

Evolution du SI

V. 1.0 juillet 2019

Evolution du SI

- La fonction IT
- La stratégie IT
- L'urbanisation
- Les principes d'évolution des SI
 - cartographie du système d'information
 - Open data, Open innovation, Bring Your Own Device

Cartographie du SI

Qu'est-ce qu'une cartographie ?

Pourquoi réaliser une cartographie de son système d'information ?

Comment construire une cartographie du système d'information ?

Facteurs clés de réussite

Cartographie du SI

cartographie : représentation schématique d'un ensemble d'informations.

la cartographie du permet de représenter le système d'information d'une entité ainsi que ses connexions avec l'extérieur :

- biens **matériels**,
- **logiciels**,
- les **réseaux** de connexion,
- et les informations, activités et processus qui reposent sur ces biens

Cartographie du SI

Objectifs :

- réaliser l'inventaire patrimonial du système d'information (liste des composants du SI et leur description)
- présenter le système d'information sous forme de vues (représentations partielles du SI) de ses liens et de son fonctionnement.
- rendre lisibles et compréhensibles différents aspects du système d'information.

Cartographie du SI : composition

0. Vue de l'écosystème

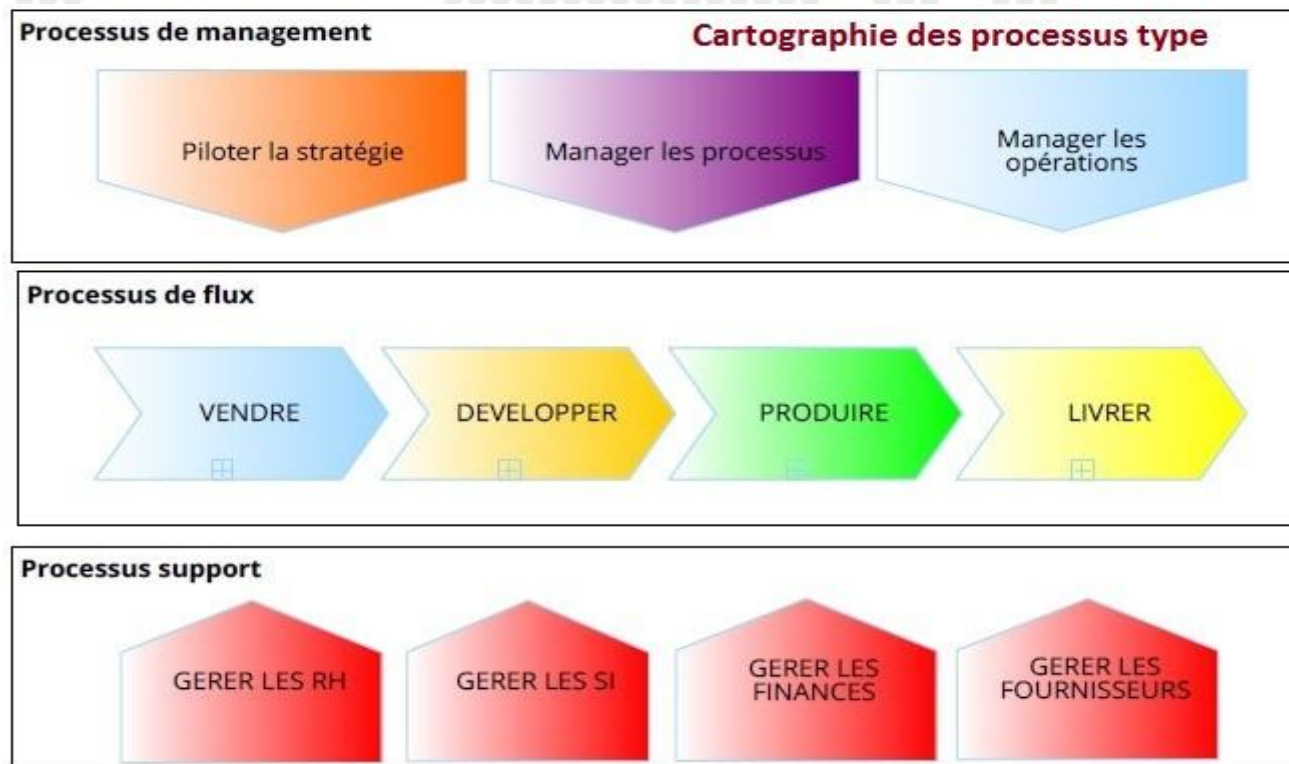
La vue de l'écosystème décrit **l'ensemble des entités ou systèmes qui gravitent autour du système d'information** considéré dans le cadre de la cartographie. Cette vue permet à la fois de délimiter le **périmètre de la cartographie**, mais aussi de disposer d'une **vision d'ensemble de l'écosystème**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

Objet	Attribut
Entité ou système	Identification et description
	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
	Point de contact sécurité de l'entité (ex. : RSSI)
Relation	Nature (ex. : fourniture de biens, de services, partenariat commercial, etc.)
	Lien contractuel ou réglementaire
	Niveau d'importance fonctionnelle de la relation

Cartographie du SI : composition

1. Vision métier (processus)

- Présentation des différentes entités ou systèmes avec lesquels le SI interagit pour remplir sa fonction.



Cartographie du SI : composition

1. Vision métier (processus)

Objet	Attribut
Macro-processus	Identification et description
	Éléments entrants et sortants
	Liste des processus qui le composent
	Besoins de sécurité (DICT)
	Propriétaire
Processus	Identification et description
	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
	Liste des applications qui le soutiennent
	Besoins de sécurité (DICT)
	Propriétaire
Activité	Identification et description
	Liste des opérations qui la composent
Opération	Identification et description
	Liste des tâches qui la composent
	Liste des acteurs qui interviennent
Tâche	Identification et description
Acteur	Nom et moyens de contact
	Nature : personne, groupe, entité, etc.
	Type : interne ou externe à l'organisme

Cartographie du SI : composition

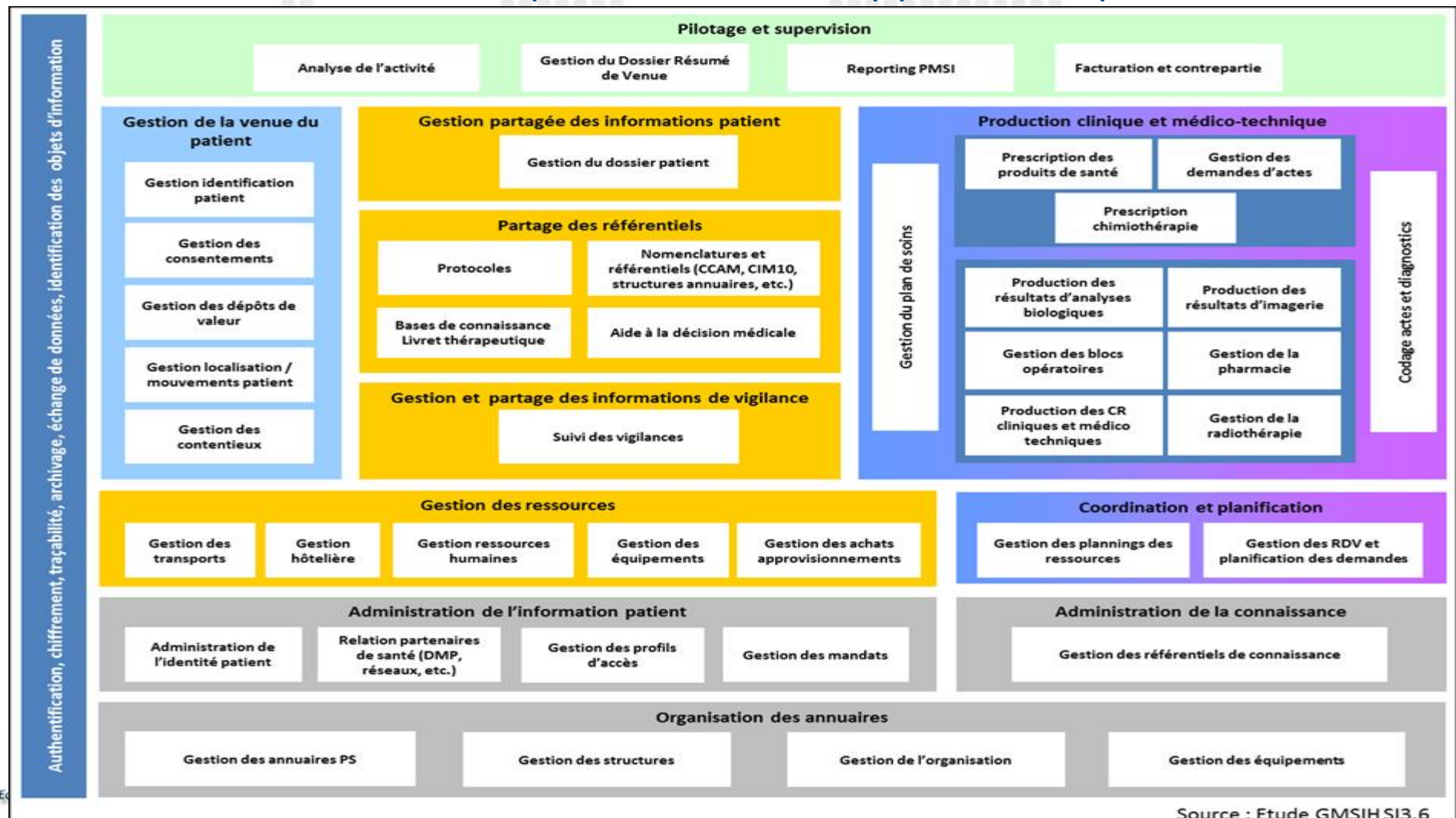
1. Vision métier (processus)

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

Cartographie du SI : composition

2. Vision fonctionnelle

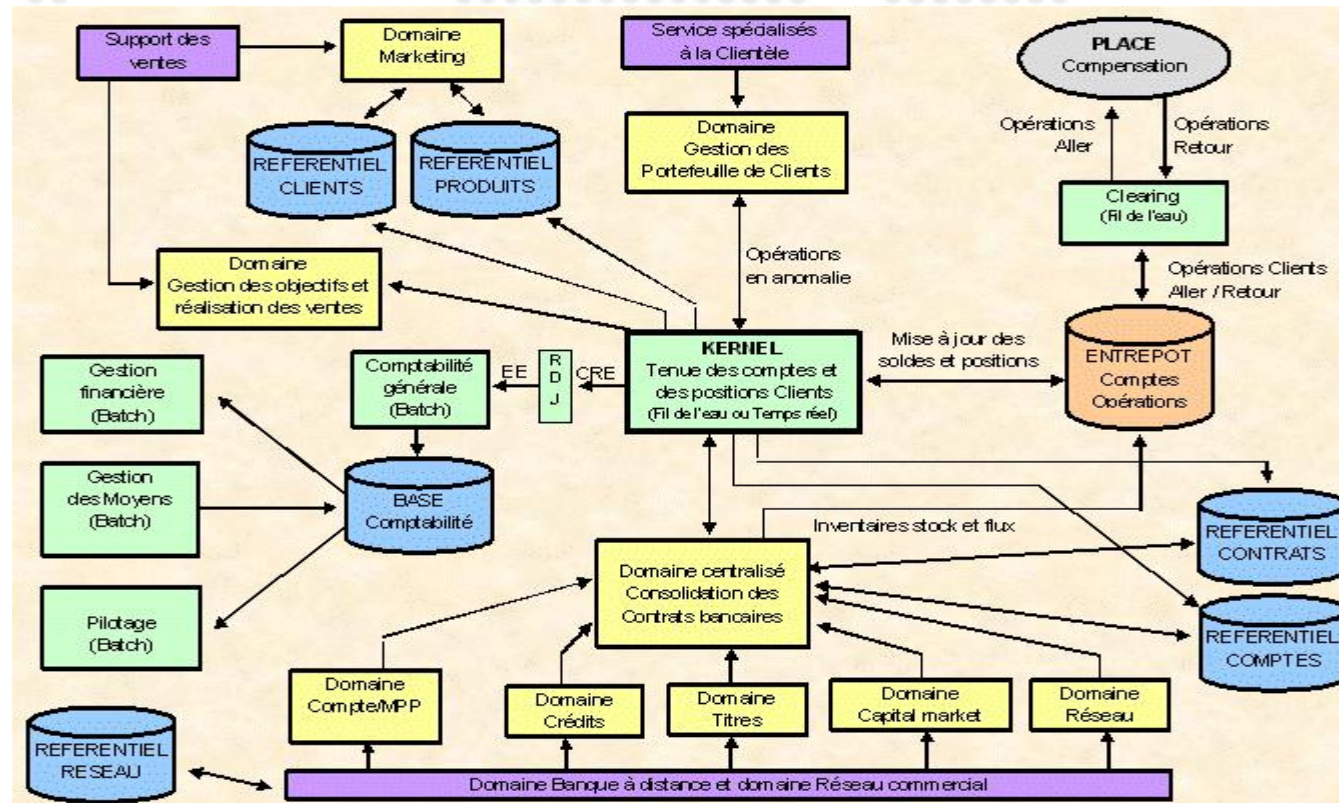
- Décrit les fonctions du SI permettant de supporter les processus



Cartographie du SI : composition

3. 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.



Cartographie du SI : composition

3. Vision applicative

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

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

Cartographie du SI : composition

4. Vision administrative



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**.

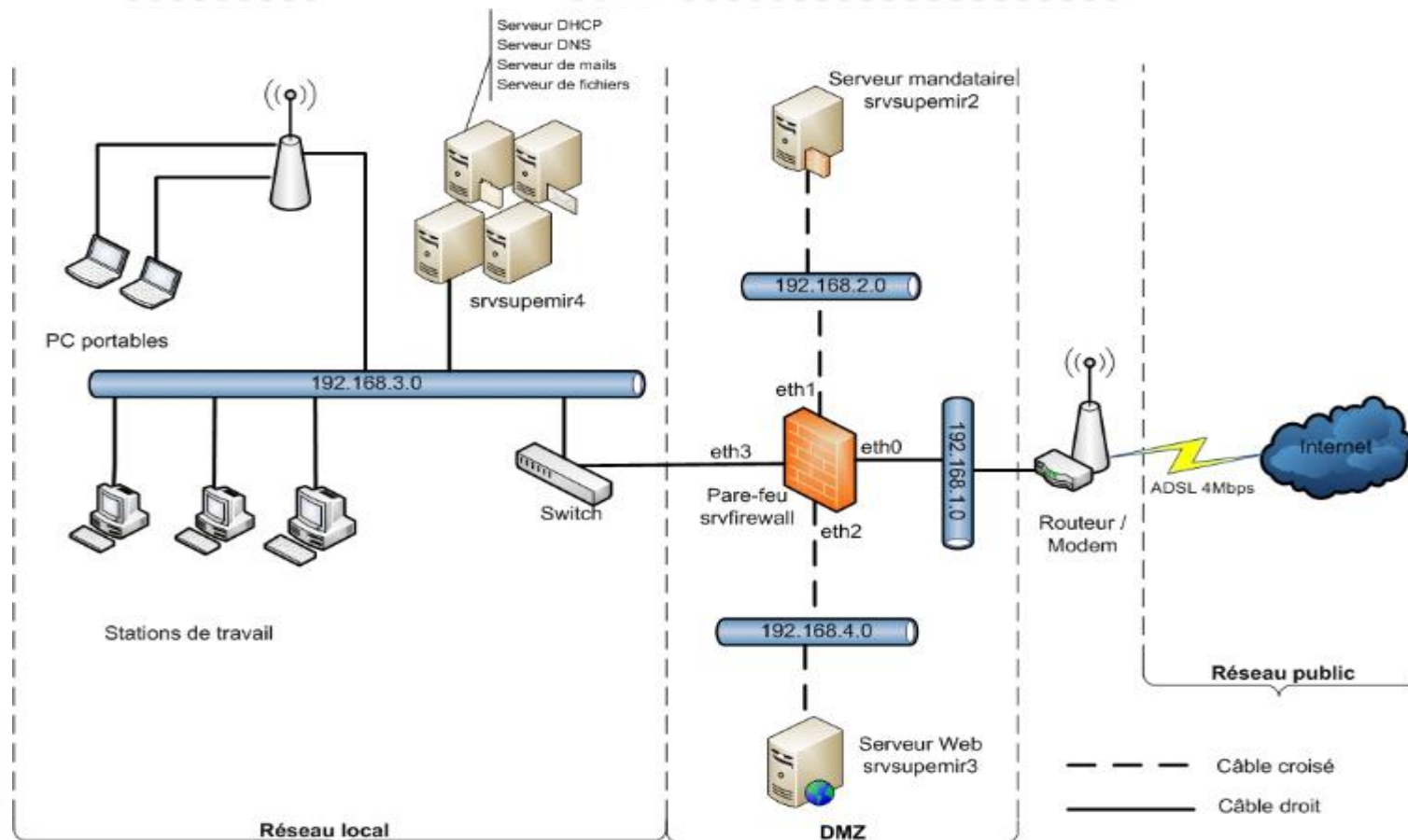
La représentation schématique de cette vue n'est utile que s'il existe une gestion centralisée des droits d'administration sur les équipements comportant plusieurs périmètres d'administration. Dans le cas où les droits sur les équipements sont gérés par des comptes locaux, elle est réduite à la constitution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

Cartographie du SI : composition

4a. Vision infrastructure logique (technique)

- 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 ;



Cartographie du SI : composition

4a. Vision infrastructure logique (technique)

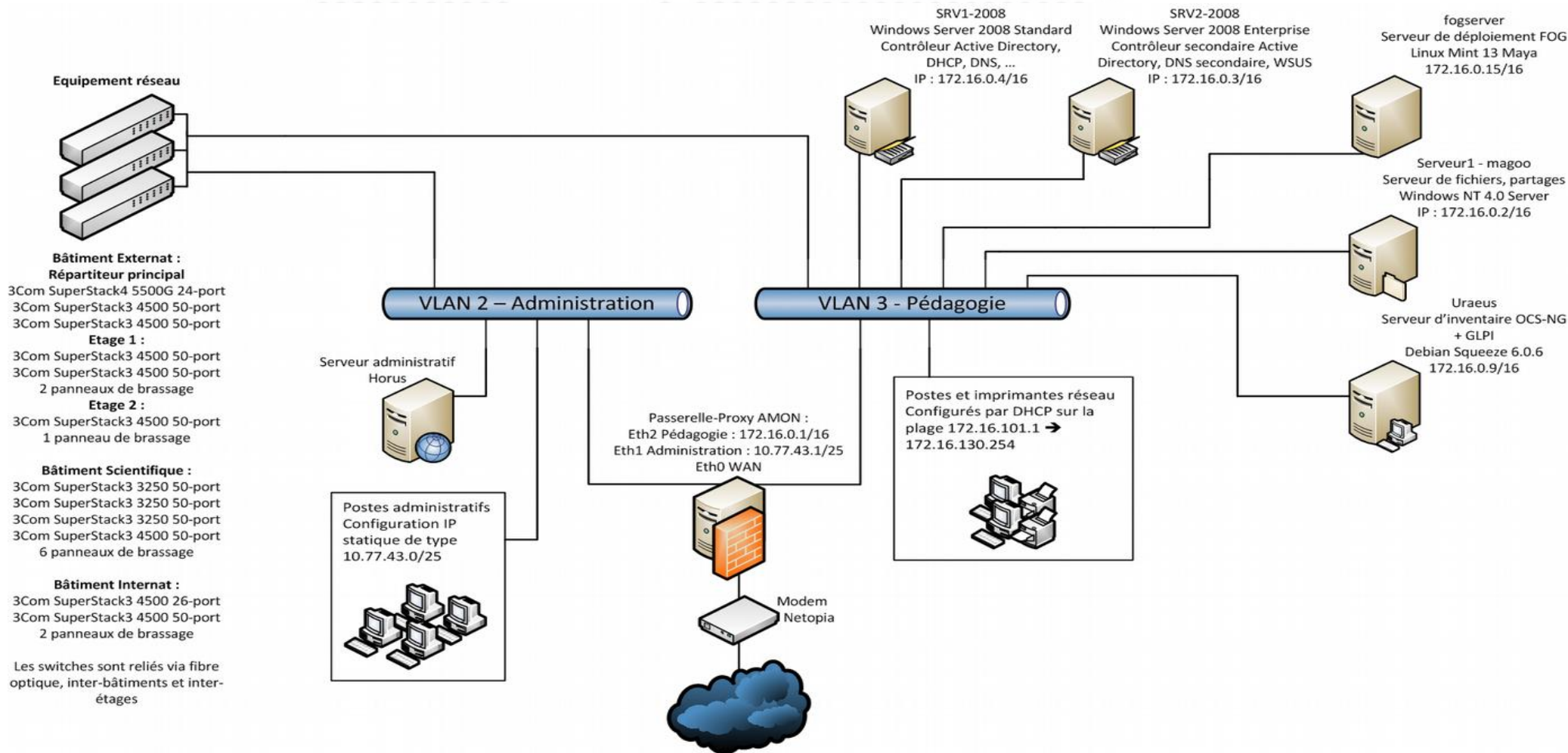
Objet	Attribut
Réseau	Identification et description
	Type de protocole
	Responsable d'exploitation
	Responsable SSI
	Sous-réseaux rattachés
	Niveau de sensibilité ou de classification
Sous-réseau	Identification et description
	Adresse/Masque
	Passerelle
	Plage d'adresses IP : adresse de début, de fin
	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
	IP publique et privée
	Type d'authentification
Entité extérieure connectée	Nom, Responsable SSI, contacts SSI
	Réseaux internes interconnectés à l'entité

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

Cartographie du SI : composition

4b. Vision infrastructure physique (technique)

- La vue des infrastructures physiques décrit les équipements physiques qui composent le système d'information ou utilisés par celui-ci.



Cartographie du SI : composition

4b. Vision infrastructure physique (technique)

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

Objet	Attribut
Périphérique	Identification
	Caractéristiques techniques : type (imprimante, scanner, etc.), modèle
	Responsable d'exploitation
Téléphone	Identification
	Caractéristiques techniques : type (fixe ou portable), modèle
	Emplacement physique : site, bâtiment, salle
Commutateur physique	Identification
	Commutateur(s) logique(s) rattaché(s)
	Caractéristiques techniques : niveau (L1, L2, L3, etc.), modèle, version du logiciel embarqué
	Emplacement physique : site, bâtiment, salle, baie
	VLAN associé
Routeur physique	Identification
	Routeur logique associé
	Caractéristiques techniques : modèle, version du logiciel embarqué
	Emplacement physique : site, bâtiment, salle, baie
	VLAN associé
Borne wifi	Identification
	Caractéristiques techniques : modèle
	Emplacement physique : site, bâtiment, salle, baie
Équipement de sécurité physique	Identification (identifiant, adresse IP, adresse MAC) et description
	Équipement(s) de sécurité logique(s) rattaché(s)
	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
	MAN ou LAN rattachés

Objet	Attribut
MAN	Identification
	LAN rattachés
LAN	Identification
VLAN	Identification et description
	Commutateurs associés

Cartographie du SI : composition

Pourquoi avoir fait ces différents travaux de cartographie ?

- Avoir une vue globale à différents niveaux pour maîtriser un SI souvent complexe
- Partager cette vue au sein de l'entreprise
- Participer aux travaux d'urbanisation
- Maîtriser autant que possible la sécurité globale du SI (identifier les points critiques, imaginer et anticiper les attaques)
- Réagir plus rapidement en cas d'attaque du SI
- Servir de base aux PRA/PCA
- Permettre une évolution cohérente à C/P/R maîtrisés

Construire sa Cartographie du SI

Le travail à réaliser est potentiellement immense et sans fin.

Il faut être pragmatique, s'inscrire dans le temps avec une collaboration constante.

C'est un processus qui s'appuie sur les cartes déjà réalisées.

Cela peut se faire schématiquement en 5 étapes.



Construire sa Cartographie du SI

Étape 1a : initier la démarche

Il faut impliquer la DSI, le RSSI et les directions métiers.

Étape 1b : définir le périmètre

Le périmètre étant large, il faut commencer par définir ce qui est critique et le plus vulnérable (du point de vue de la sécurité, des finances, de la production, ...).

Construire sa Cartographie du SI

Étape 2 : se mettre d'accord sur un modèle de cartographie

Il convient de choisir les objets et attributs à représenter ainsi que leur format.

Les relations entre les objets peuvent aussi faire partie du modèle.

Les attributs sont des informations essentielles aux futures analyses, dont certaines ont trait à la sécurité numérique.

La convention de représentation des cartes.

Exemple : pour la carte applicative, on peut choisir de faire figurer chaque application, sa/ses directions métier utilisatrices, distinguer son origine (développement interne, logiciel, progiciel, etc.), ses besoins de sécurité, son exposition vis-à-vis de l'extérieur.

NB : il faut trouver un équilibre entre l'exhaustivité, les efforts pour créer et maintenir les cartes, la lisibilités, etc...

Construire sa Cartographie du SI

Étape 3 : se doter d'outils

Les outils choisis doivent satisfaire les besoins suivants :

- 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 n'y a pas d'outils parfait. Il sera bon de s'appuyer sur les outils de gestion de parc, d'adressage réseau, etc.

Construire sa Cartographie du SI

Étape 4 : construire pas à pas

La cartographie se fait de façon à la fois itérative (on améliore ou amende les cartes existantes) et incrémentale (on ajoute de nouvelles cartes).

Les cartes doivent être datées et versionnées.

NB : certaines informations peuvent être critique, le RSSI doit valider le niveau d'accès et de diffusion des cartes réalisées.

Construire sa Cartographie du SI

Étape 4 : pérenniser la démarche

4.a. La cartographie doit régulièrement être communiquées aux acteurs en respectant les éventuels niveaux de confidentialité.

4.b La cartographie doit être mise à jour via un processus d'amélioration continue.

4.c Une gouvernance doit être établie sur ce processus. En particulier, on doit pouvoir répondre aux questions :

- 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 ?

Facteurs Clés de Succès de la Cartographie du SI

La démarche de cartographie est complexe et se heurte à des difficultés organisationnelles, humaines, techniques ou calendaires.

1. Travailler en mode projet au sein d'un processus clair impliquant les directions métiers.
2. Travailler par itérations.
3. Se définir un langage commun pour la cartographie.
4. Communiquer à toutes les étapes.
5. Entretenir la cartographie (retour au processus).

Cartographie du SI : cas pratique

L'exemple ci-après a été produit par l'ANSSI.

Il s'agit d'étudier le SI d'une infrastructure routière (un tunnel) avec une approche plutôt axée sur la sécurité.



Cette annexe propose un exemple d'application s'appuyant sur une étude de cas sur un tunnel routier réalisée par l'ANSSI¹⁵.

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.

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 (télémessures, téléalarmes, télésignalisation) : la supervision ;
- le contrôle des équipements par envoi de télécommandes et de téléajustages : 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.

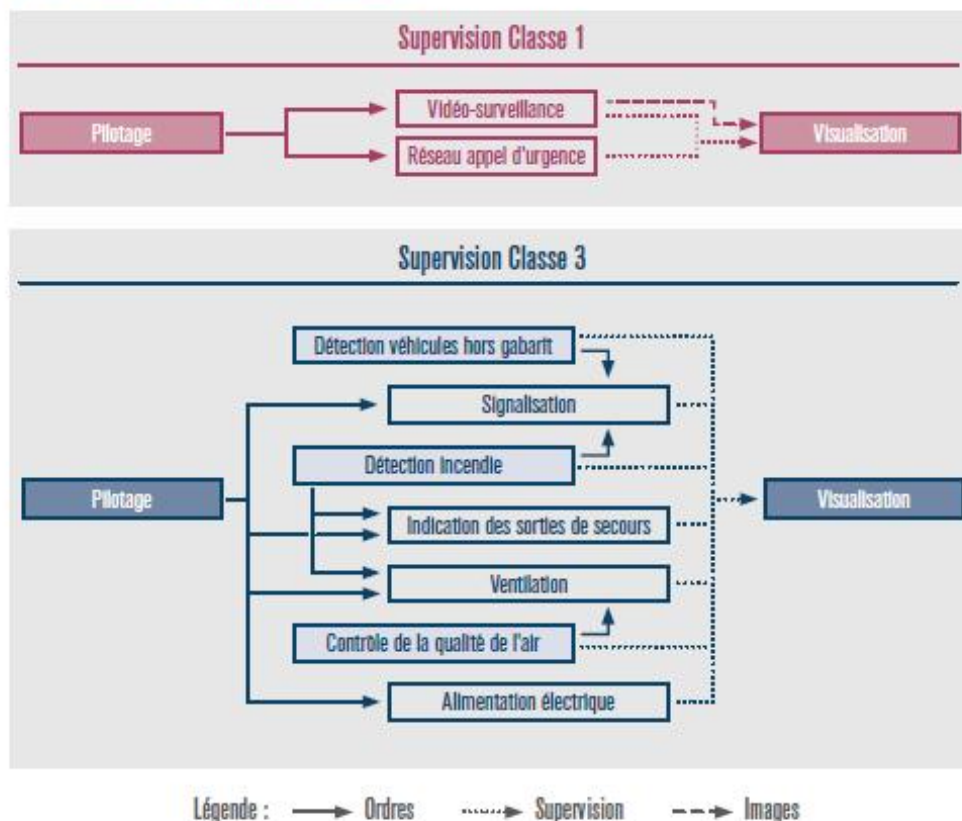
Pour les systèmes industriels, la méthode formalisée dans le guide propose trois classes numérotées de 1 à 3, par ordre croissant de criticité et dont les couvertures sont :

- 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



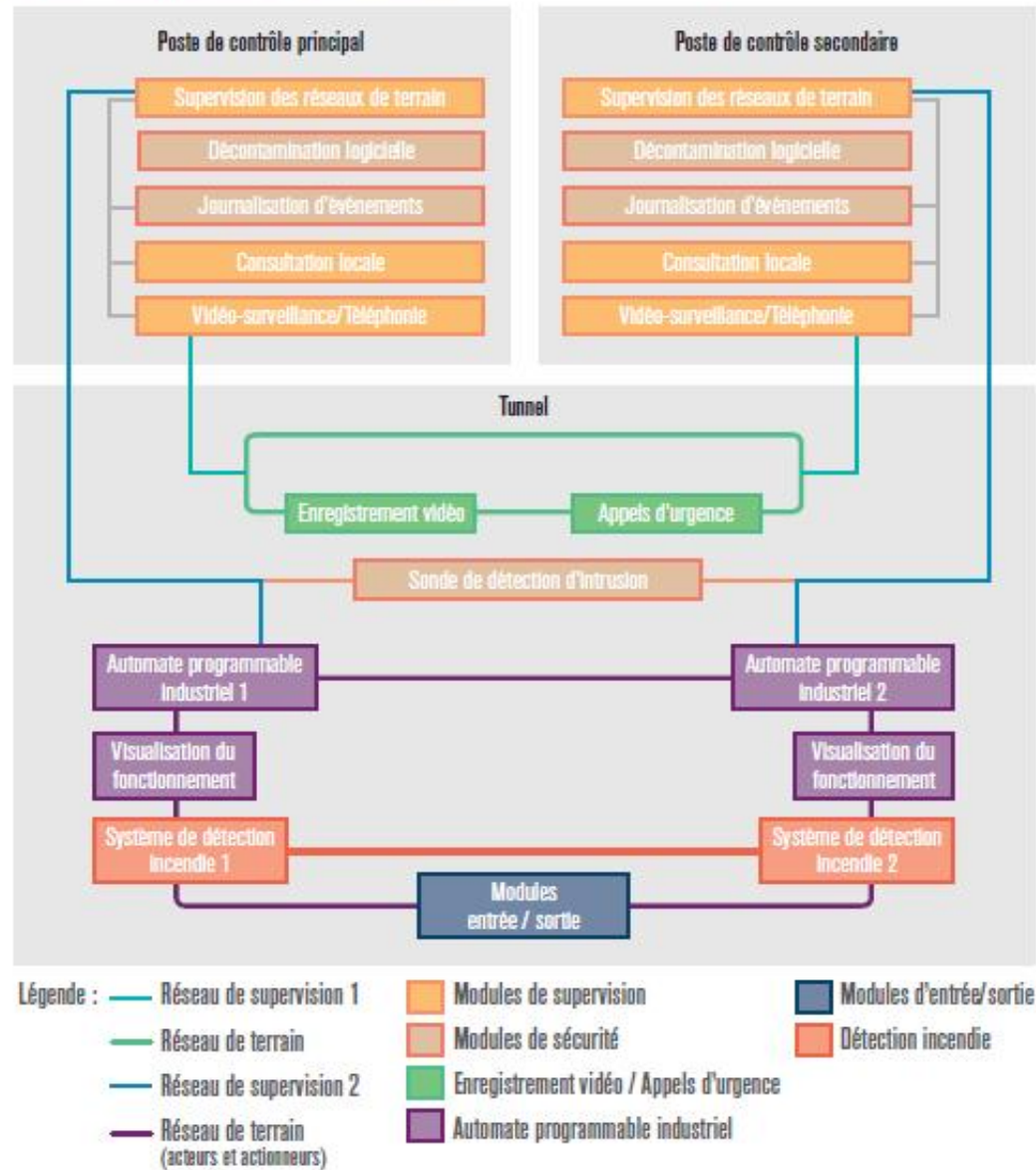
Question 1

D'après vous, quels types de métiers (services de l'entreprise) sont impliqués dans la description de la vue métier ?

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



Question 2

D'après vous, pourquoi les concepteurs de la vue applicative ont-ils doublé une partie de leur schéma ?

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.

Questions 3

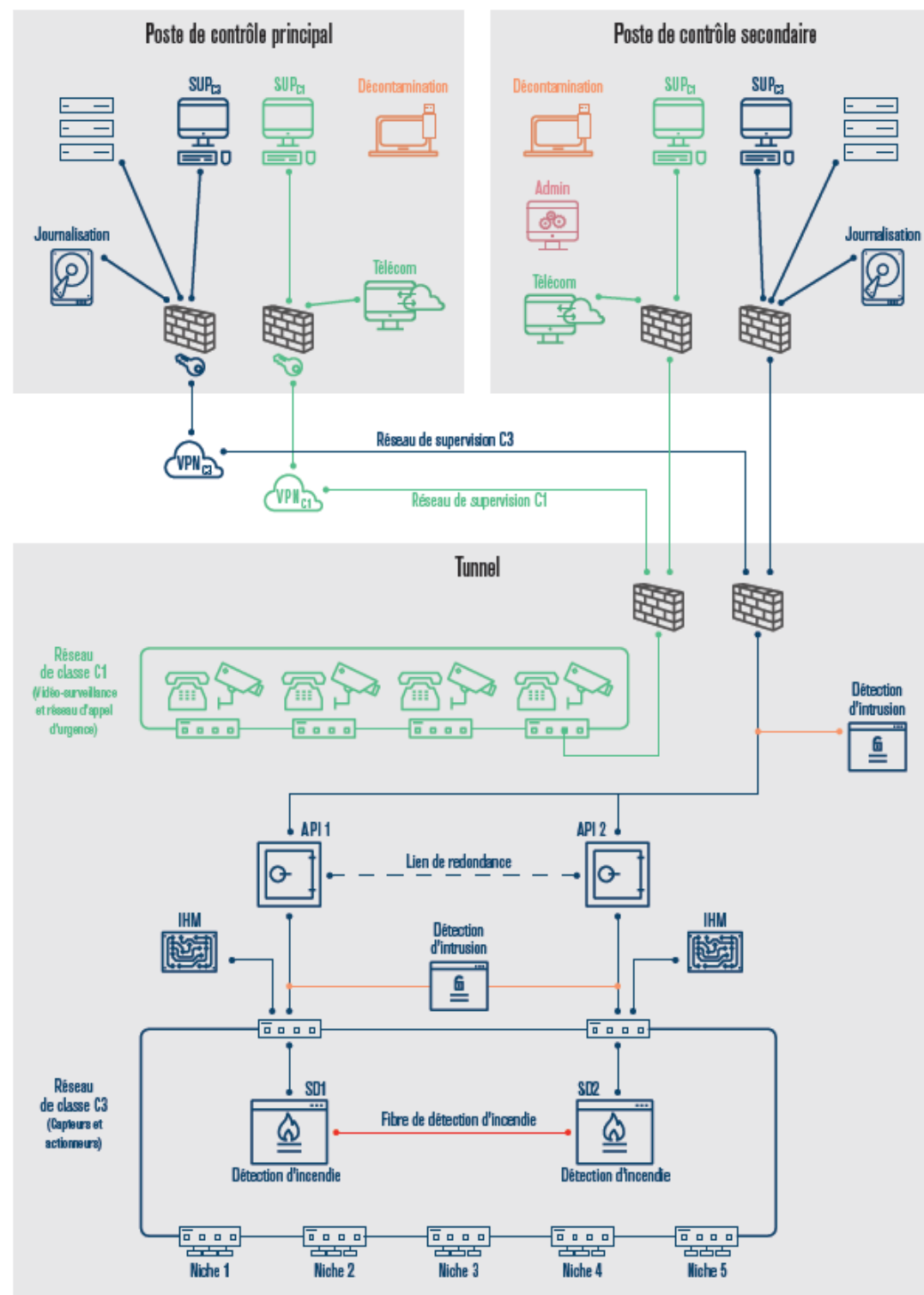
Combien y-a-t-il de sous-réseaux isolés pour gérer ce tunnel routier ?

Par combien de caméras est-il surveillé ?

Sur quel(s) site(s) se trouve(nt) le(s) poste(s) d'administration général ?

Sur quel(s) site(s) se trouve(nt) le(s) poste(s) de détection d'intrusion ?

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



Stratégie IT : schéma directeur

« CARTOGRAPHIE DU SYSTÈME D'INFORMATION Guide d'élaboration en 5 étapes, »
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION ANSSI - 51,
boulevard de la Tour-Maubourg - 75700 PARIS 07 Sp www.ssi.gouv.fr/

<https://www.supinfo.com/articles/single/8139-cartographie-si-cartographie-risques>

<https://www.ssi.gouv.fr/uploads/2018/11/guide-cartographie-systeme-information-anssi-pa-046.pdf>

http://democritique.org/TI/URSI_Teaching_Class.svg.xhtml