R2S®

4 CARE

Le cadre de référence du Smart Hospital

Comment mettre le numérique au service du bâtiment hospitalier et de tous ses usagers

Mai 2026

SBA

Remerciements

La Smart Buildings Alliance remercie chaleureusement toutes les personnes qui ont contribué à la réalisation de cet ouvrage, l'ensemble des membres de la commission Smart Hospital de la SBA, ainsi que les membres du club RéuSITH animé par **Eric Bardouillet**, Responsable du service technique et biomédical au CHIC Marmande Tonneins, et **Frédéric Hamon**, ingénieur hospitalier au CHU de Nantes.

Ce cadre de référence n'aurait pu voir le jour sans, **Christophe Clément-Cottuz** (CCube Expertise) et **Jérémy Dréan** (Artelia), co-Présidents de la commission Smart Hospital, qui animent ce groupe de travail depuis plusieurs années.

Nous remercions également **François Reynier**, Expert Immobilier de l'ANAP pour sa contribution, le bureau et le conseil d'administration de la SBA, ainsi que tous les acteurs de l'écosystème hospitalier avec qui nous avons pu échanger et faire grandir notre vision du Smart Hospital.

Conception graphique et illustrations : Marie Boscher
Imprimé en France

À propos de la commission Smart Hospital de la SBA

De l'idée stratégique d'un hôpital numérique ou digital à sa réalisation concrète ne restent souvent que des modèles de conception qui contournent ou ignorent la transformation des organisations portée par la numérisation des activités. Passer de l'idée de Smart Hospital à sa réalisation concrète est difficile du fait que ce n'est pas seulement un projet technologique mais une transformation systémique ; transformer un système aussi complexe qu'un hôpital demande de changer en même temps des infrastructures, des pratiques, des cultures professionnelles et des modèles économiques.

C'est de ce constat qu'est née l'idée d'un groupe de travail Smart Hospital au sein de la SBA. Son objectif est de concevoir de manière collaborative un outil de création de programmation Smart qui puisse, aux côtés de leurs conseils et programmistes, aider les décideurs, conducteurs d'opérations et les ingénieurs chefs de projet à porter au bout leur projet de Smart Hospital.

À propos du club RéuSITH

Le club RéuSITH (Réflexions, Études, et Usages du Système d'Information Technique Hospitalier) est constitué d'ingénieurs et de techniciens issus des différents domaines logistiques de l'hôpital (services techniques, biomédicaux, informatiques, ...).
Ce groupe de travail a pour ambition de proposer une architecture numérique intégrée adaptée aux métiers techniques de l'hôpital.

Grâce aux travaux de ses différentes commissions, aux échanges entre établissements et aux rencontres avec les industriels, l'objectif opérationnel du club RéuSITH est de mettre à la disposition de la communauté hospitalière un référentiel de propositions, de retours d'expériences et de bonnes pratiques. Son partenariat croissant avec la commission Smart Hospital de la SBA est révélateur de sa vision holistique commune du Smart Hospital.

RéuSITH
Réflexions Études Usages du Système Information Technique Hospitalier

CENTRE HOSPITALIER MARMANDE · TONNEINS

CHU NANTES

Préambule

Qu'est-ce que le cadre de référence Ready to Services for Care ?

Le présent document constitue le cadre de référence « Ready to Services for Care » (ou « R2S4 Care » ou « R2S4C »). Un cadre de référence sert à exposer un point de vue commun et structuré et est constitué de principes déclinés en recommandations. Il propose une vision organisée, afin d'accompagner les acteurs dans la mise en œuvre opérationnelle d'un projet Smart Hospital. Il se distingue d'un label, dans le sens où le cadre de référence précise ce qui doit être mis en place, mais ne comprend pas un processus menant à l'obtention d'une labellisation. Concrètement, le cadre de référence va décrire des thématiques et recommandations répondant aux enjeux du sujet, mais ne comprend pas d'intervention de la part d'un acteur tiers (audits, rapports de vérification...).

À qui est destiné ce cadre de référence ?

Ce cadre méthodologique a vocation à accompagner tous les acteurs du bâtiment hospitalier dans leur transformation numérique et leur transition environnementale. Il s'adresse à tous les professionnels qui recherchent une aide méthodologique dans la mise en application d'un projet de Smart Hospital ou de bâtiment hospitalier connecté et communicant, dans le cadre d'une construction neuve ou d'une rénovation, d'un établissement, d'un bâtiment ou d'un pôle de soins, quelle qu'en soit sa taille.

Quels sont les objectifs de ce cadre de référence ?

- Structurer un projet Smart Hospital par conception
- Identifier et sélectionner les services numériques associés au Smart Building qui permettront d'améliorer l'accueil, l'efficacité opérationnelle et la qualité de vie des usagers du bâtiment hospitalier
- Proposer une organisation du projet numérique qui fera de la donnée le quatrième fluide du bâtiment en accompagnant les réflexions sur la gouvernance, le management, l'interopérabilité et la sécurité.
- Déterminer un socle technique et organisationnel sur lequel pourront s'appuyer tous les acteurs concepteurs du projet, et ceux qui proposent des services aux usagers d'un bâtiment hospitalier.
- Définir les conditions qui permettent aux services du bâtiment hospitalier d'évoluer dans le temps en minimisant l'impact sur les équipements et infrastructures de communication éventuellement déjà installées.
- Faciliter la modularité et flexibilité du bâtiment face aux évolutions rapides des techniques médicales, des organisations hospitalières, et des besoins et crises sanitaires, grâce aux infrastructures numériques techniques du bâtiment.
- Ce cadre de référence s'adresse à l'ensemble des métiers et fonctions de l'hôpital, et non uniquement aux services techniques. En effet, le numérique constitue une véritable stratégie d'entreprise et ne peut être cantonné à une seule direction.

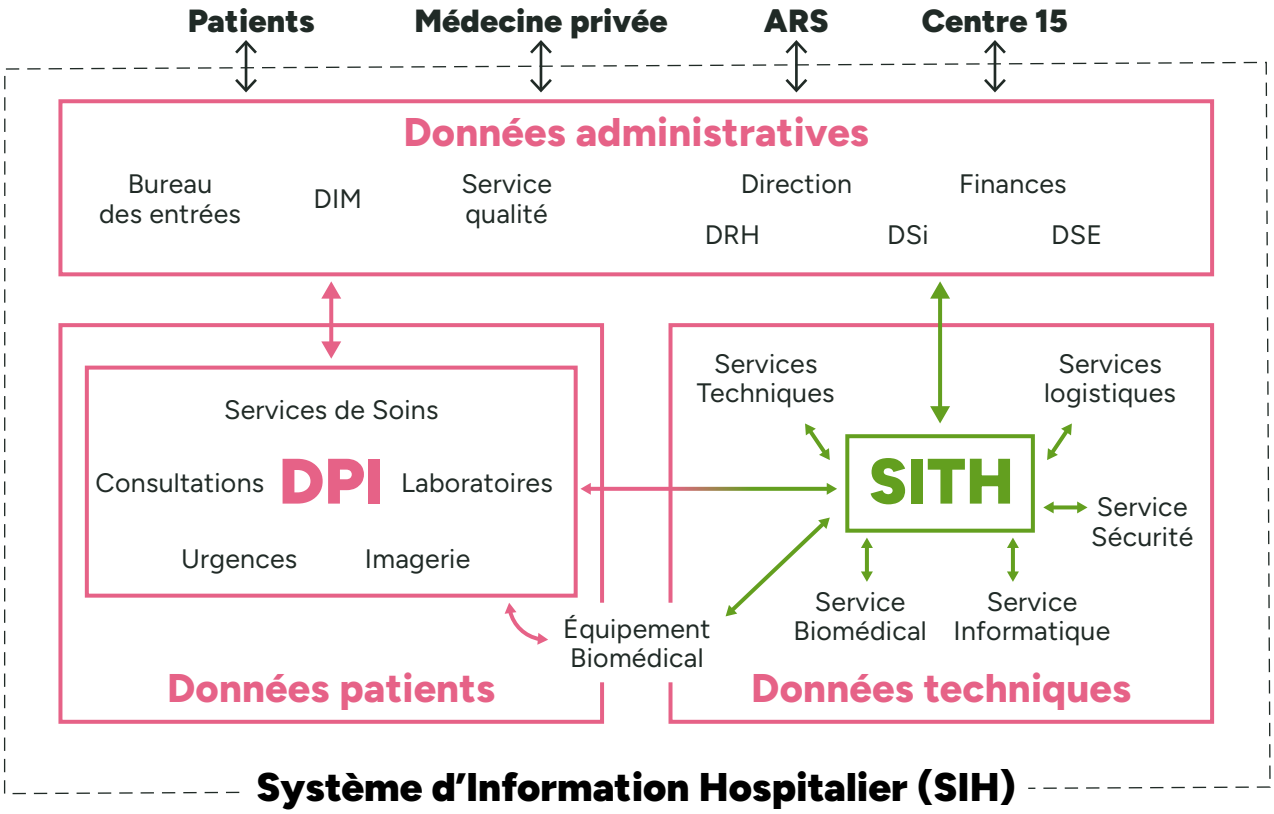
Il concerne autant les équipes médicales, administratives, logistiques ou managériales, qui sont toutes impliquées dans la transformation et l'évolution de l'hôpital connecté et communiquant : le Smart Hospital.

Le SITH est le périmètre technique couvert par le cadre de référence.

Le périmètre du R2S4Care est le Système d'Information Technique Hospitalier (ou SITH). C'est l'ensemble des composants numériques appliqués à un bâtiment ou actif immobilier : logiciels, systèmes et capteurs connectés (OT), réseaux, applications et bases de données (dont font partie les maquettes numériques) relatifs à l'usage de l'ouvrage.

Ce que le cadre de référence R2S for Care ne traite pas :

- Le déploiement des applications du Système d'Information Hospitalier (SIH) (même s'il permet d'échanger des informations avec les applications du Smart Hospital) ;
- Les services numériques minimum usuels attendus dans un établissement hospitalier.



LE SITH EST UNE PARTIE DU SIH

Introduction

QUELQUES DÉFINITIONS

Système d'information hospitalier (SIH)

C'est l'ensemble organisé des applications, données, règles et échanges qui permettent de gérer le fonctionnement d'un établissement de santé, notamment les informations administratives, cliniques, logistiques et financières. Il inclut le SITH.

Le SIH sert à collecter, stocker, traiter et diffuser les informations utiles aux soignants, aux services administratifs et à la direction. En pratique, il soutient la prise en charge du patient, la coordination des équipes et le pilotage de l'hôpital.

Système d'Information Technique Hospitalier (SITH)

C'est l'ensemble des composants numériques appliqués à un bâtiment ou actif immobilier : logiciels, systèmes et capteurs connectés (OT), réseaux, applications et bases de données (dont font partie les maquettes numériques) relatifs à l'usage de l'ouvrage.

Il assure les mécanismes d'interopérabilité, de fiabilité et de consolidation des données générés par ces équipements et permet une gouvernance de données, adaptable à l'ensemble du cycle de vie d'un ouvrage.

Il fait du bâtiment hospitalier, une plateforme de services numériques au service de ses usagers.

Building Operating System (BOS)

Le BOS est une couche logicielle d'intermédiation intégrée au SITH. Il gère le référentiel partagé du bâtiment, orchestre l'interopérabilité des services, coordonne les échanges de données entre les systèmes. Il contribue à la bonne gouvernance des données de l'ouvrage.

C'est la colonne vertébrale numérique du SITH et du bâtiment. Dans cette approche, la donnée n'est plus considérée comme un simple sous-produit des équipements techniques, mais comme une ressource distribuée et pilotée au même titre que :

- l'électricité ;
- l'eau ;
- les fluides médicaux.

La donnée devient ainsi le « 4e fluide » du bâtiment.

Building Information Modeling (BIM)

Le BIM, ou Building Information Modeling, est une méthode de travail collaborative basée sur une maquette numérique 3D enrichie de données sur le bâtiment, utilisée tout au long de son cycle de vie, de la conception à l'exploitation.

- **Le BIM conception** désigne l'usage de la maquette numérique pendant les phases de programmation, d'architecture, d'ingénierie et de coordination du projet. Il sert surtout à concevoir, coordonner, détecter les conflits et préparer la construction à partir d'une représentation numérique partagée du bâtiment.

– **Le BIM GEM** (Gestion d'Exploitation et de Maintenance) correspond à l'usage du BIM une fois le bâtiment livré, pour exploiter les données de la maquette dans la maintenance, la gestion patrimoniale, la GMAO et le suivi des équipements.

Réseau « Smart »

Le réseau « Smart » est le réseau fédérateur d'un bâtiment R2S, orienté services (SOA) et utilisant le protocole IP. Il est sécurisé et utilise exclusivement le standard Ethernet sur le réseau local et le standard Internet depuis l'extérieur du bâtiment. Les écosystèmes matériels, quel que soit leur protocole, communiquent sur le réseau « Smart », à l'aide d'API ou de Web Services exposées sur le « réseau « Smart » » et sur le World Wide Web. Le périmètre du réseau « Smart » est laissée libre au porteur de la démarche. ».

Espaces hospitaliers et non-hospitaliers

Par défaut, les espaces non-hospitalier et d'activités hospitalières où s'appliquent les niveaux de recommandation du cadre de référence R2S4Care pourront être définies de la façon suivante :

– Espaces non-hospitaliers : espaces du bâtiment susceptibles d'être fréquentés par tous les occupants du bâtiment, les visiteurs, les prestataires en charge de la sécurité/sûreté, de la maintenance et de l'exploitation des systèmes et services du bâtiment, et le public le cas échéant.
– Espaces d'activités hospitalières : espaces du bâtiment fréquentés uniquement par les occupants auxquels ils sont destinés pour leurs activités et par les visiteurs autorisés par les occupants.

Dans le contexte français, la définition des espaces non-hospitalier et des espaces d'activité hospitalière s'appuie sur les référentiels immobiliers mis à disposition par l'ANAP et particulièrement la base OSCIMES qui propose une catégorisation des espaces immobilier entre « Espaces non-hospitaliers » et « Services Hospitaliers ». La nature de chaque espace est définie par le maître d'ouvrage qui devra être en mesure de qualifier la qualité de service attendue en proposant une approche quantitative et qualitative des fréquentations, usages et performances attendus.

LE NUMÉRIQUE AU SERVICE DU BÂTIMENT HOSPITALIER ET DE TOUS SES USAGERS

Le numérique est devenu, en l'espace d'une génération, un moteur central de notre développement économique et un agent puissant de transformation de notre vie quotidienne : une transformation accélérée par l'intelligence artificielle (IA) Il (inter)agit sur les objets qui nous entourent, les lieux où nous vivons, ceux où nous travaillons, sur nos modes de vie en général. De nouveaux objets connectés voient le jour, de nouveaux services apparaissent, et de nouveaux usages émergent, offrant à chacun un choix toujours plus vaste, stimulant ainsi nos capacités d'interaction avec le monde qui nous entoure.

Ce phénomène impacte le secteur du bâtiment et plus particulièrement du bâtiment hospitalier, qui doit relever de nouveaux défis liés à la transition numérique :

– Assurer la continuité et la qualité de service des réseaux de télécommunication et une connexion internet optimale ; l'hôpital est une organisation qui fonctionne 24H/24 et 7j/7Répondre aux demandes de tous les métiers de l'hôpital ;

- Assurer la sécurité des réseaux et la protection des données personnelles ;
- Augmenter la durabilité des installations ;
- Assurer la traçabilité numérique du bâtiment de sa conception, son exploitation et sa destruction.
- Conjuguer révolution numérique et développement durable ;
- Favoriser l'intégration de l'hôpital dans la ville numérique et durable.

La transition numérique implique une nouvelle manière de concevoir, de construire et d'exploiter le bâtiment hospitalier. L'humain doit par ailleurs rester au centre des préoccupations, la raison d'être de l'hôpital étant le soin. La finalité du bâtiment hospitalier est d'apporter aux utilisateurs plus de confort, plus de lien social, plus d'efficacité au travail, pour simplifier leur quotidien, tout en préservant l'environnement.

Deux notions sont à distinguer entre le bâtiment connecté et le bâtiment communicant.

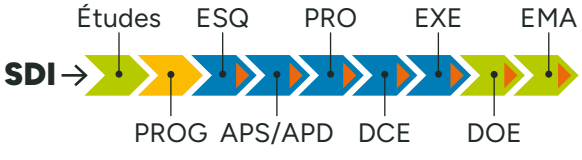
- Un bâtiment connecté est relié de façon physique, sécurisée et résiliente aux réseaux opérateurs ou privés de communication.
- Un bâtiment communicant assure la communication à l'intérieur de son enceinte, en permettant la mise à disposition des données pertinentes en temps réel à n'importe quel endroit afin de répondre à l'ensemble des besoins des usagers. Le Smart Hospital est un bâtiment, plateforme de services riche et évolutive, qui dispose des moyens techniques et organisationnels pour assurer :
- Des communications performantes à l'intérieur de ses murs pour l'ensemble des personnels hospitaliers et des usagers (hôpital communicant) avec un socle de connectivité fiable avec les opérateurs télécom (hôpital connecté),
- L'interopérabilité des systèmes, jadis silotés, en intégrant des standards de communication communs pour mettre le patient au centre du système,
- L'hébergement d'une multitude de services numériques qui facilitera l'adaptation aux évolutions de l'activité hospitalière,
- L'interaction avec son environnement pour, à terme, l'inscrire dans une démarche de ville durable et intelligente.

Le Smart Hospital est donc par nature ouvert, interopérable et alimente un écosystème logiciel, vecteur de services en développement et à venir. Cet écosystème a vocation à être intégré dans la stratégie et la gestion numérique de l'organisation hospitalière en partageant des référentiels, des bonnes pratiques et une politique de sécurité.

LA DÉMARCHE READY TO SERVICES FOR CARE (R2S4CARE, R2S4C)

Concevoir, réaliser et exploiter un bâtiment hospitalier serviciel

La « révolution numérique » en favorisant le développement de nouveaux services qui accompagnent et répondent aux évolutions des usages dans notre société, constitue un défi pour la filière du bâtiment appelée à intégrer ces nouveaux outils et les savoir-faire associés, et ce, à toutes les phases du projet : schéma directeur immobilier, études préalables - programmation – conception – construction - exploitation - maintenance - renouvellement - déconstruction et recyclage, valorisation ou cession.



▲ livrable à approuver pour chaque étape

Que ce soit dans le cadre d'un projet de développement neuf, d'une opération de rénovation, ou de l'enrichissement d'une offre de services pour les usagers du bâtiment, la mise en œuvre d'un projet bâtimentaire intégrant le numérique nécessite de s'appuyer sur une méthodologie appropriée.

C'est la raison pour laquelle la Smart Buildings Alliance (SBA) a développé Ready to Services for Care (R2S4Care, R2S4C), le cadre de référence qui signe la « Haute Qualité Digitale » d'un projet bâtimentaire hospitalier et s'inscrit dans une démarche globale qui part de la connectivité du bâtiment pour permettre à ce dernier de fournir une palette de services, riche et évolutive en s'appuyant sur un socle fédérateur commun et sécurisé : celui de l'infrastructure réseau du bâtiment et des équipements connectés qui y sont reliés et génèrent et échangent les données qui constituent le 4ème fluide du bâtiment.

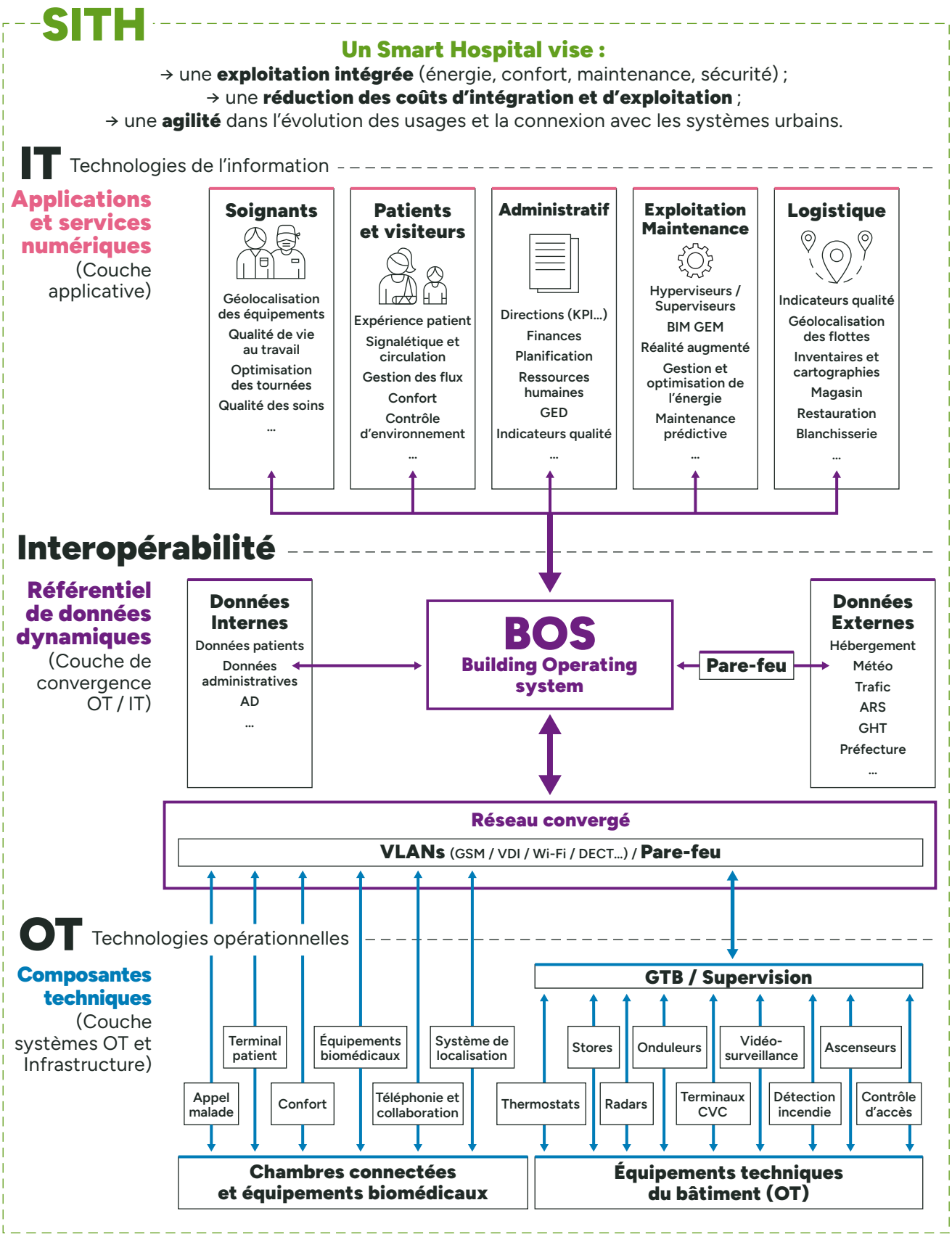
Les principes-clé de l'architecture technique du SITH

L'approche R2S4Care privilégie les moyens techniques destinés à assurer des communications performantes et l'interopérabilité des systèmes, en intégrant des **protocoles communs** (IP -Internet Protocol-) et des **services dotés d'APIs** (Interfaces de programmation) ouvertes.

Les interfaces choisies au sein du bâtiment hospitalier connecté permettent aux fonctions de pilotage et aux informations d'être accessibles à l'intérieur comme à l'extérieur du bâtiment. **La sécurité numérique** est le corollaire de ce principe d'ouverture : protection des données, résilience et sécurité informatique.

L'approche R2S4Care présente trois couches indépendantes. Elles offrent au bâtiment hospitalier une grande flexibilité et évolutivité en dissociant la couche applicative (les services), la couche communication (l'infrastructure réseau du bâtiment) et la couche des écosystèmes matériels (les équipements). L'architecture du SITH est organisée en trois couches fonctionnelles, correspondant au modèle OT → IT → Services.

Le modèle R2S4Care pose la règle d'interchangeabilité de chaque couche, sans modification des deux autres, afin qu'un service n'impose pas un écosystème matériel ou une infrastructure réseau dédié et réciproquement. Ainsi ces trois couches communiquent, interagissent, échangent des données qui convergent via le réseau « Smart » du bâtiment.



L'ARCHITECTURE DU SITH (SYSTÈME D'INFORMATION TECHNIQUE HOSPITALIER)

Couche haute

Supervision – Analyse – Services

Cette couche exploite les données collectées pour produire des services métier dont :

- supervision temps réel des installations ;
- visualisation sur plans ou maquette BIM ;
- maintenance prédictive ;
- gestion énergétique ;
- sûreté et sécurité ;
- géolocalisation ;
- tableaux de bord et alertes.

Couche intermédiaire

Collecte et structuration des données

Cette couche joue le rôle de passerelle entre le terrain et les applications.

Ses fonctions principales sont :

- agréger les données issues des équipements,
- convertir les protocoles OT vers des formats IP, trier, historiser et sécuriser les données,
- séparer les flux internes des flux externes.

Couche basse

Réseaux de terrain et objets connectés (OT)

Cette couche regroupe les équipements numériques physiques du bâtiment : les réseaux de terrain regroupant les services techniques du bâtiment et les objets connectés. Ils communiquent via des bus propriétaires/ouverts et des réseaux sans-fil.

Les données : 4ème fluide du bâtiment

Le bâtiment n'est plus uniquement traversé par des réseaux physiques ; il est également traversé par un réseau de données continu, structuré et partagé dont le BOS constitue le « réseau de distribution » de ce 4e fluide.

Dans cette vision :

- les capteurs sont les producteurs ;
- les réseaux et API sont les canalisations ;
- le BOS est la centrale de distribution ;
- le BIM est le réservoir et la cartographie ;
- les applications, l'IA et les utilisateurs sont les consommateurs.

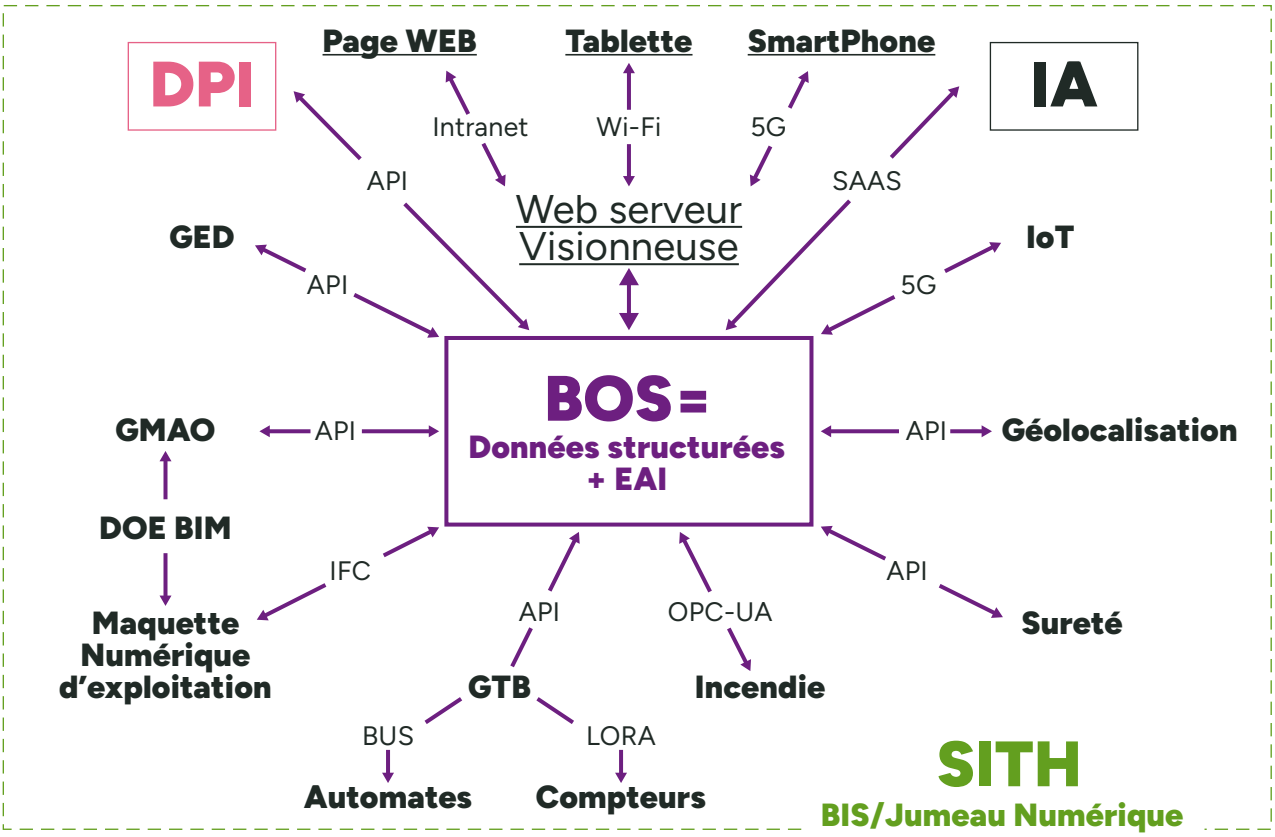
Le Smart Hospital devient ainsi un bâtiment piloté par la circulation maîtrisée de la donnée, au même titre qu'il est piloté par l'électricité, l'eau ou les fluides médicaux.

Le schéma ci-dessous ne représente pas seulement une architecture informatique : il décrit un changement de paradigme.

Dans cette approche, la donnée n'est plus considérée comme un simple sous-produit des équipements techniques, mais comme une ressource distribuée et pilotée au même titre que :

- l'électricité ;
- l'eau ;
- les fluides médicaux.

La donnée devient ainsi le « 4e fluide » du bâtiment.



LE CONCEPT CIBLE DU SITH

Les moyens techniques et organisationnels de la démarche R2S4Care

R2S4Care décrit, en six thèmes, les moyens techniques et organisationnels à mettre en place pour qu'un bâtiment hospitalier réponde aux enjeux de la transformation des usages par le numérique :

LE R2S FOR CARE [R2S4C]

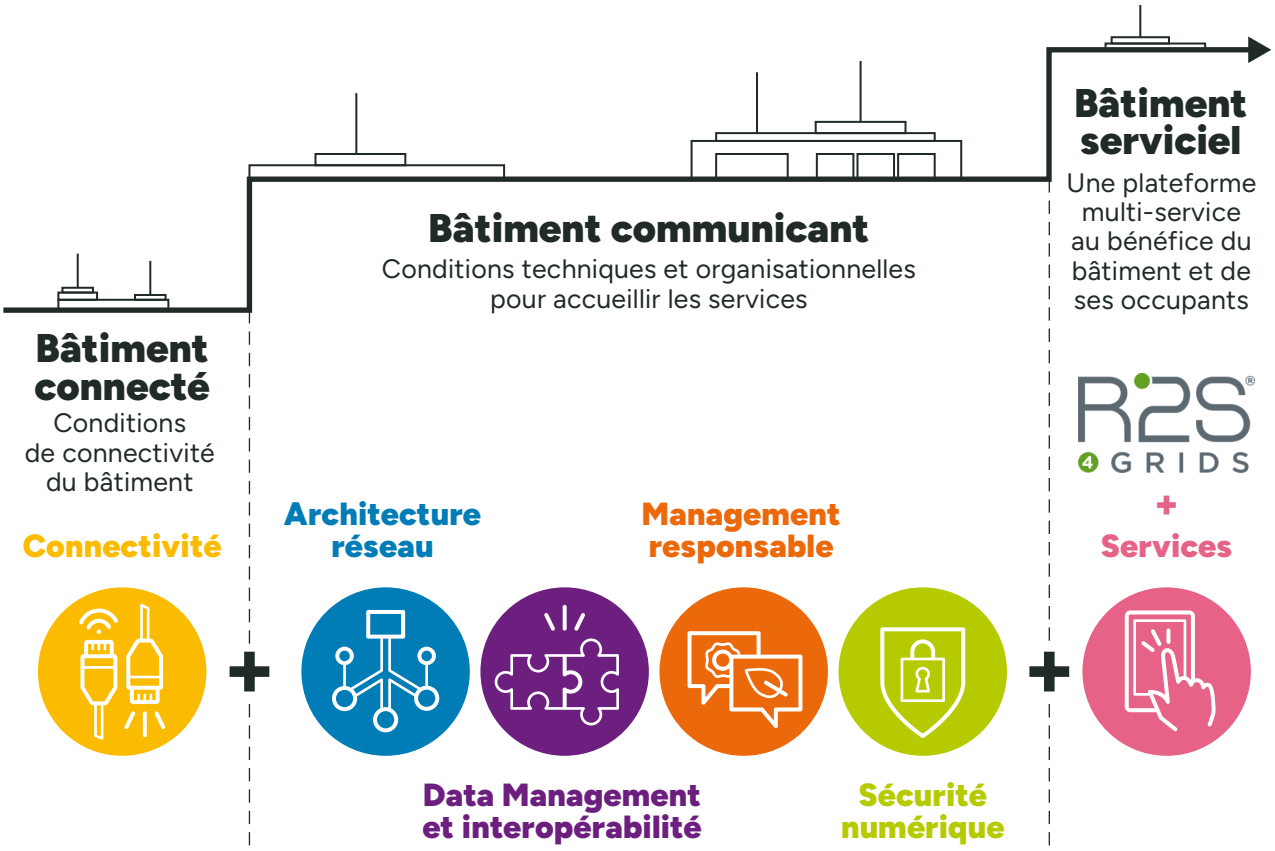
A chaque projet immobilier son périmètre R2S4Care

Un établissement hospitalier est par nature **complexe et hétérogène, notamment d'un point de vue espace** (espace non-hospitalier, espace d'activité hospitalière). Il peut être composé de différents bâtiments, plateaux techniques, unités de soins, espaces d'usage tertiaire ou administratif, ou d'hébergement. Le périmètre du projet **R2S4Care est lié aux services que l'on veut fournir aux usagers**. Il peut donc être construit **avec des sous-catégories** (ou zones) avec des niveaux de recommandation correspondant aux attentes et contraintes spécifiques à chacune de ces sous-catégories.

Une démarche qui se construit par étape

Le R2S4Care s'inscrit dans une dynamique de transformation visant à renforcer la performance du bâtiment, l'efficacité opérationnelle des équipes techniques et, au final, la qualité, la coordination des soins. Conçu comme un cadre méthodologique partagé, il permet aux différents acteurs de structurer leurs actions autour d'objectifs communs et mesurables.

Le R2S4Care est une démarche qui se développe progressivement, étape après étape, afin de garantir une appropriation durable par l'ensemble de ces acteurs. Chaque phase contribue à consolider les pratiques, à sécuriser les processus et à favoriser l'amélioration continue.

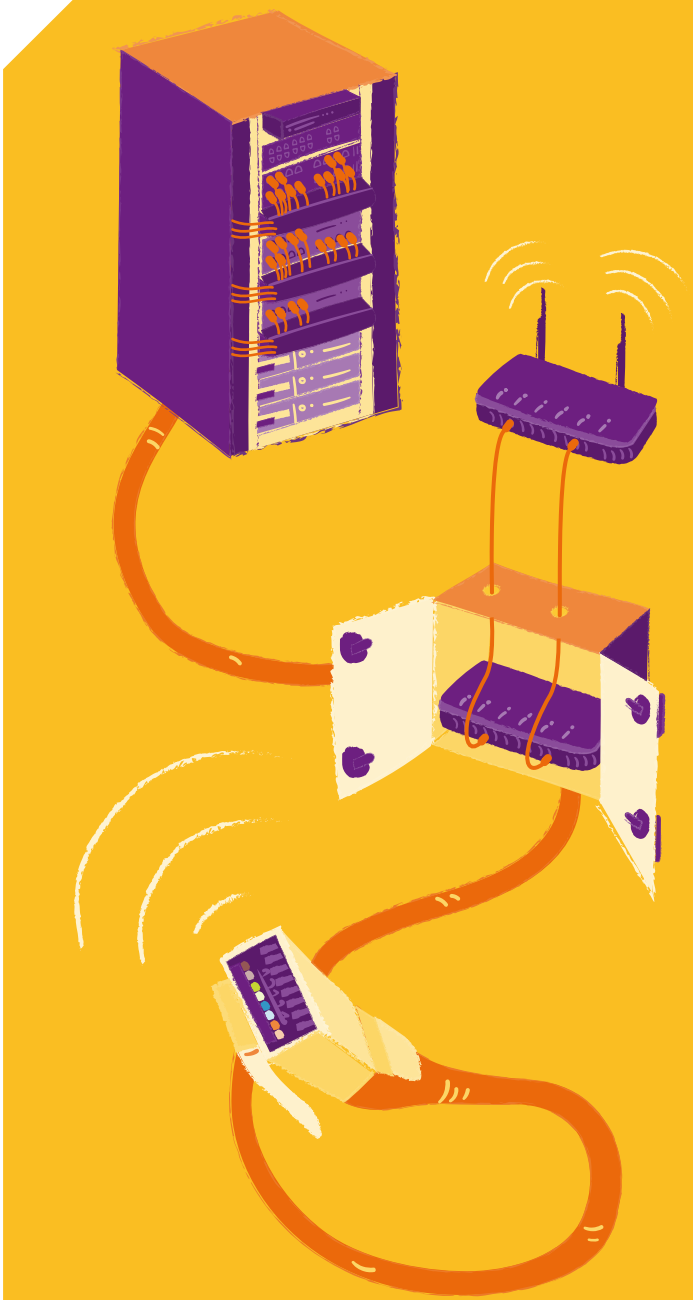


Sommaire

Connectivité

Le réseau « Smart » est le réseau fédérateur du Smart Hospital utilisant le protocole IP. Il est sécurisé et utilise exclusivement le standard Ethernet sur le réseau local et le standard Internet depuis l'extérieur du bâtiment. Les écosystèmes matériels, quel que soit leur protocole, communiquent sur le réseau « Smart », à l'aide d'API ou de Web Services exposées sur le réseau « Smart » et sur le World Wide Web. Ce périmètre ne peut pas être réduit à un réseau logique (ex : VLAN GTB), mais doit comprendre le réseau dans son entièreté : réseaux filaires et réseaux sans fil.

Ce thème vise à assurer une connectivité performante du Smart Hospital en construisant le réseau « Smart », ce qui constitue un socle nécessaire à la mise en place de services numériques.



Le raccordement aux réseaux externes du réseau « Smart » constitue une étape essentielle pour garantir une connectivité optimale du bâtiment. Ce raccordement permet de faciliter toutes les connexions et échanges de données tout en respectant les standards publics internationaux. Il assure ainsi une compatibilité avec l'ensemble des dispositifs et systèmes communicants présents ou futurs.

Le câblage du réseau « Smart » se distingue par sa capacité d'adaptation et son évolutivité. Il est possible d'associer ou de dissocier les câblages sans devoir effectuer des réfections, ce qui permet de répondre rapidement aux nouveaux besoins des utilisateurs ou à l'intégration de nouveaux systèmes communicants.

Afin d'assurer la fiabilité de la connectivité, une redondance de rattachement du bâtiment aux opérateurs de réseaux ainsi qu'aux équipements actifs du réseau « Smart » est mise en place. Cette redondance garantit une continuité de services en cas de défaillance d'un opérateur de réseau

Un système de protection est indispensable pour sécuriser l'infrastructure du réseau « Smart » contre toute tentative de malveillance. Ce dispositif protège l'ensemble des équipements et assure la sécurité des échanges de données.

Recommandations	Niveaux de maturité		Pages
CO 1 – Raccordement aux réseaux externes du bâtiment			→ p.17
CO 1.1 – ADDUCTION TÉLÉCOM, LOCAUX ET CHEMINEMENTS	● Niveau 1	Capacité de rattachement aux réseaux externes et locaux centraux	
	●● Niveau 2	Installation des conteneurs standardisés	
	●●● Niveau 3	Qualité de l'ouvrage	
	●●●● Niveau 4	Desserte interne	
CO 1.2 – REDONDANCE DE RATTACHEMENT DU BÂTIMENT AUX RÉSEAUX EXTERNES	● Niveau 1	Création d'un second ouvrage VRD	
	●● Niveau 2	Existence d'un second local opérateur	
CO 2 – Connectivité aux réseaux filaires			→ p.19
CO 2.1 – CÂBLAGE DES ESPACES NON HOSPITALIERS	Unique	Câblage fédérateur	
CO 2.2 – PRÉDISPOSITION DE CÂBLAGE DES ESPACES D'ACTIVITÉ HOSPITALIÈRE DU BÂTIMENT	Unique	Précâblage « as a service »	
CO 2.3 – REDONDANCE ET SÉCURISATION DU CÂBLAGE	● Niveau 1	Présence de deux parcours de distribution des câblages	
	●● Niveau 2	Présence de deux locaux de répartition générale	
CO 2.4 – EXPLOITABILITÉ ET ÉVOLUTIVITÉ DU CÂBLAGE	● Niveau 1	Capacité d'extension pour l'ajout de prises réseau	
	●● Niveau 2	Proximité des points de sous-répartition	
CO 2.5 – ALIMENTATION DES ÉQUIPEMENTS CONNECTÉS PAR LE RÉSEAU	● Niveau 1	Prévoir dès la conception l'utilisation du PoE	
	●● Niveau 2	Déployer effectivement des ports PoE	
	●●● Niveau 3	Garantir une capacité d'extension du budget PoE	

Recommandations	Niveaux de maturité			Pages
CO 3 – Connectivité aux réseaux sans fil				→ p.23
CO 3.1 – NATURE ET QUALITÉ DES RÉSEAUX SANS FIL	●	Niveau 1	Définition des objectifs et recensement des usages et des équipements	
	●●	Niveau 2	Fourniture d'une étude de couverture	
CO 3.2 – RÉSEAUX CELLULAIRES – GSM	●	Niveau 1	Étude de couverture GSM	
	●●	Niveau 2	Système mono-opérateur	
	●●●	Niveau 3	Système multiopérateurs	
CO 3.3 – RÉSEAU WI-FI	●	Niveau 1	Étude de couverture	
	●●	Niveau 2	Mise en place du réseau Wi-Fi et intégration au réseau « Smart »	
	●●●	Niveau 3	Respect de la PSSI-S pour la segmentation et cloisonnement des réseaux Wi-Fi	
CO 3.4 – RÉSEAU IOT BASSE CONSOMMATION	●	Niveau 1	Étude préalable de couverture et de recensement des cas d'usage	
	●●	Niveau 2	Réseau IoT opéré ou indépendant	
	●●●	Niveau 3	Réseau IoT connecté au réseau « Smart ».	
CO 3.5 – INFRASTRUCTURE DE GÉOLOCALISATION	●	Niveau 1	Étude préalable de couverture et des cas d'usage pour une infra mutualisée	
	●●	Niveau 2	Mise en place d'une infrastructure de géolocalisation	
	●●●	Niveau 3	Infrastructure de géolocalisation activée	
CO 4 – Alimentation électrique de l'infrastructure				→ p.30
	●	Niveau 1	Alimentation électrique sans interruption des équipements actifs	
	●●	Niveau 2	Redondance de l'alimentation	
CO 5 – Contrôle des accès et protection des infrastructures				→ p.31
	●	Niveau 1	Protection des locaux techniques et des points de répartitions sans traçabilité	
	●●	Niveau 2	Protection des locaux techniques et des points de sous-répartition avec traçabilité	
CO 6 – Rafraîchissement des locaux informatiques				→ p.32
	●	Niveau 1	Systèmes de climatisation adaptés	
	●●	Niveau 2	Supervision et contrôle continu	

CO 1 – Raccordement aux réseaux externes du bâtiment

CO 1.1 – ADDUCTION TÉLÉCOM, LOCAUX ET CHEMINEMENTS

Le bâtiment du Smart Hospital est prédisposé pour être rattaché aux réseaux externes des opérateurs et pour permettre la distribution de tout type de liaison opérée vers son local de répartition générale.

●

Capacité de rattachement aux réseaux externes et locaux centraux

Niveau 1

Cette recommandation vise à garantir :

- La capacité de rattachement du bâtiment hospitalier aux réseaux filaires des opérateurs télécoms par l'intermédiaire d'un ouvrage VRD créé jusqu'en limite de domaine public ;
- La réalisation d'une adduction jusqu'à un local opérateur en intérieur bâtiment ;

●●

Installation des conteneurs standardisés

Niveau 2

Installation d'un conteneur standardisé [19"] pour les équipements actifs du réseau dans le local opérateur pour faciliter l'installation, la mise en service et la maintenance.

Si un second local opérateur existe, installation d'un contenant également dans ce local.

●●●

Qualité de l'ouvrage

Niveau 3

Le local opérateur et le local répartiteur général disposent chacun d'une surface de plancher dédiée [8 m² avec une largeur minimale de 2,4 mètres]. Ces locaux doivent être dédiés à leur usage et ne pas être mutualisés.

Le local répartiteur général doit permettre une évacuation efficace de la chaleur générée par les équipements qu'il contient.

●●●●

Desserte interne

Niveau 4

La desserte interne correspond au câblage reliant les locaux opérateurs à l'abonné. Elle doit être installée depuis les locaux opérateurs jusqu'à un coffret dédié dans chaque espace susceptible d'être occupé par un abonné indépendant (par exemple, plateaux de bureau).

En cas de multiples locaux opérateurs, la desserte interne doit être réalisée depuis chaque local opérateur vers chaque espace pouvant être occupé par un abonné indépendant.

CO 1.2 – REDONDANCE DE RATTACHEMENT DU BÂTIMENT AUX RÉSEAUX EXTERNE

Le Smart Hospital prévoit les dispositions nécessaires pour assurer une redondance de connexion aux réseaux opérateurs. Le but est de rendre possible la continuité de services en cas d'endommagement d'un des ouvrages VRD rattachant le bâtiment aux réseaux externes.

Il est pourvu d'au moins deux locaux ou espaces opérateurs permettant le raccordement à au moins deux opérateurs distincts.

●

Création d'un second ouvrage VRD

Niveau 1

Le Smart Hospital dispose d'un second ouvrage VRD, distant du premier de 8 m ou plus, jusqu'en limite de domaine public, et permettant le rattachement sous fourreaux du bâtiment aux réseaux d'au moins deux opérateurs.

●●

Existence d'un second local opérateur

Niveau 2

L'objectif est de rendre possible la continuité de services en cas d'indisponibilité d'un des deux locaux opérateurs. En complément du second ouvrage VRD, le Smart Hospital dispose d'un second local ou espace opérateur qui dispose d'une surface de plancher identique au premier.

Chaque bâtiment est par ailleurs doté d'une seconde gaine opérateurs, espacée de la première d'au moins 8 mètres (ou 2 mètres avec un coupe-feu sur toutes les faces sur au moins une gaine) à maintenir sur l'ensemble des parcours redondants opérateurs (compris locaux techniques).

CO 2 – Connectivité aux réseaux filaires

CO 2.1 – CÂBLAGE DES ESPACES NON HOSPITALIERS

Le bâtiment est pourvu d'un câblage pour le réseau « Smart » rassemblant les liaisons et connexions de l'ensemble des systèmes communicants.

Câblage fédérateur

Niveau unique

Le bâtiment doit donc être pourvu d'un câblage fédérateur unique rassemblant les liaisons et connexions de l'ensemble des systèmes communicants du réseau « Smart ».

Cela induit :

- L'installation d'un contenant 19 pouces dans le local répartiteur général destiné à recevoir les équipements actifs centraux du réseau « Smart » et les serveurs locaux…
- Des cheminements depuis le local de répartition général supportant le câblage du réseau « Smart »
- L'installation du câblage du réseau « Smart » vers les switchs d'accès et les terminaux

CO 2.2 – PRÉDISPOSITION DE CÂBLAGE DES ESPACES D'ACTIVITÉ HOSPITALIÈRE DU BÂTIMENT

Les différents espaces d'activités hospitalières du bâtiment sont conçus pour être pré-équipés d'un câblage flexible, modulaire et évolutif, selon le principe du « Cabling as a Service ».

Un précâblage modulaire est mis en œuvre et réparti de manière homogène dans l'ensemble des espaces destinés à recevoir des utilisateurs.

Des points de consolidation, actifs ou passifs, sont installés de façon à éviter toute centralisation du câblage dans un unique local par niveau ou pour l'ensemble du bâtiment. La densité des points de consolidation est déterminée en fonction de l'effectif maximum potentiel de chaque espace ; les points de consolidation couvrent une surface maximale de 60 m². Le câblage tient compte des éventuelles divisions des espaces entre plusieurs occupants afin de garantir la flexibilité et l'adaptabilité de l'infrastructure aux différents usages.

Le câblage est également dimensionné pour permettre l'installation de points d'accès Wi-Fi dans ces mêmes espaces.

Des conteneurs (19") sont installés pour accueillir le câblage et les équipements actifs associés. Ces conteneurs bénéficient des alimentations électriques nécessaires et d'un traitement d'air adapté pour garantir le bon fonctionnement et la pérennité des installations.

Enfin, la mise en place de rocades dans une topologie adaptée permet d'établir des liaisons entre les contenants 19" mentionnés, les locaux opérateurs, les locaux de répartition générale et, le cas échéant, les locaux informatiques hébergeant le SIH.

Précâblage "as a service"

Niveau unique

Un précâblage modulaire est mis en œuvre et réparti de manière homogène dans l'ensemble des espaces destinés à recevoir des utilisateurs. Cette prédisposition vise à garantir une infrastructure adaptée aux besoins évolutifs des utilisateurs et des équipements connectés.

CO 2.3 – REDONDANCE ET SÉCURISATION DU CÂBLAGE

Après avoir valorisé la redondance du rattachement du bâtiment aux réseaux externes, il s'agit de prolonger la redondance de la distribution des rocades jusqu'au point de sous répartition, avec un second local répartiteur général et entre local répartiteur général et les points de sous répartition. L'objectif est d'avoir un câblage redondant ne disposant d'aucun SPOF (« Single Point of Failure » : ou point unique de défaillance) entre les nœuds de connexion des prises et le répartiteur général recevant les équipements actifs centraux.

●

Présence de deux parcours de distribution des câblages

Niveau 1

Le but de cette recommandation consiste à valoriser la prédisposition du bâtiment à recevoir un câblage redondant. Chaque bâtiment est doté de deux gaines techniques verticales, espacées d'au moins 8 mètres (ou 2 mètres avec un coupe-feu sur toutes les faces sur au moins une gaine).

Ces gaines sont équipées de cheminements dédiés aux liaisons de communication, permettant ainsi de disposer de deux parcours distincts pour distribuer chacun des niveaux du bâtiment à partir du ou des locaux de répartition générale.

Remarque : ces gaines verticales peuvent être partagées avec d'autres réseaux VDI/CFA

●●

Présence de deux locaux de répartition générale

Niveau 2

Cette recommandation complémentaire a pour objet de vérifier que le bâtiment est prédisposé à une redondance de ses équipements centraux. Il nécessite la présence dans le bâtiment d'un second local de répartition générale. En cas de multiplicité des parcours de distribution des câblages, les locaux de répartition générale sont disposés sur des verticalités différentes.

Remarque : le second local de répartition générale peut être mutualisé avec d'autres locaux liés au courant faible (Local Opérateur, Poste Central de Sécurité…), à l'exception du 1er local répartiteur général.

CO 2.4 – EXPLOITABILITÉ ET ÉVOLUTIVITÉ DU CÂBLAGE

Le(s) câblage(s) du bâtiment permet(tent) aisément d'ajouter, supprimer, modifier la densité ou l'emplacement des points de connexion des équipements communicants. Il s'agit ici de promouvoir la facilité d'adaptation du câblage.

Cette adaptabilité est en effet nécessaire selon différents scenarii :

- Pour l'intégration de systèmes ou d'équipements communicants complémentaires ;
- Pour la redistribution et/ou la révision de la densité de prises dans les espaces d'activité hospitalière, suivant les réaménagements effectués et l'évolution des besoins de connectivité des occupants du bâtiment.

Remarque : cette recommandation s'applique au câblage des services hospitaliers.

●

Capacité d'extension pour l'ajout de prises réseau

Niveau 1

En conception et en réalisation, ce niveau concerne la capacité d'ajout de prises réseau dans le bâtiment. Il requiert une capacité d'extension non équipée de minimum 30% pour l'ajout ultérieur de prises réseau sur le réseau « Smart ». En exploitation, la capacité d'extension non équipée doit être connue pour faciliter la planification des évolutions futures du réseau « Smart ».

Cette capacité d'extension doit porter *a minima* sur les points suivants :

- Les cheminements de câbles entre le cœur de réseau et les switchs d'accès ainsi que les cheminements principaux issus des switchs d'accès
- Les contenants recevant les switchs d'accès
- Les arrivées dédiées à l'alimentation électrique et au traitement climatique des locaux techniques recevant les équipements actifs du réseau « Smart » (répartiteurs généraux et points de sous-répartition). L'exigence ne porte pas sur le câblage ni sur les équipements actifs.

●●

Proximité des points de sous-répartition

Niveau 2

Ce niveau d'exigence concerne la capacité à pouvoir ajouter des équipements avec un câblage cuivre en tout point du bâtiment, sans avoir à créer de point de sous-répartition complémentaire. Tout point du bâtiment est situé dans un rayon de 70 m au plus autour d'un switch d'accès. Dans le cas où tous les niveaux ne sont pas équipés de switch d'accès, ce rayon est réduit de la longueur du parcours vertical.

CO 2.5 – ALIMENTATION DES ÉQUIPEMENTS CONNECTÉS PAR LE RÉSEAU

Le PoE (Power over Ethernet) est une technologie réseau qui permet de transporter simultanément les données et l'alimentation électrique sur un seul câble Ethernet (RJ45).

Dans le réseau « Smart », les switchs d'accès doivent pouvoir alimenter électriquement les équipements terminaux qu'ils raccordent conformément aux standards internationaux. Le PoE est utile pour :

- Simplifier le déploiement du réseau (un seul cable)
- Alimenter les équipements intelligents connectés
- Centraliser et sécuriser l'énergie
- Favoriser les architectures modernes et smart.

●

Prévoir dès la conception l'utilisation du PoE

Niveau 1

Prévoir dès la conception des mesures conservatoires pour rendre possible un futur déploiement du PoE sans modifier l'infrastructure (câblage, terminaisons, équipements, par ex. switchs prêts PoE avec emplacements d'alimentations) ;

●●

Déployer des ports PoE

Niveau 2

Déployer effectivement des ports PoE au minimum dans les zones de services aux usagers pour faciliter l'installation d'objets connectés, points d'accès Wi-Fi et équipements de sûreté ;

●●●

Garantir une capacité d'extension du budget PoE

Niveau 3

Garantir une capacité d'extension du budget PoE (30% de puissance supplémentaire en conception/réalisation) et, en exploitation, connaître la réserve de puissance disponible par switch afin de planifier les évolutions du réseau.

CO 3 – Connectivité aux réseaux sans fil

CO 3.1 – NATURE ET QUALITÉ DES RÉSEAUX SANS FIL

L'hôpital communicant repose largement sur les réseaux sans fil, parce qu'ils relient en mobilité les soignants, les dispositifs médicaux, les patients et les services administratifs. Le bâtiment dispose d'une couverture adéquate à l'intérieur de ses différents espaces, pour les principaux réseaux radio (cellulaire, Wi-Fi, ...).

Pour cela, les services attendus des réseaux radio doivent être définis en termes d'objectifs (communication voix, données, localisation indoor), de nature d'équipements connectés (téléphones mobiles professionnels de l'établissement, professionnels tiers, patients et visiteurs, PCs, dispositifs médicaux connectés, équipements, Io(M)T incluant tags de localisation, boutons d'appel etc.), d'objectifs de service.

La qualité de la couverture des réseaux sans fil (exemples : puissance de réception, multiplexage, communications simultanées...) doit être définie par le maître d'ouvrage de façon cohérente avec les services qui doivent être apportés par l'intermédiaire de ces réseaux.

En pratique, le Wi-Fi est central, mais il peut être complété par DECT pour la téléphonie, BLE pour la localisation de proximité, RFID pour l'identification, 4G/5G pour certains cas d'usage critiques, et Li Fi pour des zones sensibles aux ondes. Le bon choix dépend du niveau de criticité, de la mobilité attendue et des contraintes d'interférences électromagnétiques.

La perspective : vers le Wi-Fi 6/6E et la 5G indoor :

Dans un avenir proche, le Smart Hospital combinera

- Wi-Fi 6/6E pour la densité et la performance,
- 5G privée pour les usages critiques,
- Edge computing pour réduire la latence .

Cette hybridation permet de supporter les cas d'usage les plus exigeants : chirurgie augmentée, ambulances connectées, monitoring massif, jumeaux numériques.

Définition des objectifs et recensement des usages et des équipements

Niveau 1

Garantir que le bâtiment dispose d'une couverture radio intérieure adaptée aux usages attendus pour :

- les réseaux cellulaires ;
- les réseaux Wi-Fi ;
- les systèmes de localisation indoor ;
- les équipements Io(M)T et dispositifs connectés.

Pour chaque zone du bâtiment (chambres, blocs, urgences, bureaux, circulations, sous-sols, locaux techniques, halls, parkings, extérieurs proches), établir une matrice :

Zone	
Cas d'usage	
Type d'équipement	
Niveau de criticité	

Les équipements doivent être regroupés au minimum en :

- téléphones mobiles du personnel ;
- téléphones de prestataires ou professionnels tiers ;
- smartphones des patients et visiteurs ;
- PC portables et tablettes ;
- dispositifs médicaux connectés ;
- équipements Io(M)T : tags de localisation, capteurs, boutons d'appel, bracelets, équipements biomédicaux.

D'une façon générale, la qualité de service demandée sera égale ou supérieure à 99% pour la majorité des cas d'usage.

Fourniture d'une étude de couverture

Niveau 2

L'enjeu de cette recommandation est de donner aux futurs usagers une visibilité sur la qualité d'accès, à l'intérieur du bâtiment, aux principaux réseaux radio (cellulaire, Wi-Fi, ...). Il convient donc de fournir une étude de couverture des réseaux radio suivant leur disponibilité locale.

Ce niveau de recommandation demande :

- La fourniture d'une mesure de couverture intérieure des réseaux de téléphonie mobile publics disponibles en 4G/5G suivant leur disponibilité locale
- La mise en place de mesures conservatoires visant à faciliter la mise en place ultérieure d'un système DAS (Distributed Antenna System) de GSM.

CO 3.2 – RÉSEAUX CELLULAIRES – GSM

Les réseaux cellulaires 3G/4G/5G sont indispensables dans le bâtiment hospitalier parce qu'ils assurent une continuité de service là où le Wi-Fi seul ne suffit pas, notamment pour la mobilité du personnel, les appels critiques et la couverture des zones difficiles comme les sous-sols ou certains blocs techniques. Le cellulaire ne remplace pas le Wi-Fi hospitalier, il le complète. Le bon modèle est souvent une architecture mixte : Wi-Fi pour les usages locaux, et réseau cellulaire indoor pour la continuité, la mobilité critique et les zones à forte exigence de disponibilité

Ces réseaux cellulaires 3G/4G/5G sont incontournables dans la mesure où :

- Ils garantissent une couverture mobile intérieure plus homogène pour les soignants, les patients et les visiteurs, surtout dans les zones mal desservies par le signal public.
- Ils supportent la téléphonie critique et la protection des travailleurs isolés, avec des alertes et communications en temps réel.
- Ils permettent de séparer les usages entre accès public, accès soignant et flux critiques, ce qui est utile pour la sécurité et la maîtrise des priorités réseau.
- Ils servent de support à la remontée de données d'objets connectés médicaux et à des applications à faible latence comme la supervision ou certaines briques de télémédecine.
- Ils renforcent la disponibilité quand l'hôpital couvre plusieurs bâtiments ou de grandes surfaces, où une architecture mobile privée ou hybride devient plus pertinente

Ce qu'apporte la 5G :

La 5G privée ou hybride apporte surtout trois atouts : faible latence, sécurité renforcée et capacité à gérer de nombreux équipements en parallèle. C'est pour cela qu'elle est particulièrement adaptée aux hôpitaux qui veulent connecter à la fois des usages critiques, des objets médicaux et des services de confort sans tout faire passer par le même réseau.

Étude de couverture GSM
Niveau 1

Ce niveau de la recommandation vise à apporter une garantie d'accès, dans tous les espaces intérieurs du bâtiment inclus dans le périmètre du projet, aux réseaux cellulaires disponibles des opérateurs.

Une étude de couverture indoor GSM vise à mesurer, cartographier et corriger la qualité du réseau mobile à l'intérieur du bâtiment hospitalier afin d'assurer une couverture homogène, en particulier dans les zones critiques comme les sous-sols, les circulations et les étages profonds.

Elle prévoit la mise en place de mesures conservatoires visant à faciliter la mise en place ultérieure d'un système DAS (Distributed Antenna System) de GSM.

Système mono-opérateur
Niveau 2

Cette recommandation s'appuie sur 2 critères :

- le bâtiment est équipé d'un système de GSM indoor raccordé à un opérateur ;
- le système mis en place a la capacité de supporter ultérieurement un changement d'opérateur

Le niveau peut également être atteint si la couverture naturelle depuis l'extérieur du bâtiment est satisfaisante pour au moins 2 opérateurs. La couverture est jugée satisfaisante quand la communication voix et data est ininterrompue lors des déplacements dans les espaces traités, un plan indiquant le parcours suivi lors de l'essai dans le bâtiment doit alors être produit, celui-ci doit traiter les zones proches des façades et celles situées au cœur du bâtiment des zones couvertes. Les zones couvertes devront *a minima* être les parties communes, la couverture des autres zones (y compris ascenseurs, escaliers et espaces de stationnement) est laissée au libre au choix du maître d'ouvrage selon sa définition du périmètre des parties communes.

●●●

Système multi opérateurs
Niveau 3

A ce niveau de recommandation, le Smart Hospital est équipé d'un système de GSM indoor raccordé à au moins deux opérateurs.

CO 3.3 – RÉSEAU WI-FI

Le réseau Wi-Fi est l'une des infrastructures vitales du Smart Hospital. Le Wi-Fi n'est plus un « service utile » : c'est une infrastructure critique, au même titre que l'électricité ou l'eau. Il permet la connectivité des équipements médicaux, des capteurs IoT, des applications cliniques, de la mobilité des soignants et de l'expérience patient.

Dans un Smart Hospital, le Wi-Fi doit être :

- hautement sécurisé (données de santé, IoMT),
- segmenté (patients / soignants / biomédical / IoT),
- redondé (pas de coupure possible),
- supervisé en temps réel.
- sécurisé (la cybersécurité devient un enjeu majeur)

●

Étude de couverture
Niveau 1

Ce niveau de la recommandation vise à apporter une garantie d'accès, dans tous les espaces intérieurs du bâtiment inclus dans le périmètre du projet, au réseau WI-FI.

L'étude de couverture WI-FI combine analyse, simulation, mesures terrain et recommandations techniques, afin d'assurer une connectivité robuste pour les usages cliniques, logistiques, techniques et patients.

Elle permet de valider le plan de déploiement, d'identifier les zones d'ombre, les interférences, les besoins en points d'accès et les contraintes techniques

Les trois moments où l'on réalise une étude de couverture WI-FI :

- Avant le déploiement (pré déploiement) : pour comprendre la nature RF du site et anticiper les contraintes.
- À l'étape « Commissionnement » : pour vérifier que l'installation correspond au plan.
- En cours d'exploitation : pour diagnostiquer des problèmes ou optimiser le réseau.

●●

Mise en place du réseau Wi-Fi et intégration au réseau « Smart »
Niveau 2

Cette recommandation vise à structurer le projet WI-FI en fonction de l'étape commissionnement qui valide l'atteinte des objectifs :

- La couverture et la qualité radio dans les zones cibles, avec mesures et tests de performance.
- La capacité à supporter les usages prévus, comme le DPI, les terminaux mobiles, le Wi-Fi invité et les objets connectés.
- La séparation correcte des réseaux, par exemple personnel, visiteurs et équipements, avec cloisonnement réseau adapté.
- La sécurité d'accès, notamment l'authentification forte, l'administration sécurisée et les journaux de connexion.
- La résilience et l'exploitation, avec supervision, tests de charge et procédures de maintenance.

●●●

Le respect de la PSSI-S pour la segmentation et cloisonnement des réseaux Wi-Fi

Niveau 3

Le réseau Wi-Fi respecte, par conception, les recommandations de la PSSI-S (Politique de Sécurité des Systèmes d'Informations) de l'institution. Voir les documents « Thématiques de sécurité ».

CO 3.4 – RÉSEAU IOT BASSE CONSOMMATION

Les réseaux IoT basse consommation, principalement LoRaWAN, Sigfox, et parfois BLE/Bluetooth Low Energy, permettent de connecter les milliers de capteurs hospitaliers avec une très longue autonomie, une portée étendue et un coût d'exploitation très faible.

Ils sont essentiels au Smart Hospital, car ils complètent le Wi-Fi et la 5G pour des usages non critiques mais massifs.

●

Étude préalable de couverture et de recensement des cas d'usage

Niveau 1

Une étude préalable à la mise en œuvre d'un réseau IoT sert à vérifier que le besoin métier, le réseau, la sécurité et l'exploitation sont compatibles avant tout déploiement. Elle doit cadrer les cas d'usage, la volumétrie, les contraintes d'autonomie, les technologies de connexion et les impacts sur les SI existants, SIH et SITH.

Ce qu'elle doit couvrir :

- Les objectifs métier et les données à collecter, pour éviter de déployer des capteurs sans finalité claire.
- Le périmètre technique, avec les sites, les zones à couvrir, la mobilité ou non des objets, et les contraintes d'autonomie.
- Le choix de la connectivité : Wi-Fi, BLE, LPWAN, 4G/5G, réseau privé ou public, selon le niveau de criticité et de débit.
- L'interopérabilité avec les applications et systèmes existants, notamment la plateforme de collecte, la supervision et la gouvernance des données.
- La cybersécurité, avec segmentation, authentification, chiffrement, mises à jour et gestion des accès.

●●

Réseau IoT opéré ou indépendant

Niveau 2

L'établissement a choisi de ne pas intégré le réseau IOT avec le réseau « Smart » mais a défini le niveau de contrôle, de performance et de sécurité qu'il vise en objectif.

Le choix entre réseau IoT opéré et réseau IoT indépendant dépend surtout du niveau de contrôle voulu, des compétences internes, du coût total et des exigences de couverture.

- Un réseau opéré est géré par un opérateur. Il convient quand on veut aller vite, réduire la charge de maintenance et s'appuyer sur une infrastructure déjà gérée par un tiers ;

– Un réseau indépendant est déployé et administré localement par les équipes du Smart Hospital. Il est pertinent pour garder la maîtrise de l'architecture, des données, des fréquences et des évolutions techniques. Il demande en revanche de disposer des bonnes compétences pour assurer la maintenance, l'évolution et la supervision du réseau. Il devient souvent plus rentable quand le volume d'objets est important ou quand le besoin de souveraineté est fort

Dans cette exigence, sont concernés les réseaux étendus à basse consommation/ LPWAN, exemples : EnOcean, Zigbee, LoRaWAN, NB-IoT, LTE-M, Wi-Fi Halow (IEEE 802.11ah)...

Cette recommandation vise à structurer le projet IOT en fonction de l'étape commissionnement qui valide l'atteinte des objectifs

●●●

Réseau IoT connecté au réseau « Smart »

Niveau 3

Le réseau IoT est connecté au réseau « Smart » de l'hôpital signifie que :

– les capteurs IoT (température, portes, maintenance, localisation, etc.)
– les passerelles (LoRaWAN, BLE, Wi-Fi IoT)
– les plateformes de supervision
– les systèmes métiers (GMAO, GTB, DPI, logistique) s'intègrent dans une architecture numérique unifiée, cohérente et sécurisée. L'IoT n'est pas un système isolé, il alimente, renforce et étend les capacités du Smart Hospital.

Cette recommandation vise, également, à structurer le projet IOT en fonction de l'étape commissionnement qui valide l'atteinte des objectifs.

CO 3.5 - INFRASTRUCTURE DE GÉOLOCALISATION

Définir une infrastructure de géolocalisation dans un Smart Hospital revient à concevoir un système capable de localiser en temps réel les équipements, les patients, les soignants ou les flux logistiques, de manière fiable, sécurisée et intégrée au système d'information hospitalier.

●

Étude préalable de couverture et des cas d'usage pour une infrastructure mutualisée

Niveau 1

Une étude préalable à la mise en œuvre d'une infrastructure de géolocalisation sert à vérifier que les besoins métiers, les technologies, le réseau, la sécurité et l'exploitation sont compatibles avec une infrastructure de géolocalisation mutualisée et avant tout déploiement. Elle doit cadrer les cas d'usage, la volumétrie, les contraintes d'autonomie, les technologies de connexion et les impacts sur les SI existants, SIH et SITH.

Ce qu'elle doit couvrir :

– Les objectifs métier et les objets et personnes à géolocaliser avec le niveau de précision ;
– L'architecture technique : tags/capteurs, antennes/point d'accès ; le logiciel de géolocalisation (RTLS),
– L'interopérabilité avec les applications et systèmes existants : GTB, GMAO, DPI, supervision logistique, sécurité.
– L'intégration au réseau « Smart » et la cybersécurité, avec segmentation, authentification, chiffrement, mises à jour et gestion des accès

Mise en place d'une infrastructure de géolocalisation

Niveau 2

L'infrastructure de géolocalisation devra idéalement être intégrée au réseau « Smart » pour l'alimentation et la contextualisation des balises. Au niveau 1, l'infrastructure doit être installée mais non activée. Le propriétaire du bâtiment doit être informé des démarches à accomplir pour son activation. L'infrastructure de géolocalisation devra à minima être mise en place sur au moins 50% de la surface utile du projet. L'intention de l'exigence est de valoriser la couverture des espaces d'activités d'un bâtiment.

Infrastructure de géolocalisation activée

Niveau 3

Cette recommandation vise à structurer le projet WI-FI en fonction de l'étape commissionnement qui valide l'atteinte des objectifs.

- Le cahier des charges récapitule toutes les exigences définies dans l'étude préalable. Il précise la couverture, la précision, la fiabilité et la sécurité exigées pour la mise en œuvre de l'infrastructure de géolocalisation mutualisée dans l'environnement critique qu'est la Smart Hospital.
- Le commissionnement de l'infrastructure de géolocalisation mutualisée à l'échelle de l'hôpital est une étape déterminante : c'est elle qui garantit que le système de géolocalisation (RTLS - Real Time Location System) fonctionne dans le respect des exigences du cahier des charges.

CO 4 – Alimentation électrique de l'infrastructure

L'ensemble des équipements du réseau « Smart » du bâtiment dispose de systèmes de distribution électrique garantissant la stabilité et la sécurité de leur alimentation électrique. Il est à noter que cette exigence est incluse dans les projets de construction hospitalière.

Le but est de s'assurer de la la disponibilité d'un courant dont la tension et la fréquence sont régulées, afin de préserver la meilleure garantie de continuité fonctionnelle des équipements du réseaux Smart.

Alimentation électrique sans interruption des équipements actifs

Niveau 1

Cette recommandation requiert une alimentation électrique sans interruption (exemples : ASI, onduleur avec batterie…) des équipements actifs du réseau « Smart » (cœurs de réseau, routage, pare-feu, switch, équipements d'interface avec les réseaux opérateurs de télécommunication) et les serveurs centraux qui y sont rattachés. L'alimentation électrique doit être en adéquation avec l'usage du bâtiment (à minima pour la protection des serveurs, jusqu'à 1h comme décrit dans la NFC15-211 - installation électrique basse tension dans les locaux à usage médical).

Redondance de l'alimentation

Niveau 2

Cette recommandation, complémentaire de la précédente, concerne la continuité de services des équipements actifs centraux du réseau « Smart » et les serveurs qui y sont rattachés, en cas de défaillance d'un circuit d'alimentation.

La recommandation réclame la présence d'une alimentation normale ou stabilisée redondante en énergie électrique, sans point individuel de défaillance (SPOF). Les équipements actifs centraux et les serveurs qui y sont rattachés doivent disposer de deux alimentations indépendantes et redondantes. Celles-ci doivent être alimentées par deux tableaux électriques différents.

CO 5 – Contrôle des accès et protection des infrastructures

Dans un Smart Hospital, une attaque ne passe pas seulement par le cyberespace : un accès physique non maîtrisé peut permettre de brancher un équipement pirate, de débrancher une baie, de capter des informations ou de perturber des services critiques. La sécurité doit donc couvrir ensemble le bâtiment, le réseau et les dispositifs connectés.

Le contrôle des accès et la protection des infrastructures physiques du réseau « Smart » consistent à empêcher l'accès non autorisé aux locaux, aux armoires réseau, aux salles serveurs, aux baies, aux équipements radio et aux zones techniques sensibles. Cet objectif repose à la fois sur des barrières physiques, des droits d'accès tracés et une surveillance continue des zones critiques.

Mécanismes de contrôle :
- Badges, lecteurs RFID, codes ou biométrie pour limiter l'accès selon les habilitations.
- Gestion par rôles et horaires, avec ouverture limitée aux personnes autorisées.
- Journalisation de toutes les entrées et sorties pour assurer la traçabilité.
- Vidéosurveillance et intégration avec les systèmes d'alarme et de supervision.
- Cloisonnement des zones sensibles, avec principes de segmentation physique et logique.

Bon niveau de mise en œuvre :
Un bon dispositif combine contrôle d'accès par badges ou biométrie, enregistrement des accès, séparation des zones, surveillance vidéo, sécurisation des armoires et intégration avec le SOC ou la supervision technique.

C'est cette combinaison qui réduit le risque d'intrusion, de sabotage et de compromission du réseau hospitalier.

Protection des locaux techniques et des points de répartition sans traçabilité

Niveau 1

Selon les niveaux d'exigence, un système de protection avec ou sans traçabilité doit être mis en place sur différents types de locaux (opérateurs, répartiteurs général, serveurs, points de sous répartition). L'accès à ces locaux/espaces doit être accessible uniquement au personnel autorisé.

Ce niveau d'exigence requiert la protection de l'accès sans traçabilité aux locaux opérateurs et de répartition générale ainsi que de sous-répartition, exemples : clé (hors carré, triangle), code, ...

Protection des locaux techniques et des points de sous-répartition avec traçabilité

Niveau 2

Ce niveau de recommandation requiert la protection et la traçabilité des accès décrits dans les deux niveaux précédents, via par exemple un cylindre électronique, badge de contrôle d'accès, vidéosurveillance couplée à un verrouillage, moyens humains, boîte à clefs électronique...

CO 6 – Rafraîchissement des locaux informatiques

Cette recommandation vise à garantir le rafraîchissement des locaux informatiques pour en assurer le bon fonctionnement des équipements.

Systèmes de climatisation adaptés

Niveau 1

Ce sont des solutions spécifiquement conçues pour refroidir des environnements contenant des équipements sensibles : serveurs, switches, contrôleurs Wi-Fi, gateways IoT, stockage, onduleurs, etc.

Dans un Smart Hospital, ces systèmes doivent garantir stabilité, redondance, précision et continuité 24/7, car la moindre surchauffe peut impacter les soins.

Supervision et contrôle continu

Niveau 2

Assurer une supervision et un contrôle continu des systèmes de climatisation dans le Smart Hospital, c'est garantir que les locaux informatiques (salles serveurs, locaux de répartition, ...) restent stables, sécurisés et opérationnels 24/7.

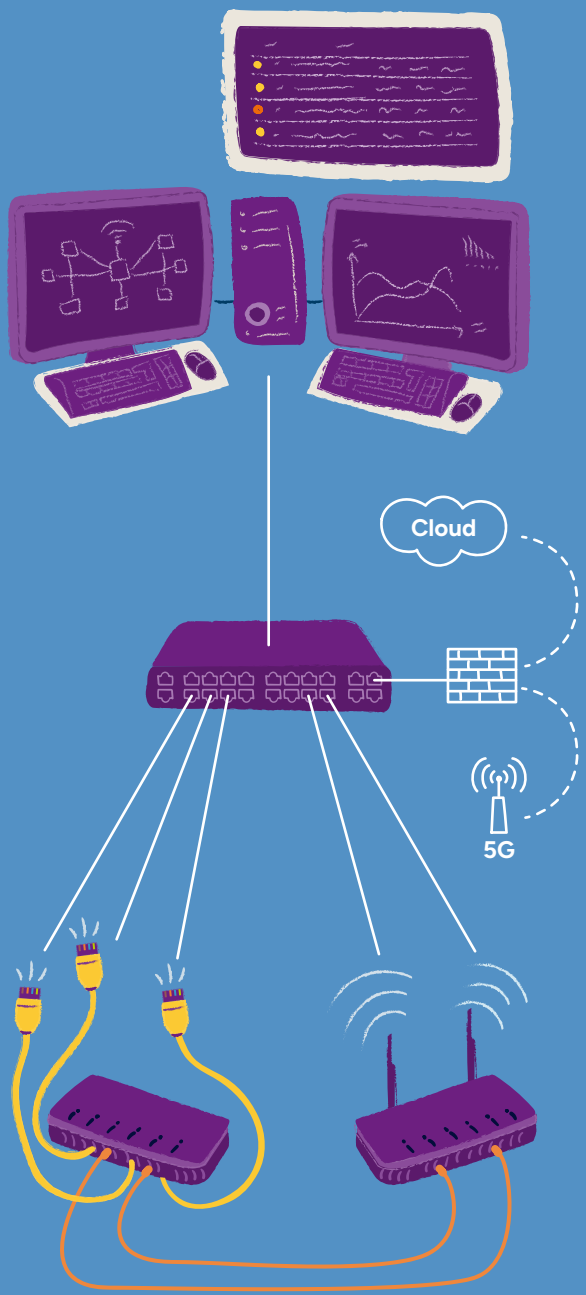
C'est un pilier de la résilience numérique hospitalière.

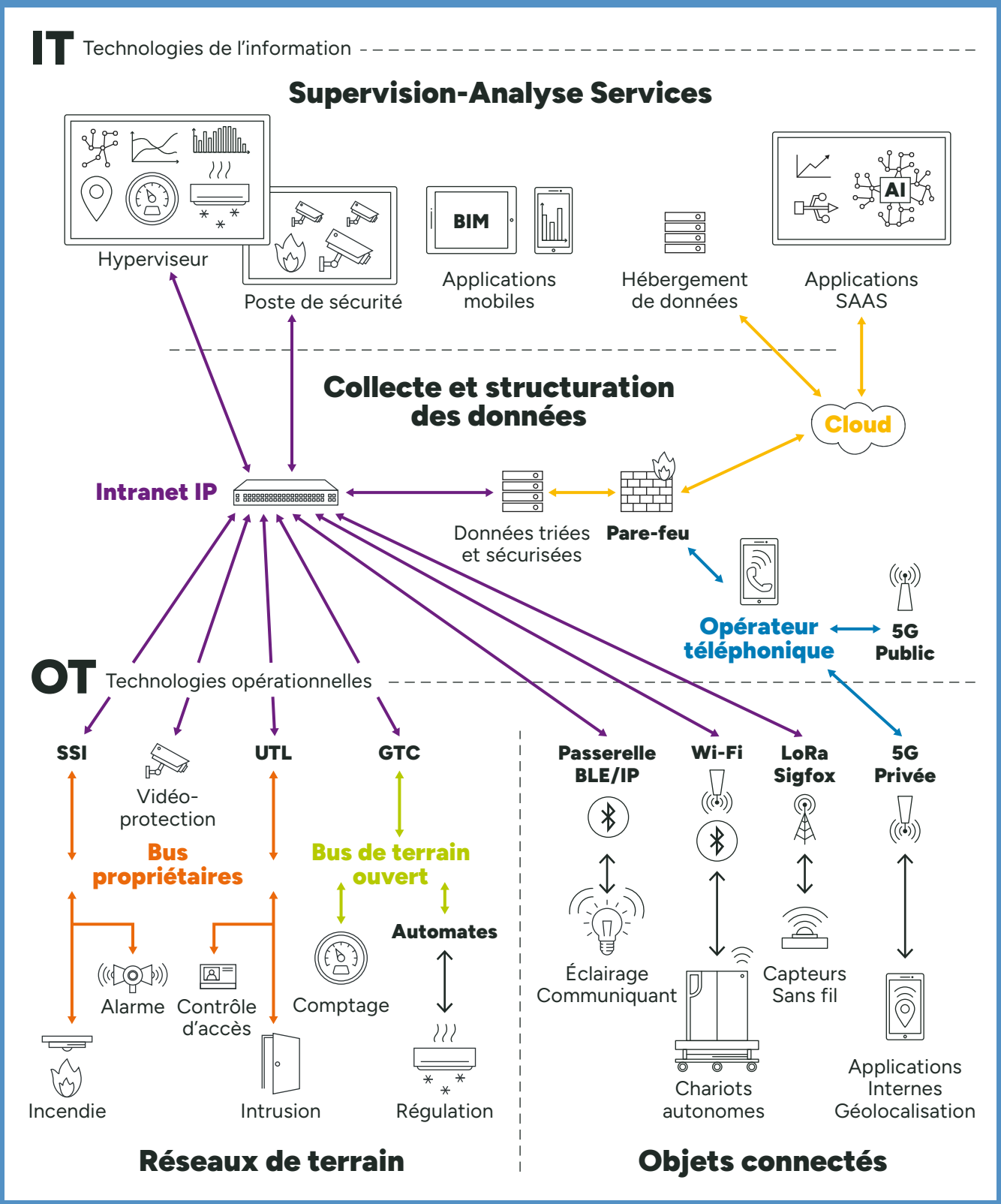
Architecture réseau

Ce thème a pour enjeu d'assurer la circulation du 4ème fluide du bâtiment, c'est-à-dire les données, qui constituent sa colonne vertébrale. Le cadre de référence R2S4Care pose comme prérequis la présence d'un réseau « Smart ». Le réseau « Smart » est le réseau fédérateur d'un bâtiment hospitalier R2S4Care orienté Services (SOA) et utilisant le protocole IP. Il est sécurisé et utilise exclusivement le standard Ethernet sur le réseau local et le standard Internet depuis l'extérieur du bâtiment.

La première partie du thème concerne la mise en place du réseau « Smart », des fonctionnalités permettant aux équipements de communiquer entre eux et la technologie PoE permettant de simplifier l'installation des équipements. Une attention est prêtée aux capacités de résilience du réseau « Smart » avec notamment la double connexion des équipements actifs d'accès et la détection d'anomalies sur le réseau.

Dans la deuxième partie, le thème s'intéresse à l'administration des équipements réseau afin d'améliorer l'exploitation, la surveillance des équipements, prioriser le trafic de certains réseaux en cas de surcharge, garantir le débit et le temps de rétablissement de la connexion internet en cas de panne.





LE RÉSEAU « SMART » : UNE ARCHITECTURE EN TROIS COUCHES

Recommandations		Niveau de maturité		Pages
RE 1 – Mettre en place le réseau « Smart »				→ p.36
RE 1.1 – DÉFINIR L'ARCHITECTURE LOGIQUE CIBLE		Prérequis	Cartographie du réseau physique	
	●	Niveau 1	Formaliser une segmentation logique et les règles de flux	
	●●	Niveau 2	Industrialiser et sécuriser l'architecture logique pour l'exploitation	
RE 1.2 – CRÉER UN RÉSEAU FÉDÉRATEUR IP UNIQUE		Prérequis	Existence d'une architecture cible	
	●	Niveau 1	Déployer un réseau unique, opéré et documenté	
	●●	Niveau 2	Homogénéiser, sécuriser et industrialiser le déploiement LAN/WLAN	
RE 1.3 – SEGMENTER LE RÉSEAU PAR USAGES	●	Niveau 1	Segmentation par VLAN et filtrage inter usages maîtrisés	
	●●	Niveau 2	Cloisonnement fort, micro segmentation et exploitation industrialisée	
RE 1.4 – UTILISER UNIQUEMENT DES PROTOCOLES OUVERTS	●	Niveau 1	Imposer des standards de communication et d'exploitation	
	●●	Niveau 2	Renforcer l'interopérabilité et la réversibilité	
RE 2 – Continuité et protection fonctionnelle du réseau « Smart »				→ p.40
RE 2.1 – CAPACITÉ DE RÉSILIENCE DU RÉSEAU « SMART »	●	Niveau 1	Double connexion des équipements actifs d'accès	
	●	Niveau 1	Résilience du mécanisme de redondance	
RE 2.2 – DÉTECTION D'ANOMALIES ET PROTECTION DU RÉSEAU « SMART »	●	Niveau 1	Détection et protection socle sur les équipements d'accès	
	●●	Niveau 2	Protection renforcée et réponse automatisée supervisée	
RE 3 – Management du réseau « Smart »				→ p.42
RE 3.1 – ADMINISTRATION DES RÉSEAUX ET DE LEURS ÉQUIPEMENTS	●	Niveau 1	Plateforme centralisée d'administration des switchs du réseau « Smart »	
	●●	Niveau 2	Plateforme d'administration de tous les équipements du réseau « Smart »	
RE 3.2 – PRIORISATION ET CONTINUITÉ DE SERVICE DES RÉSEAUX	●	Niveau 1	Définir et appliquer une qualité de service minimale de bout en bout	
	●●	Niveau 2	Piloter la performance et garantir la continuité en cas de surcharge	
RE 3.3 – GESTION DE DOMAINE ET ADRESSAGE DYNAMIQUE	●	Niveau 1	Mettre en place DNS/DHCP sur au moins un segment du réseau « Smart »	
	●●	Niveau 2	Généraliser, sécuriser et rendre résilients DNS/DHCP sur le réseau « Smart »	
RE 3.4 – CONTINUITÉ DE SERVICE INTERNET	●	Niveau 1	Fiabilisation de l'accès internet	
	●●	Niveau 2	Fiabilisation renforcée de l'accès internet	

RE 1 – Mettre en place le réseau « Smart »

Après avoir défini les objectifs de connectivité (raccordements externes, réseaux filaires et sans fil, redondance et continuité de service), il convient de structurer ces capacités au sein d'une architecture réseau « Smart » cohérente. Cette architecture décrit l'organisation du réseau de bout en bout (cœur, distribution, accès), les principes de segmentation, de sécurisation et d'exploitation, ainsi que les services réseau nécessaires pour supporter durablement les usages du Smart Hospital.

RE 1.1 – DÉFINIR L'ARCHITECTURE LOGIQUE CIBLE

La connectivité, abordée dans le thème précédent, garantit que les équipements et utilisateurs peuvent se connecter avec un niveau de performance et de disponibilité attendu : l'architecture physique du réseau « Smart » est définie et documentée.

L'architecture logique du réseau « Smart » décrit l'organisation fonctionnelle et logique des flux d'information, des protocoles de communication, des services et des mécanismes de sécurité, indépendamment du matériel physique utilisé.il s'agit de préciser qui communique avec qui, comment, dans quel but, et selon quelles règles.

L'architecture logique précise :

- segmentation par usages (VLAN/VRF),
- règles de routage inter VLAN,
- plan d'adressage IPv4/IPv6,
- services réseau (DNS/DHCP/NTP) et les règles de filtrage,
- la politique de qualité de service avec la priorisation des flux critiques/temps réel.

Cartographie du réseau physique

Prérequis

Le réseau « Smart » défini dans le thème « Connectivité » est cartographié et ses composants documentés.

Formaliser une segmentation logique et les règles de flux

Niveau 1

Définir les zones/segments par usages (ex. SI, biomédical, GTB, sûreté, Wi-Fi usagers, IoT) et les matérialiser en VLAN (Virtual Local Area Network) et/ou VRF (Virtual Routing and Forwarding) si nécessaire.

Établir la matrice « qui parle à qui » : flux autorisés/interdits, ports/protocoles, sens des communications, principes de filtrage (Access Control List - ACL/pare-feu) entre segments.

Définir le plan d'adressage (IPv4 et trajectoire IPv6) et les services réseau associés (DNS/DHCP/NTP) en précisant où ils sont hébergés et comment ils sont redondés.

Définir les principes de routage inter VLAN (niveau 3) et les points de sortie/peering (cœur, pare-feu, accès Internet, interconnexion SI).

Définir une politique de qualité de service minimale : identification des flux critiques/temps réel, classes de trafic et règles de priorisation.

Industrialiser et sécuriser l'architecture logique pour l'exploitation

Niveau 2

Mettre en place un vrai zonage de sécurité (macro-segmentation + micro-segmentation si pertinent) avec principes de moindre privilège et journalisation des flux inter zones.

Prévoir des VRF/instances de routage pour isoler des domaines sensibles (ex. biomédical, sûreté) et encadrer les interconnexions via pare-feu/politiques explicites.

Généraliser IPv6 selon une trajectoire définie (double stack, exigences d'accessibilité des services/API), avec règles de filtrage IPv6 équivalentes à IPv4.

Définir l'exploitation : conventions de nommage (VLAN, équipements, SSID), gestion des changements, sauvegarde/restauration, supervision et remontée d'alertes.

Compléter la qualité de service par des objectifs mesurables et des tests de validation en recette (congestion simulée, priorisation effective des flux critiques).

RE 1.2 – CRÉER UN RÉSEAU FÉDÉRATEUR IP UNIQUE

Le réseau « Smart » est un réseau IP fédérateur unique pour le bâtiment, l'ensemble de bâtiments ou le campus, supportant les réseaux filaires (LAN) et sans fil (WLAN) et permettant l'interconnexion maîtrisée des différents usages (SI, biomédical, GTB, sûreté, IoT, usagers). Il intègre également, lorsqu'ils sont déployés sur site, les réseaux cellulaires (4G/5G) et leurs équipements d'infrastructure (ex. DAS, small cells, routeurs cellulaires) dans une logique d'architecture et d'exploitation cohérente.

Le réseau «Smart» constitue le socle commun de connectivité et doit éviter la multiplication de réseaux isolés non maîtrisés.

Existence d'une architecture cible

Prérequis

Existence d'une architecture cible précisant segmentation, services réseau (DNS/DHCP/NTP), règles de filtrage et principes d'exploitation ; disponibilité des locaux techniques, des cheminements et du câblage (cuivre/fibre) permettant de raccorder les équipements actifs et les points d'accès Wi-Fi.

Déployer un réseau unique, opéré et documenté

Niveau 1

Déployer une infrastructure filaire Ethernet unique (cœur/distribution/accès) pour l'ensemble des besoins du bâtiment ;

Déployer le réseau Wi-Fi comme un service du réseau « Smart » ;

Intégrer les équipements de couverture cellulaire (4G/5G) au réseau « Smart » lorsqu'ils existent ;

Mettre en place les services réseau nécessaires au fonctionnement (adressage, DNS/DHCP/NTP) et les mécanismes de base de sécurité (filtrage inter segments, séparation des usages Wi-Fi).

Assurer la cohérence d'exploitation : plan de nommage, documentation à jour, procédures de mise en service et de modification.

●●

Homogénéiser, sécuriser et industrialiser le déploiement LAN/WLAN

Niveau 2

Standardiser les équipements et configurations afin de réduire l'hétérogénéité et faciliter le maintien en condition opérationnelle.

Mettre en œuvre une séparation forte des usages et un contrôle des accès réseau pour les segments sensibles.

Encadrer les réseaux cellulaires par des exigences de sécurité et d'exploitation en cohérence avec la politique globale de cybersécurité de l'établissement ;

Formaliser les critères de recette LAN/WLAN : couverture et capacité Wi-Fi, performance (débit/latence), itinérance, segmentation effective, bascule en cas de défaillance, et conformité des configurations livrées.

RE 1.3 – SEGMENTER LE RÉSEAU PAR USAGES

Segmenter le réseau par usages consiste à séparer logiquement les équipements/services en zones (souvent des VLAN, éventuellement des VRF pour une isolation plus forte) puis à contrôler explicitement les flux autorisés entre ces zones (routage + filtrage).

Concrètement :

- Lister les usages et classer leur criticité (SI interne, biomédical, GTB/GTC, IoT bâtiment, Wi-Fi usagers, invités/prestataires, ...)
- Créer les segments : 1 usage = 1 VLAN (règle simple de départ) + éventuellement sous-segmentation (par bâtiment/étage) en fonction de la volumétrie.
- Définir la « matrice des flux » (qui parle à qui)
- Mettre en œuvre le routage et le filtrage inter VLAN au niveau cœur/distribution ;
- Marquer/prioriser les flux critiques (voix, temps réel, sûreté si besoin).
- Documenter : liste VLAN/VRF, plan d'adressage, règles, responsabilités d'exploitation, tests de recette.

●

Segmentation par VLAN et filtrage inter usages maîtrisés

Niveau 1

Définir des usages et les traduire en VLAN avec un plan de nommage et un plan d'adressage cohérents.

Définir et maintenir une matrice de flux (autorisations/interdictions) entre VLAN : ports/protocoles, sens, justification métier.

Appliquer un principe interdit par défaut et n'ouvrir que les flux nécessaires, via ACL et/ou pare feu aux points d'interconnexion.

Aligner les réseaux Wi-Fi sur la segmentation : 1 SSID (ou profil) → 1 VLAN/usage, avec séparation stricte des usagers/invités/objets/administration.

Valider la segmentation par des tests de recette : isolation inter VLAN, accès aux services requis (DNS/DHCP/NTP), accès SI/Internet selon usage.

●●

Cloisonnement fort, micro segmentation et exploitation industrialisée

Niveau 2

Isoler les domaines sensibles (ex. biomédical, sûreté) et contrôler les échanges uniquement via des points de passage sécurisés (pare feu, politiques explicites, journalisation).

Mettre en œuvre une micro segmentation quand nécessaire (par type d'équipement, service, salle/zone) pour limiter la propagation latérale en cas d'incident.

Standardiser les profils (ports, VLAN, Qualité de service, SSID) et automatiser/industrialiser le déploiement (modèles, procédures, contrôles de conformité).

Renforcer la traçabilité : logs de sécurité, supervision des flux inter-zones, alertes sur comportements anormaux (scans, tempêtes, dépassements).

Étendre la recette : tests de contournement (accès non autorisé), tests en charge/Qualité de service et tests de bascule si redondance.

RE 1.4 – UTILISER UNIQUEMENT DES PROTOCOLES OUVERTS

L'utilisation de protocoles ouverts vise à garantir l'interopérabilité, la pérennité et la réversibilité du réseau « Smart ». Elle limite les dépendances à un constructeur, facilite l'intégration d'équipements hétérogènes (SI, biomédical, GTB, sûreté, IoT) et permet une exploitation/outillage standard (supervision, logs, automatisation).

●

Imposer des standards de communication et d'exploitation

Niveau 1

Utiliser IP sur l'ensemble du réseau « Smart » (LAN/WLAN), avec Ethernet sur le réseau local et une trajectoire IPv6 définie en cohérence avec l'architecture logique.

S'appuyer sur des standards ouverts pour la segmentation et l'accès : IEEE 802.1Q (VLAN), et lorsque pertinent IEEE 802.1X (contrôle d'accès) ; éviter les mécanismes propriétaires équivalents.

- Utiliser des services réseau ouverts : DNS, DHCP, NTP.
- Superviser et administrer via des protocoles ouverts et sécurisés quand disponibles (ex. SNMPv3), et s'appuyer sur des mécanismes de journalisation standard (ex. syslog) selon les pratiques de l'établissement.
- Pour la résilience de niveau 2 (RE2.1/ RE2.2), privilégier des standards largement supportés (ex. RSTP/MSTP, LACP) en cohérence avec l'architecture retenue.

●●

Renforcer l'interopérabilité et la réversibilité

Niveau 2

Vérifier que tout équipement/solution livré(e) fournisse une documentation publique des protocoles utilisés et de leurs versions, et qu'aucune fonction critique ne dépende d'un protocole propriétaire non publié.

Exiger la compatibilité multi-constructeurs des fonctions réseau clés (segmentation, routage, Wi-Fi entreprise, supervision) et encadrer contractuellement les éventuelles extensions propriétaires .

Mettre en place des mécanismes standard de collecte de logs et d'observabilité (supervision, métriques, événements) compatibles avec les outils de l'établissement, pour éviter l'enfermement dans une console unique.

RE 2 – Continuité et protection fonctionnelle du réseau « Smart »

RE 2.1 – CAPACITÉ DE RÉSILIENCE DU RÉSEAU « SMART »

Le réseau « Smart » supporte des mécanismes de détection de coupure de réseau et d'auto-cicatrisation (fonctions de résilience des réseaux locaux IP du réseau « Smart »).

●

Double connexion des équipements actifs d'accès

Niveau 1

Ce niveau d'exigence requiert que chaque équipement actif d'accès du réseau « Smart » dispose de deux connexions au minimum avec d'autres switchs, assurant de fait une redondance de liaison et une résilience du réseau (exemples : protocoles STP, RSTP, MSTP).

●●

Résilience du mécanisme de redondance

Niveau 2

Ce niveau d'exigence requiert :

- l'atteinte du niveau précédent ;
- la présence de mécanisme de redondance apportant une résilience plus rapide, nécessaires au services temps réel d'une durée maximale d'une demi-seconde (exemples : protocole LACP avec un cœur virtualisé, ou G.8032, ou MRP).

RE 2.2 – DÉTECTION D'ANOMALIES ET PROTECTION DU RÉSEAU « SMART »

Au sein du bâtiment hospitalier connecté et communicant, les switchs du réseau « Smart » utilisent le protocole SNMP V3 supportent des mécanismes de détection d'anomalies (exemples : saturation d'un port, tempête de broadcast) et sont en mesure d'agir automatiquement sur les ports réseaux.

La détection d'anomalies par les switchs du réseau « Smart » implique la mise en place des fonctions suivantes :

- Détection de tempête de broadcast et d'émergence de boucles, et protection du réseau « Smart » contre ces types d'anomalies ;
- Remontée d'information SNMP V3 auprès de l'administrateur ;
- Détection et actions correctives du ou des ports Ethernet concernés par l'anomalie (exemples : fermeture automatique, remontée d'alarme).

●

Détection et protection socle sur les équipements d'accès

Niveau 1

Mettre en place, sur les équipements réseau, des protections de base pour détecter et contenir les incidents qui peuvent perturber fortement le réseau (ex. trop de messages envoyés en même temps ou création accidentelle d'une boucle).

Ces protections doivent s'appuyer sur des seuils définis, adaptés aux usages et documentés.

●●

Protection renforcée et réponse automatisée supervisée

Niveau 2

Repérer aussi les problèmes plus « fins » qui dégradent le service ou qui peuvent annoncer un incident : lenteurs persistantes, erreurs répétées sur une connexion, coupures/reconnexions fréquentes, volumes de messages anormalement élevés, ou comportements inhabituels de certains équipements.

Regrouper ces alertes dans un outil de supervision unique, pour comprendre rapidement d'où vient le problème (zone/équipement/connexion concernée) et quels services sont impactés, en particulier les services les plus critiques.

Prévoir des réactions automatiques pour limiter un incident (par exemple isoler temporairement un équipement, réduire son trafic ou bloquer une connexion), tout en gardant une traçabilité et des règles de prudence (délai, validation, réouverture contrôlée) afin d'éviter des coupures non souhaitées.

Définir des tests de vérification lors de la réception :pour vérifier que les alertes remontent bien à l'administrateur et que les protections agissent comme prévu, sans interrompre les services prioritaires au delà d'un niveau acceptable.

RE 3 – Management du réseau « Smart »

Le management du réseau « Smart » regroupe l'ensemble des processus, outils et responsabilités permettant de piloter, exploiter et sécuriser durablement l'infrastructure réseau (LAN/WLAN, équipements actifs, services réseau).

Il couvre notamment la gouvernance (rôles, responsabilités, règles d'accès), l'administration et la supervision, la gestion des changements, la gestion des incidents, la tenue à jour de la documentation et le maintien en condition opérationnelle et de sécurité.

RE 3.1 – ADMINISTRATION DES RÉSEAUX ET DE LEURS ÉQUIPEMENTS

L'administration des réseaux et de leurs équipements permet de configurer, contrôler, maintenir et faire évoluer l'infrastructure réseau (switchs, routeurs, pare-feu, contrôleurs/points d'accès Wi-Fi, services réseau), afin d'assurer la disponibilité, la performance, la sécurité et la traçabilité du réseau « Smart ».

Les activités, à minima, d'administration sont :

- Gestion des habilitations : comptes nominatifs, rôles (lecture/écriture), authentification forte si applicable, traçabilité des actions d'admin.
- Gestion de la configuration : modèles, paramétrages (VLAN/VRF, routage, ACL/pare-feu, Qualité de service, Wi-Fi), gestion de versions, conformité aux standards.
- Supervision et exploitation : états/liens/ports, capacité/performance, détection d'anomalies, gestion des alertes, tableaux de bord et rapports.
- Gestion des incidents : diagnostic, escalade, rétablissement, analyse des causes (RCA) et actions correctives/préventives.
- Maintien en condition opérationnelle (MCO) : inventaire, obsolescence, gestion des licences/contrats, capacité (ports/PoE), planification des extensions.

Ces activités sont outillées par une ou plusieurs plateformes d'administration selon le niveau visé : centralisation, supervision, collecte d'événements, gestion de configuration.

Le périmètre du management du réseau « Smart » doit couvrir :

- l'inventaire et la documentation (schémas, plan de nommage, plans de brassage),
- la gestion de configuration (sauvegarde/restauration, référentiel de versions),
- la supervision et la gestion des alertes (états, performances, liens, anomalies),
- la gestion des comptes et habilitations d'administration,
- la gestion des incidents (diagnostic, escalade, rétablissement),
- le MCO/MCS (correctifs, mises à jour, obsolescence, durcissement).

Plateforme centralisée d'administration des switchs du réseau « Smart »

Niveau 1

L'objectif est de mettre en place une plateforme logicielle d'administration qui permet la centralisation de l'administration et des remontées d'informations et d'anomalies des équipements actifs du réseau.

Ce niveau d'e recommandation implique :

- La mise en place d'une plateforme logicielle centralisée d'administration. Cette plateforme peut être localisée sur le réseau « Smart » ou hébergée sur le cloud
- Le paramétrage des équipements supervisés pour assurer la remontée de leurs états et défauts dans un protocole ouvert et interopérable (exemple : SNMP v3°
- La supervision des liens actifs ou en défaut ainsi que les anomalies constatées sur les éléments actifs du réseau « Smart ».

Remarque : Le cadre de référence n'est pas prescriptif sur le protocole à mettre en place, si un protocole différent du SNMP est choisi il devra permettre les mêmes fonctionnalités que le protocole SNMP V3 (ouverture, interopérabilité, authentification, chiffrement…).

●●

Plateforme d'administration de tous les équipements du réseau « Smart »

Niveau 2

Ce deuxième niveau de recommandation implique qu'une unique plateforme unique et centralisée supervise et administre tous les éléments constituant le réseau « Smart » :

- Les équipements actifs du réseau « Smart » (c'est à ditx couverts par le niveau précédent + routeurs, pare-feu, équipements d'interface avec les réseaux opérateurs de télécommunication),
- Les contrôleurs Wi-Fi locaux et/ou aux points d'accès Wi-Fi,
- Les serveurs centraux

RE 3.2 – PRIORISATION ET CONTINUITÉ DE SERVICE DES RÉSEAUX

La priorisation correspond à la mise en œuvre de mécanismes de Qualité de Service (QoS) pour garantir, en situation de congestion, la performance des flux critiques (ex. voix, temps réel, sûreté, applications SI).

La continuité de service vise à maintenir un niveau de service conforme aux engagements de qualité de service (SLA) : débit, latence, gigue, perte.) grâce à une exploitation/supervision permettant d'anticiper et de traiter les surcharges.

●

Définir et appliquer une qualité de service minimale de bout en bout

Niveau 1

Pour atteindre ce niveau, les actions et fonctionnalités à mettre en œuvre sont :

- Identifier les flux critiques et formaliser les objectifs associés (latence/gigue/perte) en cohérence avec le(s) engagements de qualité de service ;
- Définir des classes de trafic (ex. critique, prioritaire, best effort, non critique) et les règles de marquage associées (principe : marquer au plus près de la source et conserver le marquage).
- Configurer les équipements en fonction des classes et des priorisations ;
- Définir des règles de gestion de congestion (seuils, limitation si nécessaire) ;

●●

Piloter la performance et garantir la continuité en cas de surcharge

Niveau 2

– Étendre la qualité de service au Wi-Fi (priorisation cohérente avec le filaire) et aux interconnexions externes (WAN/Internet) pour garantir la continuité des usages mobiles et des services hébergés.
– Mettre en place un monitoring des indicateurs de performance (taux d'occupation, pertes, latence, gigue) et des alertes sur dépassement de seuils, avec capacité d'analyse des causes
– Définir des plans d'action en cas de surcharge (réallocation des classes, limitation des flux non critiques, extension de capacité) et des procédures d'exploitation associées (MCO/MCS).
– Réaliser des tests en charge (congestion simulée) pour vérifier l'efficacité de la priorisation et la tenue des engagements de qualité de service (SLA) sur les flux critiques.

RE 3.3 – GESTION DE DOMAINE ET ADRESSAGE DYNAMIQUE

La gestion de domaine et l'adressage dynamique reposent sur :

– un service de résolution de noms (DNS) pour accéder aux équipements et services par des noms plutôt que par des adresses,
– un service DHCP pour attribuer automatiquement des adresses IP (ainsi que les paramètres réseau) et éviter les conflits liés aux configurations statiques non maîtrisées.

La gestion de domaine et l'adressage dynamique reposent sur :

– un service de résolution de noms (DNS) pour accéder aux équipements et services par des noms plutôt que par des adresses,
– un service DHCP pour attribuer automatiquement des adresses IP (ainsi que les paramètres réseau) et éviter les conflits liés aux configurations statiques non maîtrisées.

L'objectif est de mettre en place une fonction qui évite les pannes causées par des doublons d'adresses pouvant apparaître lors de la mise en œuvre d'un adressage statique.

Remarque : Il n'y a pas de préconisation sur l'équipement qui assure le rôle de serveur DNS et DHCP (serveurs, coeur de réseau…).

●

Mettre en place DNS/DHCP sur au moins un segment du réseau « Smart »

Niveau 1

Activer un service DHCP pour au moins un VLAN/segment du réseau « Smart » (ex. équipements mobiles, Wi-Fi usagers, postes d'exploitation) afin de réduire les risques de doublons d'adresses.

Définir un plan d'adressage par segment (plages, passerelles, DNS, options) et documenter les règles d'attribution (dynamique, réservations, statique autorisé/interdit).

Superviser *a minima* les services (disponibilité, saturation de plages, erreurs) et intégrer les journaux DHCP/DNS aux processus d'exploitation.

●●

Généraliser, sécuriser et rendre résilients DNS/DHCP sur le réseau « Smart »

Niveau 2

Déployer DHCP et DNS sur l'ensemble des segments avec des conventions de nommage uniformes (équipements, sites, VLAN, services) et une documentation exploitable.

Assurer la redondance des services (au moins deux instances/serveurs, tolérance à la panne) et définir les comportements en mode dégradé (baux, caches, bascule).

Renforcer la sécurité : droits d'administration restreints, durcissement, journalisation, et mesures de protection contre les services non autorisés (ex. serveurs DHCP « sauvages ») selon les capacités du réseau.

Mettre en place une supervision avancée (taux d'utilisation des plages, collisions, temps de réponse DNS, erreurs) et des alertes, avec procédures de remédiation.

RE 3.4 – CONTINUITÉ DE SERVICE INTERNET

Il s'agit de faciliter la mise en place de services, apporter un accès internet aux utilisateurs, réaliser des opérations de télémaintenance, ou encore faciliter les opérations de mise à jour par la mise en place d'un accès à internet au réseau « Smart ». Les niveaux 2 et 3 valorisent une sécurisation de l'accès internet du réseau « Smart ».

●

Fiabilisation de l'accès internet

Niveau 1

Le réseau « Smart » dispose d'un accès internet permanent (exemples : fibre optique, DSL, à l'exclusion de moyens provisoires de chantier comme une clé 4G/5G).

La disponibilité de l'accès internet du réseau « Smart » peut être fiabilisée en faisant l'objet d'un engagement contractuel de l'opérateur qui apporte une Garantie de Temps de Rétablissement (GTR) en cas d'interruption du service, dont la durée maximale doit être définie en cohérence avec les enjeux de continuité de service du Smart Hospital.

La fiabilisation peut également être apportée par l'existence d'au moins deux accès internet indépendants apportant une redondance des connexions entrantes et sortantes.

●●

Fiabilisation renforcée de l'accès internet

Niveau 2

Ce niveau d'exigence requiert la mise en place d'au moins deux accès internet indépendants ET une GTR (Garantie de Temps de Rétablissement) sur au moins un de ces accès internet.

Remarque, lorsque plusieurs accès internet sont activés, chacun d'eux doit faire l'objet d'une connectivité indépendante dans le bâtiment afin de bénéficier d'une redondance de cheminement.

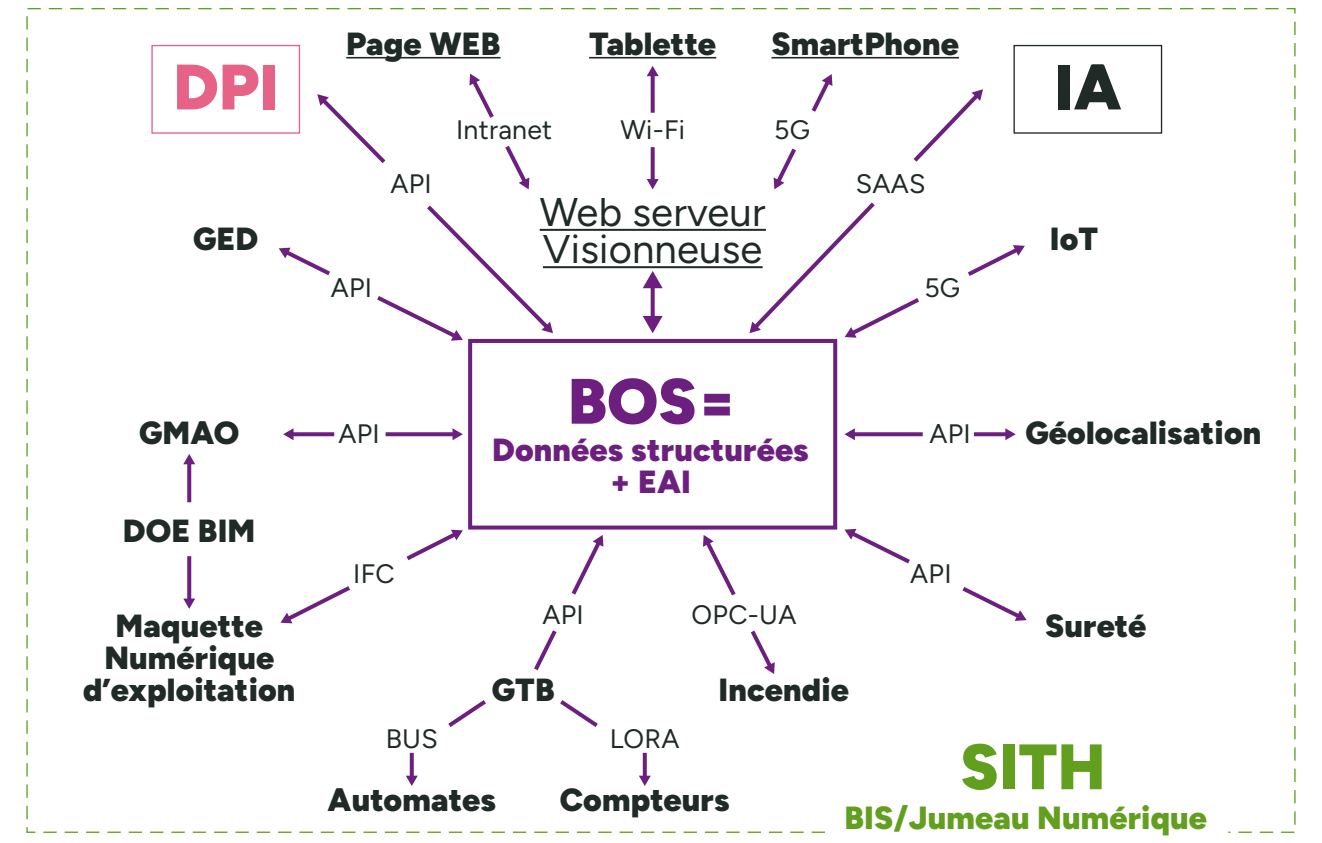
Data management et interopérabilité

Le concept de Smart Hospital repose sur la mise en œuvre du SITH et son objectif de faire de la donnée le 4ème fluide du bâtiment hospitalier. Dans cette approche, la donnée n'est plus considérée comme un simple sous-produit des équipements techniques, mais comme une ressource distribuée et pilotée au même titre que l'électricité, l'eau, les fluides médicaux.

Le schéma, ci-après, montre la multiplicité des sources de données que le SITH doit pouvoir circuler entre tous les environnements, mais toujours en restant interopérable, sécurisée, gouvernée.

La structuration des données constitue un enjeu central dans le développement d'un Smart Hospital. Elle vise à organiser, fiabiliser et rendre exploitables les informations issues du patrimoine bâti, des équipements techniques et des systèmes en exploitation. Dans un environnement hospitalier caractérisé par la complexité des installations, la multiplicité des acteurs et la criticité des usages, la donnée -quatrième fluide du bâtiment- conditionne directement la performance des activités d'exploitation, de maintenance et de pilotage.

LE SITH EST UNE PARTIE DU SIH



La structuration des données doit reposer sur une organisation claire des référentiels, distinguant les différentes sources :

- **les données patrimoniales** (maquette numérique),
- **les données techniques** (caractéristiques des équipements),
- **les données opérationnelles** (issues des systèmes en exploitation).

Les recommandations de ce thème visent :

- **une exploitation intégrée** (énergie, confort, maintenance, sécurité, support aux services de soins) ;
- **une réduction des coûts d'intégration et d'exploitation** ;
- **une agilité dans l'évolution des usages** et la connexion avec les systèmes urbains (smart grid, smart city).

Deux fonctions complémentaires sont abordées : la data management et l'interopérabilité.

- **Le data management** vise à organiser, gouverner, stocker, sécuriser et valoriser les données du Smart Hospital.
- **L'interopérabilité** permet à ces données de circuler entre plusieurs systèmes, applications ou services du SITH. Cette fonction est assurée par le BOS (Building Operating System) et les API (Application Programming Interface).

Grâce au data management à l'interopérabilité, le Smart Hospital a la possibilité d'ouvrir les données du bâtiment et de les rendre accessibles pour une optimisation de ses usages.

- **Sans interopérabilité**, le data management reste limité, car les données sont enfermées dans des silos.
- **Sans bonne gestion des données,** l'interopérabilité risque de diffuser des données incohérentes ou de mauvaise qualité.

Ensuite un focus est mis sur trois composants essentiels dans la mise en œuvre de ces fonctions : **le BOS**, **les API** et **le BIM**.

- **Le BOS** est une couche logicielle intermédiaire intégrée au SITH. Il gère le référentiel partagé de données, orchestre l'interopérabilité des services, coordonne les échanges entre les systèmes et assure la gouvernance des données de l'ouvrage.

– **Les API** (Application Programming Interface), ou interface de programmation d'application, est un ensemble de règles qui permet à deux logiciels de communiquer et d'échanger des données ou des fonctionnalités.

– **Le BIM** produit et organise toutes les données d'un bâtiment pendant son cycle de vie : conception, construction, exploitation et maintenance. Le data management permet de gérer ces données pour qu'elles restent fiables, cohérentes et accessibles.

Recommandations	Niveau de maturité		Pages
IN 1 – Le data management			→ p.49
IN 1.1 – LES OBJECTIFS DU DATA MANAGEMENT	Prérequis	« by design », la data 4ème fluide du bâtiment	
IN 1.2 – LES OUTILS DU DATA MANAGEMENT	● Niveau 1	Socle de collecte, fiabilisation et restitution	
	●● Niveau 2	Gouvernance avancée, traçabilité et convergence OT/IT	
IN 1.3 – LE RÉFÉRENTIEL			
Les éléments du référentiel du SITH			
Référentiel technique et données DOE	● Niveau 1	Socle de langage commun (interopérabilité minimale)	
	●● Niveau 2	Référentiel industrialisé (gouvernance avancée et extension multi-sources)	
IN 2 – L'interopérabilité des équipements et systèmes			→ p.54
IN 2.1 – PROTOCOLES ET INTÉGRATION DES ÉQUIPEMENTS AU RÉSEAU « SMART »			
IN 2.2 – API ET COMMUNICATION INTER SYSTÈMES			
API terrain et API centrales			
Continuité de fonctionnement des équipements communicants			
Modèle économique des API			
Rétrocompatibilité des API	Prérequis	Capacité des équipements à s'interfacer avec une API au réseau « Smart »	
	● Niveau 1	Socle d'exposition et d'intégration (API opérationnelles)	
	●● Niveau 2	Industrialisation, gouvernance et qualité de service des API	
IN 3 – Le Building Operating Sytem (BOS)			→ p.58
IN 3.1 – LES OBJECTIFS DU BOS			
IN 3.2 – LES FONCTIONNALITÉS DU BOS	Prérequis	Définition le périmètre et les objectifs du projet.	
	● Niveau 1	Définition de l'architecture du SITH et justification du BOS	
	●● Niveau 2	Le projet BOS	
IN 4 – Le Building Information Modeling (BIM)			→ p.62
IN 4.1 – LE BIM CONCEPTION			
IN 4.2 – LE BIM GEM			
IN 4.3 – LE RÉFÉRENTIEL DU BIM (NORME ISO 19650)			
IN 4.4 – DU BIM AU JUMEAU NUMÉRIQUE	● Niveau 1	Socle BIM Conception + BIM GEM (référentiel exploitable)	
	●● Niveau 2	BIM industrialisé et transition vers le jumeau numérique	

IN 1 – Le data management

Le data management pour le Smart Hospital correspond à l'ensemble des dispositifs organisationnels, méthodologiques et techniques permettant de produire, qualifier, sécuriser, partager et conserver des données fiables, traçables et conformes aux exigences réglementaires du secteur de la santé (voir thème « Sécurité Numérique »).

Le data management désigne donc un ensemble de processus, de rôles et d'outils visant à transformer des données brutes en données exploitables, gouvernées et interprétables, dans le respect des règles de confidentialité, d'intégrité et de disponibilité.

Dans le Smart Hospital, il couvre la définition des structures de données, les contrôles de cohérence, la standardisation des dictionnaires, la validation, le suivi des anomalies et la documentation du modèle de données.

Il est le prérequis à l'utilisation de l'intelligence artificielle.

IN 1.1 – LES OBJECTIFS DU DATA MANAGEMENT

Le Data Management cherche à garantir que les données de l'entreprise soient fiables, accessibles, sécurisées et utiles pour soutenir la prise de décision et la performance. Il d'en faire un actif stratégique fiable, maîtrisé et exploitable.

Les objectifs du Data Management dans l'infrastructure du réseau « Smart » sont :

Éviter la dispersion et le cloisonnement des données
Réduire les silos d'information en centralisant, harmonisant et rendant interopérables les données afin d'assurer une vision cohérente, partagée et gouvernée du patrimoine informationnel.

Créer et maintenir une référence unique, fiable et cohérente pour les données, afin d'améliorer leur gouvernance, leur exploitation, la cohérence du SITH
Constituer un référentiel de confiance, partagé par l'ensemble des acteurs, assurant la qualité, la traçabilité et l'interopérabilité des données au service du pilotage et de la performance du SI.

Faciliter l'accès et la partage pour favoriser la coopération et l'efficacité opérationnelle
Mettre à disposition des données fiables, accessibles et partageables pour favoriser la coopération inter-structures et améliorer l'efficacité opérationnelle.

Développer la traçabilité des évènements et activités des processus
Les données assurent la traçabilité des événements et des activités en enregistrant, de façon horodatée et structurée, qui a fait quoi, quand, sur quel ensemble de données, et avec quel résultat.

Sécuriser les données en tant qu'actif stratégique du Smart Hospital
Mettre en place les mesures de sécurité, de traçabilité et de gouvernance nécessaires à leur protection et à leur valorisation : confidentialité, Intégrité, disponibilité, gouvernance.

IN 1.2 – LES OUTILS DU DATA MANAGEMENT

Les outils du data management relèvent de plusieurs catégories selon la fonction : intégration, qualité, gouvernance, référentiels, stockage, sécurité et visualisation. Ils servent à connecter les sources, fiabiliser les données, organiser les règles d'usage et fournir une base commune de référence.

Les outils du Data Management servent à collecter, stocker, nettoyer, sécuriser, analyser et gouverner les données. Ils couvrent plusieurs fonctions complémentaires.

Collecte et intégration des données
Ils permettent de récupérer les données depuis différentes sources (ERP, CRM, capteurs, fichiers, bases de données, IoT).

Outils de stockage des données
Ils centralisent les données dans une base unique. Data Warehouse pour des données structurées et destinées au reporting. Data Lake pour stocker de gros volumes de données variées (structurées, non structurées, son, images, ...).

Qualité des données
Ils vérifient si les données sont complètes, cohérentes et sans doublons.

Gouvernance de catalogue de données et Master Data Management
Ils permettent d'avoir une version unique et cohérente des données critiques : patients, séjours, bâtiments, équipements, fournisseurs, ...Ils centralisent les métadonnées, les glossaires métier, les règles, la propriété des données pour soutenir la conformité et l'usage opérationnel.

Analyse et visualisation
Ils transforment les données brutes en rapports, tableaux de bord et indicateurs exploitables pour le pilotage.

Sécurité et conformité
Les outils de sécurité et de conformité en data management servent à protéger les données, surveiller les accès, prouver la conformité et automatiser les contrôles. Ils couvrent généralement la gouvernance, le chiffrement, la gestion des accès, les journaux d'audit, la confidentialité et la préparation des audits.

Socle de collecte, fiabilisation et restitution

Niveau 1

- Collecte & intégration : mettre en place des connecteurs/flux d'ingestion pour les principales sources (ERP, GMAO, GTB, capteurs, fichiers) avec une stratégie de fréquence (temps réel, quasi temps réel, batch) et de gestion des erreurs.
- Stockage : disposer d'un stockage central (Data Warehouse pour le reporting structuré, Data Lake pour les volumes et formats variés) avec une séparation claire des zones (brut, préparé, publié).
- Qualité des données : définir des contrôles minimum (complétude, doublons, cohérence, unités, horodatage) et un traitement des anomalies (quarantaine, corrections, rapprochements).
- Sécurité de base : appliquer l'authentification, la gestion des rôles, la segmentation des accès et un chiffrement adapté, en cohérence avec les exigences SI/SSI hospitalières.
- Analyse & visualisation : produire des tableaux de bord et indicateurs « prêts à piloter » (exploitation, maintenance, énergie) avec une définition partagée des KPI et des règles de calcul.

●●

Gouvernance avancée, traçabilité et convergence OT/IT

Niveau 2

- Gouvernance, catalogue & MDM (Master Data Management) : déployer un catalogue de données (métadonnées, glossaire, propriétaires, règles d'usage) et un MDM pour les données critiques (patients/séjours, bâtiments, équipements, fournisseurs), afin d'assurer une « version de référence » et de faciliter l'interopérabilité.
- Traçabilité & auditabilité : généraliser la journalisation (logs), la traçabilité des transformations (data lineage), l'horodatage et l'identification des actions pour reconstituer le parcours complet de la donnée et soutenir les contrôles/audits.
- Sécurité & conformité renforcées : automatiser les contrôles (revues d'accès, détection d'anomalies, politiques de rétention), mettre en place des preuves de conformité et préparer les audits (journaux, rapports, alertes).
- Convergence OT/IT : privilégier une architecture unifiée capable d'ingérer, superviser en temps réel et analyser les données opérationnelles (automates, capteurs IoT) tout en respectant les contraintes de cybersécurité (segmentation, passerelles, API management).
- Industrialisation : standardiser les pipelines (CI/CD données), la gouvernance des schémas et versions, et les mécanismes de reprise (résilience, supervision, SLA), afin de sécuriser l'exploitation à l'échelle du patrimoine.
- Les données assurent la traçabilité des événements et des activités en enregistrant, de façon horodatée et structurée, qui a fait quoi, quand, sur quel objet de données, et avec quel résultat. Cette traçabilité repose sur les logs, la traçabilité, les métadonnées, les identifiants d'utilisateur et les journaux d'audit, qui permettent de reconstituer le parcours complet d'une information.

IN 1.3 – LE RÉFÉRENTIEL

Le référentiel désigne un ensemble d'ontologies (liens entre objets) et de règles sémantiques (tags, attributs) qui permettent de décrire un « langage commun » partagé entre les différentes composantes d'un système afin de permettre leur compatibilité, leur compréhension mutuelle par tous les acteurs d'un projet.

Ces niveaux peuvent être déployés de façon progressive : le Niveau 1 fixe le « minimum vital » pour intégrer des systèmes au SITH, tandis que le Niveau 2 sécurise l'évolutivité, la qualité et l'auditabilité du référentiel dans la durée.

Tant qu'un système, un équipement ou une application ne parle pas le langage du SITH (ne partage pas le référentiel), alors il ne fait pas partie du SITH.

L'API est l'outil logiciel qui réalise concrètement la traduction et l'intégration entre les systèmes.

Les éléments du référentiel du SITH

Le référentiel n'est pas une description unique, il est composé d'un ensemble de sous référentiels parmi lesquels :

- Le référentiel du BIM GEM
- Autres référentiels structurés/organisationnels et hiérarchiques :
- Profils des salles, charte immobilière ;
- Profils (identifiants) utilisateurs.
- Référentiel sémantique :
  - → Description des composants du SITH ;
  - → Typologies entités physiques ou logiques partagées (mesure, alarme, consigne, tickets, événements, équipements, objets BIM…) ;
  - → Caractéristiques partagées (attributs, tags, métadonnées, conventions de nommage…).
- Référentiel de synchronisation temporelle :
  - → Temps ;
  - → Unités.
- Référentiel d'unités unifiées et partagées.

Référentiel technique et données DOE

Le référentiel technique regroupe l'ensemble des informations nécessaires à l'exploitation et à la maintenance des équipements et des installations. Il s'appuie principalement sur les données issues des dossiers d'ouvrages exécutés (DOE), incluant les caractéristiques techniques, les fiches équipements, les certificats et les documents d'exploitation.

La structuration de ce référentiel repose sur une organisation rigoureuse des DOE, incluant des arborescences standardisées, des règles de nommage homogènes, des formats de données exploitables, des contrôles pour la conformité du « tel que construit ». Cette organisation permet de garantir la qualité, la traçabilité et l'accessibilité des informations.

Socle de langage commun (interopérabilité minimale)

Niveau 1

- Définir le périmètre du référentiel : objets couverts (bâtiments, locaux, équipements, points de mesure/alarme/consigne, tickets/événements), acteurs, systèmes concernés et cas d'usage prioritaires.
- Établir un noyau sémantique partagé : dictionnaire/typologies d'entités, attributs et tags obligatoires, règles d'identification (ID uniques) et conventions de nommage.
- Standardiser le temps et les unités : référentiel d'unités unifiées, formats temporels, granularités et règles d'horodatage (indispensables aux historiques et comparaisons).
- Gouvernance de base : définir les rôles (propriétaire, gestionnaire, contributeur), les règles de création/modification, et une procédure simple de validation avant publication.
- Rendre le référentiel utilisable : exposer les objets et métadonnées via des API documentées (consultation, recherche, mise à jour contrôlée) pour que les systèmes « parlent le langage du SITH ».

●●

Référentiel industrialisé (gouvernance avancée et extension multi-sources)

Niveau 2

- Structurer une ontologie complète et extensible : aligner les sous-référentiels (BIM GEM, DOE, référentiels organisationnels, MDM) et gérer explicitement les liens entre objets (local ←→ équipement ←→ système ←→ point ←→ service).
- Gestion du cycle de vie et du versioning : historiser les évolutions du modèle (versions, dépréciations), gérer la rétrocompatibilité et documenter les changements pour éviter les ruptures d'intégration.
- Outillage de gouvernance : cataloguer le référentiel (métadonnées, glossaire, règles), tracer les modifications (journalisation, audit), et outiller les workflows d'approbation.
- Contrôles automatiques de conformité : automatiser les validations (complétude, cohérence, unités, nommage, cardinalités, liens attendus) et produire des rapports d'écarts (qualité du « tel que construit » / DOE).
- Contractualisation et interopérabilité fournisseurs : imposer le respect du référentiel dans les marchés (formats, API, dictionnaires, preuves), et organiser les tests d'intégration/recette sur un jeu de données de référence.
- Convergence OT/IT et exploitation : assurer la cohérence du référentiel entre données statiques (BIM/DOE) et données dynamiques (GTB/capteurs IoT), afin de soutenir la supervision temps réel, l'analyse et la maintenance.

IN 2 – L'interopérabilité des équipements et systèmes

L'interopérabilité, c'est la capacité de plusieurs systèmes, logiciels, appareils ou organisations à fonctionner ensemble et à échanger des informations de façon compréhensible.

Dans le Smart Hospital, l'interopérabilité consiste à faire communiquer différents équipements, logiciels et protocoles afin qu'ils fonctionnent ensemble, même s'ils proviennent de fabricants différents.

Par exemple :

- Une gestion coordonnée du chauffage, de l'éclairage et des stores pour le confort des patients
- Le pilotage énergétique avec des compteurs intelligents
- La performance de l'organisation avec la GTB et le Système d'Hypervision
- Le parcours des patients avec un dossier médical partagé entre plusieurs hôpitaux ;
- Le partage de la connaissance avec un fichier créé dans Microsoft Word qui peut être ouvert dans LibreOffice Writer.

Il existe plusieurs niveaux d'interopérabilité :

- Technique : les systèmes peuvent se connecter et échanger des données.
- Syntaxique : ils utilisent le même format de données.
- Sémantique : ils donnent le même sens aux données échangées.
- Organisationnelle : les procédures et règles permettent une vraie collaboration.

L'interopérabilité repose souvent sur des standards communs, comme :

- JSON, XML, RDF pour le web
- HL7, DICOM pour la santé
- BacNet, KNX, Modbus, LonWorks, M-Bus pour le Smart Building

Dans le Smart Hospital, l'interopérabilité permet aux données, 4ème fluide du bâtiment, de circuler entre plusieurs systèmes, applications ou services du SITH. Cette fonction est assurée par le BOS (Building Operating System) et les API (Application Programing Interface).

IN 2.1 – PROTOCOLES ET INTÉGRATION DES ÉQUIPEMENTS AU RÉSEAU « SMART »

Préalable à l'interopérabilité et au partage de données, les équipements communicants du bâtiment doivent être reliés au réseau « Smart ». Le réseau « Smart » est le réseau Ethernet-IP du bâtiment, tel que défini dans les thèmes « Connectivité » et « Architecture Réseau ».. Tout système ou objet communicant intégré au périmètre du projet, doit exposer ses données sur le réseau « Smart » :

- Via un routeur ou une passerelle protocolaire de liaison, dans le cas spécifique de périphériques (capteurs, actionneurs, mesureurs, détecteurs, etc.) exposant leurs données :

  - → sur des bus de terrain filaires (BACnet, LonWorks, KNX…) ;
  - → au travers de liaisons radios (LoRa, Bluetooth, ZigBee, EnOcean…) ;
  - → par l'intermédiaire de protocoles de communication réseaux communs à de nombreux constructeurs (HTTP/HTTPS, OPC UA MQTT, …) ;
  - → ces différents moyens doivent respecter les protocoles standards internationaux ISO/EN/CEA/IEEE ou être communs à de nombreux constructeurs (exemple : Modbus).
- Nativement via une interface IP (filaire ou non filaire) ;
- À défaut, via leur système central où est située l'API.

Cette exigence d'intégration s'applique aux équipements et systèmes intégrés au périmètre du projet.

IN 2.2 – API ET COMMUNICATION INTER SYSTÈMES

API terrain et API centrales

Les équipements communicants du bâtiment doivent exposer leurs données d'interfaçage accessibles via des API terrain afin de les rendre accessibles à la couche services. Ces données peuvent être exposées localement via le réseau « Smart » du bâtiment, et/ou être disponibles de façon sécurisée sur Internet. Dans tous les cas, les équipements produisant ou utilisant des données doivent décrire leur interface au travers d'API.

De même, tous les écosystèmes matériels communicants du bâtiment, doivent exposer leurs données d'interfaçage via des API centrales afin de les rendre accessibles à la couche services en transitant par le réseau « Smart » du bâtiment (architecture orientée services ou SOA).

Les données peuvent être exposées soit localement sur le réseau « Smart » du bâtiment et sur Internet à l'aide d'API adaptées aux services requis. Les écosystèmes matériels qui exposent leurs données d'interfaçage (Input/Output) seront dotés d'API.

Les API doivent être documentées pour être compréhensibles, utilisables et maintenables. La documentation est indispensable pour :

- Accélérer l'intégration : la documentation indique les endpoints, paramètres, formats et exemples d'appels.
- Réduire les erreurs : elle précise les codes de réponse, les cas d'échec et les messages d'erreur.
- Faciliter l'adoption : une API bien documentée est plus simple à comprendre et à réutiliser par des équipes internes ou des partenaires.
- Améliorer la maintenance : quand l'API évolue, la documentation permet de garder une vision claire de ce qui change.
- Renforcer la qualité de service : elle aide à identifier plus vite les bugs, incohérences et problèmes de conception.
- Soutenir la sécurité et la gouvernance : la gestion des API doit s'inscrire dans la politique de sécurité du système d'information.

Continuité de fonctionnement des équipements communicants

Il s'agit d'assurer la continuité fonctionnelle, en mode restreint ou dégradé des systèmes, en cas de panne de tout ou partie du réseau ou de sa connexion à Internet par exemple.

Les équipements intégrés au périmètre du réseau « Smart » (Cf. exigence IN 1.1) doivent comprendre un mode « dégradé de fonctionnement en cas de dysfonctionnement du réseau « Smart » ;et/ou de l'accès à Internet ; et/ou un dysfonctionnement des applications de la couche services.

Ce mode dégradé doit permettre de fonctionner en mode autonome et automatique dans des conditions compatibles avec la poursuite du fonctionnement basique des installations pour les utilisateurs et usagers du bâtiments.

Périmètre : le mode dégradé doit porter sur les systèmes considérés essentiels pour les utilisateurs et les usagers. Ces systèmes ont été identifiés dans l'analyse de risques imposée par la règlementation et dont les principales modalités sont dans les recommandations du thème « Sécurité Numérique ».

Modèle économique des API

Il s'agit d'être informé du modèle économique associé à l'exposition des données du bâtiment via leur(s) API. Les développeurs et éditeurs de logiciels doivent renseigner leurs modèles économiques quelle que soit la méthode utilisée (licence perpétuelle, abonnement…). Ces informations doivent permettre à l'établissement de faire un choix éclairé concernant le modèle économique des API en considérant les phases conception, réalisation, exploitation/maintenance.

Rétrocompatibilité des API

Il s'agit de garantir d'une évolutivité sans rupture des systèmes du bâtiment. Il est demandé un engagement de l'éditeur à la rétrocompatibilité (*a minima* pour la version n-1) des API définies dans l'exigence « IN 2.1 – Existence d'API et exposition des données ».

Rappel : dans le cas d'interface protocolaire (définies dans l'exigence « IN3.1 – Systèmes disposant d'interfaces protocolaires »), le respect de la norme garantit la rétrocompatibilité avec la version antérieure.

Capacité des équipements à s'interfacer avec une API au réseau « Smart »

Prérequis

Les équipements s'interfacent avec une API au réseau « Smart », ces API doivent être documentées et consultables. Ce prérequis est appliqué *a minima* pour toutes les catégories suivantes lorsque le projet les prévoit :

- les systèmes de gestion technique et énergétique du bâtiment ;
  - → air / eau (CVC Chauffage ventilation climatisation/plomberie) :
  - → gestion de la ventilation, qualité de l'air (blocs opératoires, laboratoires…)
  - → production et distribution eau chaude, eau froide, eau chaude sanitaire ;
  - → confort : terminaux de traitement de l'air, éclairage et stores ;
  - → télémétrie des fluides (exemples : eau potable, traitement d'air, électricité, fluides médicaux,…) ;
  - → régulation du chauffage et de la climatisation ;
  - → régulation de l'éclairage, éclairage connecté ;
  - → équipements de contrôle d'accès (portails, portes automatiques etc.) ;
  - → équipements de surveillance ;
- les équipements biomédicaux, dispositifs médicaux, systèmes d'appel malade
- les systèmes de géolocalisation des biens et des personnes ;
- les systèmes de logistique : convoyeurs et systèmes de logistique intrahospitalière : convoyeurs, Automatic Guided Vehicles (AGV), Autonomous Mobile Robots (AMR), transports pneumatiques etc.), ascenseurs et escalators connectés ;
- les systèmes de gestion des déchets ;
- les terminaux multimédias patients.

●

Socle d'exposition et d'intégration (API opérationnelles)

Niveau 1

– Existence d'API terrain et/ou centrales : tout équipement ou système produisant/utilisant des données expose des points d'accès (Input/Output) permettant l'intégration au SITH (local réseau « Smart » et/ou accès sécurisé via Internet selon les besoins).
– Documentation minimale et exploitable : description des endpoints, paramètres, formats, exemples d'appels, codes de retour et cas d'erreur (documentation consultable au format numérique).
– Sécurité « de base » : authentification, contrôle d'accès, échanges chiffrés lorsque requis, et cohérence avec la politique SSI/SI de l'établissement.
– Disponibilité fonctionnelle : capacité à maintenir un fonctionnement acceptable en cas de perte réseau/Internet (mode autonome / dégradé) pour les systèmes essentiels.
– Évolutivité sans rupture : engagement de rétrocompatibilité *a minima* sur la version n 1 des API, ou respect des normes dans le cas d'interfaces protocolaires.
– Transparence du modèle économique : information claire sur les coûts/licences/abonnements associés à l'exposition et à l'usage des API sur tout le cycle (conception → exploitation/maintenance).

●●

Industrialisation, gouvernance et qualité de service des API

Niveau 2

– Gestion centralisée des API (API management) : mise en place d'une passerelle (gateway), politiques de sécurité, limitation de débit, quotas, clés/jetons, et publication contrôlée.
– Gouvernance et cycle de vie : versioning explicite, règles de dépréciation, gestion des changements et communication des évolutions (release notes) pour préserver les intégrations.
– Qualité de service : supervision des appels (métriques, latence, erreurs), journalisation et alerting, avec objectifs de service (SLA) adaptés aux usages critiques.
– Portail développeurs et réutilisation : catalogue d'API, environnements de test/sandbox, exemples et SDK si nécessaire, afin d'accélérer l'intégration multi-éditeurs.
– Tests et conformité : tests automatisés (contrats, non-régression), contrôle de conformité aux normes/profils retenus, et preuves d'audit (traçabilité des accès, logs).
– Résilience et mode dégradé cadré : scénarios de continuité formalisés (fonctionnement local, files d'attente, reprise), et validation par analyse de risques sur le périmètre des systèmes essentiels.
– Contractualisation fournisseurs : exigences API intégrées aux marchés (documentation, sécurité, rétrocompatibilité, modalités de support, modèle économique) et critères de recette associés.

IN 3 – Le Building Operating System (BOS)

Le Building Operating System (BOS) constitue la couche de convergence des données au sein du système d'information technique. Il permet de centraliser, structurer et exploiter les données issues de référentiels hétérogènes.

Le BOS agrège ainsi les données patrimoniales issues du BIM, les données techniques issues des DOE et des outils métiers (GMAO), ainsi que les données opérationnelles en temps réel provenant de la GTB et des capteurs IoT.

Grâce à l'utilisation d'identifiants uniques partagés, il permet de relier ces différentes sources d'information, d'assurer leur cohérence et de faciliter leur exploitation. Il offre ainsi des capacités d'analyse, d'historisation et de pilotage, permettant d'optimiser les performances du bâtiment, d'améliorer la maintenance et d'améliorer les démarches de pilotage énergétique.

IN 3.1 – LES OBJECTIFS DU BOS :

Améliorer l'interopérabilité
Le BOS améliore l'interopérabilité en faisant dialoguer des systèmes qui fonctionnent souvent en silos : GTB, capteurs IoT, outils IT métiers et BIM. Il sert de couche d'intégration qui centralise les données, harmonise les échanges et facilite l'ajout de nouveaux équipements ou applications sans refaire toute l'architecture. Il relie l'OT, l'IT et le BIM dans un même environnement de données. Il normalise les flux et les interfaces pour que des systèmes hétérogènes puissent échanger plus facilement.

Centralisation des données
L'objectif pour la donnée est de passer d'une collecte dispersée à une exploitation structurée et interopérable. Le BOS a pour objectif, dans la gestion des données, de collecter, centraliser, structurer et rendre exploitables les données du bâtiment afin de les transformer en informations utiles pour l'exploitation. Il sert aussi à unifier des données hétérogènes issues de la GTB, des capteurs IoT et des logiciels métiers dans un format commun, ce qui facilite l'analyse et l'action. Le BOS ne se limite pas à stocker des données : il permet de les gouverner, les croiser et les valoriser pour le pilotage énergétique, la maintenance, le confort et les services numériques.

Gouvernance des données
Le BOS joue un rôle central dans la gouvernance des données : il permet d'en organiser l'usage, les droits, les responsabilités et les règles de partage. Le BOS devient la couche qui transforme des données techniques dispersées en patrimoine informationnel gouverné.

L'évolutivité
L'objectif est de créer un environnement technique capable de s'adapter en permanence aux usages et aux évolutions technologiques des bâtiments. La mise en œuvre du BOS favorise l'évolutivité du SITH en permettant d'ajouter ou de modifier des services sans remettre en cause les infrastructures existantes. Cette capacité d'adaptation constitue un levier essentiel pour maintenir la valeur des bâtiments et environnements techniques dans la durée, notamment dans

un contexte de transition énergétique et de mutation des besoins des professionnels de l'hôpital.Il réduit la dépendance à un fournisseur unique en évitant l'enfermement propriétaire et en facilitant les intégrations

La collaboration et le partage

Le BOS en production soutient une gouvernance collaborative des données au service de la valeur d'usage. Elle crée un langage commun entre les acteurs (direction, services techniques, occupants, usagers et prestataires) et favorise une meilleure coordination entre eux. En structurant les données autour d'objectifs partagés, cette approche transforme le bâtiment en une plateforme de services intelligents, capable de générer des gains en matière de performance, de durabilité et d'attractivité.

La sécurité

Le BOS renforce la sécurité numérique en centralisant la gestion des accès, des flux de données et de la supervision dans un cadre plus cohérent que des systèmes éclatés. Il peut aussi améliorer la cybersécurité en s'appuyant sur une architecture « secure by design », avec API gateway, rôles et permissions granulaires, et traçabilité des actions.

Point important :

Le BOS n'est pas « sécurisé par nature » : sa sécurité dépend de son architecture, de la gestion des droits, du durcissement des composants et de la gouvernance des données. En pratique, un BOS bien conçu peut aider à mieux protéger le bâtiment, mais un BOS mal configuré peut aussi créer de nouveaux risques face aux menaces et aux suivis réglementaires.

IN 3.2 – LES FONCTIONNALITÉS DU BOS

Les fonctionnalités du BOS couvrent surtout la collecte, la structuration, la supervision et l'exploitation des données du bâtiment. Il sert aussi à centraliser le pilotage des équipements, des usages et des performances sur une seule plateforme.

Gérer le référentiel du SITH

- Création et l'administration du référentiel ;
- Définition et formalisation des éléments du référentiel, et de la modélisation du bâtiment
- Constitution de l'unique point de partage des données du référentiel avec les systèmes du SITH et les systèmes externes ;

Structurer la qualité des données partagées par l'automatisation d'une chaîne de traitement

- Intégration des données partagées ;
- Homogénéité des données partagées hétérogènes dans un format unifié ;
- Caractérisation et contextualisation de toutes les données partagées vis-à-vis du référentiel
- Organisation de la mise en qualité et de l'intégrité des données partagées

Gérer le partage des données du bâtiment (partagées et externes) :

- Orchestration de la gestion active et la cadence des échanges des données du référentiel ;
- Orchestration de la gestion active et la cadence des échanges des données associées au référentiel ;
- Unification des API à l'échelle du bâtiment ou du patrimoine immobilier ;
- Exposition d'un portail d'API unique du bâtiment documenté avec des droits d'usage ouverts à des tiers

– Fourniture des fonctions d'API management (API gateway) définissant le cadre minimum du contrat de partage des données avec les applicatifs et systèmes tiers ;
– Fourniture des connecteurs ou drivers.

Gérer les droits et les accès des utilisateurs et applicatifs

– Gestion de l'authentification (de ses utilisateurs ou des services applicatifs connectés)
– Gestion des droits administrateurs et intégrateur pour la gestion du référentiel ;
– Gestion de la sécurité et les droits sur le référentiel ;
– Gestion de la sécurité et les droits sur les données associées au référentiel.

Organiser l'évolutivité

– Fourniture d'un cadre et des outils permettant l'évolution, le développement par des tiers de :
  → Nouveaux modèles de données ;
  → Nouveaux drivers ;
  → Nouveaux connecteurs ;
  → Nouvelles API ;
  → Nouvelles applications ;
  → Nouveaux modules de sécurisation.
– Fourniture d'une documentation permettant l'usage des outils d'évolution par un tiers compétent ;
– Fourniture d'un cadre contractuel d'usage de ces outils d'évolution.

Le maître d'ouvrage a défini le périmètre et les objectifs du projet.

Prérequis

Suivant les recommandations du thème « Management Responsable », ces éléments sont construits itérativement dans le Schéma Directeur Immobilier, le cadrage du projet immobilier, le programme technique détaillé.

Définition de l'architecture du SITH et justification du BOS

Niveau 1

L'architecture du SITH désigne la façon dont l'ensemble des composants informationnels, applicatifs, techniques et organisationnels de l'établissement sont structurés pour soutenir ses objectifs.

La réflexion sur l'architecture du SITH va permettre de justifier l'installation d'un BOS et de documenter les services attendus en matière d'interopérabilité et de gestion des données.

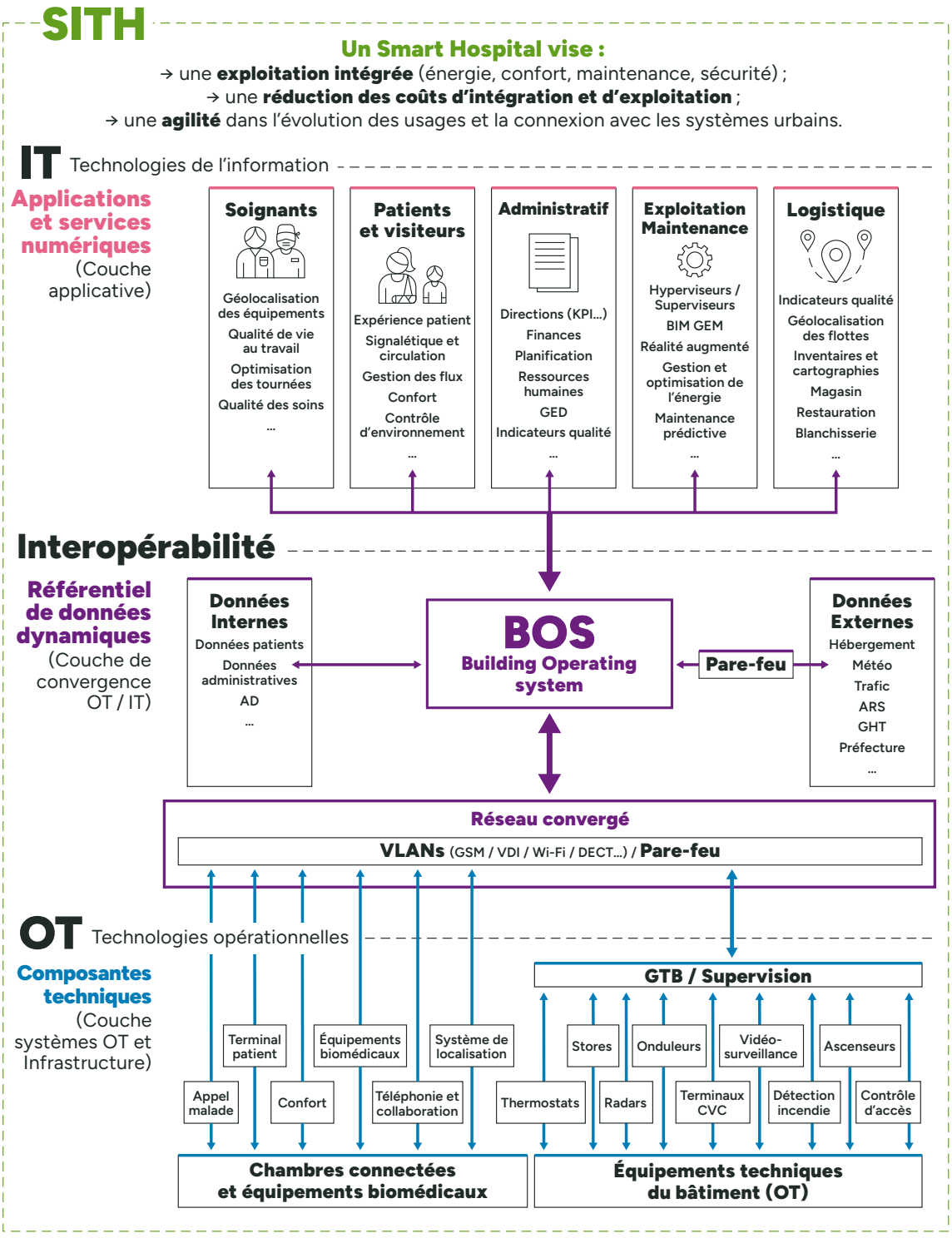
Une bonne architecture permet d'aligner le SI sur la stratégie de l'entreprise, de réduire la redondance des applications et des données, d'améliorer l'interopérabilité, de renforcer la sécurité, de faciliter l'évolution du système et de maîtriser les coûts

Elle décrit :

– **La couche métier**
  les services numériques documentés dans le thème « Services » du R2S4Care (Gestion de l'énergie, éclairge, géolocalisation, ...)
– **La couche fonctionnelle**
  Les grandes fonctions attendues du SITH, indépendamment des logiciels utilisés.(prendre une mesure, historiser les mesures, ...)
– **La couche applicative**
  Les applications et logiciels qui réalisent les fonctions.
– **La couche données (BOS)**
  Les données manipulées, leur localisation, leur structure, leur qualité, leurs échanges et leur gouvernance.
– **La couche technique (BOS)**
  Les infrastructures qui hébergent et font fonctionner le SI.

Le projet BOS
Niveau 2

L'organisation du projet BOS est planifiée et provisionné en termes de ressources humaines et budgétaire. Les conditions de son maintien en condition opérationnelle sont prévues dans le plan projet.



L'ARCHITECTURE DU SITH (SYSTÈME D'INFORMATION TECHNIQUE HOSPITALIER)

IN 4 – Le Building Information Modeling (BIM)

Le BIM (Building Information Management ou Modeling) couvre tout le cycle de vie d'un bâtiment, depuis la conception jusqu'à l'exploitation. Il repose sur une maquette numérique partagée contenant les données techniques, géométriques et fonctionnelles de l'ouvrage ;

Le BIM produit et organise toutes les données d'un bâtiment pendant son cycle de vie : conception, construction, exploitation et maintenance. Le data management permet de gérer ces données pour qu'elles restent fiables, cohérentes et accessibles.

On distingue deux phases dans le déploiement et l'utilisation du BIM : la conception et l'exploitation.

Synchronisation et cohérence statique/dynamique

Définir les règles de mise à jour (après intervention, après travaux, remplacements), les mécanismes de rapprochement d'identifiants et la gestion des écarts terrain vs maquette.

Cas d'usage avancés

Pilotage énergétique et carbone, optimisation de la maintenance (préventif/prédictif), supervision, continuité de service, et analyses patrimoniales à l'échelle site/patrimoine.

IN 4.1 – LE BIM CONCEPTION

En phase de conception, le BIM sert à produire un modèle numérique détaillé du futur ouvrage, à partir duquel on peut générer des vues, des plans, des quantitatifs et des analyses. C'est une phase où l'on modélise le bâtiment, on enrichit les objets avec des données techniques, et on anticipe les conflits, les coûts et les délais.

Cette phase permet aussi de travailler en collaboration entre architectes, ingénieurs, économistes et autres acteurs avec un même référentiel d'information.

Les principales fonctions du BIM en phase conception :

- Création de la maquette 3D
- Coordination entre architectes, ingénieurs et entreprises
- Détection des conflits techniques
- Estimation des coûts et des délais (4D/5D)

IN 4.2 – LE BIM GEM

Le BIM GEM (Gestion, Exploitation, Maintenance). Il prolonge le BIM de conception et de construction vers l'usage quotidien du bâtiment, avec un focus sur la maintenance, l'exploitation et le suivi des actifs

Le BIM GEM sert à réutiliser la maquette numérique comme référentiel d'exploitation pour mieux gérer les équipements, les interventions, les espaces et les données techniques du bâtiment.

Composante du SITH, il vise aussi à faire le lien entre la maquette BIM, la GMAO et les systèmes de supervision, afin d'améliorer la continuité informationnelle entre conception et usage.

Apports principaux :

- Meilleure maintenance, avec des informations plus fiables sur les équipements.
- Réduction des coûts d'exploitation, grâce à une meilleure anticipation des interventions.

– Vision centralisée du bâtiment, via une plateforme unique de données.
– Mise à jour du patrimoine numérique, pour garder une maquette utile dans la durée.
– Optimisation énergétique et opérationnelle, par l'exploitation des données statiques et dynamiques.

Le BIM GEM prolonge donc le BIM de conception vers l'exploitation réelle du bâtiment. Il transforme la maquette numérique en outil de gestion quotidienne.

IN 4.3 – LE RÉFÉRENTIEL DU BIM (NORME ISO 19650)

Le référentiel de données BIM est l'ensemble structuré des informations qui doivent être produites, nommées, classées et échangées dans la maquette numérique. Il sert de langage commun entre tous les acteurs du projet.

Pour distinguer les deux phases :

– le référentiel BIM Conception contient les données nécessaires pour concevoir et construire. Le référentiel BIM Conception vise surtout à coordonner les acteurs et fiabiliser le projet avant et pendant les travaux. Il constitue une base de données partagée de conception et de réalisation
– le référentiel BIM GEM contient les données nécessaires pour exploiter et maintenir le bâtiment après sa livraison. Le référentiel BIM GEM devient ainsi le référentiel unique d'exploitation-maintenance du bâtiment. Il est généralement connecté à une GMAO, une GTB ou un système de gestion patrimoniale. Dans le modèle Smart Hospital il est connecté au BOS qui assure son interopérabilité avec les différents systèmes du SITH.

IN 4.4 – DU BIM AU JUMEAU NUMÉRIQUE

Le BIM et le jumeau numérique sont liés, mais ce ne sont pas la même chose.

– Le BIM décrit le bâtiment tel qu'il est conçu puis construit.
– Le jumeau numérique représente le bâtiment réel en fonctionnement, alimenté en continu par des données terrain.

Le passage du BIM au jumeau numérique consiste à enrichir la maquette BIM GEM avec des flux de données dynamiques provenant du bâtiment. Un enrichissement en 3 étapes :

Étape 1 : BIM de conception
Pendant les études, on produit la maquette numérique contenant :

– géométrie ;
– matériaux ;
– équipements ;
– données techniques.

Cette maquette devient ensuite le DOE BIM puis l'AIM (Asset Information Model), c'est-à-dire la base d'information du bâtiment livré.

Étape 2 : BIM GEM
En exploitation, l'AIM est enrichi avec :

– identifiants patrimoniaux ;
– données de maintenance ;
– contrats ;
– historiques d'intervention ;
– documentation technique.

Le BIM GEM reste essentiellement statique : les données sont mises à jour manuellement après chaque intervention.

Étape 3 : Jumeau numérique

Le jumeau numérique apparaît lorsque la maquette BIM GEM est connectée en temps réel à des systèmes du bâtiment :

- capteurs IoT ;
- GTB / BMS ;
- GMAO ;
- compteurs énergétiques ;
- systèmes de supervision ;
- données météo et occupation.

Le modèle ne décrit plus seulement ce qui existe, mais ce qui se passe réellement dans le bâtiment.

Niveau	Type de données	Fréquence de mise à jour
BIM Conception	Géométrie, techniques, études	Pendant le projet
BIM GEM	Maintenance, exploitation	Après intervention
Jumeau numérique	Données temps réel, capteurs, performance	Continu

Socle BIM Conception + BIM GEM (référentiel exploitable)

Niveau 1

- Définir les usages et exigences d'information : formaliser les objectifs par phase (conception / chantier / exploitation) et les livrables attendus (DOE BIM, AIM), en cohérence avec les besoins exploitation/maintenance.
- Référentiel et règles ISO 19650 : mettre en place les conventions de nommage, classification, structures de dossiers, statuts de validation et règles d'échange (CDE/plateforme collaborative) pour garantir un langage commun.
- Qualité et complétude de la maquette : contrôler la cohérence géométrique et la présence des attributs essentiels (localisation, typologie, caractéristiques techniques, documentation associée), avec un processus de correction avant réception.
- Préparer le BIM GEM : structurer les objets « actifs » (équipements) avec des identifiants patrimoniaux uniques et une arborescence exploitable (bâtiment → zone → local → équipement).
- Connecter aux outils d'exploitation : organiser le lien entre BIM GEM, GMAO et GTB/BMS (au minimum via les identifiants et des correspondances d'objets) afin d'assurer la continuité informationnelle.
- Organisation et gouvernance : clarifier les rôles (MOA, MOE, BIM manager, exploitant), les responsabilités de mise à jour et les modalités de remise à niveau de la maquette.

●●

BIM industrialisé et transition vers le jumeau numérique

Niveau 2

- Industrialiser le cycle de vie de l'information : outiller la gestion des versions, les workflows d'approbation, et la traçabilité des modifications (qui a modifié quoi, quand, pourquoi) pour maintenir une maquette « utile » dans la durée.
- Automatiser les contrôles (BIM QA/QC) : règles de validation automatiques (niveaux de détail/LOIN, attributs obligatoires, cohérence des relations, collisions) et reporting d'écarts.
- Interopérabilité via le BOS et le référentiel SITH : aligner les entités BIM avec le référentiel (ontologies, tags, unités, temps) et exposer les données via des API afin de faciliter l'intégration multi-systèmes.
- Enrichissement dynamique (vers jumeau numérique) : connecter l'AIM/BIM GEM à des flux opérationnels (GTB/BMS, GMAO, capteurs IoT, compteurs, météo/occupation) avec une stratégie de fréquence (évènement, quasi temps réel, batch).

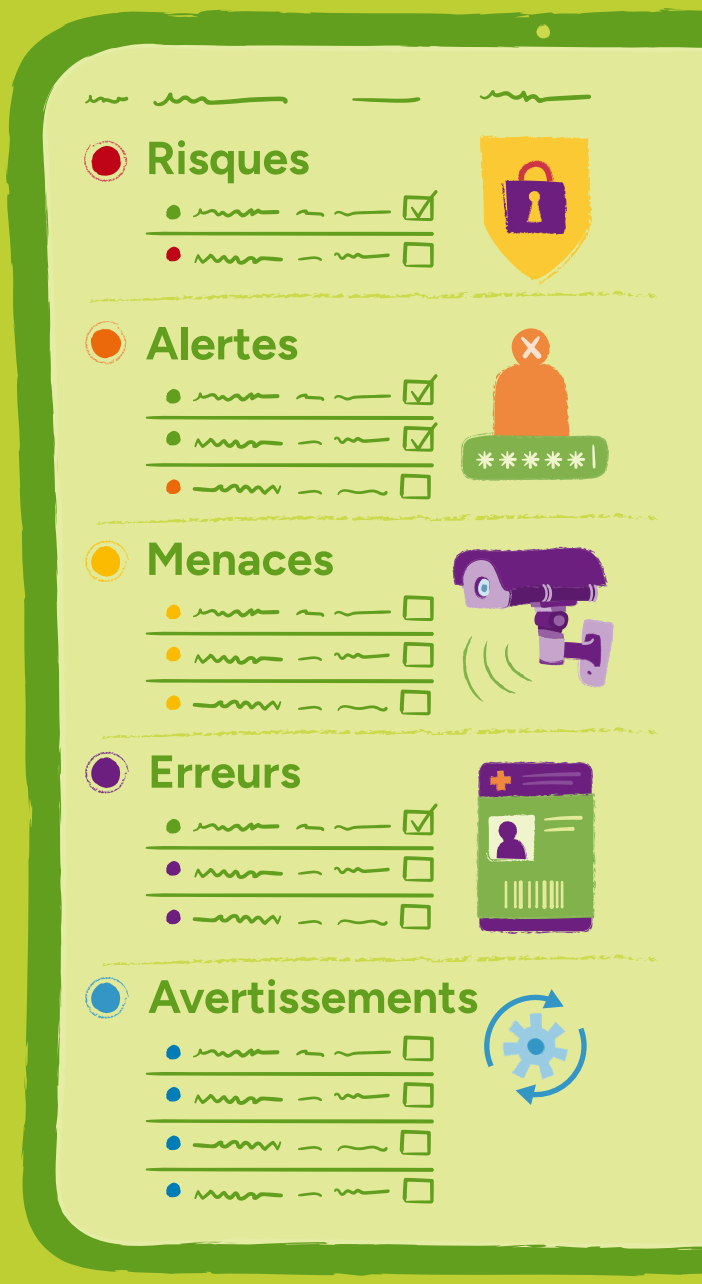
Sécurité numérique

En France, les cyber-incidents dans les établissements de santé (hôpitaux, cliniques, structures médico-sociales) sont en forte augmentation depuis plusieurs années. Ils représentent aujourd'hui une menace majeure pour la continuité de fonctionnement des établissements et la protection des données du SIH et du SITH et particulièrement les données de santé.

Actant cette montée des risques, la règlementation européenne NIS2, intégrée en 2026 dans le cadre de la PGSSI-S, classe une majorité des hôpitaux dans la catégorie des « Entités Essentielles ». Il impose des obligations en matière de sécurisation des systèmes d'information, de gestion des incidents, de responsabilité des dirigeants et expose à des sanctions financières. Ces obligations s'appliquent aux deux ensemble SIH et SITH.

Pour améliorer leur performance, les hôpitaux utilisent et prévoient de mettre en service une très grande diversité d'équipements qui vont des équipements biomédicaux aux capteurs des systèmes de gestion des bâtiments en passant par les équipements réseaux, les imprimantes ou les téléphones IP. Ce qui, combiné avec la multiplicité des fournisseurs, expose les hôpitaux à un grand nombre de menaces quant à la continuité de fonctionnement et à l'intégrité des données.

Ce thème vise à mettre en place un plan organisé, répondant aux exigences de sécurité d'une « Entité Essentielle » conforme aux évolutions de la PGSSI-S et de la NIS 2.



Recommandations	Niveau de maturité		Pages
SE 1 – Système de management de la sécurité informatique « by design »			→ p.69
SE 1.1 – SÉCURITÉ NUMÉRIQUE « BY DESIGN »	● Niveau 1	Prise en compte du « by design »	
SE 1.2 – GOUVERNANCE ET LEADERSHIP	● Niveau 1	La direction désigne un responsable de la sécurité numérique du projet Smart Hospital	
	●● Niveau 2	Coopération entre responsable de la sécurité et le responsable de la sécurité numérique	
SE 1.3 – ANALYSE DES RISQUES	● Niveau 1	Réalisation d'une analyse de risques	
	●● Niveau 2	Gestion et mise à jour des vulnérabilités	
SE 1.4 – POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION	★ Unique	Une PSSI existe et est validée par la direction	
SE 1.5 – CONFORMITÉ RÈGLEMENTAIRE	★● Niveau 1	Respect du cadre de la PGSSI-S	
	●● Niveau 2	Certification ISO 27001	
SE 2 – Sécurité des réseaux et systèmes du bâtiment			→ p.73
SE 2.1 – SEGMENTER LE RÉSEAU ET METTRE EN PLACE UN CLOISONNEMENT ENTRE CES ZONES	● Niveau 1	Le réseau est segmenté et cloisonné	
	●● Niveau 2	Cloisonnement renforcé pour les systèmes critiques	
SE 2.2 – SÉCURITÉ DES RÉSEAUX D'ACCÈS WI-FI ET SÉPARATION DES USAGES	● Niveau 1	Sécurisation de base des accès Wi-Fi	
	●● Niveau 2	Sécurisation avancée et cloisonnement renforcé	
SE 2.3 – UTILISER DES PROTOCOLES RÉSEAUX SÉCURISÉS DÈS QU'ILS EXISTENT	● Niveau 1	Utilisation des protocoles sécurisés standards	
	●● Niveau 2	Gestion avancée et surveillance active des protocoles	
SE 2.4 – METTRE EN PLACE UNE PASSERELLE D'ACCÈS SÉCURISÉ À INTERNET	● Niveau 1	Installation et configuration de base du pare-feu	
	●● Niveau 2	Supervision avancée et gestion fine des accès	
SE 2.5 – CLOISONNER LES SERVICES VISIBLES DEPUIS INTERNET	● Niveau 1	Cloisonnement de base et filtrage des accès	
	●● Niveau 2	Cloisonnement renforcé et supervision continue	
SE 2.6 – SÉCURISER LES INTERCONNEXIONS RÉSEAU DÉDIÉES AVEC LES ENTITÉS EXTÉRIEURES	● Niveau 1	Gestion et contrôle des flux	
	●● Niveau 2	Passerelle dédiée à l'interconnexion	
SE 2.7 – CONTRÔLER ET PROTÉGER L'ACCÈS AUX SALLES SERVEURS ET AUX LOCAUX TECHNIQUES	● Niveau 1	Contrôle d'accès physique de base	
	●● Niveau 2	Gestion avancée et supervision des accès	

★ Obligation réglementaire

Recommandations		Niveau de maturité		Pages
SE 3 – Procédures de sécurité réseau				→ p.78
SE 3.1 – DÉTECTION ET RÉPONSE AUX INCIDENTS				
Surveillance et journalisation	●	Niveau 1	Mise en place d'un contrôle d'accès et d'une journalisation basique	
	●●	Niveau 2	Surveillance avancée et centralisation des logs	
Continuité d'activité et sauvegarde	●	Niveau 1	Plan de continuité et de reprise d'activité	
	●●	Niveau 2	Exercice de test annuel des PCA/PRA dont sauvegardes	
Audit et actions correctives	★	Étape technique	Réalisation d'un diagnostic approfondi	
		organisationnelle	Élaboration et suivi d'un plan d'actions correctives	
Gestion des incidents de sécurité	●	Niveau 1	Gestion réactive des incidents de sécurité numérique	
	●●	Niveau 2	Gestion proactive des incidents de sécurité numérique	
SE 3.2 – MISE À JOUR ET LUTTE CONTRE L'OBSOLESCENCE	●	Niveau 1	Gestion réactive et conformité minimale	
	●●	Niveau 2	Gestion proactive et automatisée	
SE 4 – Procédures de sécurité réseau				→ p.83
SE 4.1 – IDENTIFIER NOMMÉMENT CHAQUE PERSONNE ACCÉDANT AUX SERVICES ET DISTINGUER LES RÔLES UTILISATEUR/ ADMINISTRATEUR	●	Niveau 1	Identification basique et gestion manuelle	
	●●	Niveau 2	Identification centralisée et gestion automatisée	
SE 4.2 – SÉCURISATION DE L'ACCÈS AUX APPLICATIONS	●	Niveau 1	Contrôle d'accès basique	
	●●	Niveau 2	Contrôle d'accès avancé et gestion centralisée	
SE 4.3 – PRÉVENTION ET GESTION DES RISQUES	●	Niveau 1	Approche réactive et documentation minimale	
	●●	Niveau 2	Approche proactive et gestion structurée	
SE 5 – Protection des données				→ p.86
SE 5.1 – GOUVERNANCE DES DONNÉES	●	Niveau 1	Structurer la gestion des accès et des droits	
	●●	Niveau 2	Formaliser les processus de gouvernance	
SE 5.2 – CONFORMITÉ AU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES	★●	Niveau 1	Formalisation et suivi des procédures de traitement des données	
	★●●	Niveau 2	Formation et responsabilisation des acteurs	

★ Obligation réglementaire

SE 1 – Système de management de la sécurité informatique « by design »

SE 1.1 – SÉCURITÉ NUMÉRIQUE « BY DESIGN »

Security by Design (sécurité dès la conception) est un principe qui consiste à intégrer les exigences de sécurité numérique dès la phase de conception d'un système, d'une application ou d'une infrastructure, et non après sa mise en service.

Ce principe vise à construire des systèmes nativement sécurisés, en anticipant les menaces et les risques. Corriger une faille après déploiement coûte souvent beaucoup plus cher que de l'intégrer dès la conception.

Dans le projet Smart Hospital, l'établissement ou le groupement définit une stratégie qui fixe les objectifs, les règles et les principes de sécurité permettant de protéger les systèmes d'information. Les sujets Security by design à aborder sont :

- Cartographier le réseau « Smart » et l'architecture du SITH
- Sécuriser le réseau « Smart » et l'architecture du SITH
- Sécuriser les accès aux systèmes et les dispositifs connectés
- Intégrer la protection des données
- Intégrer la gestion des incidents
- Sensibiliser les professionnels et usagers du bâtiment
- Respecter les normes et règlementation

Prise en compte du « by design »

Niveau 1

Le maître d'ouvrage et les pilotes du projet ont intégrer l'approche « by design » dès la phase APS.

SE 1.2 – GOUVERNANCE ET LEADERSHIP

La gouvernance constitue un fondement de la sécurité numérique.

La direction de l'établissement de santé approuve formellement les politiques de sécurité et est tenue responsable de leur mise en œuvre.

La direction désigne un responsable de la sécurité numérique du projet Smart Hospital

Niveau 1

En lien avec le RSSI, ses responsabilités sont de :

- Définir la politique de sécurité et la faire approuver par la direction
- Mettre en œuvre la politique de sécurité en collaboration avec les responsables des équipes techniques en charge des engagements de qualité de service :

→ Protéger les systèmes et les données
→ Gérer les accès et les identités
→ Prévenir et gérer les incidents de sécurité
→ Sensibiliser les utilisateurs
→ Gérer la conformité règlementaire.

Coopération entre responsable de la sécurité et le responsable de la sécurité numérique

Niveau 2

Le périmètre de la sécurité à l'hôpital désigne l'ensemble des mesures et des zones organisées pour garantir la sécurité des patients, du personnel et des usagers.

Les activités de sécurité s'appuient de plus en plus sur des technologies numériques.

Les deux acteurs de la sécurité coopèrent pour :

– Protéger les patients (surtout les vulnérables)
– Éviter les intrusions ou actes malveillants
– Gérer les situations d'urgence (attentat, épidémie, incendie)
– Assurer la confidentialité des soins.

SE 1.3 – ANALYSE DES RISQUES

Dans l'approche de la politique de sécurité « by design » la première action recommandée est de réaliser une analyse de risque.

Une analyse de risque est une méthode structurée permettant de :

– Identifier les actifs numériques (cartographie des systèmes, données, équipements, automatismes et capteurs)
– Identifier les menaces (cyberattaques, erreurs humaines, pannes)
– Identifier les vulnérabilités (mise à jour des logiciels, mots de passe, équipements obsolètes, segmentation réseau, formation utilisateurs, …)
– Évaluer la probabilité et les impacts potentiels des incidents (financier, opérationnel, juridique, impacts sur les usagers, …)
– Définir les mesures de sécurité adaptées (réduire le risque, accepter le risque, transférer le risque).

L'objectif est de réduire les risques à un niveau acceptable.

Réalisation d'une analyse de risques

Niveau 1

L'établissement a identifié, évalué et traiter les risques qui peuvent affecter les systèmes d'information. Pour le Smart Hospital, le SITH est le périmètre de l'analyse de risque qui vise à protéger les données, garantir la continuité de l'exploitation et prévenir les cyberattaques.

Gestion et mise à jour des vulnérabilités

Niveau 2

L'établissement met régulièrement à jour sa matrice d'analyse des risques. La gestion Les activités essentielles à sa mise en œuvre :

- Disposer d'un inventaire à jour des composants et de suivre les annonces de vulnérabilités
- Anticiper l'obsolescence et la fin de maintenance
- Appliquer régulièrement les correctifs de sécurité,

L'ANSSI et l'ANS recommandent d'utiliser la méthode EBIOS Risk Manager et ses 5 étapes (cadrage, identification des sources, scénarios, traitement, suivi).

Autres méthodes disponibles : ISO 27005, MEHARI (Clusif), NIST Risk Framework (Etats-Unis).

SE 1.4 – POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

La PSSI (Politique de Sécurité des Systèmes d'Information) est un document stratégique qui définit les objectifs, les règles et les principes de sécurité permettant de protéger les systèmes d'information du Smart Hospital. Il est obligatoire dans le cadre de la PGSSI-S et un prérequis pour l'éligibilité aux programmes de support financés par la puissance publique.

Validé par la direction, il :

- Définit la vision et les objectifs de sécurité de l'organisation
- Précise le périmètre des systèmes concernés
- Établit les règles de protection des informations et des systèmes informatiques
- Précise les responsabilités des acteurs (gouvernance)
- Encadre les mesures de sécurité à appliquer (gestion des incidents)
- Développe un programme de formation et de sensibilisation des utilisateurs et usagers du Smart Hospital
- Assure la conformité règlementaire (PGSSI-S, NIS2, RGPD, ...)

Trois principes de sécurité sont mis en œuvre :

- Confidentialité : Les informations ne doivent être accessibles qu'aux personnes autorisées.
- Intégrité : les données doivent être exactes et non modifiées de manière non autorisée.
- Disponibilité : les systèmes et les informations doivent être accessibles lorsque nécessaire.

★

Une PSSI existe et est validée par la direction

Niveau unique et obligatoire

Le responsable sécurité désigné par la direction a rédigé le document PSSI. La direction a validé les objectifs et les moyens de la mise en œuvre de cette PSSI.

SE 1.5 – CONFORMITÉ RÈGLEMENTAIRE

Pour donner un point de vue commun et structuré dans la compréhension des contraintes règlementaires liées à la conformité règlementaire de la sécurité numérique, le R2S4Care prend en compte quatre corpus règlementaires :

- La PGSSI-S documentée et supportée par l'ANS et les autorités de régulation
- La NIS2 et son introduction dans le droit français supportée par l'ANSSI.
- Guide d'hygiène ANSSI
- ISO 27001-2022

●★

Respect du cadre de la PGSSI-S

Niveau 1 et obligatoire

La PGSSI-S est un cadre de référence qui sert de socle pour le numérique en santé en France. Il s'applique à tous les établissements de santé.

L'OPSSIES (Observatoire Permanent de la sécurité des SI en Santé) suit la maturité des établissements de santé en matière de sécurité numérique et évalue les actions mise en oeuvre.

●●

Certification ISO 27001

Niveau 2

La certification ISO27001 est une norme internationale qui permet aux organisations de mettre en place un Système de Management de la Sécurité de l'Information (SMSI) afin de protéger leurs données et leurs systèmes d'information.

Elle atteste qu'un établissement de santé applique des pratiques reconnues de gestion des risques et de sécurité de l'information.

SE 2 – Sécurité des réseaux et systèmes du bâtiment

SE 2.1 – SEGMENTER LE RÉSEAU ET METTRE EN PLACE UN CLOISONNEMENT ENTRE CES ZONES

Lorsque le réseau est « à plat », sans aucun mécanisme de cloisonnement, chaque machine du réseau peut accéder à n'importe quelle autre machine. La compromission de l'une d'elles met alors en péril l'ensemble des machines connectées. Un attaquant peut ainsi compromettre un poste utilisateur et ensuite « rebondir » jusqu'à des serveurs critiques.

Dès la conception de l'architecture réseau, Il est donc important, , de raisonner par segmentation en zones composées de systèmes ayant des besoins de sécurité homogènes (serveurs métiers, serveurs technique, automatismes, passerelles IOT, ...).

Une zone se caractérise alors par des VLAN et des sous-réseaux IP dédiés voire par des infrastructures dédiées selon sa criticité. Ainsi, des mesures de cloisonnement telles qu'un filtrage IP à l'aide d'un pare-feu peuvent être mises en place entre les différentes zones.

●

Le réseau est segmenté et cloisonné

Niveau 1

Le réseau est segmenter et cloisonné en zones regroupant des systèmes ayant des besoins de sécurité homogènes

●●

Cloisonnement renforcé pour les systèmes critiques

Niveau 2

Des dispositifs de filtrage renforce le cloisonnement des segments hébergeant des systèmes critiques.

SE 2.2 – SÉCURITÉ DES RÉSEAUX D'ACCÈS WI-FI ET SÉPARATION DES USAGES

L'usage du Wi-Fi dans les établissements de santé est aujourd'hui généralisé mais présente toujours des risques de sécurité bien spécifiques :

- Faibles garanties en matière de disponibilité,
- Pas de maîtrise de la zone de couverture pouvant mener à une attaque hors du périmètre géographique de l'entité,
- Configuration par défaut des points d'accès peu sécurisée, etc.

●

Sécurisation de base des accès Wi-Fi

Niveau 1

Les accès Wi-Fi sont protégés par un chiffrement robuste (WPA2/AES), une authentification centralisée si possible, et un mot de passe complexe régulièrement renouvelé. Les flux issus du Wi-Fi sont filtrés pour limiter l'exposition du système d'information, et les connexions des terminaux personnels ou visiteurs sont isolées des équipements de l'établissement.

●●

Sécurisation avancée et cloisonnement renforcé

Niveau 2

L'accès Wi-Fi repose sur une authentification forte par certificats clients, avec segmentation stricte des réseaux (SSID et VLAN dédiés selon le profil utilisateur). Les points d'accès sont administrés via des interfaces sécurisées, et chaque connexion est surveillée afin de détecter toute activité suspecte ou non autorisée. Les accès des terminaux invités sont systématiquement séparés avec un accès Internet dédié et sans possibilité d'interaction avec les systèmes critiques.

SE 2.3 – UTILISER DES PROTOCOLES RÉSEAUX SÉCURISÉS DÈS QU'ILS EXISTENT

La sécurité n'est plus optionnelle. C'est pourquoi de nombreux protocoles réseaux ont dû évoluer pour intégrer cette composante et répondre aux besoins de confidentialité et d'intégrité qu'impose l'échange de données.

Bien qu'il soit difficile d'en dresser une liste exhaustive, les protocoles les plus courants reposent sur l'utilisation de TLS et sont souvent identifiables par l'ajout de la lettre « s » (pour secure en anglais) à l'acronyme du protocole. Pour le Smart Hospital, parmi les protocoles dédiés aux équipements du bâtiment ;

- BACnet (Building Automation AND Control Network) et sa version sécurisé
- KNX et sa version sécurisée
- Lorawan sécurisé par cryptage des données
- Zigbee sécurisé par cryptage des données
- Modbus
- …

●

Utilisation des protocoles sécurisés standards

Niveau 1

L'établissement s'assure que l'ensemble des échanges critiques repose sur des protocoles réseau intégrant des mécanismes de chiffrement et d'authentification, comme TLS pour HTTPS, IMAPS, SMTPS, ou encore l'utilisation de versions sécurisées de protocoles dédiés aux équipements du bâtiment. Les configurations par défaut sont systématiquement revues pour activer les options de sécurité disponibles et limiter l'utilisation des protocoles obsolètes ou non sécurisés.

●●

Gestion avancée et surveillance active des protocoles

Niveau 2

Au niveau avancé, l'organisation déploie une politique de gestion centralisée des protocoles réseau, incluant l'inventaire, la supervision et l'analyse régulière des flux pour détecter l'utilisation de protocoles non conformes ou vulnérables. Des outils de détection d'anomalies et de contrôle d'intégrité sont mis en œuvre pour assurer la conformité continue et réagir rapidement en cas d'incident ou de tentative d'utilisation de protocoles non autorisés.

SE 2.4 – METTRE EN PLACE UNE PASSERELLE D'ACCÈS SÉCURISÉ À INTERNET

L'accès à Internet, devenu indispensable, présente des risques importants : sites Web hébergeant du code malveillant, téléchargement de fichiers « toxiques » et, par conséquent, possible prise de contrôle du terminal, fuite de données sensibles, etc.

●

Installation et configuration de base du pare-feu

Niveau 1

Le pare-feu est installé à l'entrée du réseau, avec une configuration minimale assurant le filtrage des flux et l'activation des fonctions de sécurité essentielles telles que l'antivirus ou le système de prévention d'intrusions. Les règles de filtrage sont établies selon les besoins courants, et la journalisation des flux acceptés ou refusés est mise en place pour assurer un premier niveau de traçabilité.

●●

Supervision avancée et gestion fine des accès

Niveau 2

Une cartographie détaillée des flux traversant le pare-feu est réalisée afin de n'autoriser que les communications strictement nécessaires. Le pare-feu est paramétré avec des critères avancés (adresses IP, ports, protocoles) et sa configuration est régulièrement revue.

Une surveillance active des flux et des alertes en cas d'anomalies sont déployées pour garantir la sécurité continue et la conformité aux politiques de l'organisation.

SE 2.5 – CLOISONNER LES SERVICES VISIBLES DEPUIS INTERNET

Un établissement de santé peut choisir d'héberger en interne des services visibles sur Internet (site web, serveur de messagerie, etc.). Au regard de l'évolution et du perfectionnement des cyberattaques sur Internet, les infrastructures d'hébergement Internet doivent être physiquement cloisonnées de toutes les infrastructures du système d'information qui n'ont pas vocation à être visibles depuis Internet.

●

Cloisonnement de base et filtrage des accès

Niveau 1

À un premier niveau de maturité, les services visibles depuis Internet sont séparés du reste du système d'information par l'intermédiaire d'un réseau distinct ou d'une segmentation logique, et un filtrage des flux réseau est appliqué via un pare-feu. Seuls les ports et protocoles strictement nécessaires sont autorisés entre la zone hébergeant ces services et le système d'information interne, afin de limiter la surface d'attaque potentielle.

Cloisonnement renforcé et supervision continue

Niveau 2

Au niveau avancé, l'infrastructure hébergeant les services exposés sur Internet est isolée dans une zone démilitarisée (DMZ) dédiée, physiquement ou virtuellement séparée du reste du système d'information. Des mécanismes de segmentation réseau supplémentaires sont mis en œuvre, tels que le filtrage strict des flux entre la DMZ et les autres zones, l'utilisation de pare-feu applicatifs, ainsi qu'une surveillance continue des accès et des communications. Des audits réguliers de la configuration et des tests d'intrusion sont réalisés pour s'assurer de l'étanchéité du cloisonnement et de la résilience face aux attaques.

SE 2.6 – SÉCURISER LES INTERCONNEXIONS RÉSEAU DÉDIÉES AVEC LES ENTITÉS EXTÉRIEURES (PARTENAIRES, FOURNISSEURS D'ÉQUIPEMENTS, MAINTENEURS, INSTITUTIONNELS…)

Pour ses besoins opérationnels, un établissement de sante est amené à établir une interconnexion réseau dédiée avec des entités extérieures (ex : GHT, infogérance, maintenance, échange de données, flux monétiques, etc.).

Cette interconnexion peut se faire au travers d'un lien sur le réseau privé de l'entité ou directement sur Internet. Dans le second cas, il convient d'établir un tunnel site à site, de préférence IPsec, en respectant les préconisations de l'ANSSI.

Gestion et contrôle des flux

Niveau 1

L'interconnexion avec les entités extérieures repose sur un filtrage IP rigoureux via un pare-feu positionné à l'entrée du réseau. Les flux entrants et sortants sont limités au strict nécessaire opérationnel, et une matrice des flux est tenue à jour pour assurer la conformité de la configuration des équipements. Il est également essentiel de disposer d'un point de contact actualisé chez le partenaire afin de pouvoir réagir rapidement en cas d'incident de sécurité.

Passerelle dédiée à l'interconnexion

Niveau 2

Pour les établissements présentant un niveau de maturité avancé ou considérés comme « Entité Essentielle », une passerelle dédiée est mise en place pour les connexions partenaires. L'équipement de filtrage IP est exclusivement réservé à cet usage, et l'ajout d'un dispositif de détection d'intrusions (IDS/IPS) est recommandé pour renforcer la sécurité. Des audits réguliers et une supervision continue permettent de garantir l'intégrité de l'interconnexion et de prévenir les risques liés aux accès non autorisés.

SE 2.7 – CONTRÔLER ET PROTÉGER L'ACCÈS AUX SALLES SERVEURS ET AUX LOCAUX TECHNIQUES

La sécurité physique doit faire partie intégrante de la sécurité des systèmes d'information et être à l'état de l'art afin de s'assurer que les dispositifs mis en œuvre ne puissent pas être contournés aisément par un attaquant. Il convient donc d'identifier les mesures de sécurité physique adéquates et de sensibiliser continuellement les utilisateurs aux risques engendrés par le contournement des règles.

●

Contrôle d'accès physique de base

Niveau 1

L'accès aux salles serveurs et aux locaux techniques est assuré par des dispositifs simples tels que des serrures mécaniques ou des badges d'accès individuels. Les visiteurs et prestataires extérieurs doivent être accompagnés en permanence, et un registre manuel ou électronique des accès est tenu à jour pour tracer les entrées et sorties. Une revue régulière des droits d'accès permet d'identifier rapidement toute anomalie.

●●

Gestion avancée et supervision des accès

Niveau 2

Le contrôle d'accès repose sur des systèmes électroniques sophistiqués, intégrant la gestion centralisée des autorisations, la limitation des accès selon des plages horaires et la surveillance vidéo des points sensibles. Les accès sont strictement individualisés, avec une traçabilité automatisée et une alerte en cas de tentative d'accès non autorisé. Des audits périodiques de la configuration des systèmes et des simulations d'incident sont réalisés afin de renforcer la sécurité physique et la réactivité en cas de problème.

SE 3 – Procédures de sécurité réseau

SE 3.1 – DÉTECTION ET RÉPONSE AUX INCIDENTS

Surveillance et journalisation

L'objectif est de disposer de journaux permettant, par l'analyse pas à pas d'évènements passés, d'améliorer la connaissance de réseau « Smart », et de contribuer à la mise en place d'un plan de reprise d'activité.

Cette recommandation concerne la mise en place d'un système de journalisation, en principe centralisé, des événements qui se produisent sur le réseau « Smart » (exemples : connexion des utilisateurs, connexion d'équipements sur les switchs du réseau « Smart »...).

Cette exigence demande :

- L'existence d'un service de journalisation (exemple : serveur Syslog) sur le réseau « Smart »
- La configuration d'équipements, *a minima* des switchs du réseau « Smart », pour qu'ils envoient leurs événements au service de journalisation.

Remarque : Cette exigence ne porte pas sur la gestion des alarmes « process » de systèmes tels que la GTB ou la sûreté, bien que celles-ci puissent également être collectées par le service de journalisation du réseau « Smart ».

●

Mise en place d'un contrôle d'accès et d'une journalisation basique

Niveau 1

Mettre en place des contrôles d'accès physiques ou électroniques aux salles serveurs et locaux techniques, avec une journalisation des entrées et sorties afin de tracer les accès et détecter toute anomalie ou tentative d'accès non autorisée.

●●

Surveillance avancée et centralisation des logs

Niveau 2

Déployer un système de surveillance électronique avec gestion centralisée des accès, journalisation automatisée et alertes en temps réel, complété par des audits et des simulations d'incident pour assurer la sécurité et la réactivité du système.

Continuité d'activité et sauvegarde

L'activité du Smart Hospital fonctionne 7jours/7 et 24h/24 , la qualité de service attendue pour les systèmes d'information SIH et SITH est une disponibilité proche des 100% et le respect des engagements de services. Suite à un incident d'exploitation ou en contexte de gestion d'une intrusion, la continuité de l'activité est un impératif.

Les experts de la sécurité numérique en santé soulignent explicitement « une protection des sauvegardes insuffisante » comme cause récurrente d'incidents graves, avec augmentation des cas où les données deviennent inaccessibles. Même quand la cause première du sinistre est une cyberattaque ou une panne, l'absence ou la faiblesse des sauvegardes est souvent ce qui transforme l'incident en catastrophe

La donnée étant le quatrième fluide du bâtiment, la recommandation pour la continuité d'activité est de mettre le focus sur la politique de sauvegarde de l'établissement.

Plan de continuité et de reprise d'activité

Niveau 1

En complément de la PSSI :

- Des plans de reprise et continuité d'activité (PCA/PRA) sont rédigés, validés et testés
- Ils incluent une politique de sauvegarde qui intègre :
  - → La liste des données jugées vitales et les serveurs concernés
  - → Les différents types de sauvegarde et leur fréquence (par exemple le mode hors ligne) ;
  - → La procédure d'administration et d'exécution des sauvegardes ;
  - → Les informations de stockage et les restrictions d'accès aux sauvegardes
  - → Les procédures de test de restauration ;

Exercice de test annuel des PCA/PRA dont sauvegardes

Niveau 2

Un fois cette politique de sauvegarde établie et testée, il est souhaitable de planifier au moins une fois par an un exercice de restauration des données et de conserver une trace technique des résultats.

Audit et actions correctives

L'audit informatique a pour objectif d'évaluer de manière systématique les systèmes d'information (SIH et SITH pour le Smart Hospital) pour identifier risques, faiblesse de sécurité et conformité aux normes.

À l'issue de ces audits, des actions correctives doivent être identifiées, leur application planifiée et des points de suivi organisés à intervalles réguliers. Pour une plus grande efficacité, des indicateurs sur l'état d'avancement du plan d'action pourront être intégrés dans un tableau de bord à l'adresse de la direction.

Ces audits et contrôles réguliers permettent de mesurer les écarts pouvant persister entre la règle définie dans la PSSI et les PRA/PCA et la pratique.

La réalisation d'audits réguliers (au moins une fois par an) du système d'information est imposée par la NIS2 par le statut Entité Essentielle ou Entité Importante et les pouvoirs publics français notamment au travers du programme CARE de la DGOS. En 2026, l'audit des systèmes d'information est une obligation règlementaire.

Deux étapes essentielles pour l'audit et la mise en œuvre d'actions correctives sont les suivantes :

Étape technique ★

Réalisation d'un diagnostic approfondi des systèmes d'information, incluant l'analyse des configurations, la vérification des mises à jour de sécurité et l'examen des journaux d'événements. Cette phase permet d'identifier précisément les failles et les non-conformités techniques.

Étape organisationnelle

Élaboration et suivi d'un plan d'actions correctives impliquant les parties prenantes, avec la définition de responsabilités, de délais et d'indicateurs de suivi. Cette étape garantit que les mesures sont effectivement appliquées et leur efficacité évaluée lors des points de contrôle réguliers.

Gestion des incidents de sécurité

Les manifestations d'un incident informatique sont souvent progressives et peuvent être détectées par des signes techniques ou organisationnels inhabituels. Elles nécessitent une vérification rapide pour limiter les dégâts. Une mauvaise réaction en cas d'incident de sécurité peut faire empirer la situation et empêcher de traiter correctement le problème.

Les bonnes pratiques de l'ITIL ont documenté les processus à mettre en œuvre dans la gestion des incidents, un processus en5 étapes : identification catégorisation et priorisation, diagnostic et enquête, résolution et rétablissement, clôture.

Les incidents de sécurité (ransomware, fuite, intrusion) suivent le même flux mais avec escalade immédiate vers équipe sécurité et activation d'une procédure crise si incident majeur.

Pour le traitement de ces incidents de sécurité dont les impacts sont à la fois financiers et qualitatifs car impactant pour la production de soins, l'établissement dispose d'une équipe sécurité (SIEM), internalisée ou externalisée

Gestion réactive des incidents de sécurité numérique

Niveau 1

L'établissement s'appuie sur des mécanismes de journalisation et de surveillance de base pour détecter les incidents. La réaction aux incidents est déclenchée après leur survenue, avec des procédures d'identification, de diagnostic et de résolution suivant les bonnes pratiques ITIL. Les équipes sont mobilisées pour limiter les impacts, mais la détection repose sur l'analyse manuelle des journaux ou sur des alertes simples. Ce niveau inclut :

- La mise en place d'un service de journalisation centralisé (ex : serveur Syslog) pour consigner les événements du réseau « Smart » ;
- La configuration des équipements, notamment les switchs, pour l'envoi de leurs événements au service de journalisation ;
- Des plans de continuité et de reprise d'activité formalisés, intégrant la cartographie du réseau, la sécurisation des accès et la gestion des incidents ;
- La sensibilisation des professionnels et usagers aux risques et aux procédures d'incident ;
- Des audits réguliers pour identifier les faiblesses et planifier des actions correctives.

Ce niveau vise à garantir la traçabilité des événements et à permettre une réaction structurée en cas d'incident, sans anticipation ni automatisation avancée.

Gestion proactive des incidents de sécurité numérique

Niveau 2

La gestion des incidents est proactive, intégrant des outils et pratiques avancées. L'établissement est en capacité de prévenir les incidents grâce à une surveillance automatisée, une corrélation des événements (SIEM), et une équipe dédiée à la sécurité interne ou externalisée. Les processus de détection s'appuient sur des indicateurs de compromission, des alertes en temps réel et des retours d'expérience pour anticiper les menaces. Les plans d'action sont continuellement améliorés grâce à des audits périodiques et des exercices de simulation d'incidents. Ce niveau inclut :

- L'intégration de solutions SIEM pour la détection avancée et la corrélation des incidents ;
- La supervision continue des accès et des événements critiques du réseau « Smart » ;
- La réalisation d'exercices de restauration et de simulation de crise au moins une fois par an ;
- Une politique de sauvegarde robuste, testée et auditée régulièrement ;
- La coopération entre les responsables sécurité et numérique pour anticiper et traiter les incidents selon les standards ANSSI, ISO27001 et ITIL ;
- La mise à jour régulière des procédures, outils et matrices de risques pour tenir compte des nouvelles menaces et vulnérabilités.

SE 3.2 – MISE À JOUR ET LUTTE CONTRE L'OBSOLESCENCE

Le maintien de la sécurité du réseau « Smart » repose sur l'application systématique des dernières mises à jour concernant l'ensemble des équipements et logiciels qui le composent. Cette démarche inclut l'intégration régulière des correctifs de sécurité et des mises à jour émises par les fabricants ou éditeurs, afin d'assurer la fiabilité et la sécurité des systèmes. Elle permet de réduire les vulnérabilités, de garantir la conformité aux standards en vigueur et de minimiser les risques liés à l'obsolescence des composants.

Les équipements du réseau doivent être mis à jour ; par ailleurs, l'établissement bâtiment et/ou son prestataire doit disposer d'un protocole formalisé de mise à jour des équipements et logiciels intégrés au réseau « Smart ».

Les mises à jour concernent :

- Les équipements du Smart Réseau (logiciels des cœurs de réseau, routeurs, capteurs…)
- Les pares-feux (licences, politiques de sécurité, micrologiciels)
- Les serveurs et postes clients locaux (systèmes d'exploitation, couches de virtualisation éventuelles, pilotes de périphériques, antivirus)
- Les logiciels métiers (exemples : supervision, GTB, géolocalisation, GMAO…)

Lors de l'installation, les systèmes doivent être livrés dans leur version la plus récente proposée par le fabricant ou l'éditeur. En exploitation, tout équipement ou logiciel obsolète qui n'est plus supporté doit être remplacé, afin de garantir la mise à jour et la fiabilité du réseau. La conservation d'équipements ou de logiciels obsolètes est possible uniquement si les risques associés sont clairement identifiés et acceptés par le propriétaire de l'installation.

Gestion réactive et conformité minimale

Niveau 1

L'établissement applique les mises à jour correctives sur les équipements et logiciels du réseau « Smart » principalement en réponse à des alertes de sécurité ou à des obligations réglementaires. Les processus sont essentiellement manuels, avec une gestion des obsolescences ponctuelle et souvent déclenchée par la détection d'un problème ou lors d'audits périodiques. La documentation des actions reste limitée, ce qui peut entraîner des délais dans la prise en compte des vulnérabilités. Les équipements ou logiciels obsolètes sont remplacés au cas par cas, sans politique systématique.

Gestion proactive et automatisée

Niveau 2

L'établissement met en place une politique proactive de gestion des mises à jour et de lutte contre l'obsolescence, intégrant des outils automatisés de supervision et d'inventaire. Les mises à jour sont programmées régulièrement, avec une validation systématique de la compatibilité et de la sécurité avant déploiement. Un guide formalisé définit les procédures, et un suivi rigoureux permet d'anticiper les cycles de vie des équipements. Les risques associés au maintien d'éléments obsolètes sont analysés et documentés, et toute exception fait l'objet d'une décision éclairée par la direction de l'établissement ou l'exploitant du réseau.

SE 4 – Sécurité d'accès aux services

SE 4.1 – IDENTIFIER NOMMÉMENT CHAQUE PERSONNE ACCÉDANT AUX SERVICES ET DISTINGUER LES RÔLES UTILISATEUR/ ADMINISTRATEUR

La cartographie réalisée dans l'analyse de risque identifie les des ressources du système qui peuvent constituer une cible précieuse aux yeux d'un attaquant (répertoires contenant des données sensibles, bases de données, boîtes aux lettres électroniques, etc.). Il est donc primordial d'établir une liste précise de ces ressources et pour chacune d'entre elles de :

- Définir quelle population peut y avoir accès ;
- Contrôler strictement son accès, en s'assurant que les utilisateurs sont authentifiés et font partie de la population ciblée ;
- Éviter sa dispersion et sa duplication à des endroits non maîtrisés ou soumis à un contrôle d'accès moins strict.
- Par exemple, les répertoires des administrateurs regroupant de nombreuses informations sensibles doivent faire l'objet d'un contrôle d'accès précis. Il en va de même pour les informations sensibles présentes sur des partages réseau :
- Exports de fichiers de configuration, documentation technique du système d'information, bases de données métier, etc. Une revue régulière des droits d'accès doit par ailleurs être réalisée afin d'identifier les accès non autorisés

Identification basique et gestion manuelle

Niveau 1

Au premier niveau de maturité, l'identification des comptes et des rôles repose principalement sur des méthodes manuelles. Les comptes sont généralement créés à la demande, sans procédure formalisée de revue périodique. Les rôles attribués sont parfois peu documentés, et il existe un risque de confusion entre les droits réels des utilisateurs et leurs besoins métier. La traçabilité des modifications et des attributions de rôles reste limitée, ce qui peut compliquer la gestion des accès en cas d'incident ou d'audit.

Identification centralisée et gestion automatisée

Niveau 2

À ce stade, l'organisation met en place un système centralisé d'identification des comptes et de gestion des rôles, souvent via un annuaire ou une solution d'Identity & Access Management (IAM). Les processus d'attribution et de révocation des droits sont automatisés, avec une validation systématique des besoins et une documentation exhaustive des rôles. Des revues d'accès régulières sont réalisées pour s'assurer de la conformité des droits et de l'adéquation avec les fonctions exercées. Ce niveau permet une meilleure traçabilité et une réactivité accrue face aux évolutions organisationnelles.

SE 4.2 – SÉCURISATION DE L'ACCÈS AUX APPLICATIONS

Il s'agit de garantir la confidentialité des échanges, en empêchant des tiers de lire ou de corrompre les messages échangés, sans nécessité d'ajout des mécanismes intermédiaires de sécurité (type VPN, qui permettent de créer une connexion sécurisée entre un appareil et le réseau internet) entre ces personnes/équipements.

●

Contrôle d'accès basique
Niveau 1

L'accès aux applications repose sur des mécanismes simples tels que l'authentification par mot de passe et la gestion manuelle des droits. Ces droits sont attribués au cas par cas, sans documentation exhaustive, ce qui peut entraîner une confusion quant aux privilèges réels et accroître les risques en cas d'incident.

●●

Contrôle d'accès avancé et gestion centralisée
Niveau 2

L'établissement met en œuvre une gestion centralisée des accès, souvent via une solution IAM ou un annuaire, permettant l'automatisation de l'attribution et de la révocation des droits. Les rôles et privilèges sont clairement définis et documentés, et des revues périodiques des accès sont réalisées pour garantir la conformité et l'adéquation des droits avec les fonctions exercées. Les applications intègrent des mécanismes d'authentification forte (MFA, certificats numériques) et une traçabilité renforcée, assurant une meilleure sécurité et une réactivité face aux évolutions organisationnelles.

SE 4.3 – PRÉVENTION ET GESTION DES RISQUES

L'objectif est de pérenniser la sécurité numérique du bâtiment par la mise en place de procédures de gestion et prévention des risques.

L'établissement de santé doit avoir mis en place et mis en application une procédure de gestion et prévention des risques portant sur les API, les équipements actifs du réseau « Smart » et les serveurs et clients locaux, intégrant :

- La gestion des droits d'accès : la procédure doit inclure *a minima* les types de profils et les autorisations associées
- La stratégie de gestion des mots de passe et autres moyens d'authentification : la procédure doit inclure *a minima* la complexité des mots de passes, la gestion de renouvellement des mots de passes et des certificats

●

Approche réactive et documentation minimale
Niveau 1

La prévention et la gestion des risques reposent sur des mesures ponctuelles prises en réaction à des incidents ou alertes. Les procédures ne sont pas formalisées, et la documentation des incidents ainsi que des réponses apportées demeure limitée. Les responsabilités sont souvent mal définies, et la sensibilisation des équipes reste insuffisante, ce qui expose l'organisation à une vulnérabilité accrue face aux menaces numériques.

Approche proactive et gestion structurée

Niveau 2

Ce niveau se caractérise par l'adoption d'une démarche structurée, intégrant des procédures formalisées de prévention et de gestion des risques numériques. Des audits réguliers sont réalisés, les rôles et responsabilités sont clairement définis, et un plan de gestion des incidents est mis en place. La sensibilisation et la formation des équipes sont assurées, permettant une anticipation des menaces et une réaction rapide et efficace en cas d'incident.

SE 5 – Protection des données

SE 5.1 – GOUVERNANCE DES DONNÉES

La gouvernance des données est l'ensemble des règles, processus et responsabilités permettant de gérer les données de manière fiable et sécurisée. Ses objectifs sont de :

- Garantir la qualité et la fiabilité des données
- Protéger les données sensibles
- Assurer la conformité réglementaire
- Améliorer la prise de décision.

●

Structurer la gestion des accès et des droits

Niveau 1

Des procédures précises existent pour attribuer, contrôler et révoquer les droits d'accès aux données, en fonction des profils utilisateurs et des besoins métiers. La mise en place d'une politique de gestion des mots de passe et d'authentification robuste est également essentielle.

●●

Formaliser les processus de gouvernance

Niveau 2

Les rôles et responsabilités liés à la gestion des données sont clairement définis. L'établissement est en capacité d'assurer la formation et la sensibilisation des équipes, de documenter toutes les actions et incidents.

Des audits réguliers pour garantir la conformité et la fiabilité du dispositif doivent être réalisés.

SE 5.2 – CONFORMITÉ AU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Il s'agit de déployer une stratégie de gestion des données à caractère personnel et se mettre en conformité avec l'obligation réglementaire que constitue le Règlement Général sur la Protection des Données (RGPD).

Le DPO de l'établissement doit avoir vérifié la conformité de son dispositif « smart » (données rendues disponibles sur les API exposées sur le réseau « Smart ») à la réglementation concernant la protection des données :

- Respect de la loi n°78-17 du 6 janvier 1978 dite loi « Informatique et Libertés »
- Application du règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE dit « règlement général sur la protection des données » ou RGPD.

●★

Formalisation et suivi des procédures de traitement des données

Niveau 1

Les procédures pour l'enregistrement, la classification et la documentation des traitements de données personnelles sont clairement définies. Cela inclut :

- la tenue à jour du registre des activités de traitement,
- la réalisation d'analyses d'impact sur la protection des données (AIPD),
- la mise en place de mécanismes de contrôle réguliers afin de garantir la conformité et d'anticiper les risques liés à la gestion des données.

●●★

Formation et responsabilisation des acteurs

Niveau 2

Déployer un programme de sensibilisation et de formation auprès des équipes, en précisant les rôles et responsabilités de chacun dans la gestion des données personnelles. Ce dispositif permet d'assurer une compréhension collective des obligations réglementaires et d'adopter une culture de protection des données, facilitant ainsi une réaction rapide et cohérente en cas d'incident ou de demande d'exercice des droits par les personnes concernées.

Management responsable

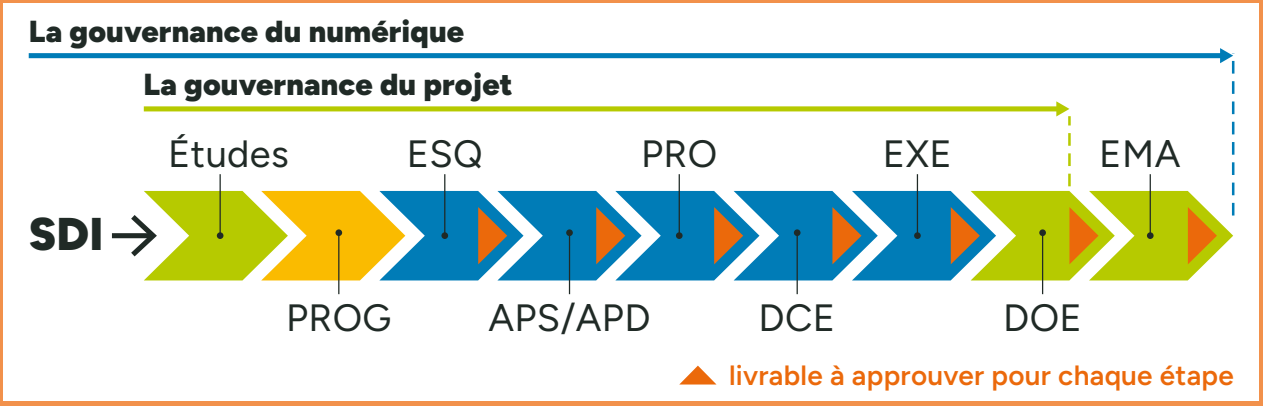
Le management responsable dans le cadre du projet Smart Hospital repose sur une approche globale et structurée intégrant plusieurs dimensions essentielles. Il s'agit de concevoir un hôpital intelligent dès l'origine (« Smart Hospital par conception »), d'instaurer une gouvernance adaptée au projet, de définir les étapes clés telles que le commissionnement, d'organiser l'exploitation et la maintenance avec un cadre de contractualisation précis, tout en développant les compétences et nouveaux métiers et en intégrant une réflexion sur les enjeux environnementaux. Cette démarche vise à concilier la transition environnementale et numérique.

Ce thème constitue un véritable outil de gestion de projet permettant d'apporter des réponses aux défis de gouvernance engendrés par l'arrivée du numérique dans le bâtiment. Ces enjeux se déclinent en trois volets principaux :

La gouvernance du numérique et du projet :
Elle comprend des éléments relatifs à la recette et à l'administration du réseau « Smart » et des services numériques, ainsi que des recommandations pour assurer une gestion optimale du numérique de l'établissement.

La propriété des données et la contractualisation des services :
Il s'agit de mener une réflexion sur la propriété des données et de l'infrastructure du réseau « Smart », tout en définissant un cadre de contractualisation pour les conditions d'accès aux services.

Les qualités environnementales :
Elles incluent des recommandations sur le bilan environnemental des équipements électroniques du bâtiment à travers les fiches PEP, ainsi que la mesure des champs électromagnétiques.



Recommandations	Niveau de maturité		Pages
MA 1 – Le Smart Hospital « par conception » ou « by design »			→ p.91
MA 1.1 – LE CONCEPT DE « BY DESIGN »	Unique	Le numérique est inclus « by design » dès l'initialisation du projet	
MA 1.2 – LA TRANSVERSALITÉ DU NUMÉRIQUE ET LA DONNÉE			
MA 1.3 – GOUVERNANCE DU NUMÉRIQUE	● Niveau 1	Les services techniques	
	●● Niveau 2	Les projets numériques du Smart Hospital	
MA 1.4 – LE SCHÉMA DIRECTEUR IMMOBILIER	● Niveau 1	Un volet numérique	
	●● Niveau 2	Une architecture cible et un plan de transformation	
MA 2 – Le projet Smart Hospital			→ p.94
MA 2.1 – GOUVERNANCE DU PROJET			
MA 2.2 – LOT NUMÉRIQUE (OU SMART) ET PIÈCES CONTRACTUELLES	● Niveau 1	Un lot numérique (ou Smart) est prévu dans le programme technique	
	●● Niveau 2	Le lot namérique ou Smart est doté d'un budget et d'une gouvernance propre	
MA 2.3 – PLANIFICATION ET ÉTAPES CLÉS DU PROJET			
MA 2.4 – LE COMMISSIONNEMENT : ÉTAPE CLÉ DU PROJET	● Niveau 1	Le commissionnement est prévu et ses exigences prévues dès la phase de conception	
	●● Niveau 2	Les exigences du commissionnement sont incluses dans le ou les cahiers des charges produits pour le projet Smart Hospital	
MA 3 – L'exploitation-maintenance et la qualité de service			→ p.97
MA 3.1 – L'EXPLOITATION/MAINTENANCE			
MA 3.2 – LA QUALITÉ DE SERVICE ET LES ENGAGEMENTS DE SERVICE	● Niveau 1	L'exploitation-maintenance est organisée	
	●● Niveau 2	Les engagements de qualité de service (SLA) sont définis et contractualisés.	
MA 4 – Compétences			→ p.99
MA 4.0 – MOA CELLULE NUMÉRIQUE	Prérequis	Mise en place d'une cellule Numérique dès la phase SDI	
MA 4.1 – AMO SMART	Prérequis	Mise en place de l'AMO Smart dès la phase de programmation	
MA 4.2 – CSSN	Prérequis	Mise en place du CSSN dès la phase de conception	
MA 4.3 – MSI	Prérequis	Mise en place du MSI dès la phase d'exécution	
MA 5 – Qualité environnementale			→ p.102
MA 5.1 – DÉTERMINATION CHAMP MAGNÉTIQUE	★● Niveau 1	Les équipements émetteurs et les zones mesurées sont cartographiés	
MA 5.2 – IMPACT ENVIRONNEMENTAL : LE NUMÉRIQUE RESPONSABLE			
Les FDES			
La démarche numérique responsable	● Niveau 1	La démarche numérique responsable est engagée dès la phase conception	
	●● Niveau 2	La démarche numérique responsable est appliqué au cycle de vie	
MA 5.3 – EFFICIENCE ÉNERGÉTIQUE DU RÉSEAU « SMART », DES SERVICES ET SYSTÈMES NUMÉRIQUES	● Niveau 1	Identification des consommations électriques du réseau « Smart »	
	●● Niveau 2	Maîtrise des consommations du réseau « Smart »	
MA 5.4 – IMPACT ENVIRONNEMENTAL DU CLOUD			
L'IA et ce qui aggrave l'empreinte			
Leviers de réduction	Unique	La démarche « Numérique Responsable » est appliquée dans la sélection des services externalisés	

★ Obligation réglementaire

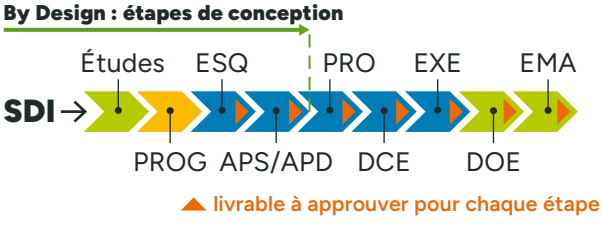
MA 1 – Le Smart Hospital « par conception » ou « by design »

MA 1.1 – LE CONCEPT DE « BY DESIGN »

Le concept « by design » désigne une approche où le numérique est intégré dès la conception du projet Smart Hospital et non ajouté a posteriori, pour maximiser performance et innovation, garantir une cohérence optimale et anticiper les budgets nécessaires au déploiement et à l'exploitation des systèmes.

Le principe consiste à penser le numérique comme ADN du projet : données, IA, interopérabilité et interfaces utilisateurs (UX) au cœur des choix stratégiques, plutôt qu'en surcouche technique.

Cela signifie concevoir le Smart Hospital où les services numériques du SITH (GTB, Géolocalisation, usage des locaux, sécurité des accès, ...) dialoguent nativement en eux et avec ceux du SIH (DPI, GTB, DPI, logistique et smart building dialoguent nativement dès le SDI (Schéma Directeur Immobilier).



Le numérique est inclus « by design » dès l'initialisation du projet

Niveau unique

Le numérique fait partie de l'ADN du projet et est intégré dans la réflexion le plus tôt possible : idéalement dès le SDI.

MA 1.2 – LA TRANSVERSALITÉ DU NUMÉRIQUE ET LA DONNÉE

L'ubiquité du numérique à l'hôpital est une réalité : une « infrastructure invisible » qui traverse tous les métiers, du soin à l'énergie, la logistique, ... et reconfigure l'approche de la technologie autant que de l'organisation. À l'hôpital, le numérique est partout ; ce n'est plus un service support mais le socle de chaque geste de soin, de chaque mouvement de patient, de chaque kWh consommé.

La transversalité du numérique se traduit par une intégration systématique et globale de l'ensemble des outils numériques pour favoriser la coordination entre les différents métiers et domaines d'action du projet de l'établissement de santé.

Comprendre la donnée : l'enjeu de l'interopérabilité sémantique et de l'IA

Dans ce contexte, la donnée n'est plus un simple support. Elle devient la condition même du fonctionnement de l'organisation hospitalière : disposer de la bonne donnée, au bon moment et au bon endroit est une exigence opérationnelle indiscutable.

Le Smart Hospital ne peut plus être pensé uniquement à travers les outils. Il repose désormais sur une véritable ingénierie de la donnée. Dans un environnement où machines, logiciels et acteurs humains interagissent en permanence, une donnée échangée ne vaut que si elle est comprise de la même manière par tous.

Cette ingénierie de la donnée est au cœur du déploiement de l'intelligence artificielle qui exploite les masses de données produites par les applications, les matériels et, de plus en plus, les réseaux IOT.

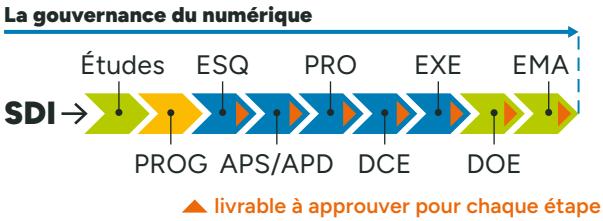
MA 1.3 – GOUVERNANCE DU NUMÉRIQUE

La transversalité du numérique, les données et l'utilisation bénéfique de l'intelligence artificielle sont les supports d'une transformation digitale sans fin et rythmée par l'émergence continue d'innovations technologiques et organisationnelles. Elle impose d'adopter une organisation spécifique pour piloter ce mouvement.

La gouvernance du numérique vise à se doter d'une stratégie qui englobe tous les systèmes d'information : c'est-à-dire le SIH et le SITH. Cette gouvernance a pour mission de structurer les décisions pour organiser et piloter l'ensemble des dispositifs numériques du Smart Hospital, en assurant la conformité, la sécurité et la performance du réseau « Smart » et surtout, mutualiser les technologies et les compétences partout où cela est possible.

Établir la gouvernance pour le numérique et structurer les décisions, coordonner les acteurs et assurer le suivi des projets exigent à minima :

- Un plan qui définit les objectifs et le cadre
- Une instance de gouvernance ou un comité stratégique
- Des rôles clés pour informer sur l'état de l'art et l'avancement des projets et pour éclairer les décisions.
- Une communication pour informer et accompagner le changement.



●

Les services techniques
Niveau 1

Les services techniques sont partie-prenante de la gouvernance du numérique

●●

Les projets numériques
Niveau 2

Les projets numériques du Smart Hospital sont inclus dans le portefeuille de projets numériques de l'établissement

MA 1.4 – LE SCHÉMA DIRECTEUR IMMOBILIER

Dans l'objectif d'intégrer dès la conception le numérique dans les projets immobiliers et dans un contexte où la grande majorité de ces projets sont parties d'un patrimoine immobilier existant, le Schéma Directeur Immobilier sert de cadre de référence pour l'organisation et le développement du projet Smart Hospital.

En en alignant la stratégie immobilière sur les objectifs du numérique, le schéma directeur immobilier est à l'hôpital ce que le plan d'urbanisme est à la ville. Il s'appuie sur un projet médical qui répond aux besoins futurs de l'établissement, à son positionnement sur son territoire de santé et sur une analyse de l'état et des potentialités du patrimoine existant.

L'objectif du SDI est ainsi de doter l'hôpital d'une vision exhaustive et évolutive des investissements immobiliers et techniques en réponse aux évolutions de la médecine, des moyens de prise en charge des patients, des impacts du changement climatique ainsi que des environnements de travail.

Le SDI du Smart Hospital incorpore un volet numérique qui sert de feuille de route pour aligner les systèmes numériques sur les objectifs de l'établissement découlant de son projet médical.

Les principaux éléments de ce volet numérique du SDI comprennent :

1 – Vision et Objectifs Stratégiques
Définition des objectifs à long terme de l'établissement et comment les systèmes d'information dont le SITH peuvent contribuer à leur réalisation.

2 – Analyse de l'Existant
Évaluation des systèmes numériques actuels, de leurs performances et de leurs limites. Cela inclut souvent un audit des infrastructures, des systèmes et des processus en place.

3 – Architecture Cible
Description de l'architecture future du SITH, incluant les technologies, les applications et les infrastructures nécessaires pour atteindre les objectifs stratégiques.

4 – Plan de Transformation
Détail des projets et des initiatives à mettre en œuvre pour passer de l'architecture actuelle à l'architecture cible. Cela inclut des feuilles de route (roadmaps), des plannings et des ressources nécessaires.

5 – Gouvernance et Sécurité
Définition des règles de gouvernance des systèmes d'information, y compris les politiques de sécurité, de conformité et de gestion des risques. (NB : voir le thème « Sécurité Numérique du R2S4Care)

6 – Budget et Ressources
Estimation des coûts et des ressources nécessaires pour la mise en œuvre du volet numérique du SDI, incluant les investissements en infrastructure, logiciels et compétences.

7 – Indicateurs de Performance
Définition des KPIs (Key Performance Indicators) pour mesurer l'efficacité et l'alignement des systèmes numériques avec les objectifs stratégiques.

8 – Plan de Communication
Stratégie pour communiquer les changements et les évolutions des systèmes numériques aux différentes parties prenantes de l'établissement.

●

Un volet numérique
Niveau 1

Dans le SDI, un volet numérique est inclus et précise une vision et des objectifs

●●

Une architecture cible et un plan de transformation
Niveau 2

Le volet numérique du SDI définit une architecture cible et un plan de transformation

MA 2 – Le projet Smart Hospital

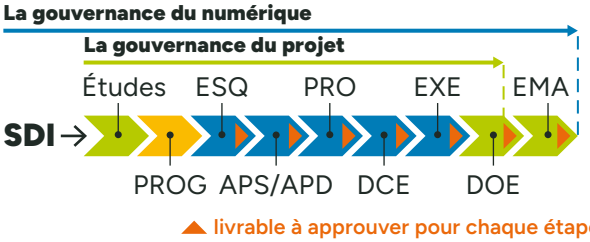
MA 2.1 – GOUVERNANCE DU PROJET

La gouvernance de chaque projet, issu du volet numérique du SDI, définit les rôles, responsabilités, processus décisionnels et contrôle pour assurer succès, alignement stratégique et maîtrise risques, particulièrement critique pour le projet numérique du Smart Hospital.

Les composants essentiels de la gouvernance sont :

- Rôles clés : Sponsor (DG), chef projet, comité pilotage (transversal : métiers, DSI, finance, CME), AMO Smart externe pour aborder la complexité des projets.
- Processus : cadrage (ESQ), planification (APS/APD), exécution (suivi KPI), clôture (retours d'expérience).
- Outils : charte projet, Matrice RACI (Réalisateur, Approbateur, consulté, informé), tableaux bord, réunions cadence (hebdo/mensuel).

En complément du R2S for Care, l'ANAP propose un ensemble de documents et d'outils pour la gestion de projets. Ils sont disponibles sur : www.anap.fr



MA 2.2 – LOT NUMÉRIQUE (OU SMART) ET PIÈCES CONTRACTUELLES

Les informations liées à la mise en œuvre du Smart Hospital doivent être présentes dans les pièces contractuelles.

Le Smart correspond à l'ensemble des solutions matériels, logiciels et applications, de prestation de mise en œuvre, coordination et d'exploitation servant à rendre le bâtiment connecté et communicant et à fournir les services numériques souhaités par le maître d'ouvrage pour l'exploitation de son patrimoine immobilier et les besoins des usagers des bâtiments.

Cette recommandation demande la présence d'informations et de spécifications sur tous les éléments dits Smart, c'est à-dire présentes sous forme d'un cahier des charges dont les exigences sont reprises dans le PTD (Programme Technique Détaillé)

Ce programme technique détaillé déterminé par le maître d'ouvrage définit l'infrastructure numérique et son périmètre qui doivent faire l'objet d'un lot numérique ou Smart. Il s'agit d'intégrer avec cohérence des systèmes hétérogènes et multi technologiques, et de déterminer les limites de prestations des fournisseurs. Contractuellement, il s'agit d'initialiser un cadre contractuel répondant aux attentes du maître d'ouvrage.

Concrètement, le document doit indiquer le périmètre du projet avec ses exigences techniques et fonctionnelles dont les interfaces permettant d'exposer les données sur le réseau « Smart » et d'assurer l'interopérabilité entre applications. En complément le cahier des charges comprendra les exigences en matière de sécurité imposée par le maître d'ouvrage.

Dans l'élaboration budgétaire des projets immobiliers issus du SDI, le lot numérique (ou Smart) dispose d'un budget dédié non fongible avec les budgets des autres lots techniques du programme.

Un lot numérique (ou Smart) est prévu dans le programme technique

Niveau 1

Ce lot est caractérisé par un cahier des charges inclus dans le programme technique détaillé qui apporte une cohérence transversale à l'ensemble des systèmes et composants numériques présents dans les lots techniques du programme et produits les services numériques attendus par le maître d'ouvrage.

Le lot numérique ou Smart est doté d'un budget et d'une gouvernance propre

Niveau 2

Existence d'un lot Smart dont le périmètre intègre *a minima* obligatoirement les équipements actifs du réseau « Smart » (en cohérence avec le périmètre du réseau « Smart ») et doit être traité comme un système à part entière.

Facultativement, cela peut comprendre la mise en place du BOS (Building Operating System), du système d'information bâtimentaire (BIS), du câblage du réseau « Smart », de la supervision GTB, GMAO, applications utilisateurs…

MA 2.3 – PLANIFICATION ET ÉTAPES CLÉS DU PROJET

Que ce soit dans le cadre d'une construction neuve ou d'une rénovation, un projet doit reposer sur une démarche globale, depuis la conception jusqu'à l'exploitation.

La planification consiste à fixer les objectifs, organiser les tâches et déterminer les ressources nécessaires à leur réalisation. Elle permet d'anticiper les événements, les impacts et les risques. Pour planifier un projet, il faut partir d'un cadrage clair, structurer la gouvernance, définir les livrables, puis dérouler le projet par phases avec des jalons de décision et de suivi.

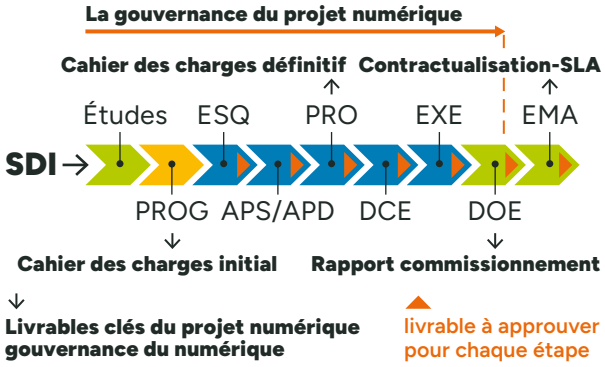
- Cadrer le projet à partir des objectifs et exigences du cahier des charges (ou CCTP)
- Découper en phases et maîtriser les risques
- Piloter dans le temps en définissant les jalons et les livrables
- Sécuriser les facteurs humains (expertise et utilisateurs)

La particularité du projet numérique du Smart Hospital s'il est conçu « by design », c'est-à-dire prévu dans le SDI et dans le périmètre des études préalables, est qu'il peut avancer en parallèle du projet de construction dans le respect des étapes clés qui seront examinées dans le paragraphe suivant.

Dans le volet maîtrise des risques, la recommandation est de ne mettre en exploitation que les technologies et systèmes préalablement testés et validés par le maître d'ouvrage. Le délai entre le lancement du projet et la rédaction du cahier des charges définitif produit pour la phase « PRO » est une opportunité pour valider les technologies et systèmes qui seront mis en exploitation avec des engagements de qualité de service.

Les livrables clés à prévoir dans l'exercice de planification sont :

- Le cahier des charges initial à produire dans la phase « Programmation »
- Le cahier des charges définitif pour la phase PRO
- Le rapport de commissionnement dans la phase DOE
- Les engagements de qualité de services à finaliser dans la phase DOE.



MA 2.4 – LE COMMISSIONNEMENT : ÉTAPE CLÉ DU PROJET

Le commissionnement désigne la démarche méthodique qui consiste à vérifier, documenter et valider qu'un système, un bâtiment ou un équipement fonctionne conformément aux besoins définis dans le cahier des charges avant sa mise en service, puis à maintenir cette performance dans le temps.

Cela implique :

- Dès la phase de conception : définir les objectifs et les critères de performance dès la phase de conception.
- Dans les phases «EXE » : dérouler et contrôler les tests, corriger les écarts et documenter les résultats
- Dans la phase DOE : valider le commissionnement et la qualité de service en deux étapes : réception (VA - Vérification d'Aptitude pour les marchés publics) et fonctionnement (VSR – Vérification de Service Régulier)
- S'assurer que la solution reste performante après la mise en service, pas seulement au moment de la mise en service de l'installation ou du système numérique.

Le commissionnement devra être réalisé sous la responsabilité d'une personne physique clairement désignée : elle peut être externe au projet (en Assistance à maîtrise d'ouvrage, AMO) ou interne à maîtrise d'ouvrage.

●

Le commissionnement est prévu et ses exigences prévues dès la phase de conception

Niveau 1

Le commissionnement n'est pas une étape finale isolée : c'est une démarche qui commence tôt, avec la planification, la définition des objectifs et l'intégration des exigences dans les plans et les spécifications du projet. C'est ce cadrage précoce qui permet de vérifier, à la réception, que les installations atteignent bien les performances attendues et peuvent les maintenir dans le temps.

●●

Les exigences du commissionnement sont incluses dans le ou les cahiers des charges produits pour le projet Smart Hospital

Niveau 2

Les exigences de commissionnement sont formalisées dans le ou les cahiers des charges techniques du projet, afin de garantir la conformité, la performance et la maintenabilité des solutions livrées.

Le commissionnement fait partie des exigences contractuelles du projet et doit être précisé dans les CCTP/CDC pour sécuriser la recette et l'exploitation.

Cela couvre :

- Les tests de conformité et de performance avant réception.
- Les modalités de recette, de documentation et de transfert de compétences.
- Les exigences de coordination entre couche réseau, couche applicative et équipements, conformément à la définition du SITH et de l'approche R2S 4 CARE.

MA 3 – L'exploitation-maintenance et la qualité de service

L'exploitation maintenance des systèmes et services numériques du Smart Hospital regroupe l'ensemble des activités de supervision, de support, de maintenance et d'évolution nécessaires pour garantir la disponibilité, la sécurité, l'interopérabilité et la performance des services numériques dans la durée.

MA 3.1 – L'EXPLOITATION/ MAINTENANCE

Dans un Smart Hospital, cette exploitation maintenance est plus exigeante parce qu'elle touche des environnements critiques : soins, imagerie, blocs, pharmacie, énergie, sûreté et réseau informatique.

L'exploitation correspond au pilotage quotidien des systèmes,

La maintenance couvre les actions préventives, curatives et prédictives nécessaires pour garantir la disponibilité, la performance et la sécurité des services.

Le Smart Hospital s'appuie sur une architecture ouverte et interopérable où les données issues des capteurs, de la GTB, du réseau « Smart » et des applications métiers convergent vers des outils de supervision, de jumeau numérique ou de tableau de bord centralisé.

Les activités principales de l'exploitation/ maintenance sont :

- La supervision des réseaux, serveurs, API, capteurs, GTB et applications métiers.
- La gestion des incidents et la continuité de service, y compris la priorisation des fonctions critiques.
- La maintenance prédictive, rendue possible par l'analyse des données et des historiques d'usage.
- Les mises à jour, correctifs de sécurité, évolutions fonctionnelles et renouvellements d'équipements.
- La gestion documentaire et contractuelle : procédures, SLA (Service Level Agreement ou engagement de qualité de service), tests, commissionnement, recettes et traçabilité

MA 3.2 – LA QUALITÉ DE SERVICE ET LES ENGAGEMENTS DE SERVICE

L'hôpital est une organisation qui fonctionne 7j/7 et 24h/24. L'organisation en charge de l'exploitation-maintenance doit garantir à la fois la disponibilité technique, la continuité des usages critiques et la qualité perçue par les métiers.

Dans le référentiel de bonnes pratiques ITIL, le SLA (Service Level Agreement ou engagement de qualité de service) définit l'engagement de qualité de service. Un SLA est un accord écrit de niveau de service entre un fournisseur et un client, qui définit les services attendus, les niveaux de qualité, les délais, la disponibilité et les modalités de mesure.

La relation client/fournisseur peut être interne ou externe.

Ce que doit couvrir un SLA :

- Disponibilité : taux de service des applications, du réseau, de la GTB et des interfaces critiques.
- Temps de réponse : délais de prise en charge, de rétablissement et de correction d'incident.
- Sécurité : exigences de sauvegarde, de reprise, de cybersécurité et de traçabilité. (voir thème Sécurité Numérique)
- Évolutivité : capacité à faire évoluer les services sans casser l'existant,
- Support : horaires, niveaux d'escalade, astreinte, support de niveau 1 à 3.

●

L'exploitation-maintenance est organisée

Niveau 1

Pour assurer la continuité de fonctionnement des systèmes et services numériques, gouvernance, supervision continue, sécurité, maintenance et amélioration continue sont formalisés et organisés. Des indicateurs mesurables sont définis.

Leviers essentiels :

- Gouvernance claire : définir les responsabilités, les niveaux de validation, les circuits d'escalade et les priorités de service.
- Supervision en continu : surveiller disponibilité, performance, capacité et incidents en temps réel pour détecter les dérives avant qu'elles n'affectent les usages.
- Sécurité et conformité : appliquer les exigences de cybersécurité, de traçabilité, de sauvegarde et de conformité RGPD pour éviter les ruptures de service et les risques patients.
- Maintenance proactive : mettre en place correctifs, mises à jour, maintenance préventive et, quand c'est possible, prédictive

●●

Les engagements de qualité de service (SLA) sont définis et contractualisés

Niveau 2

La contractualisation de la qualité de service est effective et suit les bonnes pratiques de gouvernance :

- Définir les SLA par service et non seulement par technologie : réseau, identité, API, supervision, GTB, applications métiers.
- Les SLA sont négociées et défini avec toutes les parties prenantes : la DSI, le biomédical, le technique et les fournisseurs. Tous ces acteurs sont alignés sur les mêmes engagements.
- Intégrer les SLA dès la conception et les cahiers des charges ou CCTP, pour que les exigences de performance soient contractualisées avant la mise en service.
- Réviser les engagements régulièrement en COPIL de gouvernance pour tenir compte des retours d'exploitation et des nouveaux usages.

MA 4 – Compétences

Le développement des compétences et des nouveaux métiers est indispensable pour accompagner la transition numérique et environnementale du Smart Hospital.

MA 4.0 – MOA CELLULE NUMÉRIQUE

Mise en place d'une cellule Numérique dès la phase SDI

Prérequis

La Cellule Numérique de la maîtrise d'ouvrage, copilotée par la DST et la DSI, constitue l'instance interne responsable du numérique pour le projet Smart Hospital. Elle porte la vision d'ensemble, arbitre les priorités entre usages, sécurité, coûts et délais, et assure la cohérence des décisions avec le projet médical, le SDI et les politiques de l'établissement. Véritable point de convergence, elle fait le lien avec l'ensemble des entités de l'établissement (médical et soignant, directions fonctionnelles, biomédical, institutionnel et gouvernance), garantit l'expression fidèle des besoins et organise la conduite du changement.

Sur le plan opérationnel, la Cellule structure la gouvernance numérique : préparation et animation des comités (techniques et stratégiques), tenue du registre de décisions, gestion du RACI, consolidation des cas d'usage et maintien d'un portefeuille de projets priorisé. Elle valide les dossiers d'architecture cible et les clauses du lot numérique proposés par le CSSN/AMO, en veillant à l'interopérabilité SIH/SITH, à la réversibilité des données et services et au respect des politiques cybersécurité et RGPD/PGSS-S.

Dans la phase achat, elle cadre les attentes de la MOA, sécurise les pièces de marché (y compris les critères d'évaluation) et participe aux arbitrages de l'évaluation de la valeur d'usage et le coût total de possession. En exécution, elle statue sur les étapes de validation (Tests techniques, tests d'acceptance utilisateurs, commissioning), vérifie la complétude de l'ouvrage numérique et organise le transfert vers l'exploitation : indicateurs (KPI), engagements de qualité de service (SLA), maintenance et responsabilités d'exploitation. La Cellule assume enfin un rôle de garant de la soutenabilité : trajectoires budgétaires, obsolescence maîtrisée, feuille de route d'évolutivité et pilotage des retours d'expérience pour nourrir l'amélioration continue.

MA 4.1 – AMO SMART

Mise en place de l'AMO Smart dès la phase de programmation

Prérequis

L'AMO Smart conseille la maîtrise d'ouvrage pour cadrer l'ambition numérique, transformer des besoins d'usages en exigences mesurables et sécuriser la trajectoire de valeur, du programme jusqu'à la mise en service.

Il éclaire les choix à travers des études d'opportunité, des analyses de risques et de coûts complets, en proposant des scénarios d'allotissement et de gouvernance compatibles commande publique et feuille de route du SDI.

Il structure la gouvernance projet, assiste à la rédaction des pièces contractuelles (y compris lot numérique), conçoit les critères d'évaluation et prépare les grilles d'analyse multicritères intégrant ouverture, sécurité, réversibilité et commissioning.

Il organise la preuve de concept (POC) lorsque nécessaire, cadre les modalités de recette et garantit l'alignement entre exigences R2S4CARE, objectifs d'usage, contraintes d'exploitation et enveloppe budgétaire.

Il facilite la conduite du changement et la montée en compétences des équipes internes, anticipe les impacts organisationnels et veille à la soutenabilité des choix dans le temps.

Sa neutralité vis-à-vis des solutions, sa connaissance du marché et sa maîtrise des référentiels sectoriels constituent des gages d'objectivité au service de la décision

MA 4.2 – CSSN – COORDINATEUR DES SYSTÈMES ET SERVICES NUMÉRIQUES

Mise en place du CSSN dès la phase de conception

Prérequis

Le CSSN est l'« autorité de conception » numérique du projet : il traduit les cas d'usages et services numériques dans une architecture ouverte, interopérable et sécurisée, puis en garantit la cohérence des études à l'exploitation.

Il articule en continu SIH et SITH, définit les règles de gouvernance des données et de la sécurité, prescrit le modèle d'intégration en trois couches (services, convergence via BOS, OT/IT) et fixe les critères de performance et de réversibilité.

Il conduit les ateliers de co-conception avec les usagers, consolide les cas d'usage et leurs exigences de données, puis formalise le dossier d'architecture cible et les clauses techniques du lot numérique dans les pièces de marché.

Il coordonne les interfaces multi-lots, statue sur les dérogations techniques, organise le commissioning numérique (FAT/SAT) et contrôle la complétude du DOE avant la réception.

Il prépare le RUN en définissant KPI, SLA, consignes d'exploitation et modalités de mise à jour, puis anime les revues d'amélioration continue en lien avec la DSI, le biomédical et l'exploitation.

Sa posture est indépendante, orientée valeur d'usage et coût complet, avec un niveau d'expertise couvrant IT/OT, GTB/GTIE, interopérabilité (APIs et protocoles), cybersécurité et conformité.

MA 4.3 – MSI

Mise en place du MSI dès la phase d'exécution

Prérequis

Le MSI est le réalisateur de l'intégration technique : il met en œuvre, paramètre et raccorde l'ensemble des systèmes et services au sein de l'architecture cible, sous le pilotage du CSSN et dans le respect des pièces contractuelles.

Il configure la couche de convergence (BOS/middleware), développe et documente les connecteurs et APIs, normalise les modèles de données et sécurise les flux entre équipements OT, plateformes et applications métiers.

Il prépare et exécute les essais d'intégration, automatise les tests lorsque possible, apporte la preuve de performance et de conformité lors des FAT/SAT et traite les écarts jusqu'à obtention des critères d'acceptation.

Il documente et livre un DOE exploitable : schémas as built, dictionnaire de données, sources logiciels, cahier de développement et procédures d'exploitation, en garantissant la portabilité et l'évolutivité des composants intégrés.

Il coopère avec les titulaires des lots métiers pour assurer une intégration robuste, gère le versioning et les mises à jour, applique les bonnes pratiques de cybersécurité industrielle et prépare le passage en RUN sans rupture de service.

Son engagement porte sur la qualité d'intégration, la tenue des performances et la maintenabilité, avec une obligation de résultats sur les interfaces et une obligation de moyens sur les investigations techniques.

MA 5 – Qualité environnementale

La prise en compte des enjeux de Responsabilité Sociétale des Entreprises (RSE) et plus particulièrement de la qualité environnementale des projets immobiliers est intégrée dès la phase conception et à chaque étape du projet, afin de garantir une démarche responsable et durable.

Engager un projet immobilier dans un cadre RSE, est un volet stratégique, collectif et mesurable. Il part des besoins d'usage, intègre les enjeux environnementaux et sociaux dès le cadrage, puis pilote les résultats dans la durée.

MA 5.1 – DÉTERMINATION CHAMP MAGNÉTIQUE

Issue de la directive 2013/35/UE du Parlement européen et du Conseil du 26 juin 2013, une réglementation est entrée en vigueur le 1er janvier 2017 sous forme du décret n°2016-1074 du 3 août 2016 relatif à la protection des travailleurs contre les risques dus aux champs électromagnétiques.

Ce décret vise à définir les règles de prévention contre les risques pour la santé et la sécurité des travailleurs exposés aux champs électromagnétiques, notamment contreleurs effets biophysiques directs et leurs effets indirects connus.

La réglementation demande :

- L'évaluation des risques résultant de l'exposition des travailleurs à des champs électromagnétiques ;
- Des mesures et moyens de prévention si dépassements des seuils, comme notamment la mise en œuvre d'autres procédés de travail n'exposant pas aux champs électromagnétiques ou entraînant une exposition moindre
- Pour les espaces fréquentés par les patients et usagers de l'établissement, l'exposition est inférieure aux seuils fixés par la règlementation.

●★

Cartographie

Niveau 1 (Obligatoire)

Les équipements émetteurs et les zones mesurées sont cartographiés.

MA 5.2 – IMPACT ENVIRONNEMENTAL : LE NUMÉRIQUE RESPONSABLE

Les FDES

Les fiches environnementales demandées pour un projet immobilier sont en pratique les FDES (Fiches de Déclaration Environnementale et Sanitaire), qui constituent la carte d'identité environnementale et sanitaire des produits de construction.

- Elles permettent de calculer l'empreinte environnementale d'un bâtiment sur tout son cycle de vie, via l'analyse du cycle de vie (ACV).
- Elles aident le maître d'ouvrage et la maîtrise d'œuvre à choisir des produits plus sobres et à documenter la performance du projet.
- Elles sont particulièrement utiles pour les démarches bas carbones, les labels et les exigences de performance environnementale.

Le Digital Passport Product (DPP) en cours d'introduction dans la cadre règlementaire va se positionner de manière complémentaire à la FDES. La FDES sert surtout à mesurer l'impact environnemental d'un produit de construction, tandis que le DPP sert à fournir et partager des données produit tout au long du cycle de vie. Le DPP est un élément essentiel pour développer la traçabilité numérique des bâtiments.

La démarche numérique responsable

En complément de cette évaluation de l'impact environnemental du projet immobilier, l'établissement étudie l'impact de son projet numérique sur l'environnement ; c'est la démarche numérique responsable.

Le numérique responsable est une démarche d'amélioration continue qui vise à réduire l'empreinte écologique et sociale du numérique, tout en gardant des services utiles, accessibles et durables. Il consiste à concevoir et utiliser les technologies numériques de manière plus sobre, plus durable et plus inclusive, afin de limiter leurs impacts environnementaux et sociaux.

Pour évaluer l'impact environnemental d'un projet numérique dans une démarche de numérique responsable, il faut raisonner en cycle de vie et ne pas se limiter à la seule consommation électrique en phase d'exploitation.

Pour outiller la démarche, des ressources disponibles sont :

- Les publications de l'Arcep et de l'ADEME soulignent qu'une évaluation robuste doit suivre un cadre méthodologique explicite et comparable.
- Le standard UIT-T L.1450 est cité comme référence pour l'évaluation carbone des technologies numériques selon une approche cycle de vie.
- Des outils comme My Impact ou d'autres calculateurs permettent une première estimation, puis il faut affiner avec des données réelles du projet.

  https://myimpact.isit-europe.org/fr/

Le Digital Passport Product (DPP) en cours d'introduction dans la cadre règlementaire va se positionner de manière complémentaire à la FDES. La FDES sert surtout à mesurer l'impact environnemental d'un produit de construction, tandis que le DPP sert à fournir et partager des données produit tout au long du cycle de vie. Le DPP est un élément essentiel pour développer la traçabilité numérique des bâtiments.

●

La démarche numérique responsable est engagée dès la phase conception

Niveau 1

Il s'agit d'intégrer l'architecture du système, le choix des équipements et la connaissance associée à leur impact environnemental dès la phase conception.

La démarche consiste à disposer d'une connaissance exhaustive des données et à effectuer une comparaison entre différents produits, par exemple entre le produit A et le produit B, afin de justifier une optimisation environnementale sur le sujet.

●●

La démarche numérique responsable est appliquée au cycle de vie

Niveau 2

La démarche numérique responsable prévoit l'ajout d'une Analyse du Cycle de Vie (ACV) pour aller plus loin dans l'évaluation et la justification du choix des équipements.

MA 5.3 – EFFICIENCE ÉNERGÉTIQUE DU RÉSEAU « SMART », DES SERVICES ET SYSTÈMES NUMÉRIQUES

L'efficience énergétique du réseau « Smart », des systèmes et services numériques d'un Smart Hospital repose sur une architecture pilotée par la donnée : centraliser les informations, mesurer en continu, optimiser en temps réel et réduire les consommations inutiles.

La consommation électrique doit être prise en compte dans le choix des équipements du réseau « Smart », au même titre que les performances techniques, et ce, en adéquation avec le besoin à servir, les puissances consommées augmentant généralement avec le débit (par exemple Bluetooth versus Wi-Fi).

Les systèmes et services numériques apportent surtout de la visibilité et de l'orchestration : ils agrègent les données, détectent les anomalies et déclenchent des actions automatiques ou semi-automatiques. Ils peuvent aussi réduire l'empreinte énergétique indirecte grâce à une meilleure utilisation des ressources, à condition que l'infrastructure IT soit elle-même sobre et bien dimensionnée.

Identification des consommations électriques du réseau « Smart »

Niveau 1

La consommation électrique des équipements actifs du réseau « Smart » est mesurée de façon différenciée de toute autre consommation, et doit comprendre :

- la consommation des équipements actifs du réseau « Smart » : cœurs de réseau, routeurs, pare-feu, équipements d'interface avec les réseaux opérateurs de télécommunication, commutateurs, ainsi que les points d'accès WiFi (alimentés en PoE ou non) ;
- les consommations intrinsèques des alimentations externes des équipements actifs du réseau « Smart » (onduleurs, alimentations stabilisées, transformateurs de potentiel…). Lorsque ces alimentations sont communes à plusieurs systèmes, la part de consommation liée au réseau « Smart » peut être estimée.

Maîtrise des consommations du réseau « Smart »

Niveau 2

Annuellement et toutes choses étant égales par ailleurs, le projet doit définir des objectifs de consommation du réseau « Smart » en amélioration continue ou *a minima* maintenir la performance par rapport à l'année précédente. (Les projets qui n'ont qu'une année d'exploitation devront uniquement des objectifs de consommation).

Parmi les indicateurs utiles :

- La consommation par m² et par activité.
- La part des consommations critiques versus non critiques.
- Les pics de puissance et la flexibilité de charge.
- Le taux d'anomalies détectées et corrigées.
- Le coût énergétique par séjour, par acte ou par journée d'hospitalisation.

L'efficience énergétique du réseau « Smart » est abordée par l'ajout de la consommation électrique des équipements. Il convient également de prendre en compte les effets dérivés du réseau « Smart », notamment le poids du traitement d'air et du refroidissement qui doivent être intégrés dans l'analyse. Par ailleurs, la récupération d'énergie, telle que

l'utilisation d'une chaudière numérique ou la mise en place d'une boucle d'énergie fatale produite par le smart, constitue un levier supplémentaire d'optimisation énergétique.

MA 5.4 – IMPACT ENVIRONNEMENTAL DU CLOUD

L'utilisation du cloud et plus généralement des services numériques externalisés dans le Smart Hospital soulève la question de l'impact carbone induit par la donnée et son traitement dans des data center tiers.

L'impact environnemental du cloud est réel et vient surtout de la consommation d'électricité, du refroidissement des data centers et de l'usage d'eau associé. À grande échelle, il peut aussi peser sur les émissions de CO_2, la pression sur le réseau électrique et, selon les régions, sur la disponibilité en eau.

En pratique, le cloud peut être plus sobre qu'une infrastructure locale mal gérée, mais il n'est pas automatiquement vert. Son impact dépend surtout de la conception technique, du niveau d'optimisation des usages et du mix énergétique des data centers

L'IA et ce qui aggrave l'empreinte

La croissance rapide de l'IA et des usages intensifs du cloud augmente la demande en capacité de calcul, donc en énergie et en refroidissement. Les charges mal optimisées, le surdimensionnement et une faible utilisation des serveurs dégradent aussi l'efficience environnementale. Dans certaines zones, la concentration de data centers peut créer des tensions locales sur l'électricité et l'eau.

Leviers de réduction

Les principaux leviers sont le recours aux énergies bas carbone, l'amélioration du taux d'utilisation des serveurs, la virtualisation, et des systèmes de refroidissement plus efficaces.

Le déplacement des charges vers des régions mieux alimentées en électricité bas carbone peut réduire l'empreinte, à condition de ne pas transférer le problème vers l'eau ou le réseau électrique local. Les fournisseurs cloud publient aussi des outils de mesure et des tableaux de bord pour suivre les émissions liées à l'usage de leurs services.

La démarche « Numérique Responsable » est appliquée dans la sélection des services externalisés

Niveau unique

Pour être appliquée à la sélection des services externalisés, la démarche « Numérique Responsable » doit être traduite en critères d'achat concrets dans le cahier des charges et dans l'évaluation des offres. En pratique, le numérique responsable sert ici à arbitrer entre performance, sobriété, accessibilité, sécurité et coût global.

La sélection ne porte plus seulement sur le prix ou la fonctionnalité, mais aussi sur l'empreinte environnementale du service, son niveau d'écoconception, la consommation de ressources et la durée de vie d'usage.

Dans les offres externalisées, cela concerne par exemple le cloud, l'hébergement, la maintenance applicative, la visioconférence ou les services d'IA.

Services

LE SMART HOSPITAL EST UN ÉCOSYSTÈME OUVERT, INTEROPÉRABLE ET SÉCURISÉ.

En l'espace d'une génération, le numérique est devenu un moteur central du développement économique et un puissant levier de transformation de la vie quotidienne. Cette évolution, aujourd'hui accélérée par l'intelligence artificielle (IA), agit sur les objets, les espaces, les usages et les modes de fonctionnement des organisations.

Les bâtiments, et tout particulièrement les bâtiments hospitaliers, sont directement impactés par cette transformation. Le numérique permet l'émergence de nouveaux objets connectés, de services innovants et de nouveaux usages, offrant des capacités d'interaction accrues entre les usagers, les systèmes techniques et l'environnement dans lequel s'inscrit l'hôpital.

Le Smart Hospital est un bâtiment communicant et connecté, conçu comme une plateforme de services numériques riche, évolutive et interopérable, disposant des moyens techniques et organisationnels pour assurer :

- des communications performantes pour les personnels hospitaliers et les usagers ;
- une connectivité fiable et résiliente avec les réseaux opérateurs
- l'interopérabilité des systèmes, historiquement cloisonnés, grâce à des standards de communication communs ;
- l'hébergement et le déploiement de services numériques facilitant l'adaptation de l'hôpital à l'évolution de ses activités ;
- l'interaction avec son environnement, afin de s'inscrire progressivement dans une démarche de ville intelligente et durable.

Le Smart Hospital est un écosystème ouvert, interopérable et sécurisé.

Cet écosystème s'inscrit pleinement dans la stratégie numérique globale de l'hôpital dans le projet d'établissement, le schéma directeur immobilier et le schéma directeur des systèmes d'information. Il s'appuie sur :

- des référentiels partagés,
- des bonnes pratiques communes,
- une politique de cybersécurité cohérente et maîtrisée.

Il constitue un vecteur de services présents et futurs, au service des patients, des professionnels et du territoire.

LES SERVICES NUMÉRIQUES

Le Smart Hospital s'appuie sur le numérique, les données et l'automatisation pour :

- accompagner la transition énergétique
- optimiser l'exploitation et la maintenance des actifs immobiliers
- proposer plus de confort aux usagers,
- améliorer l'efficacité du travail de l'ensemble des professionnels,
- favoriser le lien social et l'ancrage territorial.

Un service numérique est un service rendu grâce à des ressources logicielles, matérielles, réseau et humaines qui permettent à des utilisateurs de générer, traiter, stocker, échanger ou consulter des données numériques. C'est un service qui apporte de la valeur à son utilisateur et à l'établissement.

Au fil des évolutions technologiques et de l'évolution des bonnes pratiques, la liste des services numériques va s'allonger en même temps que l'écosystème va se développer. Ils constituent un ensemble évolutif qui a amené les rédacteurs du R2S for Care à considérer la documentation complète des services du Smart Hospital comme des annexes au cadre de référence R2S for Care.

Pour faciliter la compréhension et l'appropriation des service, les annexes sont rédigées sur une trame commune en trois parties :

1. Le besoin :
Quel est le problème à résoudre ?

2. La/les solution(s) :
La description du service (matériels, logiciels, services, compétences)

3. La valeur :
Les bénéfices (dont le ROI) pour les utilisateurs et l'établissement.

Ces annexes et les autres sont mises à disposition sur le site internet de la Smart Building Alliance. Elles pourront être actualisées.

1

Services
Annexe SE 2

Services énergétiques

LE BESOIN

La gestion des énergies est un besoin central dans le Smart Hospital, parce que l'hôpital fonctionne 24h/24, 7j/7, avec des usages très différents et des équipements fortement consommateurs d'énergie. Elle vise à mesurer, piloter et optimiser les consommations sans dégrader la qualité des soins, le confort ni la sécurité.

Les besoins portent sur :
— le suivi fin des consommations (par bâtiments, zones et usages),
— la détection rapide des dérives et des anomalies,
— le pilotage coordonné des installations (CVC, éclairage, ECS, réseaux, production) en intégrant les contraintes sanitaires et le confort,
— la qualité et la résilience des alimentations (priorisation des charges, modes dégradés),
— la production des indicateurs (kWh, coûts, CO_2)
— l'appui aux démarches de sobriété et d'amélioration continue.

Dans un hôpital, la maîtrise des énergies est un enjeu critique de continuité de service, de sécurité, de performance environnementale et de conformité réglementaire avec :

— le Décret Tertiaire du 23 juillet 2019
— le Décret BACS du 7 avril 2023

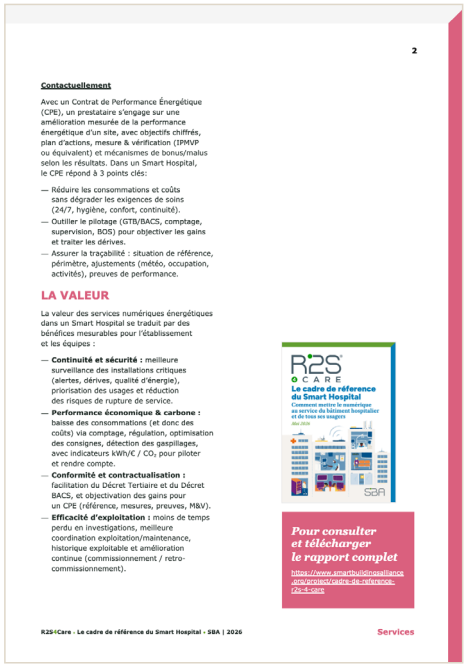
LES SOLUTIONS

Techniquement

Pour un Smart Hospital, les solutions pour une gestion optimale des énergies et une conformité aux décrets « Tertiaire » et BACS:

— GTB (Gestion Technique du Bâtiment) pour piloter les installations techniques du bâtiment et peuvent contribuer à un gain rapide d'énergie à un coût raisonnable.
— Capteurs et comptage énergétique par zone, usage ou équipement pour mesurer précisément les consommations et détecter les dérives.
— Interopérabilité des équipements via des protocoles compatibles BACS, afin d'intégrer les installations existantes sans tout remplacer.
— Supervision et alarmes pour suivre les dépassements, les anomalies et les indisponibilités techniques.
— Analyse de données / IA / SaaS pour optimiser les consignes, anticiper les usages et améliorer le performance dans la durée.

R2S4Care - Le cadre de référence du Smart Hospital - SBA | 2026 Services



2

Contactuellement

Avec un Contrat de Performance Énergétique (CPE), un prestataire s'engage sur une amélioration mesurée de la performance énergétique d'un site, avec objectifs chiffrés, plan d'actions, mesure & vérification (IPMVP ou équivalent) et mécanismes de bonus/malus selon les résultats. Dans un Smart Hospital, le CPE répond à 3 points clés:

— Réduire les consommations et coûts sans dégrader les exigences de soins (24/7, hygiène, confort, continuité).
— Outiller le pilotage (GTB/BACS, comptage, supervision, BOS) pour objectiver les gains et traiter les dérives.
— Assurer la traçabilité : situation de référence, périmètre, ajustements (météo, occupation, activités), preuves de performance.

LA VALEUR

La valeur des services numériques énergétiques dans un Smart Hospital se traduit par des bénéfices mesurables pour l'établissement et les équipes :

— **Continuité et sécurité :** meilleure surveillance des installations critiques (alertes, dérives, qualité d'énergie), priorisation des usages et réduction des risques de rupture de service.
— **Performance économique & carbone :** baisse des consommations (et donc des coûts) via comptage, régulation, optimisation des consignes, détection des gaspillages, avec indicateurs kWh/€ / CO_2 pour piloter et rendre compte.
— **Conformité et contractualisation :** facilitation du Décret Tertiaire et du Décret BACS, et objectivation des gains pour un CPE (référence, mesures, preuves, M&V).
— **Efficacité d'exploitation :** moins de temps perdu en investigations, meilleure coordination exploitation/maintenance, historique exploitable et amélioration continue (commissionnement / retro-commissionnement).

Pour consulter et télécharger le rapport complet
https://www.smartbuildingsalliance.org/project/cadre-de-reference-r2s-4-care

R2S4Care - Le cadre de référence du Smart Hospital - SBA | 2026 Services

Pour consulter et télécharger les annexes

https://www.smartbuildingsalliance.org/project/cadre-de-reference-r2s-4-care

Acronymes

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
APD	Avant-Projet Détaillé
APS	Avant-Projet Simplifié
API	Application Programming Interface
BACnet	Building Automation and Control NETWork
BOS	Building Operating System
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
IOT	Internet Of Things (Internet des Objets)
ITIL	Information Technology Infrastructure Library
NIS2	Network and Information Security Version 2
PCA	Plan de Continuité d'activité
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information en Santé
PRA	Plan de reprise d'activité
PTD	Programme Technique détaillé
RGPD	Règlement Général pour la Protection des Données
RSSI	Responsable de la Sécurité des Systèmes d'Information
SIEM	Sécurity Information and Event Management
SIH	Système d'Information Technique and Event Management
SITH	Système d'Information Technique Hospitalier
SMSI	Système de Management de la Sécurité de l'Information
VLAN	Virtual Local Area Network

Glossaire

API

Une API (Application Programming Interface) est un ensemble défini de classes, de méthodes ou de fonctions en Web Service par laquelle un logiciel offre des services à d'autres logiciels, sans que l'un connaisse le fonctionnement interne de l'autre. Certaines API sont normalisées (par exemple HL7), d'autres sont propriétaires et documentées.

API Centrale

Une API Centrale permet d'interfacer le bâtiment avec l'ensemble des équipements terrain du bâtiment qui communiquent en interfaces protocolaires ou en API terrain et expose des données contextualisées pour alimenter des services.

API Terrain

Une API Terrain permet d'interfacer les équipements de terrain (capteurs, actionneurs, passerelles et/ou automates terrain ...) à travers une interface de programmation ouverte en web service.

Building Information Modeling (BIM)

Le BIM ou maquette numérique est un format de description unifié d'un bâtiment ou d'un ouvrage bâti, stockée dans une base données structurée localement ou sur le Cloud, comprenant toute l'information technique nécessaire à sa conception, sa construction, son entretien, ses réparations, ses modifications, sa déconstruction, son ré-usage ou son recyclage. Dans sa version active, les données des écosystèmes communicants sont liées dynamiquement au BIM, faisant en sorte que le BIM contribue au jumeau numérique (Digital Twin) du bâtiment physique, en étant réactualisé en temps réel

Building Operating System (BOS)

Le Building Operating System (BOS) est le cœur du système d'information technique hospitalier (SITH). Le BOS constitue la fondation digitale du bâtiment et assure la gouvernance des données. Il est constitué d'un logiciel ou un ensemble de logiciels « cœur de plateforme » (middleware) et « building centric », qui organise, gère et partage le référentiel commun du bâtiment et met en œuvre les règles du contrat de gouvernance des données partagées. Pour en savoir plus, voir le livre blanc de la SBA « Le SITH & le BOS sont les outils de la gouvernance des données du bâtiment ».

Câblage du réseau « Smart »

C'est le câblage unique rassemblant toutes les liaisons physiques des systèmes de communication des services intégrés au bâtiment.

Cartographie du réseau

Une cartographie d'un réseau informatique est une représentation de ce réseau pouvant intégrer différents éléments comme les équipements actifs du réseau, les équipements qui y sont connectés, les logiciels installés et leurs versions, les processus, les flux entre ces dispositifs, les liens avec les réseaux tiers comme Internet. Cette représentation peut distinguer l'infrastructure de la partie applicative.

La cartographie permet d'inventorier les constituants du réseau avec pour objectif d'en avoir une meilleure maîtrise. Cette maîtrise permet d'améliorer la sécurité numérique du réseau et de rationaliser son administration. La cartographie peut être réalisée manuellement ou à l'aide d'outils logiciels spécialisés.

Équipement

Un équipement est défini comme étant un objet connectable au réseau « Smart ».

Équipement actif
Les équipements actifs d'un réseau informatique sont les briques constitutives des réseaux informatiques physiques. Ils ont pour objectif de faire dialoguer plusieurs sous réseaux initialement isolés, par l'intermédiaire de périphériques spécifiques. Au sens du cadre de référence R2S, les équipements actifs du réseau « Smart » comprennent les équipements actifs centraux du réseau « Smart » et les switchs du réseau « Smart » comprenant les switchs d'accès

Équipement actif central
Équipement central du réseau local, présentant un haut-débit de commutation, en charge du pilotage de la résilience réseau et des routages entre les réseaux locaux virtuels.

Au sens du cadre de référence R2S, les équipements actifs centraux du réseau « Smart » comprennent les cœurs de réseau, routeurs, pare-feu et les équipements d'interface avec les réseaux opérateurs de télécommunications

Équipement réseau d'accès
Équipement du réseau local exploité pour connecter les terminaux Ethernet-IP des systèmes de communications.

Équipement réseau de cœur
Équipement central du réseau local, présentant un haut-débit de commutation, en charge du pilotage de la résilience réseau et des routages entre les réseaux locaux virtuels.

Équipement terminal
Dans le domaine des télécommunications, un équipement terminal est un équipement situé en extrémité d'un réseau, il est capable de communiquer sur ce réseau et parfois d'assurer l'interface avec l'utilisateur. Exemples : ordinateur, capteur, actionneur, caméra…

Infrastructure de géolocalisation

Infrastructure assurant - ou permettant - de réaliser une localisation dans l'espace d'un bâtiment, un objet ou de façon indirecte un utilisateur.

Interopérabilité

Capacité d'un produit ou d'un système à fonctionner avec d'autres produits ou systèmes existants ou futurs, sans restriction d'accès ou de mise en œuvre et dont les interfaces sont intégralement connues.

Contrairement au concept de « compatibilité » qui est une notion verticale qui fait qu'un outil peut fonctionner dans un environnement donné en respectant des normes, l'interopérabilité est une notion transversale à plusieurs systèmes qui suppose que toutes les Interfaces (API) sont connues.

IoT

L'Internet of Things (IoT) ou l'Internet des objets (IdO) est l'interconnexion entre l'Internet et des objets, des lieux et des environnements physiques.

Jumeau numérique (ou Digital Twin)

Maquette numérique dynamique. Intègre la description physique du bâtiment (BIM) mais aussi les données numériques de son comportement en temps réel.

Ontologie

Ce terme désigne la structuration mise en place pour l'exposition, la mise à disposition des données fournies par le réseau "smart". Cette architecture permet de présenter les informations collectées suivant la sémantique de lecture de ces données. Le terme structuration désigne l'organisation, la catégorisation, la métrique et le type de classe de la donnée ou de l'API considérée.

Qualité de Services (QoS)

Ensemble d'indicateurs et de mécanismes définissant et garantissant le niveau de service attendu (SLA) :

- Sur le réseau « Smart »
- Sur les interfaces
- Sur les applications

Dans le contexte de l'architecture réseau, comprend par exemple la fonctionnalité permettant de prioriser ou de ralentir l'acheminement sur un réseau de certains trafics par rapport à d'autres. L'objectif peut être de privilégier la téléphonie et la qualité de la communication par rapport à l'acheminement d'un e-mail ou d'un fichier.

Réseau « Smart »

Le « réseau « Smart » » est le réseau fédérateur d'un bâtiment R2S orienté services (SOA) et utilisant le protocole IP. Il est sécurisé et utilise exclusivement le standard Ethernet sur le réseau local et le standard Internet depuis l'extérieur du bâtiment. Les écosystèmes matériels, quel que soit leur protocole, communiquent sur le « réseau « Smart » », à l'aide d'API ou de Web Services exposées sur le « réseau « Smart » » et sur le World Wide Web. Ce périmètre ne peut pas être réduit à un réseau logique (ex : VLAN GTB), mais doit comprendre le réseau physique dans son entièreté.

Réseau étendu WAN (Wide Area Network)

Un réseau WAN est un réseau étendu qui relie plusieurs réseaux locaux sur une grande distance, par exemple entre plusieurs sites d'un hôpital, des villes, des pays, ou à l'échelle mondiale. Il sert à interconnecter des services de soins, des datacenters, des applications cloud et d'autres infrastructures distantes.

LAN
réseau local, limité à un bâtiment ou un site.

WAN
réseau grande distance, qui relie plusieurs LAN entre eux.

Réseau local LAN (Local Area Network)

Un réseau LAN est un réseau local qui relie des appareils dans une zone géographique limitée, comme un service, un bâtiment hospitalier ou un campus.

Définition simple

Le LAN permet à des ordinateurs, imprimantes, serveurs ou autres équipements de communiquer entre eux et de partager des ressources, parfois avec un accès Internet commun. Il peut être câblé en Ethernet ou fonctionner en Wi-Fi.

Réseau local virtuel VLAN (Virtual Local Area Network)

Fonction permettant d'isoler différentes parties d'un réseau les unes des autres. Normalisée par l'IEEE 802.1q, elle permet d'identifier le réseau auquel appartient une trame Ethernet par un marquage (tagging) de son en-tête.

Résilience

Appliquée au réseau, il s'agit d'une fonction permettant de détecter la panne d'une liaison ou d'un équipement, et d'activer automatiquement un processus de recalcul de route (contournement), afin d'assurer la continuité de service du réseau malgré les défaillances rencontrées.

Serveur DHCP (Dynamic Host Control Protocol)

Fonction permettant l'attribution dynamique d'une adresse IP parmi celles disponibles sur le plan d'adressage, à un terminal lors de son ouverture de session ou lors du renouvellement du bail de son adresse. Un serveur DHCP permet également d'obtenir les adresses IP de services présents sur le réseau (DNS, NTP...). Cette fonction évite les pannes causées par des doublons d'adresses pouvant apparaître lors de la mise en œuvre d'un adressage statique, directement paramétré sur les équipements terminaux.

Serveur DNS (Domain Name Server)

Fonction permettant d'obtenir l'adresse IP qui correspond à un nom de domaine. Cette fonction est utile par exemple pour accéder à un service sans avoir besoin de spécifier son adresse. Le service peut alors changer d'adresse sans préjudice pour l'accès. Ce service peut être hébergé sur un serveur local ou sur le cloud ou peut être opéré.

Service Level Agreement (SLA)

Le Service Level Agreement, ou SLA est un contrat par lequel un prestataire informatique s'engage à fournir un ensemble de services à un client. Autrement dit, il s'agit d'une clause contractuelle qui définit les objectifs précis et le niveau de service qu'est en droit d'attendre un client de la part du prestataire.

Système d'information hospitalier (SIH)

C'est l'ensemble organisé des applications, données, règles et échanges qui permettent de gérer le fonctionnement d'un établissement de santé, notamment les informations administratives, cliniques, logistiques et financières. Il inclut le SITH.

Le SIH sert à collecter, stocker, traiter et diffuser les informations utiles aux soignants, aux services administratifs et à la direction. En pratique, il soutient la prise en charge du patient, la coordination des équipes et le pilotage de l'hôpital.

Service d'Information Technique Hospitalier (SITH)

C'est l'ensemble des composants numériques appliqués à un bâtiment ou actif immobilier : logiciels, systèmes et capteurs connectés (OT), réseaux, applications et bases de données (dont font partie les maquettes numériques) relatifs à l'usage de l'ouvrage.

Il assure les mécanismes d'interopérabilité, de fiabilité et de consolidation des données générés par ces équipements et permet une gouvernance de données, adaptable à l'ensemble du cycle de vie d'un ouvrage.

Il fait du bâtiment hospitalier, une plateforme de services numériques au service de ses usagers.

Switch

Un switch (ou commutateur réseau en français) est un équipement réseau qui permet de relier d'autres équipements au sein d'un réseau LAN. Au sens du cadre de référence R2S, les switchs du réseau « smart » comprennent tous les switchs Ethernet (de cœur, de distribution et d'accès).

Switch d'accès

Équipement du réseau local exploité pour connecter les terminaux Ethernet-IP des systèmes de communications. Cela inclut les éventuels switchs terminaux qui peuvent être installés à proximité des équipements. Le référentiel n'est pas prescriptif concernant la mise en cascade de switchs d'accès sous réserve du respect des exigences qui s'y rapportent. Lorsque qu'un switch de cœur est utilisé pour connecter des terminaux, les exigences qui concernent les switchs d'accès doivent également leur être appliquées.

Les switchs d'accès sont ceux qui sont exploités pour connecter les terminaux. Cela inclut les éventuels switchs terminaux qui peuvent être installés à proximité des équipements (exemples : armoire électrique CVC, coffret de contrôle d'accès).

Smart Buildings Alliance

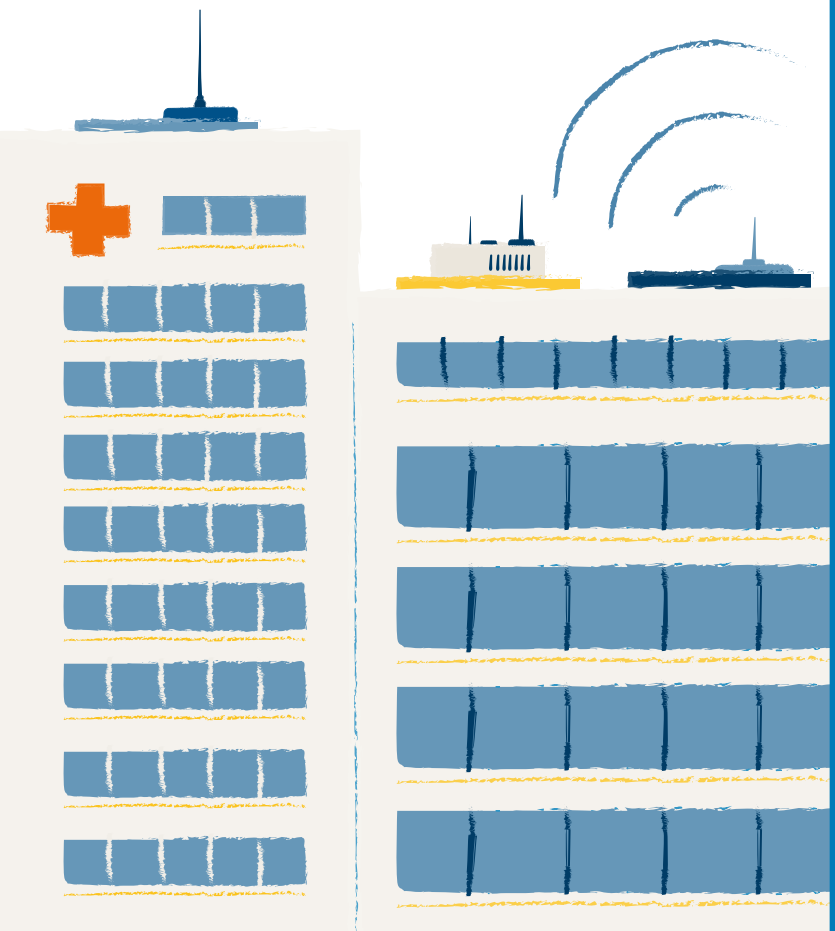
15 rue des Halles
75001 PARIS

06 69 65 14 98

www.smartbuildingsalliance.org • Linkedin • secretariat@smartbuildingsalliance.org /
communication@smartbuildingsalliance.org

R2S®

4 CARE



SBA