borne wifi	Matériel permettant l'accès au réseau sans fil wifi.
Commutateur (*switch*)	Composant gérant les connexions entre les différents serveurs au sein d'un réseau.
DICT	Besoins de sécurité : Disponibilité, Intégrité, Confidentialité, Traçabilité.
Domaine Active Directory/ LDAP	Ensemble d'éléments (membres, ressources) régis par une même politique de sécurité.
DMZ	*Demilitarized zone* – Zone réseau isolée à la fois du réseau interne et du réseau externe, contenant les services accessibles depuis l'extérieur
Entité ou système	Partie de l'organisme (ex. : filiale, département, etc.) ou système d'information en relation avec le SI qui vise à être cartographié.
Équipement de sécurité	Composant permettant la supervision du réseau, la détection d'incidents, la protection des équipements ou ayant une fonction de sécurisation du système d'information.
Flux	Échange d'informations entre un émetteur ou un récepteur (service applicatif, application ou acteur).
Forêt Active Directory/ Arborescence LDAP	Regroupement organisé de domaines Active Directory/LDAP.
Information	Donnée faisant l'objet d'un traitement informatique.
Infrastructure de stockage	Support physique ou réseau de stockage de données : serveur de stockage en réseau (NAS), réseau de stockage (SAN), disque dur…
LAN	Réseau informatique reliant des équipements sur une aire géographique réduite.
Macro-processus	Ensemble de processus.
MAN	Réseau informatique reliant des équipements sur des distances moyennement importantes. Il interconnecte généralement des LAN entre eux.
Module	Composant d'une application caractérisé par une cohérence fonctionnelle en matière d'informatique et une homogénéité technologique.
Opération	Étape d'une procédure correspondant à l'intervention d'un acteur dans le cadre d'une activité.
Passerelle d'entrée depuis l'extérieur	Composant permettant de relier un réseau local avec l'extérieur.
Périphérique	Composant physique connecté à un poste de travail afin d'ajouter de nouvelles fonctionnalités (ex. : clavier, souris, imprimante, scanner, etc.).
Poste de travail	Machine physique permettant à un utilisateur d'accéder au système d'information.
Processus	Ensemble d'activités concourant à un objectif. Le processus produit des informations (de sortie) à valeur ajoutée (sous forme de livrables) à partir d'informations (d'entrées) produites par d'autres processus.
Relation	Lien entre deux entités ou systèmes.
Réseau	Ensemble d'équipements reliés logiquement entre eux et qui échangent des informations.
Routeur	Composant gérant les connexions entre différents réseaux.
Serveur DHCP	Équipement physique ou virtuel permettant la gestion des adresses IP d'un réseau.
Serveur DNS	Serveur de noms de domaine (*Domain Name System*) – Équipement physique ou virtuel permettant la conversion d'un nom de domaine en adresse IP.
Serveur logique	Découpage logique d'un serveur physique.
Serveur physique	Machine physique exécutant un ensemble de services informatiques.
Service applicatif	Élément de découpage de l'application mis à disposition de l'utilisateur final dans le cadre de son travail. Un service applicatif peut, par exemple, être un service dans le nuage (Cloud).
Service d'annuaire d'administration	Applicatif regroupant les données sur les utilisateurs ou équipements informatiques de l'entreprise et permettant leur administration.
SIEM	*Security Information and Event Management* – outil de gestion et de corrélation de logs.
Site	Emplacement géographique rassemblant un ensemble de personnes et/ou de ressources.

Sous-réseau	Subdivision logique d'un réseau de taille plus importante.
Tâche	Activité élémentaire exercée par une fonction organisationnelle et constituant une unité indivisible de travail dans la chaîne de valeur ajoutée d'un processus.
Téléphone	Téléphone fixe ou portable appartenant à l'organisation.
Urbanisation	La démarche d'urbanisation des systèmes d'information consiste à transformer et aligner les actifs d'une organisation (technologies d'information et de communication, personnels, projets, processus) avec ses caractéristiques opérationnelles propres, sa stratégie d'évolution et son champ de contraintes, le tout dans un cadre formel, compréhensible et partagé (Cadre commun d'urbanisation du SI de l'État, DINSIC, 2012)
VLAN	Réseau local (LAN) virtuel permettant de regrouper logiquement des équipements en s'affranchissant des contraintes physiques.
WAN	Réseau informatique reliant des équipements sur des distances importantes. Il interconnecte généralement des MAN ou LAN entre eux.
Zone d'administration	Ensemble de ressources (personnes, données, équipements) sous la responsabilité d'un (ou plusieurs) administrateur(s).

Version 1.0 - Novembre 2018
ANSSI-PA-046

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI - 51, boulevard de la Tour-Maubourg - 75700 PARIS 07 SP
www.ssi.gouv.fr/ communication@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre