SBA
SMART BUILDINGS ALLIANCE
FOR SMART CITIES

R2S®
4 CARE

LE CADRE DE RÉFÉRENCE DU SMART HOSPITAL

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

Version 1, novembre 2022

À propos de la commission Smart Hospital de la SBA

Les démarches de numérisation de l'hôpital sont très souvent centrées sur le dossier patient et la production de soins. Mais, elles exploitent encore trop peu le potentiel de la mutualisation des usages et des interactions avec les données produites par le bâtiment, qui abrite l'activité hospitalière.

De l'idée stratégique d'un hôpital numérique ou digital, ne restent alors bien souvent que des modèles de conception qui sont répétés faute d'accompagnement, de compréhension ou d'outils pour libérer les transversalités. Celles-ci sont pourtant aujourd'hui un important levier pour atteindre les objectifs d'efficience et de diminution des coûts. Elles deviennent aussi nécessaires considérant les évolutions de notre système de santé et de notre société.

C'est de ce constat qu'est née la commission Smart Hospital 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.

Fidèle à l'ADN de la SBA, cette commission est constituée d'une cinquantaine d'experts, tous acteurs de l'écosystème de la construction hospitalière : maîtres d'ouvrage, assistants à la maîtrise d'ouvrage, conseils, ingénieurs, architectes, installateurs et intégrateurs, fabricants, éditeurs, associations. Son ambition est d'aider les hôpitaux et les établissements de soins à atteindre leurs objectifs, grâce à une approche innovante du 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.

Remerciements

La Smart Buildings Alliance (SBA) 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 Éric 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 Marie-Paule Dayer (ABB robotics), Jérémy Dréan (Artélia) et Christophe Clément-Cottuz (C Cube Expertise), coprésidents de la commission Smart Hospital, qui animent ce groupe de travail depuis plusieurs années.

Nous remercions également Alain Kergoat, directeur des Programmes de la SBA pour sa contribution, ainsi que tous les acteurs de l'écosystème hospitalier avec qui nous avons pu échanger et faire grandir notre vision du Smart Hospital.

Direction de la publication : Lidia Zerrouki
Direction éditoriale : Marie-Paule Dayer, Jérémy Dréan et Christophe Clément-Cottuz
Direction des programmes : Alain Kergoat
Direction marketing et communication : Pierre-Marie Pacaud
Conception graphique et illustrations © Les 5 sur 5
Dépôt légal : janvier 2023. ISBN 978-2-491340-21-6 © SBA

Qu'est-ce que le cadre de référence R2S 4CARE ?

Le présent document constitue le cadre de référence R2S 4 CARE (ou Ready2Services for Care). Un cadre de référence est constitué de **principes déclinés en recommandations**. Il propose une vision structurante, **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.

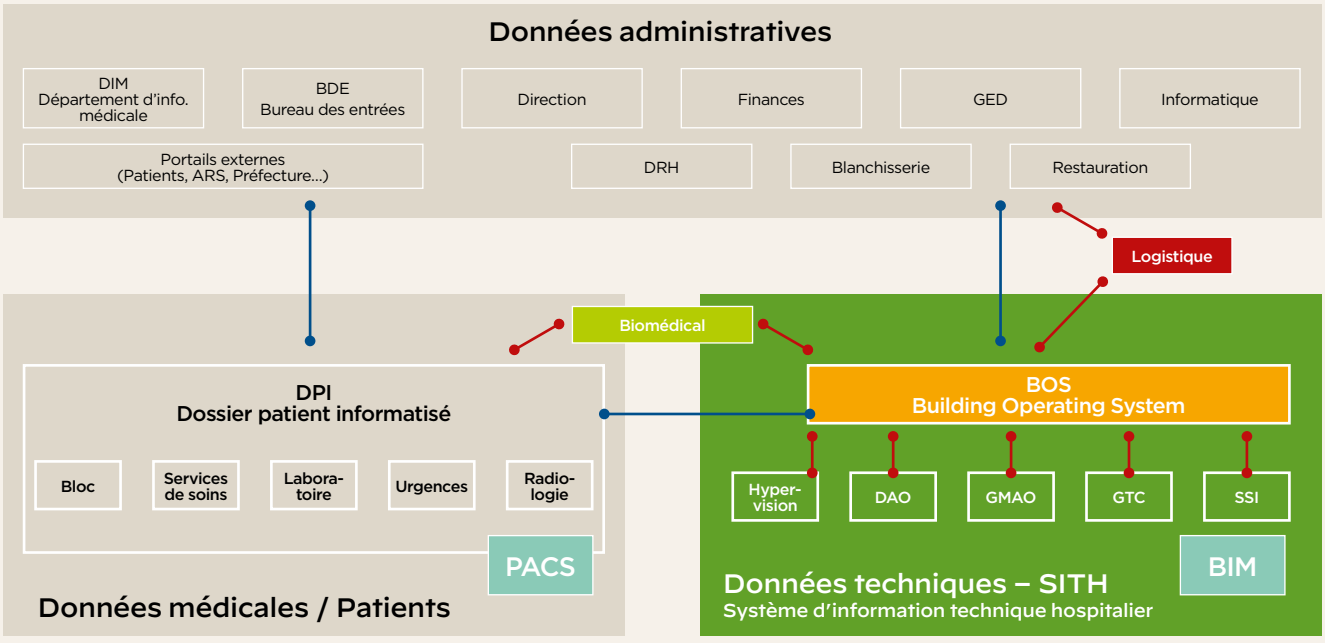
QUELS SONT LES OBJECTIFS DE CE CADRE DE RÉFÉRENCE ?

- 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 l'interopérabilité entre applications et services** de natures hétérogènes (provenant de fournisseurs et de silos métiers différents).
- Accompagner les réflexions sur la **gouvernance et le management des données**.
- Déterminer un socle sur lequel pourront s'appuyer tous les acteurs concepteurs du projet, et ceux qui proposent des services aux usagers **d'un bâtiment hospitalier, de confort, de sécurité, de performance**.
- 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.

Le cadre de référence R2S 4CARE ne traite pas :

- du déploiement des applications du SIH ;
- des services numériques minimum usuels attendus dans un établissement hospitalier ;
- de l'organisation des compétences à déployer.

PÉRIMÈTRE TECHNIQUE COUVERT PAR LE CADRE DE RÉFÉRENCE



Le SITH au cœur du SIH (Système d'information hospitalier).

INTRODUCTION

Le numérique au service du bâtiment hospitalier et de ses usagers . . . 7

CONNECTIVITÉ . . . 11

CO 1 – Raccordement aux réseaux externes du bâtiment . . . 14

CO 2 – Connectivité aux réseaux filaires . . . 16

CO 3 – Connectivité aux réseaux sans fil . . . 17

CO 4 – Exploitabilité et évolutivité du câblage . . . 18

CO 5 – Redondance et sécurisation du câblage . . . 20

CO 6 – Rafraîchissement des locaux techniques . . . 22

ARCHITECTURE RÉSEAU . . . 23

RE 1 – Réseau Smart et réseaux des usagers . . . 26

RE 2 – Continuité et protection fonctionnelle du réseau Smart . . . 28

RE 3 – Management du réseau Smart . . . 29

ÉQUIPEMENTS ET INTERFACES . . . 31

IN 1 – Interfaces de communication . . . 33

IN 2 – API terrain et API centrale . . . 36

IN 3 – Interfaces terrain . . . 38

IN 4 – API centrale . . . 40

IN 5 – Building Information Modeling (BIM) . . . 41

SÉCURITÉ NUMÉRIQUE . . . 42

SE 1 – Système de management de la sécurité informatique . . . 45

SE 2 – Sécurité des réseaux et systèmes du bâtiment . . . 46

SE 3 – Procédure de sécurité réseau . . . 49

SE 4 – Sécurité d'accès aux services . . . 50

SE 5 – Protection des données . . . 51

SE 6 – Sécurité d'accès aux services . . . 52

SE 7 – Protection des données . . . 53

MANAGEMENT RESPONSABLE 54

MA 1 – Gouvernance du projet 57

MA 2 – Propriété immobilière et responsabilités 59

MA 3 – Cadre de contractualisation des services 60

MA 4 – Qualités environnementales 61

MA 5 – Système de management 63

SERVICES 64

SE 1 – Services énergétiques 66

SE 2 – Pilotage de la performance du bâtiment 67

SE 3 – Services de géolocalisation 68

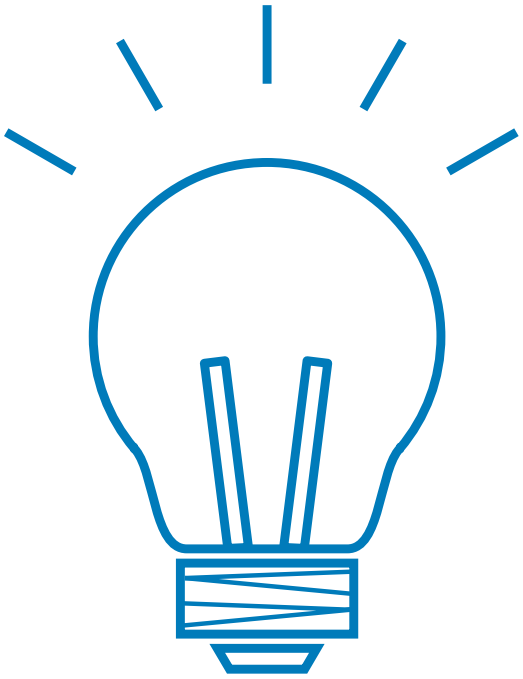
SE 4 – Bâtiment connecté et communicant pour les usagers 69

SE 5 – Mesure, gestion et optimisation de l'utilisation et de la réaffectation des espaces du bâtiment 70

SE 6 – Bâtiment connecté, à son territoire, à la Smart City 71

GLOSSAIRE 72

ANNEXE 81



INTRODUCTION

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. 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 une connexion Internet optimale;
- répondre 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;
- utiliser les outils numériques les plus adaptés en matière de construction et d'exploitation;
- 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 attentes.

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. L'interopérabilité des Systèmes d'information hospitalier (SIH) se développe, et se structure, notamment par la feuille de route numérique de l'initiative «Ma santé 2022» portée par l'Agence du numérique en santé.

La démarche R2S 4CARE

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**: programmation, conception, construction, exploitation, maintenance, renouvellement,-déconstruction et recyclage, valorisation ou cession.

Que ce soit dans le cadre d'un projet de développement **neuf**, d'une opération de **rénovation**, ou de **l'enrichisse-**

ment 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 R2S 4CARE, 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.

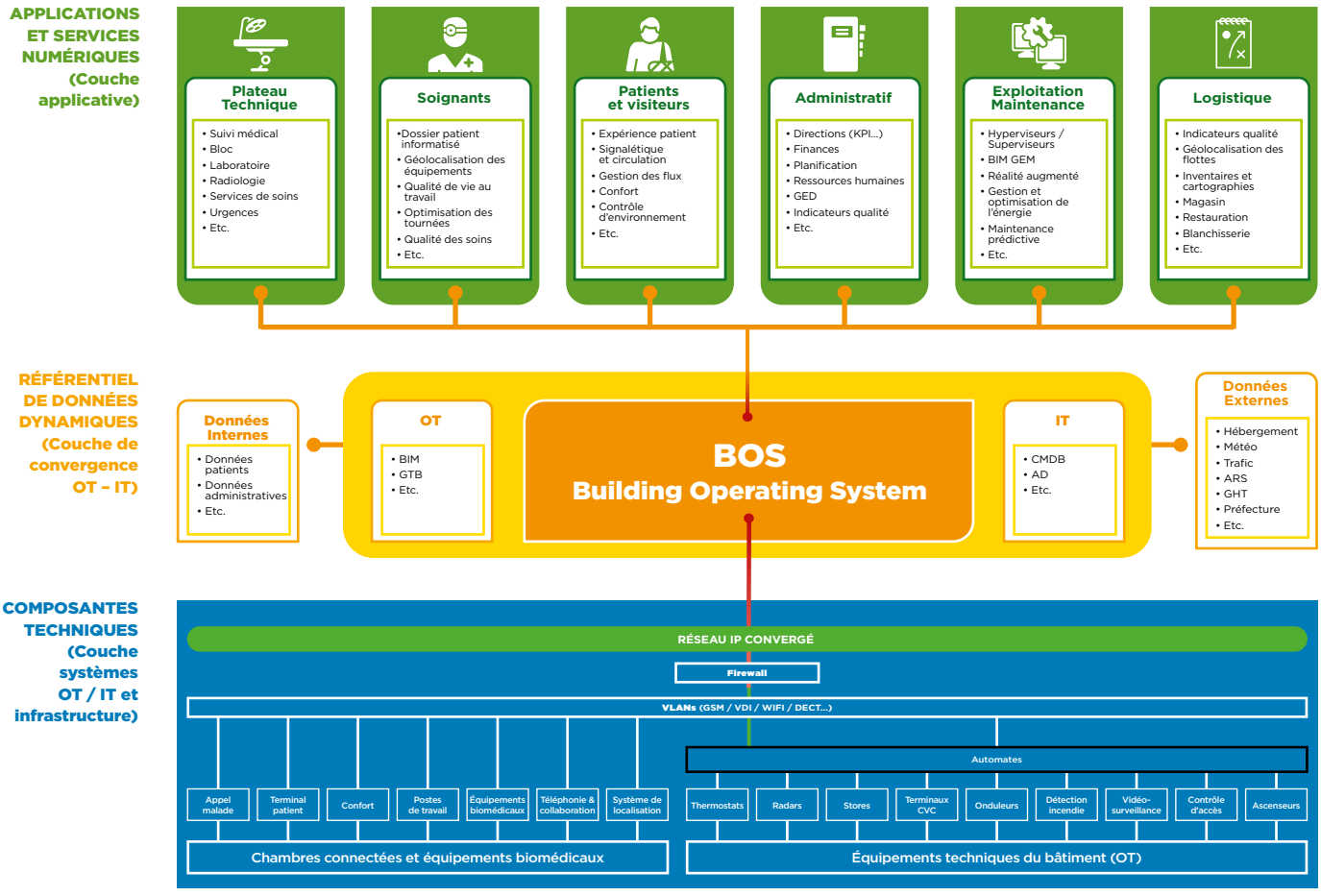
LES PRINCIPES CLÉS DE LA DÉMARCHE R2S 4CARE

L'approche R2S 4CARE 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). Le modèle R2S 4CARE 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'approche R2S 4CARE 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'ARCHITECTURE DU SITH
SYSTÈME D'INFORMATION TECHNIQUE HOSPITALIER



LES MOYENS TECHNIQUES ET ORGANISATIONNELS DE LA DÉMARCHE R2S 4CARE

R2S 4CARE 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 :

➔ **3 thèmes relatifs aux principes techniques**

CONNECTIVITÉ

Assurer une connectivité performante du bâtiment via un raccordement optimal aux réseaux de communication.

ARCHITECTURE RÉSEAU

Assurer la circulation des données à l'intérieur et à l'extérieur du bâtiment en améliorant les caractéristiques des réseaux du bâtiment.

ÉQUIPEMENTS ET INTERFACES

Mettre en relation les équipements, le réseau et les services grâce à leur interopérabilité.

➔ **2 thèmes relatifs à la gouvernance**

SÉCURITÉ NUMÉRIQUE

Sécuriser les systèmes, les interfaces et mettre en place un dispositif permettant la protection des données à caractère personnel dans le respect de la PGSSI-S et de la directive NIS2 et du RGPD.

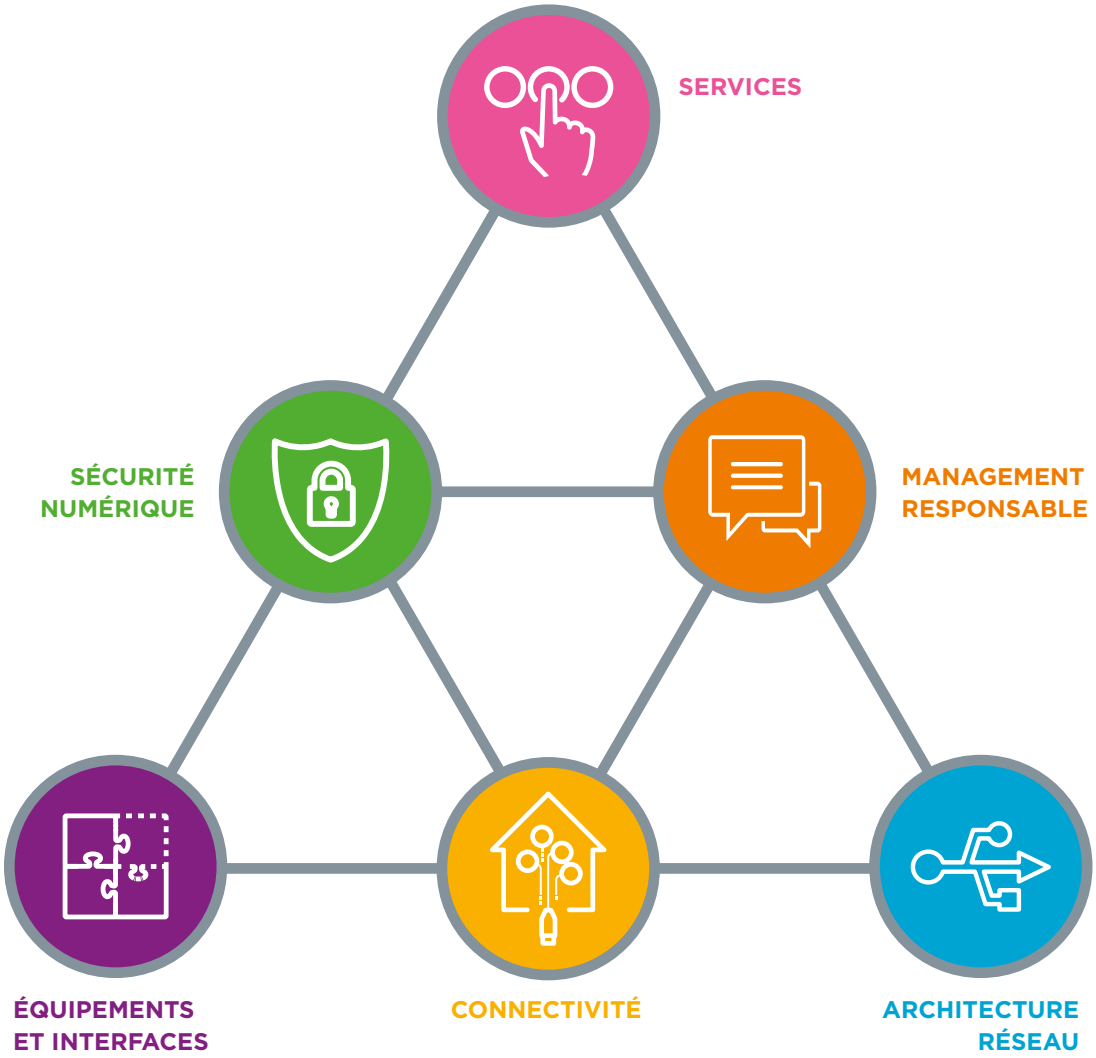
MANAGEMENT RESPONSABLE

Optimiser la gestion de projet, le commissionnement, mettre en place un cadre de contractualisation et s'entourer d'acteurs compétents.

➔ **1 thème relatif aux occupants et au bâtiment** :

SERVICES

Utiliser la capacité de connectivité et de communication du bâtiment pour le développement de services.



Les thèmes regroupent les sous-thèmes suivants :

CONNECTIVITÉ	ARCHITECTURE RÉSEAU	ÉQUIPEMENTS ET INTERFACES	SÉCURITÉ NUMÉRIQUE	MANAGEMENT RESPONSABLE	SERVICES
Raccordement aux réseaux externes du bâtiment	Caractéristiques et alimentation du réseau Smart	Équipements	Sécurité du réseau Smart et des systèmes du bâtiment	Gouvernance du projet	Pilotage énergétique du bâtiment
Connectivité aux réseaux filiaires	Continuité et protection fonctionnelle du réseau Smart	API terrain et centrale	Procédure de sécurité réseau	Propriété immobilière	Pilotage technique du bâtiment
Connectivité aux réseaux sans fil	Management du réseau Smart	Interfaces terrain	Sécurité d'accès aux services	Cadre de contractualistion des services	Géolocalisation
Exploitabilité et évolutivité du câblage		API centrale	Management de la sécurté et des données personelles	Qualité environnementale et sanitaires	Optimisation de l'utilisation et de la réaffectation des espaces
Redondance et sécurisation du câblage		BIM (Building Information Modeling)		Système de management	Interconnexion à l'environnement et au territoire
Rafraîchissement des locaux techniques					

LE PÉRIMÈTRE DU PROJET R2S 4CARE À CONSIDÉRER

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 **R2S 4CARE 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.

DÉFINITION DU RÉSEAU SMART

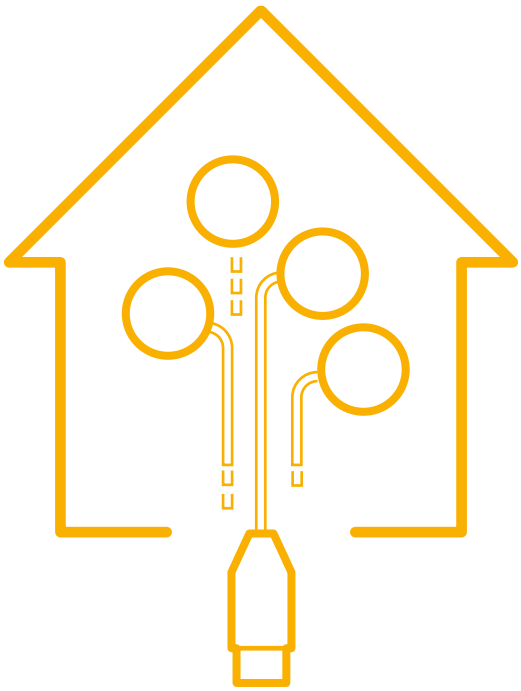
Le réseau Smart est le réseau fédérateur d'un bâtiment R2S, orienté services (SOA) et utilisant le protocole IP. Il est sécurisé et utilise exclusivement le standard Ethernet sur le réseau local et le standard Internet depuis l'extérieur du bâtiment. Les écosystèmes matériels, quel que soit leur protocole, 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, il doit cependant inclure *a minima* les équipements mentionnés dans le niveau prérequis de l'exigence « IN1.1 Intégration des équipements au réseau Smart du thème Équipements et interfaces ».

DÉFINITION DES « ESPACES »

Par défaut, les espaces non-hospitalier et d'activités hospitalières où s'appliquent les niveaux de recommandation du cadre de référence R2S 4CARE 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 les pouvoirs publics 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.



CONNECTIVITÉ

Ce thème vise à assurer une connectivité performante du bâtiment, ce qui constitue un socle nécessaire à la mise en place de services numériques. **Le Smart Hospital est raccordé aux réseaux de communication, qu'ils soient internes ou externes, filaires ou sans fil (Wi-Fi, mobile, IoT, géolocalisation…), dans les espaces hors soins et les espaces d'activités hospitalières grâce au réseau Smart.**

Ce raccordement permet d'acheminer tout type de connexions et d'échange de données en étant conforme aux standards publics internationaux. De plus, **le câblage d'un Smart Hospital se caractérise par son adaptabilité et son évolutivité**. En effet, il est possible d'associer ou de dissocier des câblages, sans réfection, pour s'adapter aux nouveaux besoins des utilisateurs des espaces et/ou à l'intégration de nouveaux systèmes communicants.

Le thème s'attache par ailleurs à assurer la fiabilité de la connectivité avec **une redondance de rattachement** du bâtiment aux opérateurs de réseaux et des équipements actifs du réseau Smart, qui permet préserver **une continuité de services en cas de défaillance** d'un opérateur réseau.

Enfin, il est demandé **un système de protection** afin de sécuriser l'infrastructure du réseau Smart contre les éventuelles malveillances.

TITRE DE L'EXIGENCE	NIVEAU	POINTS
CO 1 – RACCORDEMENT AUX RÉSEAUX EXTERNES DU BÂTIMENT		
CO 1.1 – Adduction télécom, locaux et cheminements	**Prérequis** Capacité de rattachement aux réseaux externes et locaux centraux	–
	Niveau 1 Qualité de l'ouvrage	2
	Niveau 2 Installation de contenants 19"	1
	Niveau 3 Desserte interne	3
CO 1.2 – Redondance de rattachement du bâtiment aux réseaux externes	**Niveau 1** Création d'un second ouvrage VRD	1
	Niveau 2 Existence d'un second local opérateur	2
CO 2 – CONNECTIVITÉ AUX RÉSEAUX FILAIRES		
CO 2.1 – Câblage du réseau Smart	**Prérequis** Atteint / Non atteint	–
CO 2.2 – Précâblage pérenne des utilisateurs	**Atteint / Non atteint (bonus)**	2
CO 3 – CONNECTIVITÉ AUX RÉSEAUX SANS FIL		
CO 3.1 – Nature et qualité des réseaux sans fil	**Niveau 1** Fourniture d'une étude de couverture	2
CO 3.2 – Réseaux GSM	**Niveau 1** Réseau cellulaire	2
	Niveau 2 Système mono-opérateur	3
	Niveau 3 Système multiopérateurs	4
CO 3.3 – Réseau WiFi	**Niveau 1** Mise en place du réseau WiFi	2
	Niveau 2 Réseau WiFi intégré au réseau Smart	3
	Niveau 3 Le respect des référentiels de sécurité pour la segmentation et cloisonnement des réseaux WiFi	4
CO 3.4 – Réseau IoT basse consommation	**Niveau 1** Réseau IoT opéré ou indépendant	1
	Niveau 2 Réseau IoT connecté au réseau Smart	2
CO 3.5 – Infrastructure de géolocalisation	**Niveau 1** Mise en place d'une infrastructure de géolocalisation	1
	Niveau 2 Infrastructure de géolocalisation activée	2
CO 4 – EXPLOITABILITÉ ET ÉVOLUTIVITÉ DU CÂBLAGE		
CO 4.1 – Adaptabilité de la distribution du câblage	**Niveau 1a** Capacité d'extension pour l'ajout de prises réseau	2
	Niveau 1b Distribution des terminaux et prises par des cordons ou prolongateurs préconnectorisés	1
	Niveau 1c Proximité des points de sous-répartition	1
CO 5 – REDONDANCE ET SÉCURISATION DU CÂBLAGE		
CO 5.1 – Capacité de redondance des câblages du bâtiment	**Niveau 1a** Présence de deux parcours de distribution des câblages	1
	Niveau 1b Présence de deux locaux de répartition générale	1
	Niveau 1c Redondance des liaisons desservant les points de sous-répartition du réseau Smart	1
CO 5.2 – Alimentation électrique des équipements actifs centraux	**Niveau 1** Alimentation électrique sans interruption des équipements actifs centraux	1
	Niveau 2 Redondance de l'alimentation	2
CO 5.3 – Alimentation électrique des switchs d'accès	**Niveau 1** Alimentation stabilisée des switchs d'accès	1
	Niveau 2 Autonomie en énergie électrique des switchs d'accès	2
CO 5.4 – Contrôle des accès et protection des infrastructures	**Prérequis** Protection des locaux techniques sans traçabilité	1
	Niveau 1 Protection des points de sous-répartition sans traçabilité	2
	Niveau 2 Protection des locaux techniques et des points de sous-répartition avec traçabilité	3
CO 6 – RAFRAÎCHISSEMENT DES LOCAUX TECHNIQUES		
CO 6.1 – Rafraîchissement des locaux	**Prérequis** Atteint/ non atteint	–

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.

Prérequis: **capacité de rattachement aux réseaux externes et locaux centraux.**
Ce niveau d'exigence vise à garantir la capacité de rattachement du bâtiment hospitalier aux réseaux filaires des opérateurs télécoms par l'intermédiaire d'un ouvrage VRD, qui doit être créé jusqu'en limite de domaine public, permettant de réaliser une adduction jusqu'à un local opérateur en intérieur bâtiment. Elle vise également à disposer d'un local de répartition générale destiné à recevoir les équipements actifs centraux du réseau Smart et les serveurs qui y sont rattachés.

Le bâtiment doit disposer de:
- une adduction opérateur depuis le domaine public;
- un cheminement jusqu'au local opérateur;
- un local opérateur adapté à la superficie couverte par le projet, *a minima* de 4 m² par baie (ou contenant) ou 2 m² par coffret mural (le local devant être prévu *a minima* pour recevoir une baie ou un coffret mural);
- une gaine verticale dédiée aux opérateurs, et pouvant desservir l'ensemble du bâtiment;
- un cheminement entre le local opérateur et le local de répartition générale;
- un local répartiteur général adapté à la superficie couverte par le projet, *a minima* de 4 m² par baie (le local devant être prévu pour un minimum d'une baie).

Dans un projet en rénovation ou en exploitation, les adductions et les locaux opérateurs préexistants peuvent être conservés en l'état, y compris lorsque le local opérateur n'est pas dédié à cet usage. Les locaux opérateur et répartiteur peuvent être mutualisés avec d'autres locaux.

Dans un projet neuf, le local opérateur peut être uniquement mutualisé au local de répartition générale, cependant le local de répartition générale peut être mutualisé avec d'autres locaux liés au courant faible (local opérateur, poste central de sécurité...).

Dans les deux cas, les surfaces minimales ne se cumulent pas dans le cas de mutualisations.

Niveau 1: **installation des contenants 19"**
Ces contenants sont destinés à recevoir les câblages et équipements opérateurs. Ce niveau d'exigence nécessite:
- le respect des deux niveaux précédents;
- + l'installation d'un contenant 19" dans le local opérateur;
- + s'il existe, un contenant dans le second local opérateur.

Niveau 2: **qualité de l'ouvrage**
Ce niveau d'exigence nécessite:
- le respect du niveau précédent;
- + le local opérateur et le local répartiteur général disposent chacun d'une surface de plancher de 8 m² ou plus avec 2,4 m de largeur minimum. Les deux types de locaux doivent être dédiés à leur usage et non mutualisés;
- + le local répartiteur général doit avoir la capacité d'évacuer efficacement la chaleur produite par les équipements qu'il contient.

Niveau 3: **desserte interne**
La desserte interne désigne le câblage reliant les locaux opérateurs à l'abonné. La desserte interne doit être mise en place depuis un contenant 19" des locaux opérateurs, jusqu'à un coffret prévu à cet effet dans chaque espace pouvant être occupé par un abonné indépendant (exemple: plateaux de bureau).

Ce niveau d'exigence nécessite:
- le respect des niveaux précédents;
- + la mise en place de la desserte interne depuis le local opérateur jusqu'aux coffrets;
- + 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.

Remarque: la mise en place et la gestion de la desserte interne sous la responsabilité du propriétaire du bâtiment, plutôt que par les opérateurs, sont recommandées. Elles favorisent la réutilisation du câblage en cas de changement d'occupant ou d'opérateur. Ce câblage est généralement réalisé en fibre optique monomode avec un minimum de 4 brins, mais peut être d'une autre nature pour s'adapter au contexte.

CO 1.2 – REDONDANCE DE RATTACHEMENT DU BÂTIMENT AUX RÉSEAUX EXTERNES

Le Smart Hospital prévoit les dispositions nécessaires pour assurer une redondance de connexion aux réseaux opérateurs. Il est pourvu d'au moins deux locaux ou espaces opérateurs permettant le raccordement à au moins deux opérateurs distincts.

Niveau 1: **création d'un second ouvrage VRD**
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. Plus précisément il s'agit de créer 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.

Niveau 2: **existence d'un second local opérateur**
L'objectif est de rendre possible la continuité de services en cas d'indisponibilité d'un des deux locaux opérateurs.
L'exigence demande:

- le respect du niveau précédent
- + avoir un second local ou espace opérateur qui dispose d'une surface de plancher correspondant *a minima* à ce qui est défini dans le niveau prérequis de l'exigence « CO 1.1 – Adduction télécom, locaux et cheminements » soit 4 m² par baie ou 2 m² par coffret mural. Ce local devra comprendre un contenant 19".

Chaque bâtiment est par ailleurs doté d'une seconde gaine opérateurs verticale, espacée de la première d'au moins 8 m (ou 2 m 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).

Remarque: le second local opérateur peut être mutualisé avec d'autres locaux liés au courant faible (local répartiteur général, poste central de sécurité…), à l'exception du 1er local opérateur. Par défaut et sauf mention contraire, chaque exigence du référentiel doit être traitée au niveau du bâtiment. Exception faite sur les projets regroupant plusieurs bâtiments sur une parcelle unique, si la non-sécabilité de la propriété des bâtiments est prévue dans le programme de l'opération, le projet pourra traiter l'exigence CO 1.2 au niveau du périmètre des bâtiments non sécables.

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.

Prérequis: 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" 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

Le bâtiment est prédisposé à recevoir le ou les câblages ou les équipements réseau, rassemblant les connexions des différents espaces d'activités.

Niveau unique: les espaces d'activité hospitalière sont pré-équipés d'un câblage flexible, modulaire et évolutif, «Cabling as a Service».

Cette exigence nécessite:

- la mise en œuvre d'un précâblage modulaire réparti de façon homogène avec des points de consolidation actifs ou passifs dans l'ensemble des espaces destinés à recevoir des utilisateurs (la mise en œuvre ne doit pas être centralisée dans un local unique par niveau ou pour l'ensemble du bâtiment);
- la densité des points de consolidations doit être cohérente avec l'effectif maximum potentiel de chaque espace avec la mise en place, de points de consolidation couvrant une surface au plus de 60 m^2, et d'une terminaison RJ45 par personne. Le câblage doit également être prévu pour la mise en place de points d'accès WiFi dans les mêmes espaces
- Le câblage doit tenir compte des possibles divisions des espaces entre plusieurs services
- La mise en place de contenants 19" destinés à recevoir le tenant du câblage et les équipements actifs associés. Ils disposent des alimentations électriques nécessaires et d'un traitement d'air adapté
- La mise en place des rocades dans une topologie adaptée entre:

– Les contenants 19" mentionnés dans l'exigence
– Les locaux opérateurs
– Les locaux de répartition générale
– S'ils existent, les locaux informatiques destinés aux services (exemple: des locaux nodaux). Il n'est pas nécessaire de prévoir un maillage complet, mais il doit être possible de faire des liens entre ces différents espaces.

CO 3 – Connectivité aux réseaux sans fil

CO 3.1 – NATURE ET QUALITÉ DES RÉSEAUX SANS FIL

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. Les réseaux WiFi doivent disposer d'un mécanisme permettant à un appareil de changer de point d'accès sans perdre sa connectivité et donc sans interruption de service lors de ses déplacements (mécanisme de handover, ou de roaming).

Niveau 1: **fourniture d'une étude de couverture**
L'enjeu de cette recommandation est de donner aux futurs occupants 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 d'exigence demande:
- la fourniture d'une mesure de couverture intérieure des principaux réseaux sans fil publics (4G, 5G, WiFi…) suivant leur disponibilité locale;

CO 3.2 – RÉSEAUX GSM

Niveau 1: **réseau cellulaire**
Ce niveau de la recommandation vise à apporter une garantie d'accès, dans tous les espaces intérieurs du bâtiment, aux réseaux cellulaires disponibles des opérateurs.

Ce niveau de recommandation requiert:
- le respect l'exigence CO 3.1;
- + l'équipement des espaces d'un réseau cellulaire.
- la mise en place de mesures conservatoires visant à faciliter la mise en place ultérieure d'un système DAS (Distributed Antenna System) de GSM.

Niveau 2: **système mono-opérateur**
Ce niveau d'exigence demande:
- le respect du niveau précédent;
- + 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. 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 et les parties privatives, 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.

Niveau 3: **système multiopérateurs**
Ce niveau d'exigence demande:
- le respect des niveaux précédents;
- + Le bâtiment est équipé d'un système de GSM indoor raccordé à au moins 2 opérateurs.

Le niveau peut également être atteint si la couverture naturelle depuis l'extérieur du bâtiment est satisfaisante pour au moins deux 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.

CO 3.3 – RÉSEAU WIFI

Ce niveau de recommandation vise à apporter une garantie d'accès et la disponibilité d'une couverture WiFi, dans tous les espaces intérieurs du bâtiment, à la fois dans les espaces non-hospitaliers et dans les espaces d'activité hospitalière.

Niveau 1: **mise en place du réseau WiFi**

La couverture des espaces communs doit permettre un accès à Internet à tous les occupants. Les points d'accès sont connectés à un autre réseau que le réseau Smart.

Niveau 2: **réseau WiFi intégré au réseau Smart**

Ce niveau d'exigence demande:

- le respect du niveau précédent;
- + les points d'accès du réseau WiFi sont connectés au réseau Smart.

Niveau 3: **le respect des référentiels de sécurité pour la segmentation et cloisonnement des réseaux WiFi**

Les réseaux WiFi respectent, 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

Niveau 1: **réseau IoT opéré ou indépendant**

Ce niveau d'exigence demande:

- la couverture IoT et le déploiement d'objets connectés sur ce réseau;
- le réseau IoT peut être opéré, c'est à dire utiliser le réseau public, ou être indépendant en reposant sur un réseau LAN indépendant du réseau Smart

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

Niveau 2: **réseau IoT connecté au réseau Smart**.

Ce niveau d'exigence demande:

- le respect du premier point (couverture IoT et déploiement d'objets connectés) du niveau précédent;
- + la couverture IoT doit être assurée par des points d'accès connectés au réseau Smart.

Dans cette exigence, sont concernés les réseaux étendus à basse consommation/LPWAN privatifs.

CO 3.5 – INFRASTRUCTURE DE GÉOLOCALISATION

Niveau 1: **mise en place d'une infrastructure de géolocalisation**

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 *a 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.

Niveau 2: **infrastructure de géolocalisation activée**

Ce niveau d'exigence demande:

- le respect du niveau précédent;
- + activation de l'infrastructure de géolocalisation L'infrastructure de géolocalisation devra *a 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

CO 4 – Exploitabilité et évolutivité du câblage

CO 4.1 – ADAPTABILITÉ DE LA DISTRIBUTION 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.

Niveau 1a : capacité d'extension pour l'ajout de prises réseau

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.

Niveau 1b : distribution des terminaux et prises par des cordons ou prolongateurs préconnectorisés

Ce niveau d'exigence concerne la mise en place rapide des prises terminales du réseau Smart. Il requiert que l'intégralité du câblage issu des switchs d'accès soit réalisée à l'aide de cordons ou prolongateurs préconnectorisés (sertis en atelier ou en usine).

Niveau 1c : proximité des points de sous-répartition

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 5 – Redondance et sécurisation du câblage

CO 5.1 – CAPACITÉ DE REDONDANCE DES CÂBLAGES DU BÂTIMENT

Description générale :
Après avoir valorisé la redondance du rattachement du bâtiment aux réseaux externes (exigence CO 1.2), 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.

Niveau 1a : **présence de deux parcours de distribution des câblages**
Le but de cette exigence 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 m (ou 2 m 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.

Niveau 1b : **présence de 2 locaux de répartition générale**
Ce niveau d'exigence 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 présentant des caractéristiques *a minima* identiques à ce qui est décrit dans le prérequis de l'exigence « CO 1.1 – Adduction télécom, locaux et cheminements ». Il en est espacé du premier d'au moins 8 m (ou 2 m avec un coupe-feu). En cas de multiplicité des parcours de distribution des câblages (niveau 1a), les locaux de répartition générale sont disposés sur des verticalités différentes.

Des cheminements de capacité adaptée à la quantité de câbles à installer interconnectent ce second local :
- aux cheminements de distribution des câbles dans le bâtiment ;
- au 1er local de répartition générale ;
- et au(x) local(aux) ou espaces des opérateurs.

Par défaut et sauf mention contraire, chaque exigence du référentiel doit être traitée au niveau du bâtiment. Exception faite sur les projets regroupant plusieurs bâtiments sur une parcelle unique, si la non-sécabilité de la propriété des bâtiments est prévue dans le programme de l'opération, le projet pourra traiter le niveau 2 de l'exigence CO 5.1 au niveau du périmètre des bâtiments non sécables.

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.

Niveau 1c : **redondance des liaisons desservant les points de sous répartition du réseau Smart**
Ce niveau d'exigence a pour objet de vérifier que le réseau Smart est fiabilisé par une redondance du câblage interconnectant les répartiteurs généraux et les points de sous-répartition. Il nécessite la redondance des liaisons entre les répartiteurs généraux et les points de sous-répartition. En cas de multiplicité des parcours de distribution des câblages (niveau 1a), les liaisons doivent être réparties dans les différents parcours.

CO 5.2 – ALIMENTATION ÉLECTRIQUE DE L'INFRASTRUCTURE

Le câblage des services généraux du réseau Smart du bâtiment dispose de systèmes de distribution électrique garantissant la stabilité et la sécurité d'alimentation électrique pour les nœuds de connexion réseau. Il est à noter que cette exigence est incluse dans les projets de construction hospitalière.

Niveau 1 : **alimentation électrique sans interruption des équipements actifs centraux**
Le but du niveau 1 de l'exigence est de garantir la disponibilité d'un courant dont la tension et la fréquence sont régulées, afin de préserver la meilleure garantie de continuité fonctionnelle des équipements concernés. Ce niveau d'exigence requiert une alimentation électrique sans interruption (exemples : ASI, onduleur avec batterie…) des équipements actifs centraux du réseau Smart (cœurs de réseau, routage, pare-feu, équipements d'interface avec les

réseaux opérateurs de télécommunication) et les serveurs centraux qui y sont rattachés. L'extinction automatique de ces équipements en cas de coupure prolongée de la source principale et l'autonomie de l'alimentation électrique sans interruption est suffisante pour le déroulement de ce processus. Le choix doit être en adéquation avec l'usage du bâtiment (*a minima* pour la protection des serveurs, jusqu'à 1 h comme décrit dans la NFC15-211 – installation électrique basse tension dans les locaux à usage médical).

Niveau 2 : **redondance de l'alimentation**
Ce niveau d'exigence 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.

Ce niveau d'exigence demande :
- le respect du niveau précédent de l'exigence pour au moins un circuit d'alimentation des équipements actifs centraux et des serveurs qui y sont rattachés ;
- + 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. L'exigence ne porte pas sur l'alimentation en amont de ces tableaux électriques.

CO 5.3 – ALIMENTATION ÉLECTRIQUE DES SWITCHS D'ACCÈS

Il s'agit de fiabiliser l'alimentation électrique des switchs d'accès du réseau Smart.

Niveau 1 : **alimentation stabilisée des switchs d'accès**
Le but de cette exigence est d'avoir une alimentation stabilisée ne portant plus uniquement sur les équipements actifs centraux (exigence CO 5.2), mais sur les switchs d'accès du réseau Smart. Il nécessite une alimentation stabilisée pour les points de sous-répartition des équipements actifs du réseau Smart. Cette alimentation doit être externe aux switchs d'accès, et peut être utilisée localement par d'autres équipements (exemples : concentrateur d'étage, régulation…).

Niveau 2 : **autonomie en énergie électrique des switchs d'accès**
Le but de cette exigence est de disposer d'une autonomie en énergie électrique pour les switchs d'accès en cas de coupure de l'alimentation normale.

Ce niveau d'exigence demande :
- le respect du niveau précédent de l'exigence ;
- + la présence d'une autonomie en énergie électrique en cas de coupure de l'alimentation normale (exemples : ASI, onduleur avec batterie…).

CO 5.4 – CONTRÔLE DES ACCÈS ET PROTECTION DES INFRASTRUCTURES

Prérequis :
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.

Le système de protection peut être mis en place sur :
- l'armoire directement ;
- les locaux concernés ;
- à un ensemble de locaux uniquement s'ils sont liés aux courants faibles (CFA/VDI) opérateur, répartiteur, GSM…).

Niveau 1 : **protection des locaux techniques sans traçabilité**
Ce niveau d'exigence requiert la protection de l'accès sans traçabilité aux locaux opérateurs et de répartition générale, exemples : clé (hors carré, triangle), code, …

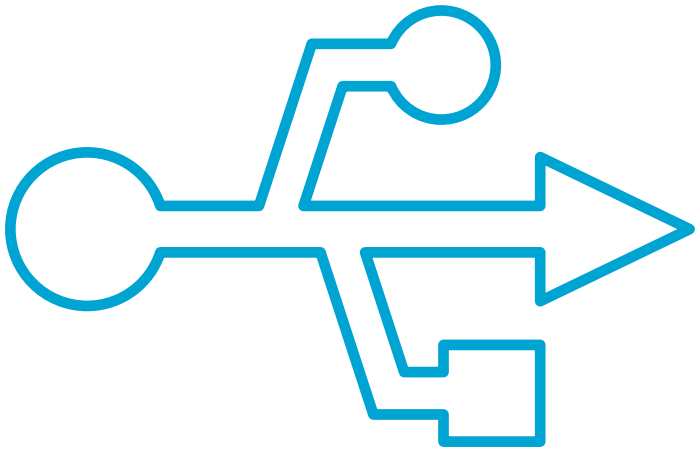
Niveau 2 : **protection des points de sous-répartition sans traçabilité**
Ce niveau d'exigence requiert :
- le respect du prérequis ;
- la protection de l'accès aux points de sous-répartition sans traçabilité. Cette sécurisation peut être apportée par un verrouillage du local ou d'une armoire technique par un moyen sans traçabilité comme par exemple une clé (hors carré, triangle), un code…

Niveau 3 : **protection des locaux techniques et des points de sous-répartition avec traçabilité**
Ce niveau d'exigence requiert :
- le respect des deux niveaux précédents ;
- 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 techniques

CO 6.1 – RAFRAÎCHISSEMENT DES LOCAUX TECHNIQUES

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



ARCHITECTURE RÉSEAU

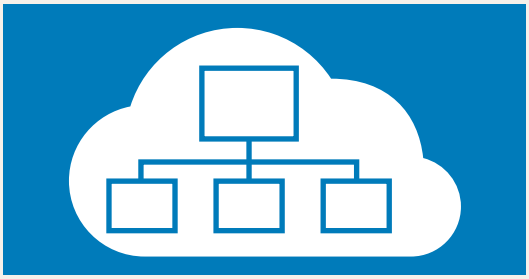
Ce thème a pour enjeu d'assurer la circulation du 4e fluide du bâtiment, c'est-à-dire les données, qui constituent sa colonne vertébrale. Le cadre de référence R2S 4CARE pose **comme prérequis la présence d'un réseau Smart**. Le réseau Smart est le réseau fédérateur d'un bâtiment hospitalier R2S 4CARE 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.

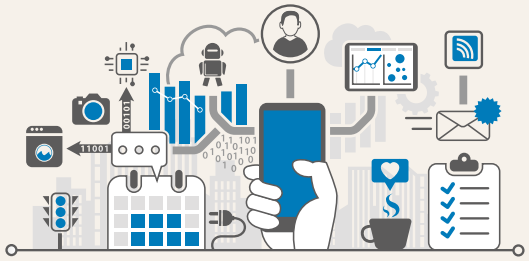
Dans la deuxième partie, le thème s'intéresse à **l'administration des équipements réseau** afin d'améliorer l'exploitation, la surveillance des équipements, prioriser le trafic de certains réseaux en cas de surcharge, garantir le débit et le temps de rétablissement de la connexion Internet en cas de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

SOCLE R2S 4CARE : ARCHITECTURE EN TROIS COUCHES

COUCHE « APPLICATIONS/ SERVICES »
Où sont stockées et traitées les données du bâtiment pour rendre des services aux usagers (occupant ou exploitant).



COUCHE « INFRASTRUCTURE DE COMMUNICATION »
Couche réseau du bâtiment où circulent les données sur un support radio et/ou filaire au standard Ethernet-IP (Internet Protocol), qui rend accessibles les équipements à la couche services et réciproquement.



COUCHE « ÉQUIPEMENTS CONNECTÉS »
Qu'ils s'agissent de capteurs, d'actionneurs, de contrôleurs, d'objets connectés… ceux-ci doivent pouvoir communiquer avec la couche supérieure, celle du réseau Ethernet-IP (Internet Protocol) du bâtiment.

TITRE DE L'EXIGENCE	NIVEAU	POINTS
RE 1 – CARACTÉRISTIQUES ET ALIMENTATION DU RÉSEAU SMART		
RE 1.1 – Caractéristiques et capacités d'extension du réseau Smart	**Prérequis** Fonctionnalités supportées par le réseau Smart	–
	Niveau 1 Capacité d'extension des switchs d'accès	2
RE 1.2 – Alimentation des terminaux de communication par le réseau	**Niveau 1** Mesures conservatoires pour le PoE	2
	Niveau 2 Ports PoE sur les switchs d'accès	3
	Niveau 3 Capacité d'extension PoE des switchs d'accès	4
RE 1.3 – Déploiement du protocole IPv6	**Atteint / Non atteint**	2
RE 2 – CONTINUITÉ ET PROTECTION FONCTIONNELLE DU RÉSEAU SMART		
RE 2.1 – Capacité de résilience du réseau Smart	**Niveau 1** Double connexion des switchs d'accès	2
	Niveau 2 Résilience du mécanisme de redondance	4
RE 2.2 – Détection d'anomalies et protection du réseau Smart	**Atteint / Non atteint**	3
RE 3 – MANAGEMENT DU RÉSEAU SMART		
RE 3.1 – Administration du réseau Smart et de leurs équipements	**Niveau 1** Plateforme centralisée d'administration des switchs du réseau Smart	2
	Niveau 2 Plateforme d'administration de tous les équipements du réseau Smart	3
RE 3.2 – Priorisation de service	**Atteint / Non atteint**	3
RE 3.3 – Gestion de domaine et adressage dynamique	**Atteint / Non atteint**	1
RE 3.4 – Continuité de service Internet	**Niveau 1** Accès Internet du réseau Smart	2
	Niveau 2 Fiabilisation de l'accès Internet	3
	Niveau 3 Fiabilisation renforcée de l'accès Internet	4

RE 1 – Réseau Smart et réseaux des usagers

RE 1.1 – CARACTÉRISTIQUES ET CAPACITÉS D'EXTENSION DU RÉSEAU SMART

Un des principes du cadre de référence R2S 4CARE est de concevoir et mettre en place le réseau Smart. Le réseau Smart a vocation à être la colonne vertébrale du bâtiment, par laquelle les données vont passer des équipements aux services. C'est le réseau fédérateur d'un bâtiment hospitalier R2S 4CARE 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.

Pour rappel, les équipements actifs centraux comprennent les éléments suivants : cœurs de réseau, routeurs, pare-feu, équipements d'interface avec les réseaux opérateurs de télécommunication.

Prérequis : fonctionnalités supportées par le réseau Smart
Ce prérequis requiert l'existence d'un réseau Smart utilisant le protocole IP et le standard Ethernet. Il doit être conforme aux standards publics internationaux TCP/IP et Ethernet. Le réseau Smart doit disposer *a minima* :

- de fonctions de routage inter-VLAN (fonctions de niveau 3) ;
- s'ils existent, de switchs d'accès, administrables et *a minima* de niveau 2.

Remarques : il est ici notamment question du support de la fonction de routage (niveau 3), la mise en application est l'objet de l'exigence « SE 1.2 – Mécanismes de routage conditionnel du réseau Smart ». Dans le cas d'un ensemble de bâtiments, la fonction de routage inter-VLAN peut être assurée au niveau de cet ensemble.

Pour cette exigence et l'ensemble du référentiel, 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).

Les équipements actifs centraux du réseau Smart et les serveurs qui y sont rattachés doivent être installés dans le local de répartition générale. Lorsque deux locaux de répartition générale sont visés au titre du niveau 1b de l'exigence « CO 5.1 – Capacité de redondance des câblages du bâtiment », la fonction de routage inter-VLAN doit être assurée en redondance dans chacun de ces locaux.

Niveau 1 : capacité d'extension des switchs d'accès
En conception et réalisation, les switchs d'accès doivent présenter une capacité d'extension de 15 % (arrondi à l'unité la plus proche) du nombre de ports downlink en plus des ports utilisés lors de la livraison du bâtiment. Les ports downlink libres ainsi que ceux qui sont brassés mais sans équipement connecté à l'extrémité sont pris en compte dans la capacité d'extension.

En exploitation, la capacité d'extension non équipée des switchs d'accès doit être connue pour faciliter la planification des évolutions futures du réseau Smart.

Ce niveau d'exigence requiert :

- l'atteinte du prérequis ;
- + en conception et réalisation, les switchs d'accès du réseau Smart disposent d'une capacité d'extension telle que décrite ci-dessus ;
- + en exploitation, connaissance de la capacité d'extension des switchs d'accès telle que décrite ci-dessus.

Remarque : lorsque que le switch de cœur est aussi utilisé comme switch d'accès pour des équipements terminaux, les exigences portant sur les switchs.

RE 1.2 – ALIMENTATION DES TERMINAUX DE COMMUNICATION PAR LE RÉSEAU

L'enjeu concerne ici les switchs d'accès connectant les équipements terminaux, qui doivent délivrer sur leurs ports downlink une alimentation électrique, pour les équipements qui y sont rattachés, en conformité avec les standards internationaux.

Niveau 1 : mesures conservatoires pour le PoE
Ce niveau d'exigence valorise la prédisposition du bâtiment à délivrer du PoE par les switchs d'accès. Il requiert que des mesures conservatoires soient prises pour faciliter la mise en place future de PoE sur le réseau Smart. Les équipements mis en place (câblage, mise en œuvre, terminaisons de câble, équipements actifs…) devront supporter le déploiement du PoE sans modification de l'infrastructure installée (exemples : switchs avec capacité PoE avec

logements libres pour l'ajout d'alimentations PoE, sans que celles-ci soient mises en place) pour l'ensemble du périmètre du réseau Smart.

Niveau 2 : ports PoE sur les switchs d'accès
Ce niveau de l'exigence implique que les switchs d'accès supportent la fonction PoE, *a minima* lorsqu'ils desservent des zones de services aux utilisateurs (exemples : lieux d'accueil, de restauration, de loisir et de bien-être) afin de faciliter la mise en place d'équipements tels que des objets connectés, points d'accès Wi-Fi, terminaux de sûreté. Il requiert l'utilisation de switchs d'accès du réseau Smart disposant de ports PoE, *a minima* pour les zones de services.

Niveau 3 : capacité d'extension PoE des switchs d'accès
En conception et réalisation, les switchs d'accès doivent présenter une capacité d'extension de 30 % de la puissance globale PoE qu'ils délivrent, en plus de la puissance utilisée lors de la livraison du bâtiment.

En exploitation, la réserve de puissance disponible sur le budget PoE de chaque switch d'accès doit être connue pour faciliter la planification des évolutions futures du réseau Smart.

Ce niveau d'exigence requiert :
- l'atteinte du niveau précédent ;
- + capacité d'extension ou connaissance de cette capacité, selon la phase du projet, tel que décrit ci-dessus.

RE 1.3 – DÉPLOIEMENT DU PROTOCOLE IPV6

Pour rappel, les équipements actifs comprennent les éléments suivants : équipements actifs centraux du réseau Smart + switchs du réseau Smart comprenant les switchs d'accès.

Les équipements actifs centraux du réseau Smart comprennent les éléments suivants : cœurs de réseau, routeurs, pare-feu, équipements d'interface avec les réseaux opérateurs de télécommunication.

Cette exigence demande qu'*a minima* les équipements actifs de niveau 3 du réseau Smart et les serveurs centraux qui y exposent une API soient configurés en adressage IPv6 en parallèle de l'adressage IPv4. Les API exposées sur le réseau Smart qui sont accessibles depuis Internet en IPv4 doivent également être accessibles en IPv6 (la connectivité IPv6 doit alors être disponible sur l'accès Internet du réseau Smart).

Les API qui font l'objet de cette exigence correspondent à celles évaluées à travers l'exigence « Équipements et interfaces 2.1 – Existence d'API et exposition des données ».

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).

Niveau 1: double connexion des équipements actifs d'accès

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).

Niveau 2: résilience du mécanisme de redondance

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).

RE 3 – Management du réseau Smart

RE 3.1 – ADMINISTRATION DES RÉSEAUX ET DE LEURS ÉQUIPEMENTS

Au niveau 1 il est possible d'avoir une ou plusieurs plateformes permettant l'administration des équipements actifs du réseau Smart, au niveau 2 cette plateforme doit être unique.

Niveau 1: plateforme centralisée d'administration des switchs du réseau Smart

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 switchs.

Ce niveau d'exigence implique:

- la mise en place et le paramétrage d'une plateforme logicielle centralisée d'administration des switchs du réseau Smart. 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 en mode lecture seule, ou mode Read);
- si l'exigence RE 2.1 est visée, les liens actifs ou en défaut doivent être supervisés sur la plateforme;
- si l'exigence RE 2.2 est visée, les anomalies constatées et le statut des ports en défaut doivent être supervisés sur la plateforme.

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

Niveau 2: plateforme d'administration de tous les équipements du réseau Smart

Ce deuxième niveau de l'exigence implique qu'une unique plateforme centralisée supervise et administre tous les éléments constituant le réseau Smart.

Il requiert:

- l'atteinte du niveau précédent;
- la présence d'une plateforme d'administration étendue à la gestion des équipements actifs du réseau Smart (c'est-à-dire ceux couverts par le niveau précédent + routeurs, pare-feu, équipements d'interface avec les réseaux opérateurs de télécommunication), aux contrôleurs WiFi locaux et/ou aux points d'accès Wi-Fi, et aux serveurs centraux;
- la plateforme d'administration doit être unique pour l'ensemble des équipements supervisés.
- les routeurs/passerelles de GTB qui convertissent des bus de terrain sur réseau Ethernet ne sont pas concernés par cette exigence.

RE 3.2 – PRIORISATION ET CONTINUITÉ DE SERVICE DES RÉSEAUX

La fonction de «qualité de service (QoS)» est disponible et activée sur les switchs du réseau Smart, conformément au(x) SLA formalisé(s) entre le fournisseur de service et les utilisateurs.

Remarque: un surdimensionnement du réseau ne peut pas être utilisé pour justifier l'atteinte de cette recommandation.

RE 3.3 – GESTION DE DOMAINE ET ADRESSAGE DYNAMIQUE

Le but de cette recommandation 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.

Les services de résolution de noms de domaine (DNS) et de mécanismes d'adressage IP dynamiques (DHCP) doivent être disponibles et paramétrés sur le réseau Smart. Ces services doivent être utilisés *a minima* sur un segment du réseau Smart (exemples: un VLAN, certains équipements, etc.).

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

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

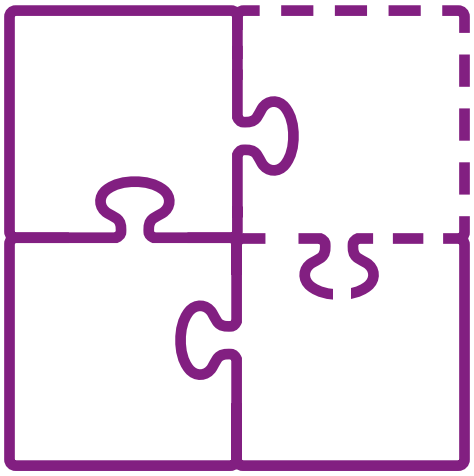
de télémaintenance, ou encore faciliter les opérations de mise à jour par la mise en place d'un accès à Internet au réseau Smart. Les niveaux 2 et 3 valorisent une sécurisation de l'accès Internet du réseau Smart.

Niveau 1: accès Internet du réseau Smart
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).

Niveau 2: fiabilisation de l'accès Internet
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 du projet. La fiabilisation peut également être apportée par l'existence d'au moins deux accès Internet indépendants apportant une redondance des connexions entrantes et sortantes. Ce niveau d'exigence requiert la mise en place d'une GTR pour l'accès Internet du réseau Smart ou la mise en place d'au moins deux accès Internet indépendants.

Niveau 3: fiabilisation renforcée de l'accès Internet
Ce niveau d'exigence requiert la mise en place d'au moins deux accès Internet indépendants ET une GTR sur au moins un de ces accès Internet.

Remarque : pour les niveaux 2 et 3, lorsque plusieurs accès Internet sont valorisés, chacun d'eux doit faire l'objet d'une pénétration indépendante dans le bâtiment afin de bénéficier d'une redondance de cheminement. La multiplicité des points de pénétration est par ailleurs valorisée par le niveau 1 de l'exigence « CO 1.2 – Redondance de rattachement du bâtiment aux réseaux externes ».



ÉQUIPEMENTS ET INTERFACES

Ce thème consiste à mettre en relation les équipements, le réseau et les services grâce à leur interopérabilité pour faciliter la conception et l'exploitation du bâtiment.

Le Smart Hospital se caractérise par **l'interopérabilité de ses systèmes**, c'est-à-dire par **leur ouverture et leur capacité à fonctionner ensemble**. Les équipements peuvent ainsi être mis en relation à l'intérieur et à l'extérieur des bâtiments, quels que soient les usages. Cette interopérabilité **repose sur des interfaces d'accès** aux services, fonctions et données des systèmes. Celles-ci sont notamment gérées par des API (**Application Programming Interface / interfaces de programmation**) standards, qui permettent aux données d'être réutilisées par des services ou applications tierces.

Grâce à l'interopérabilité, le Smart Hospital a la possibilité **d'ouvrir les données du bâtiment et de les rendre accessibles pour une optimisation des usages du bâtiment**. La stabilité des services et le fonctionnement des équipements communicants du bâtiment en mode dégradé sont également évalués.

Finalement, **la mise en place d'une maquette numérique BIM** (Building Information Modeling) est valorisée. La maquette numérique permettant d'intégrer des informations des équipements communicants du bâtiment sous la forme d'une base de données mise à jour aux différents états d'avancement du projet afin d'optimiser la gestion du bâtiment, de sa conception à l'exploitation.

TITRE DE L'EXIGENCE	NIVEAU	POINTS
IN 1 – ÉQUIPEMENTS		
IN 1.1 – Intégration des équipements au réseau Smart	**Prérequis** Intégration de la télémétrie des fluides et régulation	–
	Niveau 1 Intégration de deux systèmes	1
	Niveau 2 Intégration de trois systèmes	2
	Niveau 3 Intégration de quatre systèmes	3
IN 1.2 – Survivance des fonctions des équipements communicants	**Atteint / Non atteint**	2
IN 2 – API TERRAIN ET CENTRALE		
IN 2.1 – Existence d'API et exposition des données	**Prérequis** Périmètre minimal API et liste des interfaces	–
	Niveau 1 Exposition des données de deux systèmes	1
	Niveau 2 Exposition des données de trois systèmes	2
	Niveau 3 Exposition des données de quatre systèmes	3
IN 2.2 – Documentation technique des API	**Prérequis** Documentation technique	–
	Niveau 1 Documentation lisible au format numérique	1
IN 2.3 – Modèle économique	**Atteint / Non atteint**	2
IN 2.4 – Rétrocompatibilité des API	**Atteint / Non atteint**	1

IN 1 – Interfaces de communication

Les interfaces protocolaires permettent d'interfacer les équipements de terrain à travers des protocoles ouverts, standardisés, interopérables basés sur les normes de type ISO EN (exemple : EN 16484). Voir exigence « IN 3.1 – Systèmes disposant d'interfaces protocolaires » pour plus d'informations.

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

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

IN 1.1 – INTÉGRATION DES ÉQUIPEMENTS AU RÉSEAU SMART DU BÂTIMENT

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 l'exigence « ID 1.5 Périmètre du réseau Smart ». 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 (OPC UA…) ;
  - ces différents moyens doivent respecter les protocoles standards internationaux ISO/EN/CEA/IEEE ou être commun 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 Centrale.

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

Prérequis : intégration de la télémétrie des fluides et régulation

Ce niveau d'exigence s'applique à la Gestion technique du bâtiment (GTB), que celle-ci comporte ou non une supervision, et *a minima* aux catégories suivantes selon la description générale de l'exigence :

- télémétrie des fluides (électricité, calories, débit/volume d'eau…) ;
- régulation du chauffage et de la climatisation (CVC).

Niveau 1 : intégration de deux systèmes

Ce niveau d'exigence requiert :

- le respect du prérequis ;
- + L'intégration d'un autre système, complémentaire à la GTB, parmi les suivants dans le périmètre du réseau Smart :
  - traitement du confort des utilisateurs par espace (traitement d'air, pilotage de l'éclairage, gestion des occultations solaires motorisées en fonction de ce que comporte le projet) ;
  - contrôle d'accès ;
  - vidéosurveillance ;
  - ascenseur ;
  - infrastructure de géolocalisation ;
  - infrastructure de recharge des véhicules électriques et hybrides rechargeables ;
  - système de comptage de personnes par zone, chaque zone doit représenter au plus 20 % de la surface utile du bâtiment ;
  - système de gestion et de réservation dynamique d'espaces (exemple : espace de réunion) ;
  - signalétique dynamique (exemples : hall d'accueil, cabine d'ascenseur…) ;
  - autres à l'initiative du porteur de la démarche.

Pour être comptabilisé, le système souhaitant être valorisé doit être connecté directement sur le réseau Smart et non au travers d'un autre système (exemple : le système ascenseur ne peut pas être valorisé si la machinerie de l'ascenseur est connectée à la GTB et non directement sur le réseau Smart).

Le système doit également répondre à au moins un critère d'admissibilité suivant :

- remonter des données des équipements sur l'API centrale ;
- réaliser des interconnexions entre différents systèmes hétérogènes (exemple : asservissement entre le contrôle d'accès et la vidéosurveillance) ;
- donner un accès Internet aux équipements ;

- assurer une gestion centralisée des équipements du système ;
- réaliser une communication entre les équipements d'un même système (exemple : différents automates d'un système spécifique ayant besoin de communiquer uniquement entre eux, les connecter au réseau Smart permet de ne pas créer un réseau physique supplémentaire).

Niveau 2 : intégration de trois systèmes
Ce niveau d'exigence requiert :
- le respect du niveau précédent ;
- + intégration d'un système supplémentaire parmi ceux décrits dans le niveau 1 de l'exigence.

Ce niveau d'exigence valorise donc les systèmes décrits dans le prérequis et deux autres systèmes.

Niveau 3 : intégration de quatre systèmes
Ce niveau d'exigence requiert :
- respect du niveau précédent ;
- + intégration d'un système supplémentaire parmi ceux décrits dans le niveau 1 de l'exigence.

Ce niveau d'exigence valorise donc les systèmes décrits dans le prérequis et trois autres systèmes.

Remarque : l'exposition des données des systèmes intégrés au réseau Smart est l'objet de l'exigence « IN 2 – Existence d'API et exposition des données » pour les API et « IN 3 – Systèmes disposant d'interfaces protocolaires » pour les interfaces protocolaires.

IN 1.1 BIS – CAPACITÉ DES ÉQUIPEMENTS À S'INTERFACER AU RÉSEAU SMART GRÂCE À LEURS API

Les équipements communicants du bâtiment doivent exposer leurs données d'interfaçage 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.

Tous les écosystèmes matériels communicants du bâtiment, doivent exposer leurs données d'interfaçage 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 local (LAN) 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.

L'API doit être de type Web service, c'est-à-dire qu'elle doit permettre aux applications de dialoguer à distance via le réseau Smart et le World Wide Web indépendamment des plates-formes et des langages sur lesquelles elles reposent.

Prérequis : capacité des équipements à s'interfacer avec une API au réseau Smart
Ce niveau de recommandation évalue la capacité des équipements à s'interfacer avec une API au réseau Smart, ces API doivent être documentées et consultables. Une architecture de communication orientée services est donc requise. Les écosystèmes communicants du bâtiment doivent être dotés d'API dont la documentation est consultable au format numérique à l'aide d'un outil informatique (exemple Swagger).

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.

Niveau 1 : accessibilité des API en Web service
Ce niveau de recommandation concerne l'accessibilité des API en Web Service.
Ce niveau d'exigence requiert :
- le respect du Prérequis ;

- + pour chaque catégorie d'équipements précitées, la disponibilité d'au moins une API en Web service sur le réseau Smart au standard SOAP, oBIX, JSON RESTful, websocket ou MQTT.

En bonne pratique, les APIs respectent les exigences du cadre de référence R2S Connect 2021.

Niveau 2: intégration des données de la gestion technique et énergétique du bâtiment
Ce niveau de recommandation étend le même principe à la gestion technique et énergétique du bâtiment.

Ce niveau d'exigence requiert:
- le respect des niveaux précédents;
- + l'intégration des données issues de la gestion technique et énergétique du bâtiment. Par exemple: éclairage, régulation terminale du traitement d'air, occultations solaires... ces exemples ne sont pas exhaustifs.

Niveau 3: politique d'intégration de tout nouveau système acquis de Gestion technique et énergétique du bâtiment, dispositif médical, biomédical, système d'appel malade, système d'efficience hospitalière, système de logistique, terminal multimédia patients.
Ce niveau requiert l'existence d'un document spécifiant la politique d'intégration des équipements relevant des catégories citées, qui permette de définir:
- les équipements nécessitant un raccordement au réseau Smart;
- les données d'intérêt devant être rendues accessibles par les APIs;
- les spécifications techniques d'interfaçage, celles-ci pouvant s'appuyer sur le cadre de référence R2S Connect.

Niveau 4: tous les équipements connectés disposent d'une API
Ce niveau de recommandation étend le même principe à l'ensemble des équipements connectés au réseau Smart. Il requiert donc l'accessibilité de tous les équipements connectés au réseau Smart (*a minima* pour les informations disponibles et actions possibles par les utilisateurs dans le bâtiment) via des API en Web Service au standard SOAP, oBIX, JSON RESTful, websocket ou MQTT.

IN 1.2 – SURVIVANCE DES FONCTIONS DES ÉQUIPEMENTS COMMUNICANTS

Il s'agit d'assurer la continuité fonctionnelle, en mode restreint ou dégradé des systèmes, en cas de panne du réseau local 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 service.

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.

Périmètre: le mode dégradé doit porter sur les systèmes considérés essentiels pour les utilisateurs (exemples: régulation locale des systèmes terminaux comme l'éclairage qui doit pouvoir être assuré en cas de perte du système de pilotage au travers du réseau Smart, les utilisateurs doivent pouvoir circuler dans le bâtiment lorsque la connexion est perdue entre les équipements terminaux et le serveur...) et non nécessairement sur tous les autres systèmes de façon systématique dont une panne ne remet pas en cause le fonctionnement basique du bâtiment (exemples: géolocalisation, Wi-Fi...).

IN 2 – API terrain et API centrale

IN 2.1 – EXISTENCE D'API ET EXPOSITION DES DONNÉES

Il s'agit de disposer de « portes d'entrée numériques » sur le bâtiment au travers d'interfaces de programmation (API), avoir connaissance de l'ensemble de ces API, et leur garantir un périmètre minimal.

Prérequis : périmètre minimal API et liste des interfaces
Ce niveau d'exigence requiert :

- l'existence d'au moins une API de type web service partageant les données des systèmes mentionnés dans le prérequis de l'exigence « IN 1.1 – Intégration des équipements au réseau Smart » (données de la télémétrie des fluides et de la régulation du chauffage et de la climatisation). Il peut s'agir d'API Terrain ou d'API Centrale ;
- + lister les API qui sont présentes sur le périmètre du réseau Smart défini dans l'exigence « IN 1.1 – Intégration des équipements au réseau Smart ».

Niveau 1 : exposition des données de deux systèmes
Ce niveau d'exigence requiert :

- respect du niveau précédent ;
- + lister un système supplémentaire dont les données sont exposées via une API. Les systèmes doivent être repris parmi la liste des systèmes visés dans le niveau 1, 2 ou 3 de l'exigence « IN 1.1 – Intégration des équipements au réseau Smart ». Ce niveau d'exigence valorise donc l'existence d'une API sur les systèmes mentionnés dans le prérequis de l'exigence IN 1.1 et un autre système.

Niveau 2 : exposition des données de trois systèmes
Ce niveau d'exigence requiert :

- respect du niveau précédent ;
- + lister un système supplémentaire dont les données sont exposées via une API. Les systèmes doivent être repris parmi la liste des systèmes visés dans le niveau 1, 2 ou 3 de l'exigence « Équipements et interfaces – 1.1 Intégration des équipements au réseau Smart ». Ce niveau d'exigence valorise donc l'existence d'une API sur les systèmes mentionnés dans le prérequis de l'exigence IN1.1 et deux autres systèmes.

Niveau 3 : exposition des données de quatre systèmes
Ce niveau d'exigence requiert :

- respect du niveau précédent ;
- + lister un système supplémentaire dont les données sont exposées via une API. Les systèmes doivent être repris parmi la liste des systèmes visés dans le niveau 1, 2 ou 3 de l'exigence « IN 1.1 – Intégration des équipements au réseau Smart ». Ce niveau d'exigence valorise donc l'existence d'une API sur les systèmes mentionnés dans le prérequis de l'exigence IN 1.1 et trois autres systèmes.

IN 2.2 – DOCUMENTATION TECHNIQUE DES API

Il s'agit de faciliter l'utilisation des données collectées sur le bâtiment en mettant à disposition une documentation permettant de connaître les conditions d'accès techniques aux données.

Prérequis : documentation technique
Ce niveau d'exigence demande de fournir la documentation technique. Les API (Application Program Interface) définies dans l'exigence « IN 2.1 – Existence d'API et exposition des données » doivent disposer d'une documentation technique qui est consultable sur un format électronique (exemple : PDF). Les conditions d'accès à cette documentation sont clairement définies et accessibles au propriétaire. La documentation devra déclarer le format dans lequel l'API communique les données (exemples : JSON, XML…).

Niveau 1 : documentation lisible au format numérique
Ce niveau d'exigence demande de fournir une documentation lisible au format numérique, cela implique que la documentation des API définie dans le niveau prérequis de cette exigence doit être consultable sur un outil informatique en lecture/échange automatique de système à système (exemple : Swagger).

IN 2.3 – MODÈLE ÉCONOMIQUE

Il s'agit d'être informé du modèle économique associé à l'exposition des données du bâtiment via leur(s) API.

Les services d'accès aux données doivent renseigner leurs modèles économiques quelle que soit la méthode utilisée (licence perpétuelle, abonnement…). Ces informations doivent permettre au propriétaire du bâtiment de faire un choix éclairé concernant le modèle économique des API.

Il est demandé de préciser le modèle économique de l'accès aux données, les éventuelles options doivent être

prises comptes dans l'analyse des modèles économiques (exemples : accès aux API gratuit, mais licence payante pour l'accès à tout ou partie des données ; gratuité initiale suivi d'un abonnement payant…) :

- en conception, l'objet est d'exprimer un choix sur le modèle économique des services d'accès aux données qui seront mises en œuvre en réalisation ;
- en réalisation, un résumé du modèle économique des services d'accès aux données ;
- en exploitation, analyse des coûts d'exploitation des services d'accès aux données.

IN 2.4 – 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.

IN 3 – Interfaces terrain

IN 3.1 – SYSTÈMES DISPOSANT D'INTERFACES PROTOCOLAIRES

Il s'agit de proposer un large choix de modes de partage de données avec la mise en place d'interfaces protocolaires (voir définition ci-dessous) standards permettant une communication et une interopérabilité entre les systèmes et pouvant être complémentaires à d'autres solutions, comme les API.

Les interfaces protocolaires permettent d'interfacer les équipements de terrain à travers des protocoles ouverts, standardisés, interopérables basés sur les normes de type ISO EN (exemple: EN16484). Ces interfaces protocolaires concernent des protocoles de contrôle commande situés sur la couche terrain.
Les protocoles suivants peuvent être valorisés au titre de cette exigence:

NOM DU PROTOCOLE	NOM DE LA NORME	NOM DE L'ESTAMPILLE / CERTIFICATION	CONDITION D'ACCÈS À LA DONNÉE
BACnet	EN16484-5	Certification BTL des équipements	Fichiers EDE pour base de données supervision.
LonWorks	ISO EN14908	LonMark	Fichier XIF pour description produit, et LNS pour la base de données du site.
KNX	ISO EN14543 et EN13321	KNX™	Fichier KNXPROD pour description produit, et ETS pour la base de données du site, ou ESF pour base de données supervision.
Modbus	---	---	Table d'échange.
EnOcean	EN14543-3-10	EnOcean Alliance	---
Zigbee 6LoWPAN Thread	IEEE 802.15.4	Zigbee Alliance	---
M-Bus	EN13757-2-3	---	---
MQTT	ISO/IEC20922	---	---

D'autres protocoles peuvent être proposés, sous réserve qu'ils justifient de leur conformité aux normes ISO EN et leur certification par un organisme. Les protocoles informatiques de type SNMP ne peuvent pas être valorisés au titre de cette exigence.

Niveau 1: Interface protocolaire sur un système
Ce niveau d'exigence demande la disponibilité d'au moins une interface protocolaire sur un système valorisé au titre des niveaux 1, 2 ou 3 de l'exigence «IN 1.1 – Intégration des équipements au réseau Smart».

Niveau 2: Interface protocolaire sur deux systèmes
Ce niveau d'exigence demande:

- Le respect du niveau précédent;
- + la disponibilité d'au moins une interface protocolaire sur un système supplémentaire valorisé au titre des niveaux 1, 2 ou 3 de l'exigence «IN 1.1 – Intégration des équipements au réseau Smart».

À ce niveau d'exigence, cela valorise donc la disponibilité d'une interface protocolaire sur au moins deux systèmes différents. Le protocole valorisé à ce niveau doit être différent du protocole valorisé au niveau 1.

IN 3.2 API TERRAIN

Il s'agit d'exposer les données ouvertes, standardisées et interopérables sur le réseau Smart. Cette exigence demande que les API Terrain puissent fournir les données suivantes à un format bien défini :

- pour chaque équipement, un dictionnaire des données en précisant :
  - une description de la donnée sous la forme d'un texte court ;
  - l'identification du point à requêter pour accéder à cette donnée ;
  - la donnée qui est communiquée ;
  - l'unité associée à la donnée qui est communiquée ;
- pour chaque équipement, la liste des commandes et états ou plages possibles ;
- retourne l'acquittement de réception d'une commande.

Remarque : la liste des points GTB n'est pas suffisante pour répondre à l'exigence.

Il n'existe pas de catalogue de format de type de données standard interopérables entre les API. Chaque API devra fournir le format du document de « dictionnaire des données » dans un format qui lui est laissé libre. Il pourra par exemple prendre la forme d'un fichier *csv.

Exemple de « dictionnaire des données » :

DESCRIPTION	POINT À REQUÊTER	UNITÉ
Consommation de thermique totale du bâtiment A mesurée au point de livraison de chaleur par le réseau primaire	conso-chaleur-bat-a	kWh
Consommation électrique liée à l'éclairage du lot preneur 1 du bâtiment A	conso-eclairage-lot1-bat-a	kWh
Température de consigne de moyenne du lot preneur 1 du bâtiment A	temp-consigne-lot-1-bat-a- moy	°C

IN 4 – API centrale

IN 4.1 – STRUCTURATION DU MODÈLE DE DONNÉES

L'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. Dans cette exigence, il s'agit de permettre une découverte de l'ensemble des équipements connectés à l'API centrale via le réseau Smart.

Niveau 1a: fonction de découverte des équipements
L'API Centrale doit permettre de récupérer:
- la liste des équipements connectés au réseau Smart et accessibles depuis l'API Centrale (voir exigence «IN 2.1 – Existence d'API et exposition des données»);
- l'identifiant unique de chaque équipement;
- les données liées aux équipements.

L'exigence n'impose pas la manière dont le logiciel de l'API Centrale récupère les éléments cités précédemment, cela peut être réalisé par l'intermédiaire des moyens décrits dans l'exigence «IN 1.1 – Intégration des équipements au réseau Smart».

Remarque: la fonction découverte peut inclure les interfaces avec les bases de données des protocoles des équipements (exemples: LNS pour LonWorks, ETS pour KNX...).

Niveau 1b: fonction de découverte des interfaces des équipements terrains
Cette exigence permet de s'assurer que l'API Centrale peut communiquer avec les données des équipements découverts:
- dans le cas d'API terrain, cette exigence demande que l'API fournisse un annuaire des API disponibles au niveau de tous les systèmes qui lui sont rattachés;
- dans le cas où les données sont récupérées au travers d'interfaces protocolaires, l'API centrale doit posséder les drivers adaptés.

Niveau 1c: fonction de contextualisation en zones dans le bâtiment
L'API Centrale doit permettre de:
- récupérer la liste des équipements présents dans les zones;
- contextualiser les données à la structure physique du site (site, bâtiment, étage, zone, pièce) et l'ontologie associée, avec les imbrications des zones (zone dans les zones) et/ou créer et donner la possibilité d'accéder à travers l'API aux zones logiques (exemples: preneur A, service comptabilité...) du bâtiment et l'ontologie associée.

IN 4.2 – PILOTAGE DES ÉQUIPEMENTS ET ZONES

Il s'agit de permettre à tout service de commander dynamiquement les équipements et zones dans le bâtiment, avec une gestion des droits d'accès adaptée.

Cette exigence demande que l'API Centrale permette de piloter:
- les équipements provenant des systèmes définis dans l'exigence «IN 1.1 – Intégration des équipements au réseau Smart»
- et/ou les zones en envoyant une commande.

Un code d'erreur doit être retourné si cela ne fonctionne pas.

IN 4.3 – BUILDING OPERATING SYSTEM

Il s'agit de faciliter la mise en place et la pérennité des services grâce à une solution unifiée de partage des données. Cette exigence demande la mise en place d'un Building Operating System (BOS), répondant aux points suivants:
- couvre le périmètre de données défini dans les exigences «IN 2.1 – Existence d'API et exposition des données» et «IN 3.1 – Systèmes disposant d'interfaces protocolaires»;
- indexe et caractérise les données partagées;
- structure, qualifie et unifie les données, constituant l'environnement commun des données du projet;
- décrit les fonctionnalités de sécurité appliquées au partage de données avec les services;
- administre les droits d'accès aux données.

Remarques:
- Le BOS est une couche de gestion de données indépendant des autres systèmes.
- Le BOS peut être unique ou ses fonctions peuvent être distribuées sur plusieurs systèmes répondant à l'exigence.
- Pour plus d'informations, vous pouvez consulter le document «Le BIS et le BOS, les outils de la gouvernance des données du bâtiment» (https://bit.ly/BIS-BOS-SBA) de la SBA.

IN 5 – Building Information Modeling (BIM)

IN 5.1 DESCRIPTION DE LA MAQUETTE NUMÉRIQUE

L'objectif est d'avoir une vision de l'infrastructure numérique du bâtiment dans la maquette numérique.

Niveau 1: équipements compris dans la maquette numérique

Ce niveau d'exigence requiert que les éléments suivants soient décrits dans la maquette numérique (*a minima* en niveau LOD200):

- les équipements actifs du réseau Smart (la représentation des contenants n'est pas suffisante);
- les équipements connectés au réseau Smart, c'est à dire les capteurs (exemple: représentation des sondes de température) et actionneurs (exemple: représentation des luminaires) des systèmes visés dans l'exigence « IN 1.1 – Intégration des équipements au réseau Smart »;
- les éléments de connectivité valorisés au titre du sous-thème CO 3 du thème « Connectivité » (GSM, Wi-Fi, géolocalisation, IoT);
- *A minima* les informations de découpage du bâtiment en espaces et en pièces ainsi que la localisation des équipements et écosystèmes communicants dans ces espaces.

Niveau 2: exposition des données

Ce niveau d'exigence requiert:

- le respect du niveau précédent
- + l'existence d'une base de données des éléments non graphiques (*a minima* LOI 300: informations)

IN 5.2 – MAQUETTE DYNAMIQUE

Il s'agit de faciliter l'exploitation du bâtiment en ayant une vision dynamique de la maquette numérique.

Cette exigence demande une liaison entre la description statique de la maquette numérique et les données dynamiques circulant sur le réseau Smart. Concrètement, cela nécessite une interface entre la maquette numérique et un système type BIM exploitation / BOS / Jumeau numérique.

SÉCURITÉ NUMÉRIQUE

Les rédacteurs du présent cadre de référence adressent leur sincères remerciements au club OT cybersécurité du GIMELEC pour leur contribution à la relecture de ce thème de la sécurité numérique et qui ont également travaillé sur des cas d'usages dans le domaine des hôpitaux.

Le déploiement de réseaux basés sur le protocole TCP/IP expose les hôpitaux à **des vulnérabilités liées à la diversité et le nombre des équipements et objets** (terminaux, dispositifs médicaux, capteurs, ...) **qui leurs sont connectés**. Pour augmenter la qualité et la sécurité des soins et améliorer l'expérience patient, les hôpitaux utilisent et prévoient de mettre en service une très grande diversité d'équipements qui vont des moniteurs aux capteurs des systèmes de gestion des bâtiments en passant par les équipements réseaux, les imprimantes ou les téléphones IP.

Bien souvent, ces équipements et objets connectés **partagent les mêmes segments des réseaux installés**. 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 **sécuriser le réseau Smart et les systèmes numériques du Smart Hospital** et à mettre en place un dispositif permettant la **protection des données à caractère personnel**. En mettant les données au cœur des enjeux, le Smart Hospital avec un bâtiment connecté et communicant doit assurer une sécurité numérique efficiente d'un point de vue technique et organisationnel.

Le cadre R2S 4CARE apporte des réponses en prenant en compte ces deux volets :

- **la sécurisation des accès aux systèmes** : l'objectif est de protéger le réseau Smart, les équipements actifs du réseau et les services, via des mécanismes d'authentification, de virtualisation, de surveillance des installations ainsi que de chiffrement des communications.
- **les procédures de sécurité** : la mise en place d'une organisation structurée est indispensable au fonctionnement des exigences techniques. Cela passe par l'élaboration de procédures de sécurité réseau, traitement des incidents, prévention et gestion des risques.

TITRE DE L'EXIGENCE	NIVEAU	POINTS
SE 1 – SYSTÈME DE MANAGEMENT DE LA SÉCURITÉ INFORMATIQUE		
SE 1.1 Management de la sécurité informatique	**Atteint / Non atteint**	-
SE 2 – SÉCURITÉ DES RÉSEAUX ET SYSTÈMES DU BÂTIMENT		
SE 2.1 Mécanismes d'authentification d'accès au réseau Smart	**Prérequis** Fonctions supportées par les switchs d'accès	-
	Niveau 1 Connexions au réseau Smart avec demande d'authentification	2
	Niveau 2 Présence d'une plateforme réseau centralisée	3
SE 2.2 Sécurisation des accès au réseau Smart	**Prérequis** Fonctions supportées par les switchs d'accès	-
	Niveau 1 Connexions nominatives au réseau Smart	2
	Niveau 2 Présence d'une plateforme réseau centralisée	3
SE 2.3 Cloisonnement du réseau smart et routage	**Niveau 1** Étendue du cloisonnement et routage conditionnel	2
	Niveau 2 Fonctions avancées du cloisonnement	4
SE 2.4 Sécurisation de la supervision des systèmes	**Atteint / Non atteint**	3
SE 2.5 Mécanismes de surveillance des trafics	**Niveau 1** Fonctionnalités du pare-feu	2
	Niveau 2 Cartographie des flux	3
SE 3 – PROCÉDURES DE SÉCURITÉ RÉSEAU		
SE 3.1 Traitement des incidents et chaîne d'alerte	**Atteint / Non atteint**	2
SE3.2 Mise à jour et lutte contre l'obsolescence	**Atteint / Non atteint**	3
SE 4 – SÉCURITÉ D'ACCÈS AUX SERVICES		
SE 4.1 Sécurisation de l'accès aux applications	**Niveau 1** Chiffrement au niveau applicatif	2
	Niveau 2 Confiance numérique	3
SE4.2 Prévention et gestion des risques	**Atteint / Non atteint**	3
SE 5 – PROCÉDURES DE SÉCURITÉ RÉSEAUX		
SE 5.1 Suivi des flux et des configurations du réseau Smart	**Atteint / Non atteint**	2
SE 5.2 Traitement des incidents et chaîne d'alerte	**Atteint / Non atteint**	2
SE 5.3 Mises à jour logicielles des équipements et objets connectés	**Atteint / Non atteint**	3
SE.6 - SÉCURITÉ D'ACCÈS AUX SERVICES		
SE 6.1 Sécurisation de l'accès aux applications	**Prérequis** Atteint / Non atteint	2
SE 6.2 Prévention et gestion des risques	**Prérequis** Atteint / Non atteint	3
SE 7 – PROTECTION DES DONNÉES		
SE 7.1 Conformité au règlement général sur la protection des données	**Prérequis** Atteint / Non atteint	-

SE 1 – Système de management de la sécurité informatique

SE 1.1 – MANAGEMENT DE LA SÉCURITÉ INFORMATIQUE

L'hôpital, exploitant du bâtiment, a formalisé dans un document sa Politique de sécurité du système d'information (PSSI). Cette PSSI est alignée avec :

- la PGSSI-S : Politique générale pour la sécurité des systèmes d'information de santé contrôlée par le RSSI au niveau de l'établissement ;
- la directive NIS (Network and Information Security) transposée dans le droit français ;
- le RGPD/Règlement général pour la protection des données personnelles mis en œuvre par le DPO au niveau de l'établissement ;
- les recommandations de l'ANSSI : la cybersécurité des systèmes industriels.

Cet ensemble de documents est désigné comme le corpus documentaire sécurité dans la suite de ce chapitre dédiée à la sécurité.

De même, l'hôpital sous la responsabilité de son DPD/DPO s'assure que les traitements réalisés par les équipements du smart réseau et du bâtiment sont bien inscrits dans le registre des traitements associés à leur étude d'impact dès que ces traitements concernent des données personnelles. Pour minimiser les risques, l'hôpital met en œuvre la pratique du « Privacy by Design » prévue par le règlement du RGPD.

Les procédures mises en place devront :

- inclure le réseau Smart et les systèmes numériques du bâtiment dans le périmètre de la PSSI ;
- inclure dans le registre des traitements du DPD/DPO, tous les traitements portant sur des données personnelles avec les résultats des études d'impact ad-hoc.

Cette recommandation est à niveau unique et vise à s'assurer que la sécurité numérique et la protection des données personnelles sont abordées de manière holistique et unique par l'établissement.

SE 2 – Sécurité des réseaux et systèmes du bâtiment

SE 2.1 – MÉCANISMES D'AUTHENTIFICATION D'ACCÈS AU RÉSEAU SMART

Une part importante des équipements et objets connectés utilisés aujourd'hui dans les hôpitaux n'ont pas été conçus pour faire face aux impératifs de la sécurité numérique et particulièrement aux cyber risques. Pour assurer la sécurité de son réseau et de son système d'information, le Smart Hospital doit maîtriser les équipements et les objets qui s'y connectent, chacun constituant un point d'entrée potentiellement vulnérable.

L'authentification des terminaux et objets connectés est une recommandation pour maîtriser leur connexion aux différents réseaux d'accès, qu'ils soient filaires ou sans fil. Déroger à cette recommandation, avant tout d'ordre organisationnel, fragilise le réseau de l'hôpital et sert ainsi les intérêts d'un potentiel attaquant.

Ainsi, les ports downlink des équipements réseaux supporteront des mécanismes d'authentification des systèmes qui y sont ou souhaitant s'y connecter, en respect des standards internationaux de sécurité réseau en vigueur et les exigences et recommandations du corpus documentaire produit pour la PGSSI-S et l'ANSSI.

Au niveau 1, tous les équipements, objets connectés et utilisateurs souhaitant se connecter au réseau Smart, devront au préalable être authentifiés avant toute ouverture de session réseau.

L'usage de certificats est obligatoire pour les accès distants au réseau Smart. *A minima*, les mots de passe seront hashés obligatoirement. Tous les ports inutilisés des switches ou sur lesquels aucune session réseau n'est active, devront être logiquement fermés (sauf exceptions argumentées).

Au niveau 2, l'ajout d'une plateforme d'authentification AAA (Authentification, Authorization and Accounting) de type RADIUS (Remote Authentication Dial-In User Service) permet de centraliser la gestion des accès au réseau Smart qu'ils se fassent localement ou à distance. Les identifiants des utilisateurs de la plateforme AAA pourront être corrélés avec ceux des plateformes de contrôle d'accès au niveau applicatif des systèmes, afin de leur éviter des authentifications répétées (authentification unique, ou SSO pour Single Sign-On).

L'usage d'un mécanisme de vérification en deux étapes est obligatoire pour les accès distants au réseau Smart.

Remarque: l'authentification est une phase qui consiste à contrôler la licéité d'un utilisateur et/ou d'un équipement communicant avant toute intégration sur le réseau Smart ou dans un VLAN et avant attribution d'une adresse IP.

Prérequis: fonctions supportées par les switchs d'accès
Support par les switchs d'accès des fonctions:
- support des ACL (Access Control List);
- IEEE 802.1X en mode MAC-based et User-based, en relation avec une ACL ou une plateforme d'authentification AAA (Authentication, Autorization and Accounting).

Niveau 1: connexions au réseau Smart avec demande d'authentification
Ce niveau d'exigence requiert:
- le respect du Prérequis;
- + la présence d'un moyen sécurisé pour assurer les connexions nominatives au réseau Smart depuis d'autres réseaux (exemple: Internet). Ce moyen sécurisé assure l'authentification des utilisateurs et des équipements et des objets connectés distants et locaux, ainsi que le chiffrement des données.

Niveau 2: présence d'une plateforme réseau centralisée
Ce niveau de recommandation permet une facilité de gestion de la sécurité d'accès au réseau Smart, rendue possible par l'exploitation d'une plateforme d'authentification centralisée.

Ce niveau d'exigence requiert:
- le respect des niveaux précédents;
- + la présence d'une plateforme réseau centralisée pour l'authentification, l'autorisation, et la traçabilité (AAA, exemple: RADIUS (Remote Authentication Dial-In User Service) permettant la mise en œuvre des fonctions détaillées dans la description de la recommandation (gestion des identifiants, mécanisme de vérification...).

SE 2.2 – SÉCURISATION DES ACCÈS AU RÉSEAU SMART

Il s'agit de mettre en place un contrôle des accès qui prévient les intrusions malveillantes et apporte une sécurisation des données circulant sur le réseau Smart. Le prére-

quis apporte les éléments de sécurisation minimale des switchs d'accès. Les niveaux suivants valorisent une sécurisation accrue des accès distants au réseau Smart ainsi qu'une gestion simplifiée et plus efficace des droits et autorisations.

Prérequis : fonctions supportées par les switchs d'accès
Support par les switchs d'accès des fonctions suivantes :
- administrable (exemple : disposant d'une interface de paramétrage) ;
- ACL (Access Control List) ;
- IEEE 802.1X.

Niveau 1 : connexions nominatives au réseau Smart
Ce niveau d'exigence requiert :
- le respect du Prérequis ;
- + la présence d'un moyen sécurisé (type VPN) pour assurer les connexions des utilisateurs, nominatives et chiffrées au réseau Smart depuis d'autres réseaux (exemple : Internet).

Remarque : l'atteinte de cette exigence ne permet pas de s'affranchir des autres moyens de sécurité prévus pour d'autres exigences du référentiel.

Niveau 2 : présence d'une plateforme réseau centralisée
Ce niveau d'exigence permet une facilité de gestion de la sécurité d'accès au réseau Smart, rendue possible par l'exploitation d'une plateforme d'authentification centralisée.

Ce niveau d'exigence requiert :
- le respect des niveaux précédents ;
- + l'utilisation d'une plateforme réseau centralisée pour l'authentification, l'autorisation, et la traçabilité (AAA, exemple : RADIUS (Remote Authentication Dial-In User Service) permettant la mise en œuvre des fonctions suivantes : gestion des identifiants, authentification unique, mécanisme de vérification… Cette plateforme doit être compatible avec tous les équipements connectés au réseau Smart et ne doit pas se restreindre à une famille d'équipements ou un VLAN spécifique.

Remarque : le référentiel n'est pas prescriptif sur le protocole à mettre en place, si un protocole différent est choisi il devra permettre les mêmes fonctionnalités que mentionnées (authentification, autorisation, traçabilité, gestion identifiants, mécanisme de vérification).

SE 2.3 – CLOISONNEMENT DU RÉSEAU SMART ET ROUTAGE

L'objectif est de faciliter la mise en place d'équipements hétérogènes sur le réseau Smart et préserver son unicité en déployant plusieurs réseaux logiques au sein d'un même réseau physique et sa sécurité en permettant par exemple de limiter l'accès à certains équipements à des personnes autorisées.
Cette exigence va dans le prolongement du niveau prérequis de l'exigence « RE 1.1 – Caractéristiques et capacités d'extension du réseau Smart » qui demande notamment que la fonction de routage soit disponible, alors que cette exigence demande à ce qu'elle soit activée.

Niveau 1 : étendue du cloisonnement et routage conditionnel
Ce niveau d'exigence requiert :
- la mise en place d'un cloisonnement (exemple : VLAN, Virtual Local Area Network) satisfaisant l'ensemble des critères suivants :
  - chaque écosystème matériel et objet connecté d'un même usage (exemples : GTB, régulation des fonctions de confort des utilisateurs, systèmes de sûreté…) disposera de son ou ses propres réseaux virtuels ;
  - isolement des systèmes accessibles à des utilisateurs différents (exemple : entre différents étages ou lots immobiliers).;
  - isolement des objets connectés ;
  - les serveurs rattachés sur le réseau Smart sont isolés des terminaux ;
  - si le réseau Smart est physiquement commun avec le système d'information d'un utilisateur comme le propriétaire occupant du bien immobilier, les systèmes informatiques de l'occupant seront isolés des équipements bâtimentaires.
- la mise en place d'un routage inter-VLAN, basé sur au moins un des critères suivants :
  - le sens d'initiation de l'échange de données ;
  - le réseau de provenance et/ou de destination (VLAN, LAN, WAN) ;
  - l'adresse IP de l'émetteur et/ou du destinataire ;
  - le protocole utilisé ;
  - toute autre condition plus sélective que les critères précédents, un routage systématique sans critère défini ne permet pas de valider l'exigence.

Niveau 2 : fonctions avancées de cloisonnement
Ce niveau d'exigence requiert :
- le respect du niveau précédent ;
- + pour les équipements permanents du réseau Smart (exemples : régulateur GTB, caméra de surveillance…) : l'affectation dynamique des VLAN suivant l'équipement connecté, préférentiellement avec une authentification par identifiant et mot de passe ou certificat (exemple 802.1X), ou à défaut en cas d'incompatibilité sur la base de l'adresse MAC de l'équipement.
- + pour les autres équipements (exemple : WiFi public) : le traitement de la connexion sur le réseau Smart d'un équipement non enregistré en lui donnant des accès limités (qui doivent alors être déterminés, exemple : accès à Internet uniquement, VLAN de quarantaine), à défaut la connexion peut être rejetée.

SE2.4 – SÉCURISATION DE LA SUPERVISION DES SYSTÈMES

Il s'agit d'apporter un niveau de sécurité à la supervision des équipements connectés au réseau Smart, et ainsi favoriser la robustesse du service assuré.

Cette exigence porte sur la mise en place et l'activation de logiciels de sécurité sur la couche supervision des équipements connectés au réseau Smart (exemples : supervision de la GTB, de la sûreté, des équipements actifs du réseau Smart). Elle concerne les serveurs et clients (exemple : poste d'exploitation) connectés localement sur le réseau Smart.

Chaque serveur ou client connecté localement au réseau Smart est équipé d'une solution logicielle de pare-feu et d'antivirus activée et paramétrée spécifiquement pour répondre aux besoins de ces équipements. Ces logiciels peuvent être intégrés au système d'exploitation, ou installés séparément.

Remarques :

- cette exigence ne porte pas sur les équipements de terrain (exemples : automates, régulateurs… et leurs éventuels panneaux de contrôle locaux), bien que ceux-ci peuvent également bénéficier de tels logiciels de sécurité.
- l'atteinte de cette exigence ne permet pas de s'affranchir des autres moyens de sécurité prévus pour d'autres exigences du référentiel.

SE2.5 – MÉCANISMES DE SURVEILLANCE DES TRAFICS

L'objectif est d'apporter une protection supplémentaire au réseau Smart par une sécurisation de son interface avec des réseaux externes comme Internet. Cette exigence valorise le filtrage et l'analyse des flux de données ainsi que la conservation d'historiques facilitant le rétablissement du service après une éventuelle intrusion.

Niveau 1 : fonctionnalités du pare-feu

Le pare-feu doit disposer de fonctionnalités de sécurité comme un antivirus ou un système de prévention d'intrusion réseau (NIPS : Network Intrusion Prevention System). Au moins une de ces deux fonctionnalités doit être activée. Lorsque ces fonctionnalités nécessitent des licences, celles-ci doivent être impérativement activées.

Le pare-feu doit permettre de :

- surveiller les flux entrants et sortants du réseau Smart vers d'autres réseaux (Internet, interconnexions locales éventuelles avec d'autres LAN comme les réseaux d'occupants ou celui de la sûreté, s'ils ne sont pas mutualisé avec le réseau Smart) ;
- journaliser les traces des flux acceptés ou refusés.

Remarque : l'atteinte de ce niveau n'impose pas de suppression automatique des traces, mais une politique en ce sens peut être mise en place, par exemple pour respecter la réglementation en matière de protection des données personnelles.

Niveau 2 : cartographie des flux

Ce niveau d'exigence requiert :

- le respect du niveau précédent ;
- + une cartographie des flux franchissant le pare-feu est réalisée, et le pare-feu est paramétré pour ne laisser passer que les flux attendus, *a minima* sur des critères de couche réseau ou transport du modèle OSI (exemples : adresses IP source ou destination, port TCP…).

SE 3 – Procédures de sécurité réseau

SE 3.1 – TRAITEMENT DES INCIDENTS ET CHAÎNE D'ALERTE

L'hôpital, exploitant du bâtiment connecté et communicant dispose d'une organisation et de procédures pour traiter les incidents liés au réseau Smart, aux systèmes techniques qui y sont connectés, et aux services qu'ils délivrent.

La recommandation demande l'existence d'une organisation et d'une procédure de traitement des incidents : prévoir les procédures de collecte des informations au travers des journaux d'alarmes et d'événements, les procédures d'alertes, la gestion et la résolution des incidents.

Ces procédures sont documentées dans le SMSI (Système de management de la sécurité informatique) du Smart Hospital.

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

L'hôpital, exploitant du bâtiment et/ou le tiers qu'il aura désigné dispose de procédures formalisées de mise à jour des équipements et logiciels des systèmes du réseau Smart.

La recommandation demande l'existence de procédures formalisées de mise à jour des équipements et logiciels des systèmes du réseau Smart. Ces mises à jour peuvent porter sur des micrologiciels des équipements, des logiciels, des licences, des pilotes, des systèmes d'exploitation, politique de sécurité, définition antivirus…

Ces procédures sont documentées dans le SMSI (Système de management de la sécurité informatique) du Smart Hospital.

Maintenir le niveau de sécurité du réseau Smart par l'application des dernières mises à jour. En exploitation, permettre également un maintien en conditions opérationnelles du réseau Smart, contribuant ainsi à la sécurité des systèmes qui y sont connectés.

Les équipements constituant le réseau Smart doivent être mis à jour. En outre, le propriétaire du bâtiment et/ou l'exploitant qu'il aura désigné dispose d'un guide formalisé de mise à jour des équipements et logiciels des systèmes du réseau Smart.

Ces mises à jour doivent porter :

- sur les switchs du réseau Smart : micrologiciels ;
- sur les pares-feux : licences, politique de sécurité, micrologiciels ;
- sur les serveurs et clients locaux : micrologiciels, système d'exploitation, éventuelle couche de virtualisation, pilotes, définition antivirus ;
- sur les logiciels métiers (exemples : supervision des équipements ou systèmes connectés au réseau Smart, tel que la GTB, administration du réseau Smart) : version du logiciel, licence.

En réalisation, les systèmes doivent être livrés dans la version la plus récente proposée par le fabricant ou l'éditeur de chaque système. Des versions antérieures peuvent être acceptées sous condition que ce soit prévu contractuellement (exemple : autorisation de ne pas prendre en compte les mises à jour majeures récentes apportant de nouvelles fonctionnalités, et dont l'application serait déstabilisante pour le projet).

En exploitation, tous les équipements ou logiciels obsolètes et non supportés par leurs fabricants ou éditeurs devront être renouvelés de façon à disposer sur le réseau Smart d'équipements et logiciels à jour et fiables. Les équipements ou logiciels obsolètes peuvent être conservés uniquement si les risques qu'ils génèrent sont identifiés et pris en compte dans le SMSI.

Remarque : cette exigence s'intéresse uniquement au réseau Smart, par conséquent la mise à jour des équipements terrains n'est pas traitée dans cette exigence, même si cela peut contribuer à renforcer la sécurité de l'ensemble du réseau Smart.

SE 4 – Sécurité d'accès aux services

SE 4.1 – 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.

Niveau 1: chiffrement au niveau applicatif
Les services numériques et applications accessibles aux différents usagers du bâtiment sont dotés d'une communication sécurisée par des mécanismes de chiffrement au niveau applicatif.
Cette exigence demande que les API exposées sur le réseau Smart et valorisées au titre de l'exigence « IN 2.1 Existence d'API et exposition des données » soient accessibles et sécurisées de bout en bout (exemple : API web service accessible par le client en https).

Niveau 2: confiance numérique
Le niveau d'exigence requiert :

- le respect du niveau précédent
- + les certificats numériques utilisés pour sécuriser la communication avec les API sont signés par un tiers de confiance. Le tiers de confiance peut être interne, avec la mise en place d'une gestion des certificats sur le réseau Smart, ou externe avec une autorité de certification reconnue.

Les protocoles de communication encapsulés sur IP (exemples : LON, BACnet…) ne sont pas concernés par cette exigence, bien qu'il puisse être bénéfique d'utiliser leurs moyens de sécurisation lorsqu'ils existent.

L'atteinte de cette exigence ne permet pas de s'affranchir des autres moyens de sécurité prévus pour d'autres exigences du référentiel (exemple : comme le VPN qui n'est pas du chiffrement de bout en bout).

La valorisation de la signature des certificats au niveau 2 de l'exigence peut nécessiter une base de temps commune à l'ensemble des équipements, des services et de l'autorité de certification. Ce point ne fait pas partie de l'exigence du référentiel, mais sa prise en compte est recommandée.

SE 4.2 – 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.

Le propriétaire du bâtiment et/ou l'exploitant qu'il aura désigné 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 :
- la gestion des risques pour l'accès aux services du bâtiment sur le réseau Smart : la procédure doit inclure *a minima* une identification des risques cybers, leurs conséquences et les moyens de contenir les risques ou de traiter les incidents.

SE5 – Procédures de sécurité réseau

SE 5.1 – SUIVI DES FLUX ET DES CONFIGURATIONS DU RÉSEAU SMART

Une cartographie du réseau Smart est réalisée pour déterminer les flux attendus. Une analyse du trafic permet ensuite de vérifier que le trafic sur le réseau Smart correspond bien à celui attendu, et ainsi prévenir des dysfonctionnements ou des intrusions. Les configurations du réseau sont également contrôlées.

Cette recommandation de niveau unique demande qu'une cartographie du réseau Smart soit réalisée, ainsi que la présence d'outils de suivi des configurations, des architectures et des flux sur le réseau Smart.

La plateforme d'administration du réseau Smart dispose :
- d'une interface graphique de cartographie du réseau ;
- d'un outil répertoriant les historiques de modification de configuration logique du réseau ;
- d'un outil de suivi des charges de trafic des réseaux logiques.

Une procédure existe pour prendre en compte les flux constatés sur le réseau Smart mais non identifiés dans la cartographie.

SE 5.2 – TRAITEMENT DES INCIDENTS ET CHAÎNE D'ALERTE

L'hôpital, exploitant du bâtiment connecté et communicant dispose d'une organisation et de procédures pour traiter les incidents liés au réseau Smart, aux systèmes techniques qui y sont connectés, et aux services qu'ils délivrent.

La recommandation demande l'existence d'une organisation et d'une procédure de traitement des incidents : prévoir les procédures de collecte des informations au travers des journaux d'alarmes et d'événements, les procédures d'alertes, la gestion et la résolution des incidents.

Ces procédures sont documentées dans le SMSI (Système de management de la sécurité informatique) du Smart Hospital).

SE 5.3 – MISES À JOUR LOGICIELLES DES ÉQUIPEMENTS ET DES OBJETS CONNECTÉS

L'hôpital, exploitant du bâtiment et/ou le tiers qu'il aura désigné dispose de procédures formalisées de mise à jour des équipements et logiciels des systèmes du réseau Smart.

La recommandation demande l'existence de procédures formalisées de mise à jour des équipements et logiciels des systèmes du réseau Smart. Ces mises à jour peuvent porter sur des micrologiciels des équipements, des logiciels, des licences, des pilotes, des systèmes d'exploitation, politique de sécurité, définition antivirus…

Ces procédures sont documentées dans le SMSI (Système de management de la sécurité informatique) du Smart Hospital.

SE 6 – Sécurité d'accès aux services

SE 6.1 – SÉCURISATION DE L'ACCÈS AUX APPLICATIONS

Les services numériques et applications accessibles aux différents usagers du bâtiment sont dotés d'une communication sécurisée. Pour cela, le mécanisme de communication sécurisée doit intégrer l'utilisation de pare-feu et de mécanismes de chiffrement.

Cette recommandation de niveau unique et au statut Prérequis demande que les API exposées sur réseau Smart soient accessibles et sécurisées de bout en bout (radio et filaire). Cette disposition permet aux seules personnes qui communiquent de lire les messages échangés, sans nécessité d'ajouter des mécanismes de sécurité intermédiaires entre ces personnes.

Remarque : l'atteinte de cette recommandation ne permet pas de s'affranchir des autres moyens de sécurité prévus pour d'autres recommandations du cadre de référence.

SE 6.2 – PRÉVENTION ET GESTION DES RISQUES

Le propriétaire du bâtiment et/ou l'exploitant qu'il aura désigné doit avoir mis en place une procédure de gestion et prévention des risques intégrant :

- la gestion des droits d'accès utilisateurs et programmes ;
- les procédures de gestion des risques pour l'accès aux services du bâtiment sur le réseau Smart.

Ces procédures sont documentées dans le SMSI (Système de management de la sécurité informatique) du Smart Hospital).

Cette recommandation de niveau unique et au statut de Prérequis demande l'existence d'un document justifiant la prise en compte et la gestion des risques.

SE 7 – Protection des données

SE 7.1 – 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 propriétaire du bâtiment 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.

Cette exigence de niveau unique et au statut de Prérequis demande l'existence d'un document justifiant le respect de la législation sur la protection des données personnelles.

En réalisation, il est demandé de débuter le renseignement d'un registre de traitement des données, ou de la cartographie des données. Pour le registre de traitement des données, une version simplifiée est disponible sur le site de la CNIL.

MANAGEMENT RESPONSABLE

Le thème « Management responsable » comprend plusieurs aspects : la mise en place d'une gouvernance du projet, le commissionnement, un cadre de contractualisation, une réflexion sur la propriété immobilière ainsi que sur les enjeux environnementaux du bâtiment connecté et communicant, afin de combiner la transition environnementale et numérique.

Ce thème est un outil de gestion de projet qui permet de répondre aux enjeux de gouvernance posés par l'arrivée du numérique dans le bâtiment. Ces enjeux peuvent être synthétisés en trois volets :

- la gouvernance du projet comprend des éléments relatifs à la recette et l'administration du réseau Smart ainsi qu'à des recommandations concernant la bonne gestion du projet ;
- la propriété des données et la contractualisation des services : l'objectif est de poser la réflexion sur la propriété des données et de l'infrastructure du réseau Smart. Un cadre de contractualisation sur les conditions d'accès aux services est également présent ;
- les qualités environnementales : comprenant des recommandations liées au bilan environnemental des équipements électroniques présents sur le bâtiment par l'intermédiaire des fiches PEP, ainsi que la mesure des champs électromagnétique

TITRE DE L'EXIGENCE	NIVEAU	POINTS
MA 1 – GOUVERNANCE DU PROJET		
MA 1.1 – Schéma directeur d'intégration et de gestion des données et de la cybersécurité	**Prérequis** Atteint / Non atteint	–
MA 1.2 Informations Smart dans les pièces contractuelles	**Niveau 1** Cohérence des lots	1
	Niveau 2 Présence d'un Lot Smart	2
MA 1.3 Administration du réseau Smart et des systèmes du bâtiment	**Niveau 1** Administration du réseau Smart	2
	Niveau 2 Administration du système d'information du bâtiment	3
MA 1.4 Commissionnement Smart	**Niveau 1 a** Recette du câblage du réseau Smart	2
	Niveau 1 b Paramétrage des équipements actifs du réseau Smart	1
	Niveau 1 c Protocoles de tests de sécurité sur le réseau Smart	1
	Niveau 1 d Protocole de tests des API	1
MA 2 – PROPRIÉTÉ IMMOBILIÈRE		
MA 2.1 Propriété et capacité de cession du Réseau Smart	**Niveau 1** Propriété du réseau Smart	2
	Niveau 2 Capacité de cession du réseau Smart	3
MA 2.2 Localisation et portabilité des données	**Niveau 1 a** Localisation des données	2
	Niveau 1 b Portabilité des données	2
MA 3 – CADRE DE CONTRACTUALISATION DES SERVICES		
MA 3.1 Contrats de services (SLA) ou de maintenance avec les fournisseurs	**Niveau 1 a** Contrats de services ou de maintenance sur les équipements actifs	2
	Niveau 1 b Contrats de services ou de maintenance sur les API	1
MA4 – QUALITÉS ENVIRONNEMENTALES ET SANITAIRES		
MA 4.1 Détermination du champ électromagnétique et dispositions prises	**Prérequis** Atteint / Non atteint	–
MA 4.2 Informations et étude environnementale	**Niveau 1** Informations environnementales simples	2
	Niveau 2 Informations environnementales approfondies	3
	Niveau 3 Étude environnementale	4
MA 4.3 Efficience énergétique du Réseau Smart	**Atteint / Non atteint**	4
MA 5 – SYSTÈME DE MANAGEMENT		
MA 5.1 Management de projet	**Prérequis** Atteint/ non atteint	–
MA 5.2 Guide de développement des services	**Atteint / Non atteint**	3

MA 1 – Gouvernance du projet

MA 1.1 – SCHÉMA DIRECTEUR D'INTÉGRATION ET DE GESTION DES DONNÉES ET DE LA CYBERSÉCURITÉ

Un schéma directeur est défini, rédigé, et comporte :

- la liste des données dont l'exploitation est nécessaire ;
- la finalité du traitement cible de ces données ;
- leur modalité de stockage et de sauvegarde, les règles d'effacement ;
- leur besoin de sécurisation en transit et en stockage ;
- la politique d'accès à ces données ;
- le référentiel structure architectural.

Le schéma directeur devra aussi comporter la stratégie de gestion de la cybersécurité (spécificité, convergence). Le chef de projet peut s'appuyer sur la méthode EBIOS (Expression des besoins et identification des objectifs de sécurité), outil complet de gestion des risques SSI conforme au RGS et aux dernières normes ISO 27001, 27005 et 31000. Elle permet d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information (SSI).

Pour les données à caractère personnel ou sensible, la conformité du schéma directeur à la réglementation, en particulier RGPD et l'agrément HDS. La finalité du traitement (but précis, légal et légitime), la proportionnalité et la pertinence de la collecte (minimisation des données collectées aux fins du traitement), la durée de conservation, la sécurité et confidentialité ainsi que les droits des personnes relatifs à ces données doivent être documentés.

MA 1.2 – INFORMATIONS SMART DANS LES PIÈCES CONTRACTUELLES

Cette recommandation ne s'applique pas à la phase Exploitation.

Les informations liées à la mise en œuvre du bâtiment communicant 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.

Cette recommandation demande la présence d'informations et de spécifications sur les éléments dits Smart, c'est-à-dire présentes dans les cahiers des charges techniques pour les équipements, les infrastructures et les services conformes aux recommandations R2S 4CARE.

Cette infrastructure et son périmètre doivent faire l'objet d'un cahier des charges pour un lot Smart, déterminé par le maître d'ouvrage. Il s'agit de traiter avec cohérence des systèmes hétérogènes et multitechnologiques, et de déterminer les limites de prestations des fournisseurs.

L'objectif de cette recommandation est de s'assurer de la cohérence de la mise en place d'une infrastructure smart par de multiples acteurs en créant un cadre contractuel répondant aux attentes du maître d'ouvrage et favorisant la labellisation R2S.

Niveau 1 : cohérence des lots

Présence d'un document contractuel (exemples : CCTP Lot 0, CCTC…) qui apporte une cohérence transversale à l'ensemble des lots concernant la mise en œuvre du R2S. Concrètement, le document doit indiquer les exigences techniques relatives au référentiel s'appliquant aux lots (exemples : préciser les lots définis comme faisant partie du périmètre du réseau Smart, les interfaces permettant d'exposer les données sur le réseau Smart, la propriété des données…).

Niveau 2 : présence d'un lot Smart

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…

L'utilisation du terme « lot Smart » est recommandée, cependant une autre dénomination peut être employée si elle correspond à ce qui est demandé dans l'exigence.

MA 1.3 – ADMINISTRATION DU RÉSEAU SMART

L'hôpital est un OSE (Opérateur de services essentiels) et potentiellement un OIV (Opérateur d'importance vital). Afin de maintenir dans le temps le niveau de sécurité et de service de l'ensemble des systèmes communicants du Smart Hospital, l'administration du réseau Smart, de ses

équipements actifs, des données et des API est à gérer par une entité nommée et unique. L'administrateur met en œuvre les instructions de la PSSI (Politique de sécurité des systèmes d'information) de l'institution.

Le référentiel n'est pas prescripteur sur l'entité qui doit être nommée: cela peut être un Facility Manager, la Direction des systèmes d'information (DSI), une Entreprise de service numérique (ESN), un opérateur...

MA 1.4 – ADMINISTRATION DU RÉSEAU SMART ET DES SYSTÈMES DU BÂTIMENT

L'objectif est de maintenir en condition opérationnelle le réseau grâce à une entité chargée d'administrer le réseau Smart et le système d'information du bâtiment.

Dans les deux niveaux de cette exigence il est demandé qu'une entité soit nommée pour administrer le réseau Smart en 1er niveau et le système d'information du bâtiment en niveau 2.

Le référentiel n'est pas prescripteur sur l'entité qui doit être nommée: cela peut être un Facility Manager, la Direction des systèmes d'information (DSI) d'un locataire, une Entreprise de service numérique (ESN), un opérateur...

En réalisation, l'exigence demande qu'une entité soit nommée pour l'administration du périmètre du niveau visé, et que la transition vers la phase exploitation soit organisée (exemple: formation).

Niveau 1: administration du réseau Smart
Une entité doit être nommée pour administrer les équipements actifs du réseau Smart.

Niveau 2: administration du système d'information du bâtiment
L'exigence nécessite:
- le respect du niveau précédent;
- + une entité doit être nommée afin d'administrer le système d'information du bâtiment. Par système d'information, il est entendu: les applications, l'API Centrale, les interfaces (API...) et les données du bâtiment.

MA 1.5 – COMMISSIONNEMENT DU RÉSEAU SMART

Le commissionnement est défini comme l'ensemble des tâches pour mener à terme une installation neuve afin qu'elle atteigne le niveau attendu des performances contractuelles et pour créer les conditions pour les maintenir» (Mémento du commissionnement, 2008, COSTIC, ADEME, FFB).

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.
Pour conduire une telle démarche, il est nécessaire d'assurer, tout au long du projet, la cohérence entre les différentes étapes du projet et la cohésion entre tous les intervenants (maîtrise d'ouvrage, acteur missionné pour le commissionnement, maîtrise d'œuvre, entreprises d'installation, entreprises en charge de l'exploitation...).
Le commissionnement devra être réalisé sous la responsabilité d'un agent de commissionnement clairement désigné (personne physique). L'acteur qui assure la fonction d'agent de commissionnement peut être externe au projet (en Assistance à maîtrise d'ouvrage, AMO) ou intégré à la maîtrise d'œuvre en mission complémentaire. Dans ce cas, les tâches de commissionnement et de maîtrise d'œuvre se doivent d'être menées par des collaborateurs distincts au sein de la structure.

Niveau 1 a: recette du câblage du réseau Smart
La recette du câblage du réseau Smart est vérifiée. La recette du câblage (cuivre et fibre optique) peut être réalisée en s'appuyant sur la norme ISO/CEI 11801, en mettant en place de la réflectométrie ou photométrie pour fibre optique.

Niveau 1 b: paramétrage des équipements actifs du réseau Smart
Ce niveau d'exigence demande la conformité au cahier des charges et la vérification de l'analyse fonctionnelle du paramétrage des équipements actifs du réseau Smart. Le paramétrage doit permettre de vérifier toutes les exigences visées sur le thème «Architecture réseau», exemples: «RE 2.2 – Détection d'anomalies et protection du réseau Smart», «RE 3.2 – Priorisation de service des réseaux» ...

Niveau 1 c: protocoles de tests de sécurité sur le réseau Smart
Ce niveau d'exigence demande que le niveau de sécurité soit éprouvé avec la rédaction et la mise en œuvre d'un protocole de test de sécurité sur le réseau Smart et les équipements qui y sont connectés. Ce test est effectué par un agent de commissionnement tel que défini dans la description de l'exigence. Les protocoles de tests de sécurité doivent permettre de vérifier toutes les exigences visées sur le thème «Sécurité numérique. Exemples: «SE 1.1 – Sécurisation des accès au réseau Smart», «SE 1.2 – Cloisonnement du réseau Smart et routage»...

Niveau 1 d: protocoles de tests des API
Ce niveau d'exigence demande que l'exposition des API sur le réseau Smart soit éprouvée avec la rédaction et la mise en œuvre d'un protocole de test des API mises en place. Les protocoles de tests des API doivent permettre de vérifier toutes les exigences visées sur le thème «Équipements et interfaces». Exemples: «IN 2.1 – Existence d'API et exposition des données», «IN 4.2 – Pilotage des équipements»...

MA 2 – Propriété immobilière et responsabilités

MA 2.1 – PROPRIÉTÉ ET CAPACITÉ DE CESSION DU RÉSEAU SMART

Il s'agit de pérenniser l'infrastructure numérique et la connaissance du bâtiment dans le temps en intégrant le réseau Smart dans le périmètre de la propriété immobilière. L'objectif est d'avoir une valeur numérique du bâtiment en conservant le réseau Smart dans le bâtiment malgré les évolutions de ce dernier (changements de propriétaires, locataires…).

Niveau 1: propriété du réseau Smart
Le câblage et les équipements actifs du réseau Smart doivent être intégrés dans le périmètre de la propriété immobilière.

Niveau 2: capacité de cession du réseau Smart
Ce niveau d'exigence requiert:

- le respect du niveau précédent;
- + La capacité de cession du réseau Smart est anticipée, de telle façon que la transmission de propriété soit sans impact pour le fonctionnement du réseau Smart et les systèmes qui y sont connectés. La capacité et les conditions de cession ou de transfert des licences de fonctionnement ainsi que des contrats de maintien en conditions opérationnelles et des contrats liés à l'accès Internet du réseau Smart doivent être connus. Dans le cas où la cession concerne également des services communs à d'autres bâtiments et hébergés dans le Cloud (exemples: administration des équipements actifs, BOS…), la cession des fonctionnalités liées au bâtiment doit être réalisable sans remise en cause du contrat global.

MA 2.2 – PROPRIÉTÉ DES DONNÉES

La propriété des données issues des équipements reliés au réseau Smart doit être définie. Il s'agit aussi bien des données générées que celles stockées sur des équipements connectés au réseau Smart.

La cadre de référence R2S 4CARE porte l'attention sur les données issues des équipements servants aux fonctions de pilotage du bâtiment (capteurs, actionneurs, automates, …) ainsi que les données issues des remontées d'informations des écosystèmes matériels servant aux fonctions communes, telles que signalisation d'alarme, de panne ou de dysfonctionnement, images de vidéosurveillance, géolocalisation, etc.

Ces données techniques s'ajoutent aux données gérées par l'institution et doivent bénéficier de la même protection et du même niveau de conformité réglementaire vis-à-vis des référentiels opposables (PSSI-s, cadre d'interopérabilité, RGPD,…).

MA 2.3 – LOCALISATION ET PORTABILITÉ DES DONNÉES

L'objectif de cette recommandation est de contribuer à la confiance numérique en identifiant la localisation géographique des données du bâtiment et en leur donnant une valeur d'usage qui garantit leur pérennité d'utilisation.

Niveau 1 a: localisation des données
La localisation des données mises à disposition via les API évaluées à travers l'exigence «IN 2.1 – Existence d'API et exposition des données» est précisée (exemples: dans un équipement de terrain, sur un serveur connecté localement au réseau Smart, dans un centre de données situé en France ou Europe, avec une gestion par le propriétaire, un équipementier, un prestataire de services…). Ce niveau concerne les données stockées en local ou sur le Cloud.

Niveau 1 b: portabilité des données
La portabilité des données désigne la possibilité de récupérer des données d'un système dans un format lisible en vue de les réutiliser facilement sur un autre système.
La portabilité des données mises à disposition via les API évaluées à travers l'exigence «IN2.1 – Existence d'API et exposition des données» est précisée. Ce niveau concerne uniquement la/les API centrale(s).

MA 3 – Cadre de contractualisation des services

MA 3.1 – CONTRATS DE SERVICES (SLA) OU DE MAINTENANCE AVEC LES FOURNISSEURS

L'objectif est d'assurer une pérennité de fonctionnement du réseau Smart et des API en définissant les exigences associées à leur maintien en conditions opérationnelles.

Niveau 1 a: contrats de services ou de maintenance sur les équipements actifs

Pour rappel, les équipements actifs comprennent les éléments suivants: équipements actifs centraux du réseau Smart + switchs du réseau Smart comprenant les switchs d'accès. Les équipements actifs centraux du réseau Smart comprennent les éléments suivants: cœurs de réseau, routeurs, pare-feu, équipements d'interface avec les réseaux opérateurs de télécommunication.

Ce niveau d'exigence demande l'existence de contrat(s) de services SLA (Service-Level Agreement) ou un contrat de maintenance sur les équipements actifs du réseau Smart. Ces contrats doivent comporter des éléments de garantie sur:

- la durée de la garantie et du support;
- le niveau de service (périmètre, durée de résolution des problèmes et moyens mis en œuvre);
- le type d'engagement (moyens ou résultats);
- les services inclus dans la garantie et services complémentaires payants.

Niveau 1 b: contrats de services ou de maintenance sur les API

Ce niveau d'exigence demande l'existence de contrat(s) de services SLA ou de maintenance sur les API évaluées à travers l'exigence «IN2.1 – Existence d'API et exposition des données». Ces contrats doivent comporter des éléments de garantie sur:

- les conditions de maintenance prédictive, curative et évolutive;
- les conditions de support utilisateur et administrateur.

Remarque: les contrats de service ou de maintenance peuvent être établis avec des prestataires comme un intégrateur ou un éditeur de logiciel, ou un mainteneur multi-services.

MA 4 – Qualités environnementales

MA 4.1 – DÉTERMINATION DU CHAMP ÉLECTROMAGNÉTIQUE ET DISPOSITIONS PRISES

Cette recommandation s'applique uniquement à la phase Exploitation.

Issue de la directive 2013/35/UE du Parlement européen et du Conseil du 26 juin 2013 concernant les prescriptions minimales de sécurité et de santé relatives à l'exposition des travailleurs aux risques dus aux agents physiques (champs électromagnétiques), 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 contre leurs effets biophysiques directs et leurs effets indirects connus. Il vise ainsi à améliorer la protection de la santé et de la sécurité des travailleurs, qui reposait jusqu'alors sur les seuls principes généraux de prévention, et intègre une approche graduée des moyens de prévention et du dialogue interne à mettre en œuvre en cas de dépassement des « valeurs d'action » et des « valeurs limites ».

En résumé, 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 ou le choix d'équipements de travail appropriés émettant, compte tenu du travail à effectuer, des champs électromagnétiques moins intenses.

Pour plus d'informations, vous pouvez vous référer au Dossier Champs électromagnétiques de l'INRS.

Cette recommandation demande donc le respect de la réglementation mentionnée ci-dessus.

Elle est à reporter sur les fournisseurs des équipements actifs, les architectes et les concepteurs du bâtiment hospitalier.

MA 4.2 – FOURNITURE DES FICHES ENVIRONNEMENTALES PEP

Les deux premiers niveaux de la recommandation évoquent les fiches Profil environnemental produit (PEP). Il s'agit d'une carte d'identité environnementale d'un équipement électrique, électronique ou de génie climatique. La définition du profil environnemental d'un produit est basée sur les résultats de l'analyse en cycle de vie du produit étudié, en prenant par exemple en compte la mise en œuvre et l'exploitation du produit, les transports et les matières premières utilisées dans sa constitution. Les fiches PEP sont disponibles sur le site PEP Ecopasseport.

L'objectif d'un PEP est de fournir des informations sur la fonction et la durée de vie du produit dans l'ouvrage, avec notamment :

- les caractéristiques techniques du produit (unité fonctionnelle, matières constituantes…) ;
- les impacts environnementaux, prenant en compte les étapes de fabrication, distribution, installation, utilisation et fin de vie.

La recommandation fait référence aux fiches environnementales PEP, mais il est possible de valider la recommandation avec des fiches environnementales équivalentes, à savoir intégrant un ensemble d'indicateurs environnementaux calculés sur l'ensemble du cycle de vie du produit.

Niveau 1 : informations environnementales simples

Pour valider ce niveau de recommandation, le bâtiment doit prévoir au moins une fiche environnementale PEP ou des informations sur le poids carbone du câblage et le nombre d'équipements du réseau Smart. La fiche environnementale PEP, doit être renseignée sur un équipement du réseau Smart (câblage compris) ou qui y est connecté via une passerelle IP. Elle doit fournir les informations suivantes :

- poids carbone du câblage fibre optique du réseau Smart ;
- poids carbone câblage cuivre (lien permanent + cordon de brassage) uniquement sur la partie bâtimentaire (hors preneurs) du réseau Smart ;
- nombre d'équipements actifs du réseau Smart (avec le détail par type d'équipements : commutateur d'accès, commutateur de cœur…).

Niveau 2 : informations environnementales approfondies
Cette exigence :
- le respect du niveau précédent ;
- + le bâtiment doit prévoir au moins 3 fiches environnementales PEP et des informations sur les équipements du bâtiment :
  - nombre de ports réseaux occupés / ports totaux ;
  - mètre de câble réseau (cuivre/fibre optique) / port occupé.

Niveau 3 : étude environnementale
L'étude environnementale devra prendre *a minima* en compte :
- choix de conception prenant en compte des critères environnementaux (carbone, énergie…) du réseau Smart sur plusieurs aspects : modèle de câblage, redondances et leurs apports et conséquences, choix des équipements, choix du type de câblage (cuivre ou fibre optique)…
- étude de dimensionnement du réseau Smart : réserve de puissance, nombre d'équipements, nombre de ports réseaux…

Remarque : la capacité d'extension des commutateurs sur le PoE est l'objet de la recommandation « RE 1.1 – Caractéristiques et capacités d'extension du réseau Smart ».

MA 4.3 – EFFICIENCE ÉNERGÉTIQUE DU RÉSEAU SMART

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).

Niveau 1 : identification des consommations électriques du réseau Smart
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 ;
- la consommation des serveurs métiers locaux (supervision de GTB, de vidéosurveillance, BOS…) et des postes clients.

Cela ne comprend pas :
- la consommation des équipements terminaux connectés au réseau Smart (exemple : régulateurs, IoT, automates…) ;
- l'énergie délivrée par les switchs d'accès en PoE (sauf en ce qui concerne les points d'accès Wi-Fi). Celle-ci doit faire l'objet d'une approche indépendante (exemple : la consommation PoE peut être récupérée sur les switchs d'accès en SNMP) pour dissocier les consommations intrinsèques du réseau Smart des consommations des équipements alimentés par lui ;
- la consommation de systèmes tels que le traitement d'air des locaux, bien qu'il puisse être pertinent de mesurer ces consommations.

En conception/réalisation : il est demandé la mise en place d'un sous-comptage (kWh) des consommations du réseau Smart.

En exploitation : les consommations en kWh du réseau Smart doivent être mesurées, et il en est demandé une analyse périodique au plus annuelle. Cette analyse compare ces consommations aux consommations antérieures et aux autres postes de consommation du bâtiment.

Niveau 2 : maîtrise des consommations du réseau Smart
Ce niveau de recommandation ne concerne que la phase Exploitation, et requiert :
- le respect du niveau précédent ;
- + 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 moyens qui peuvent être mis en œuvre pour réduire les consommations du réseau Smart :
- lutilisation de la fonctionnalité adaptant la consommation des ports au contexte (longueur des liaisons, connectés ou non…) par les équipements actifs d'accès du réseau Smart (exemple : conformité à la norme IEEE 802.3az) ;
- procédure de fermeture automatique des ports réseaux ;
- procédure d'extinction d'équipements selon des plages horaires (ex : ports PoE) ;
- etc.

Remarque : ces moyens sont communiqués à titre d'exemple, la recommandation portant plus sur les résultats obtenus.

MA 5 – Système de management

MA 5.1 – MANAGEMENT DE PROJET

Le maître d'Ouvrage joue un rôle central dans la mise en œuvre, le suivi et l'amélioration du management du projet, et ses partenaires (maîtrise d'œuvre, entreprises…) sont aussi impliqués. Il est important que tous les intervenants du projet, et en premier lieu ceux de la maîtrise d'ouvrage, soient parfaitement informés des objectifs et ressources du projet. Il revient à chaque maître d'Ouvrage de définir l'organisation, les compétences, les méthodes, les moyens, la documentation nécessaire pour répondre à ses objectifs, et aux recommandations du présent cadre de référence.

Il est demandé la mise en place d'un management de projet comprenant les jalons ci-dessous détaillés.
A/ Un document d'engagement de la direction (la direction responsable est la direction de l'hôpital qui pilote la stratégie, dresse la feuille de route, passe les marchés et contrôle leur bonne exécution). Ce document d'engagement doit être diffusé à tous les collaborateurs et les intervenants de l'opération. En cas de modification des objectifs de performance visés, il doit être révisé et rediffusé.

B/ Les objectifs de performance visés pour l'opération, choisis et hiérarchisés, , ainsi que les principaux objectifs fonctionnels de l'opération.

C/ La mise en place de ressources et moyens adéquates à la bonne réalisation du projet

D/ La description et la répartition des rôles, responsabilités et autorités. Elle doit être définie par écrit, et les collaborateurs et les intervenants doivent en être informés. Cette répartition de missions est en lien avec la planification de l'opération. Les rôles, responsabilités et autorités de chaque acteur ou intervenant dans l'opération, sont définies en relation avec la planification établie pour chaque phase ou période concernée. Il doit y avoir une communication aux personnes concernées.

E/ La planification des actions. Le demandeur décrit la succession des étapes de chaque phase de l'opération, ou de chaque période en exploitation, en identifiant les éléments organisationnels suivants : les actions et activités, le calendrier, les responsabilités et autorités associées, les interfaces entre intervenants, les moyens, méthodes et documents à utiliser, les modalités de l'évaluation des performances, ainsi que les informations documentées à conserver. Des réunions de revue de projet sont programmées de manière à vérifier aux étapes-clés l'atteinte des performances visées, ou sinon de manière à réagir à temps et de façon proportionnée afin qu'elles soient atteintes.

F/ L'évaluation des performances de l'opération par rapport aux objectifs visés. Elle est réalisée aux étapes-clés (programme, conception, réalisation), ou périodiquement en phase d'exploitation, à partir de son entrée en certification, et documentée.

G/ La mise en œuvre d'actions correctives en cas d'écarts. Lorsqu'une performance attendue n'est pas atteinte, ou que le système de management ne fonctionne pas comme prévu, une action corrective est mise en œuvre afin de corriger, si possible, l'écart. Les écarts observés, tant sur les performances du bâtiment que sur le fonctionnement du système de management, font l'objet d'actions correctives, sans qu'il soit nécessaire de mettre en place une procédure dédiée.

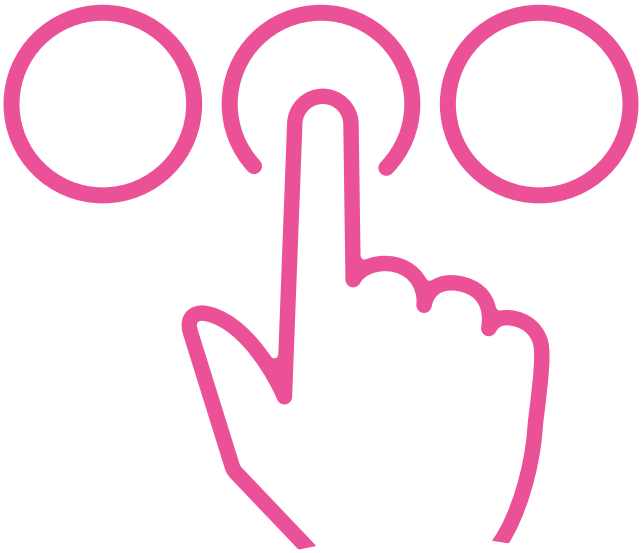
H/ La réalisation d'une enquête de satisfaction. Elle est réalisée de façon à identifier les attentes, les sujets de satisfaction et d'insatisfaction. Le numérique comportant des évolutions rapides, la satisfaction doit également être évaluée dans le temps pour comprendre les besoins et orienter ces évolutions vers davantage de satisfaction du client.

Cette recommandation de niveau unique et au statut de prérequis requiert une définition du management de projet. Le management s'inscrit ainsi dans une démarche qualité, apportant une maîtrise du projet dans sa globalité.

MA 5.2 – GUIDE D'UTILISATION DES SERVICES

Ce niveau de recommandation demande l'élaboration d'un guide à destination du ou des propriétaires afin d'expliquer comment ils peuvent développer des services. Ce guide pourra inclure une partie sur le développement de services pour les utilisateurs et usagers.

Plus précisément, le guide décrira les conditions d'accès aux services, la méthode pour avoir accès aux données des API, la compilation des documents permettant d'atteindre cet objectif.



SERVICES

Ce thème valorise la mise en place de services *a minima* attendus dans l'enceinte d'un Smart Hospital en termes de:

- réglementation;
- confort;
- sécurité;
- performance.

Les services proposés viennent en complément des services usuels et minimaux attendus d'un hôpital. La mise en place de ces services concourt notamment à l'atteinte des contraintes réglementaires actuelles et à venir.

TITRE DE L'EXIGENCE	NIVEAU
SE 1 – PLATEFORME DE SUIVI ÉNERGÉTIQUE	
	Niveau 1 Assurer la collecte et le reporting des consommations énergétiques
	Niveau 2 Assurer la régulation des consommations énergétiques en fonction d'évènements exogènes liés à l'activité hospitalière et à l'environnement
SE 2 – PLATEFORME DE PILOTAGE DU BÂTIMENT	
	Niveau 1 Superviseur(s) technique(s)
	Niveau 2 Hyperviseur (pilotage autonome)
SE 3 – GÉOLOCALISATION	
	Atteint / Non atteint (bonus)
SE 4 – BÂTIMENT CONNECTÉ ET COMMUNICANT	
	Atteint / Non atteint (bonus)
SE 5 – MESURE, GESTION ET OPTIMISATION DE L'UTILISATION ET DE LA RÉAFFECTATION DES ESPACES DU BÂTIMENT	
	Niveau 1 Évaluation et optimisation de l'utilisation
	Niveau 2 Gestion de mutabilité des espaces
SE 6 – INTÉGRATION À LA SMART CITY	
	Atteint / Non atteint (bonus)

SE 1 – Services énergétiques

SE 1.1 – PLATEFORME DE SUIVI ÉNERGÉTIQUE

Le bâtiment doit disposer d'une plateforme de suivi et de régulation des consommations énergétiques. Cette plateforme permet notamment d'alimenter la plateforme **Operat** pour assurer le suivi de la conformité à la loi **ELAN** et son décret tertiaire.

Ce service doit permettre de centraliser les informations énergétiques du bâtiment et de définir son profil de consommation / production.

Cette plateforme doit :

- permettre de suivre en temps réel l'évolution de la consommation du bâtiment, archiver et historiser des suivis de tendance afin de faciliter l'analyse et la définition du profil énergétique, voire environnemental (empreinte carbone, performance énergétique) du site ;
- intégrer des outils d'analyse et d'aide à la décision afin de faciliter la conduite de la performance ;
- bénéficier d'une interface Homme / Machine ergonomique et conviviale à différents niveaux d'accès pour permettre son usage par différentes typologies d'utilisateurs (Asset, Property, Building Manager, Occupants) ;
- permettre un suivi par comparaison ;
- Rendre possible la création de tableaux de bord personnalisés pour l'utilisateur ;
- afficher une connectivité complète sur le R2S par utilisation des API et / ou des accès directs aux données de site et aux données externes (météoNorm notamment).

Le service doit permettre l'ouverture du bâtiment à la flexibilité énergétique et constitue un des outils de dialogue avec le Grid énergétique (SmartGrid). Le cadre de référence R2S 4 Grid peut être utilisé.

Cette plateforme s'appuiera sur le cadre normatif suivant : norme NF EN 16-001 : Systèmes de management de l'énergie – exigences et lignes directrices pour leur utilisation (selon NF EN ISO 50.001 et méthode PDCA – Plan Do Check Act, 2009 et Norme NF EN 15-900 : Services d'efficacité énergétique – définitions et exigences, 2010).

Son objectif principal est de maîtriser davantage les consommations énergétiques sur le bâtiment.

Niveau 1 : assurer la collecte et le reporting des consommations énergétiques

Niveau 2 : assurer la régulation des consommations énergétiques en fonction d'évènements exogènes liés à l'activité hospitalière et à l'environnement.

SE 2 – Pilotage de la performance du bâtiment

SE 2.1 – PLATEFORME DE PILOTAGE DE LA PERFORMANCE DU BÂTIMENT

Le bâtiment doit disposer d'une plateforme d'hypervision, laquelle va permettre de :

- offrir une interface mutualisée et unique pour piloter la performance du Smart Hospital métier par métier : Gestion technique du bâtiment (GTB), Building Information Management (BIM), Gestion de maintenance assistée par ordinateur (GMAO), Internet des Objets (Io(M)T), gestion d'infrastructures de recharge des véhicules électriques, quel que soit le fournisseur des solutions ;
- élargir le champ d'action en livrant à distance une vision d'un ou plusieurs sites en consolidant des données multisources dans une logique de Big data ;
- gérer des alertes avec une remontée en temps réel des données (vidéosurveillance, sécurité Incendie…) ;
- mettre œuvre un outillage complet pour mettre en œuvre des procédures et interactions pour résoudre les alertes (Workflow) ;
- produire des rapports d'activité et des analyses basées sur les données collectées des solutions métiers et des actions réalisées.

Les bénéfices attendus sont de diminuer le coût global en permettant de :

- améliorer la coordination des services pour :
  - les économies d'énergies
  - la réduction des coûts d'exploitation
  - la diminution des coûts de maintenance
  - le développement de la maintenance préventive pour la continuité d'activité
  - l'amélioration du confort et du bien-être des occupants
- accélérer la prise de décision avec la vue mutualisée des données tout en réduisant drastiquement l'effet silo des organisations par métier ;
- documenter par la production automatisée de tableaux de bord et de rapport sur les alertes et les réponses données ;
- inscrire l'ensemble des équipes dans un process qualité d'amélioration continue et de renforcement des SLA avec la mise en commun d'une information unique sur la performance du bâtiment.

Niveau 1 : superviseur(s) technique(s)
Cette recommandation répond à l'enjeu de conformité au décret BACS (Building Automation & Control Systems, publié au Journal officiel le 21 juillet 2020). L'objectif de ce décret est d'équiper d'un système d'automatisation et de contrôle des bâtiments, d'ici le 1er janvier 2025, tous les bâtiments tertiaires non-résidentiels (neufs et existants).

Niveau 2 : hyperviseur (pilotage autonome).

SE 3 – Services de géolocalisation

SE 3.1 – SERVICE DE SUIVI DU MATÉRIEL (RTLS)

L'hôpital met en œuvre une plateforme permettant d'offrir des services de localisation et de suivi du matériel utilisé par le personnel soignant. Cette plateforme permet de chercher et retrouver de façon aisée chaque matériel avec une précision de localisation en rapport avec l'usage attendu. Elle permet de simplifier le travail des soignants en leur permettant de trouver de façon rapide des dispositifs médicaux ou des moyens de transport robotisés. Elle permet également de simplifier le travail des ingénieurs biomédical dans le cadre de leurs opérations de contrôle / maintenance du matériel. Elle doit faciliter la gestion des équipements et d'en optimiser les coûts associés.

Niveau 1**: localisation des matériels et dispositifs**, inventaire des équipements sur demande ou routine, détection de sortie et de retour de matériel (geofencing)

Niveau 2**: fonctions avancées d'analyse** de l'utilisation et de la disponibilité des matériels et dispositifs (règles métier) comme la détection d'équipements « morts » ou d'équipements surutilisés.

Niveau 3**: optimisation** de gestion de parc en connexion avec la GMAO (anticipation et facilitation de la maintenance préventive), support à la définition des investissements pour les équipements, affectation des budgets réels d'exploitation

Ces services doivent pouvoir être interopérables à différentes échelles : les différents bâtiments d'un même hôpital, différents groupements d'établissements, au niveau départemental ou national.
Ainsi, ils offrent des moyens support à la gestion des prêts d'équipements entre services et entre établissements ou groupes d'établissements.

SE 3.2 – SERVICE DE SUIVI DU PATIENT

L'hôpital doit disposer d'une plateforme permettant d'apporter la sécurité aux patients durant leur séjour dans l'hôpital.

Plusieurs cas d'usage peuvent être rencontrés :

- suivi de la position du patient au cours de son parcours depuis le parking ;
- détection de la sortie de l'hôpital ou de certaines zones de l'hôpital de patients ne devant pas sortir pour des raisons de sécurité (système anti-fugue) ;
- détection de la sortie de l'hôpital de bébé ;
- localisation pour se faire aider suite à une chute ou en cas de détresse ;
- gestion de l'ouverture des espaces avec un système de protection adapté à la vulnérabilité de chaque patient.

SE 3.3 – SERVICE DE GUIDAGE ET D'ORIENTATION DES USAGERS

L'hôpital doit disposer d'une plateforme permettant à chaque personne de pouvoir facilement se localiser dans l'hôpital et disposer d'une aide à la navigation vers les services / accueil.

Niveau 1**: guidage du visiteur**
Dans le cas d'un visiteur, la plateforme doit lui fournir un moyen simple de se localiser dans l'hôpital, de rechercher un ou plusieurs services et de naviguer simplement au sein de l'établissement hospitalier.

Niveau 2**: guidage du patient**
Dans le cas d'un patient ayant d'ores et déjà des rendez-vous de prévu, la plateforme doit lui permettre de trouver efficacement les lieux de rendez-vous dans l'hôpital en le localisant et en le guidant tout en tenant compte des heures de rendez-vous.

Niveau 3**: réorganisation du parcours patient en fonction des aléas**
La plateforme doit également permettre au personnel soignant de pouvoir ajuster le parcours patient en fonction des aléas dans les agendas des praticiens en informant les patients d'éventuels retards et en permettant de réorganiser les rendez-vous tout en informant le patient en temps réel.

SE 4 – Bâtiment connecté et communicant pour les usagers

Cette recommandation porte sur la disponibilité des informations, pour les usagers du Smart Hospital. Le bâtiment hospitalier doit être le support de transmission des informations temps réel, pour :

- permettre l'accès aux données contextualisées : les bonnes données, aux bonnes personnes, au bon endroit, au bon moment ;
- permettre l'utilisation de tout type de terminaux ;
- permettre la mise en œuvre de sous-systèmes spécialisés (Biomed, imagerie, robots, IoT…).

Ce service est un prérequis pour le bon fonctionnement de l'hôpital zéro papier, et concourt à renforcer l'attractivité de l'hôpital en améliorant tant l'expérience patient que la qualité de vie au travail pour les professionnels, tout en facilitant les échanges de connaissances, de savoir-faire et d'information, en mode collaboratif.

Quelques bénéfices du bâtiment connecté et communicant :

- disponibilité des rappels des rendez-vous où que l'on soit dans le bâtiment ;
- réservation / guidage vers une place de parking ;
- temps d'attente rdv des accompagnants sur l'avancement des soins ;
- affichage dynamique ;
- communication institutionnelle ;
- pas de rupture entre les réseaux extérieurs et l'intérieur de l'établissement ;
- contrôle d'accès dématérialisé ;
- intégration des BYOD (Bring Your Own Device) ;
- etc.

SE 5 – Mesure, gestion et optimisation de l'utilisation et de la réaffectation des espaces du bâtiment

SE 5.1 – OPTIMISATION DES ESPACES DU BÂTIMENT

L'hôpital doit être en mesure de s'adapter rapidement à des besoins changeants dépendants de nombreux facteurs tels que les épidémies, les pandémies et les crises. Des lieux dédiés à certains usages doivent pouvoir être simplement mutés afin de pouvoir être utilisés pour d'autres usages.

À cette fin, l'hôpital doit disposer d'une plateforme permettant de mesurer l'utilisation de ses services/espaces, d'organiser leur utilisation/affection afin d'en optimiser leur utilisation. Cette plateforme doit aussi fournir les moyens de pouvoir simuler le changement d'affectation d'espaces, la faisabilité technique au regard des contraintes associées aux usages.

Niveau 1: évaluation et optimisation de l'utilisation
La fréquentation des espaces doit être mesurée:

- état des lieux d'utilisation réelle;
- identification des surfaces sur- ou sous-utilisées;
- réservation/affection des espaces;
- services d'aménagement des espaces (space planning, transformation de l'usage d'un bâtiment, gestion du mobilier).

Niveau 2: gestion de mutabilité des espaces
Cette recommandation prend appui sur la maquette numérique ou le jumeau numérique du bâtiment. Appliquer la recommandation IN 2.2 est donc un prérequis. Il est recommandé de créer et maintenir un Référentiel structure architecturale.

Ce niveau permet d'utiliser les outils suivants:

- analyse numérique / faisabilité;
- simulation de réaffectation;
- réaffectation réactive des espaces.

SE 6 – Bâtiment connecté, à son territoire, à la Smart City

Cette recommandation couvre plusieurs aspects. Un bâtiment hospitalier connecté à son territoire ou son quartier intègre dans sa politique les services suivants:

- **Gestion réseaux énergétiques**:
  - infrastructures de recharge de véhicules électriques (voir cadre de référence R2S 4 Mobility notamment)
  - connexion aux réseaux électriques (voir cadre de référence R2S 4 Grid)
- **Services offerts par et avec les prestataires de la ville**:
  - usages tertiaires (réservation salle, de cantine ou d'amphithéâtre pour et par des tiers, conciergerie, crèche, covoiturage, ...)
- **Santé populationnelle**:
  - support à la prévention;
  - support au suivi à domicile;
  - connexion avec les maisons de santé.

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.

ARCHITECTURE ORIENTÉE SERVICES (SOA)
L'architecture orientée services (Service-Oriented Architecture) est une approche permettant de créer une architecture qui s'appuie sur l'utilisation de services. Ces services (les services Web RESTful, par exemple) remplissent de petites fonctions, telles que la production de données, la validation d'un client ou la mise à disposition d'analyses simples.
L'architecture SOA consiste en fait à revoir les architectures existantes en traitant la plupart des principaux systèmes en tant que services, et en les extrayant pour les rassembler dans un domaine unique où ils sont élaborés en solutions.
L'une des clés de l'architecture SOA tient à ce que les interactions ont lieu avec des services modulaires (couplage flexible) qui fonctionnent de façon indépendante. SOA permet de réutiliser les services, ce qui évite de repartir de zéro lorsque des mises à niveau et autres modifications sont nécessaires. Il s'agit d'un avantage indéniable pour les entreprises cherchant à économiser du temps et de l'argent.

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 INFORMATION SYSTEM (BIS)
Le Building Information System (BIS) est un système d'information conçu et architecture pour organiser la gouvernance des données et permettre l'évolution digitale du bâtiment sur tout son cycle de vie. C'est un système d'information « Building Centric ». Le BIS apporte une vision holistique et transverse de la gestion des données partagées du bâtiment sur lequel il est déployé. Le BIS est organisé autour d'un référentiel commun et partagé du bâtiment et d'un contrat de gouvernance de données. Pour en savoir plus, voir le livre blanc de la SBA « Le BIS & le BOS, les outils de la gouvernance des données du bâtiment ».

BUILDING OPERATING SYSTEM (BOS)
Le Building Operating System (BOS) est le cœur du système d'information bâtimentaire BIS (Building Information System). 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 BIS & le BOS, les outils de la gouvernance des données du bâtiment ».

BRING YOUR OWN DEVICE (BYOD)
Littéralement, en français « AVEC » pour « Apportez votre équipement personnel de communication », le BYOD est une pratique qui consiste à utiliser ses équipements de communication personnels (smartphone, ordinateur portable, tablette électronique) dans un contexte professionnel.

CÂBLAGE BANALISÉ
Câblage comportant des liens à paires torsadées aptes à supporter des liaisons de type (xDSL, Ethernet First Mile, liaisons analogiques et numériques) et à fibres optiques aptes à supporter les protocoles à haut débit Ethernet normalisés par l'IEEE ou de la famille PON normalisés par l'ITU, entre le répartiteur général et les locaux techniques ou les nœuds de connexion de zone ou d'étage.

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.

CHIFFREMENT DE BOUT EN BOUT

Le chiffrement est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (de)chiffrement. Le chiffrement de bout en bout est une méthode de chiffrement, il consiste à chiffrer les messages sur un dispositif pour que seul le dispositif auquel il est envoyé puisse le déchiffrer. Le message effectue tout le voyage entre l'expéditeur et le destinataire sous forme chiffrée.

CLOUD COMPUTING

Le Cloud Computing est un concept général qui désigne la mise à disposition de services hébergés sur un serveur extérieur au bâtiment et accessible par Internet. Le Cloud Computing permet aux entreprises de consommer les ressources informatiques à la demande (comme elle le ferait d'un service public tel que l'électricité), en leur évitant de créer et de gérer des infrastructures en interne.

COMITÉ IEEE

Comité de standardisation International Institute of Electrical and Electronics Engineers, regroupant les industriels des produits de réseaux locaux. Ce comité normalise les protocoles de liaison par paquets tels qu'Ethernet sur paires torsadées et fibres optiques, Wi-Fi, Bluetooth, LiFi, CPL (Courant Porteur en Ligne) sur câble basse tension, etc.

COMITÉ ITU

Comité de standardisation international International Telecommunication Union, regroupant les opérateurs de télécommunications mondiaux. Ce comité normalise les protocoles de liaison sur circuit réel ou virtuel exploités par les opérateurs, tels que les protocoles de la famille DSL (Digital Suscriber Line) sur paires torsadées, de la famille PON (Passive Optical Network) sur fibres monomodes, de la famille ATM (Asynchronous Transfer Mode) sur fibres monomodes, de la famille DOCSIS (Data over Cable Service Interface Specification) sur fibres monomodes et câble coaxial, etc.

DISTRIBUTION CENTRALISÉE

Un câblage à distribution centralisée, consiste à distribuer les prises à partir d'un local ou d'une armoire technique, conformément aux modèles de câblage ISO 11801 et FTTZ (Fibre To The Zone).

DISTRIBUTION RÉPARTIE

Un câblage à distribution répartie, consiste à distribuer les prises à partir de nœuds de connexion locaux disséminés dans le bâtiment et/ou dans les espaces d'activités et disposés à proximité des prises qu'ils distribuent, conformément aux modèles de câblage ISO 11801 et FTTZ avec Points de Consolidation Passifs, POL (Passive Optical LAN), FTTO (Fibre To The Office) et FTTACP (Fibre To The Active Consolidation Point).

ÉCOSYSTÈME TECHNIQUE

Communauté d'équipements ou de logiciels compatibles entre eux et en capacité d'échanger des données et d'interagir. Un écosystème peut réunir des équipements de plusieurs constructeurs ou éditeurs de logiciels dans un esprit d'ouverture et d'interopérabilité.

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-debit 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 situe 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…

ESPACES

Par défaut, les espaces non-hospitalier et d'activités hospitalières où s'appliquent les niveaux de recommandation 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 et 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 les pouvoirs publics et particulièrement la base OSCIMES (https://www.oscimes.fr/) 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.

GEOFENCING

Détection du franchissement d'une frontière déterminée au sein d'un espace.

HANDOVER, OU ROAMING WI-FI

Pour les réseaux sans-fil, la fonction de handover permet à un équipement connecté au réseau de basculer d'un point d'accès du réseau sans-fil à un autre sans perdre sa connectivité. Cette bascule peut être utile lorsque l'équipement se déplace, ou pour équilibrer la charge entre les différents points d'accès du réseau.
Les standards IEEE 802.11F et IEEE 802.11r définissent la fonction de handover pour les réseaux WiFi réalisés avec des équipements issus de différents constructeurs (interopérabilité). Cette fonction est cependant assurée généralement de façon propriétaire avec des équipements d'un constructeur unique.
Pour les réseaux Wi-Fi, la notion de roaming est également utilisée pour désigner la fonction de handover. Pour les réseaux de téléphonie mobile, la notion de roaming désigne la fonction d'itinérance. Cette fonction permet l'utilisation d'un réseau radio d'un opérateur mobile autre que le sien, par exemple dans une zone dans laquelle son opérateur ne diffuse pas son propre réseau.

HTML

HTML (Hypertext Markup Language) représente l'ensemble des codes de balisage insérés dans un fichier en vue de l'affichage d'une page dans un navigateur Web. Le balisage indique au navigateur Web comment présenter à l'utilisateur les mots et les images d'une page Web sur Internet. Bien que chaque code de balisage individuel soit un élément à proprement parler, on les appelle communément des balises. Certains éléments, présentés sous forme de paires, indiquent le début et la fin de l'effet d'affichage.
Recommandation formelle du World Wide Web Consortium (W3C), HTML est respecté par tous les navigateurs, Internet Explorer de Microsoft, Chrome de Google, Firefox de Mozilla et Safari de Apple) même si l'affichage peut varier d'un navigateur à l'autre.

HTTP

HTTP (Hypertext Transfer Protocol) est l'ensemble de règles régissant le transfert de fichiers (texte, images, son, vidéo, et autres fichiers multimédias) sur le Web. Dès qu'un utilisateur se connecte au Web et ouvre un navigateur, il utilise indirectement le protocole http. HTTP est un protocole d'application qui s'exécute au-dessus de la suite de protocoles TCP/IP.
L'un des concepts du protocole HTTP inclut l'idée que les fichiers peuvent contenir des références à d'autres fichiers (d'où la notion d'hypertexte) dont la sélection va solliciter d'autres demandes de transfert.
Tous les serveurs Web contiennent, en plus des fichiers de pages Web qu'ils servent, un daemon HTTP, c'est-à-dire un programme conçu pour attendre les demandes HTTP et les traiter à leur arrivée.

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.

INTERFACE PROTOCOLAIRE

Les interfaces protocolaires permettent d'interfacer les équipements de terrain à travers des protocoles ouverts, standardisés, interopérables basés sur les normes de type ISO EN dont EN16484, CEI61850.
Le tableau des interfaces protocolaires est décrit dans l'exigence « Systèmes disposant d'interfaces protocolaires » du thème "Équipements et interfaces" du cadre de référence R2S. Pour plus d'informations vous pouvez également consulter la définition du mot « Protocole ».

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.

IP

Protocole informatique de connexion (Internet Protocol) qui gère la transmission des données par Internet, basé sur l'attribution d'un numéro d'identification unique à chaque appareil connecté à un réseau utilisant le protocole Internet (adresse IP). Il existe plusieurs versions de ce protocole, principalement IPv4 et IPv6.

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.

JSON

JSON (JavaScript Object Notation) est un format d'échange de données en texte lisible. Il est utilisé pour représenter des structures de données et des objets simples dans un code qui repose sur un navigateur Web. JSON est parfois également utilisée dans les environnements de programmation, côté serveur et côté poste de travail. A l'origine, JSON est issue du langage de programmation JavaScript.
Sur Internet, JavaScript utilise JSON comme substitut à XML pour l'organisation des données. A l'instar de XML, JSON est indépendant des langages, et peut se combiner avec nombre de ces derniers, dont C++, Java, Python ou Lisp.
Toutefois, contrairement à XML, JSON n'est qu'un mode de représentation des structures de données, par opposition à un langage de marquage intégral. Les documents JSON sont relativement légers et leur traitement côté serveur Web est donc rapide (ce qui fait son succès).

LIENS PRÉCONNECTÉS, PRÉCONNECTORISÉS OU PRÉTERMINÉS

Câbles à fibres optiques ou paires torsadées pré-équipés de ses connecteurs à ses deux extrémités, montés et testés par l'industriel et fournis avec leurs fiches de mesures.

LOCAL RÉPARTITEUR GÉNÉRAL

C'est le local technique central de distribution des câblages du bâtiment, il reçoit les connexions aux liaisons externes et les équipements centraux des réseaux et des systèmes TIC. Sa dénomination normalisée par le standard ISO 11801 est Building Distributor ou Répartiteur Général de Bâtiment.

LOCAL OU ESPACE OPÉRATEURS

C'est un local ou un espace dans le local répartiteur général, réservé aux opérateurs de télécommunications, il collecte leurs arrivées de câbles et leurs terminaisons, dans une baie ou un coffret dédié à chaque opérateur.

MAQUETTE NUMÉRIQUE

Autre appellation du BIM (Building Information Modeling), faisant généralement référence à la base de données structurée du BIM, sans représentation graphique (2D ou 3D).

MODÈLE OSI

Le modèle OSI (Open Systems Interconnection) est un cadre conceptuel qui définit comment les systèmes réseau communiquent et envoient des données d'un expéditeur à un destinataire. Il est utilisé pour décrire chaque composant de la communication de données pour pouvoir établir des règles et des normes pour les applications et l'infrastructure du réseau.
Le modèle OSI contient sept couches qui s'empilent conceptuellement de bas en haut

- Physique (exemples : transmission par câble, fibre optique, radio...)
- Liaison des données (exemple : Ethernet...)
- Réseau (exemples : IPv4, IPv6...)
- Transport (exemple : TCP, UDP...)
- Session
- Présentation
- Application (exemples : HTTP, Modbus, Bacnet, SNMP...)

MODÈLE TCP/IP

Le modèle TCP/IP est dérivé de l'ARPANET et deviendra plus tard Internet (World Wide Web).
L'ARPANET était à la base un projet militaire de l'armée américaine dont le but était de connecter, via les lignes téléphoniques, une centaine d'universités et d'installations gouvernementales entre elles. L'objectif était de maintenir les communications coûte que coûte après une attaque nucléaire.
Il en découle un réseau basé sur le routage de paquets à travers une couche appelée Internet. La connexion de cette couche est de type connection-less (sans connexion préalable) : tous les paquets transitent indépendamment les uns des autres et sont routés suivant leur contenu. Le modèle TCP/IP est donc le modèle utilisé pour Internet.
Le nom de modèle TCP/IP est étroitement lié à deux protocoles : le protocole TCP (Transmission Control Protocol) et le protocole IP (Internet Protocol). Ceci est en partie dû au fait que ce sont les deux protocoles les plus utilisés pour Internet. Contrairement au modèle OSI, il n'y a que quatre couches pour le modèle TCP/IP.

MOT DE PASSE HASHÉ
Un mot de passe Hashé est un mot de passe qui utilise une fonction de hachage pour chiffrer les mots de passe stockés sur un serveur. On nomme fonction de hachage, (de l'anglais *hash*: recouper et mélanger) par analogie avec la cuisine, une fonction particulière qui, à partir d'une donnée fournie en entrée, calcule une empreinte servant à identifier rapidement, bien qu'incomplètement, la donnée initiale. Seul le client informatique est capable de reconstituer le mot de passe.

NETWORK INTRUSION PREVENTION SYSTEM (NIPS)
Système utilise pour protéger la confidentialité, l'intégrité et la disponibilité d'un réseau informatique. Sa fonction principale est de surveiller le réseau pour tout comportement indésirable et d'empêcher un tel comportement. Il peut y avoir une distinction entre un système de détection d'intrusion (IDS) et un système de prévention d'intrusion (IPS).

NOEUD DE CONNEXION OU DE RÉPARTITION
C'est un point de répartition du câblage, il peut être général, d'étage, de zone ou local.

NOEUD LOCAL DE CONNEXION OU DE RÉPARTITION
Boitier de distribution des prises situé dans l'environnement proche de ces dernières, suivant le modèle de câblage appliqué, il peut être constitué par un boîtier de connectiques pour point de consolidation passif (modèles ISO 11801 et FTTZ), par un boitier de splitting optique (modèle POL), par un boîtier d'épanouissement optique (modèle FTTO) ou par un point de consolidation actif (modèle FTTACP).

NORMES IEEE
L'Institute of Electrical and Electronics Engineers ou IEEE est une association professionnelle regroupant des ingénieurs électriciens, informaticiens et professionnels du domaine des télécommunications. L'IEEE assure notamment la publication de normes qui constituent des standards, en lien avec le cadre de référence R2S nous pouvons notamment citer:
- IEEE 802.1xx: sur la sécurité des réseaux informatiques
- IEEE 802.3xx: sur les réseaux informatiques et le protocole Ethernet
- IEEE 802.11xx: sur les réseaux sans fil locaux (Wi-Fi)

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.

OUVRAGE VRD OU AÉRIEN D'ADDUCTION OPÉRATEUR
Ouvrage de voirie et réseau divers, constitué par des fourreaux souterrains destinés au cheminement des câbles de télécommunications depuis la limite du domaine public jusqu'à leur pénétration dans le bâtiment. Les adductions des opérateurs de télécommunication peuvent également être réalisées en aérien.

POINT DE CONSOLIDATION
Il s'agit de points de répartition stationnaires permettant une gestion souple d'un câblage d'étage. Ils sont également appelés distributeurs d'étages.

POINT DE SOUS-REPARTITION
Répartiteur informatique relie en amont à un répartiteur général et en aval à un ensemble de prises; assure l'éclatement de câbles et leur répartition vers les différents points d'utilisation dans le bâtiment.

PORTS DOWNLINK
Ce sont les ports des équipements réseau exploités pour la connexion des terminaux.

PORTS UPLINK
Ce sont les ports des équipements réseau exploités pour interconnecter les équipements du réseau local entre eux.

POWER OVER ETHERNET (POE)
La technologie PoE permet de faire passer une puissance électrique en plus des données dans un seul câble. C'est une fonction supportée par les équipements d'accès au réseau, normalisée par les standards IEEE:
- 802.3af: PoE, 15 W,
- 802.3at: PoE+, 30 W
- 802.3bt: 4PPoE, 60 W à 100 W.

La puissance indiquée est celle disponible en sortie de switch, la puissance disponible au niveau de l'équipement est réduite des pertes sur le câble. Par exemple en 802.3bt, la puissance disponible en sortie de switch peut aller jusqu'à 100 W, et la puissance maximale disponible au niveau de l'équipement alimente est de 71 W.

PROTOCOLE
Dans le domaine de l'IT, un protocole renvoie à l'ensemble de règles utilisées par les points de terminaison d'un réseau pour communiquer lors d'une connexion de télécommunication. Les protocoles détaillent les interactions entre les entités qui communiquent. Ils interviennent à plusieurs niveaux d'une connexion de télécommunication. Par exemple, certains protocoles régissent l'échange de données au niveau du matériel et d'autres au niveau du programme d'application. Dans le modèle standard OSI, les deux extrémités de l'échange doivent reconnaître et observer au moins un protocole à chaque couche de l'échange de télécommunication. Les protocoles sont souvent décrits dans une norme sectorielle

ou internationale.
Les protocoles Internet TCP/IP, couramment utilisés, sont constitués de plusieurs protocoles :
- le protocole TCP (Transmission Control Protocol), qui utilise un ensemble de règles pour l'échange des messages avec d'autres points Internet au niveau du paquet d'information ;
- le protocole Internet (IP), qui utilise un ensemble de règles pour l'envoi et la réception des messages au niveau de l'adresse Internet ;
- d'autres protocoles, dont HTTP et FTP (File Transfer Protocol), qui définissent des ensembles de règles à utiliser avec les programmes correspondants, ailleurs sur Internet.
- Il existe de nombreux autres protocoles Internet, comme BGP (Border Gateway Protocol) ou DHCP (Dynamic Host Configuration Protocol).

Le terme protocole est emprunté au grec protocollon, désignant la feuille de papier collée sur un volume manuscrit et qui en décrit le contenu.

PROTOCOLES XDSL
Protocole de la famille Digital Suscriber Line : ADSL (Asymetrical Digital Suscriber Line), SDSL (Symetrical Digital Suscriber Line), VDSL (Very high speed Digital Subscriber Line), supporté sur paires torsadées téléphoniques.

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.

RÉFÉRENTIEL STRUCTURE ARCHITECTURALE
Le J.O du 10 Octobre 1998 donne une définition complémentaire de la notion de référentiel : il s'agit d'un « Ensemble structuré d'informations ou de données, utilisé pour l'exécution d'un logiciel, et constituant un cadre commun à plusieurs applications ». Ce sont des informations importantes et cohérentes auxquelles les maîtres d'ouvrage se réfèrent pour leurs besoins métiers. Les données de référence de ces informations s'imposent à toutes les applications supportant les services du Smart Hospital. Le référentiel structure architecturale doit permettre à tous les services du Smart Hospital de bénéficier d'un langage commun pour :
- Une vue globale du patrimoine immobilier et de chacun de ses bâtiments et composants
- Une vue descriptive de chaque bâtiment : surfaces, niveaux, pièces et leur destination
- Une catégorisation des surfaces par usage
- Une catégorisation des objets utilisés pour répondre aux usages.

Ces données seront reprises dans la mise en œuvre du BIM et du Jumeau Numérique pour alimenter l'Asset Information Model prévu dans la norme ISO 19650-1.

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)
C'est le réseau IP externe au bâtiment sur le domaine public.

RÉSEAU LOCAL LAN (LOCAL AREA NETWORK)
C'est le réseau Ethernet-IP interne au bâtiment à terminaisons WiFi ou non.

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.

REST
REST (REpresentational State Transfer) est un style d'architecture pour les systèmes hypermédia distribués, permettant la réalisation d'applications pour un utilisateur humain ou la réalisation d'architectures orientées services destinées à la communication entre machines.
L'architecture REST, permet le découplage intégral du client et du serveur informatique. L'interface utilisateur est séparée de celle du stockage des données. Cela permet aux deux d'évoluer indépendamment (exemple : découplage des trois couches R2S).

RESTFUL
Désigne une API compatible REST, qui fait appel à des requêtes IP pour obtenir (GET), placer (PUT), publier (POST) et supprimer (DELETE) des données.

SAAS
Le SaaS (Software as a Service) correspond à un mode de commercialisation des logiciels dans lequel ceux-ci sont installés sur des serveurs distants plutôt que sur la machine de l'utilisateur. Les clients ne paient pas de licence d'utilisation pour une version, mais utilisent librement le service en ligne ou, plus généralement, payent un abonnement. Ce modèle est aussi utilisé pour les plateformes (PaaS pour plateforme as a Service).

SÉCURITÉ DES SYSTÈMES D'INFORMATION
La sécurité des systèmes d'information ou plus simplement sécurité informatique, est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher l'utilisation non-autorisée, le mauvais usage, la modification ou le détournement du système d'information. En complément des recommandations du thème 4 « Sécurité Numérique » du R2S 4CARE, un guide rédigé par l'ANSSI peut être consulté au sujet de la sécurité des systèmes industriels (voir en particulier l'annexe B).

SERVEUR CENTRAL
Serveur qui assure la coordination, la gestion et le pilotage d'un ensemble d'équipements ou d'un système (exemple : supervision d'un système de GTB).

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.

SERVICES GÉNÉRAUX DE COMMUNICATIONS
Ce sont les services apportés par les systèmes de communications intégrés au bâtiment pour sa sûreté/sécurité (hors système de sécurité incendie), surveillance et la gestion de ses systèmes techniques, d'une part et pour le confort et les services de ses usagers, d'autre part, ces systèmes peuvent être installés dans les espaces communs et dans les espaces privatifs du bâtiment.
Les services généraux de communications peuvent être :
- Des services d'acheminement de liaisons apportés par une infrastructure de câblage ou radio
- Des services de connexion réseau, apportés par des équipements réseau administrés
- Des services applicatifs, apportés par des systèmes de communications et des logiciels
- SITH (Système d'Information Technique Hospitalier)
- Architecture logicielle cible regroupant toutes les applications concernant les données techniques d'un hôpital hors donnée médicale. Jumeau numérique basé sur un BOS.
- Le SIH (Système d'Information Hospitalier) regroupe le Dossier Patient et le SITH.

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.

SPOF (SINGLE POINT OF FAILURE)
Un SPOF (ou point unique de défaillance), désigne un équipement ou une fonction qui, par sa défaillance, entraîne l'interruption totale du service auquel il contribue.

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 exploite 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).

SYSTÈME
Communauté d'équipements ou de logiciels compatibles entre eux et en capacite d'échanger des données et d'interagir. Un système peut réunir des équipements de plusieurs constructeurs ou éditeurs de logiciels dans un esprit d'ouverture et d'interopérabilité.

SYSTÈME CENTRAL
Système qui est le support de l'API Centrale, il peut être en local ou dans le cloud.

SYSTÈME TIC
Système communicant s'appuyant sur les Technologies de l'Information et de la Communication, quel que soit l'objet, le contenu et la nature des échanges d'informations.

TRANSMISSION CONTROL PROTOCOL (TCP)
TCP (Transmission Control Protocol ou protocole de contrôle de transmission) est l'un des principaux protocoles de transport utilisés sur les réseaux IP. Il est décrit en détail par la RFC 793 de l'IETF. En utilisant des systèmes de séquençage des paquets et d'acquittement des émissions/réceptions de données, TCP fournit aux différents postes du réseau des informations essentielles sur la bonne transmission des paquets IP à leur destinataire.
Lorsque des paquets ont été perdus sur le réseau (ce qui peut par exemple arriver lorsque le réseau est saturé), TCP sait retransmettre les données manquantes pour reconstituer le message dans son ensemble. TCP fournit d'autres capacités intéressantes, comme la possibilité d'employer des techniques de contrôle de flux pour limiter le débit d'une connexion.

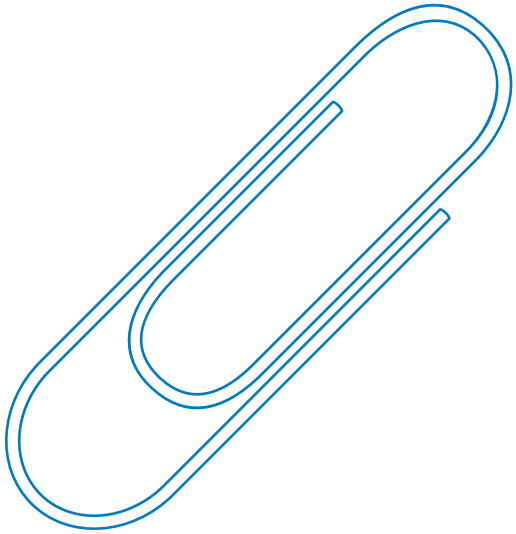
Il est à noter que TCP est le protocole de transport sous-jacent d'HTTP le protocole du Web, mais aussi de la plupart des grandes applications d'Internet. TCP est plus rarement utilisé pour les applications temps réels, pour lesquelles on lui préfère souvent un autre protocole de transport Internet, UDP.

VÉRIFICATION EN DEUX ÉTAPES
La double authentification (Two-factor authentication en anglais, 2FA) ou vérification en deux étapes est une méthode par laquelle un utilisateur peut accéder à une ressource informatique (un ordinateur, un téléphone intelligent ou encore un site web) après avoir présenté deux preuves d'identité distinctes à un mécanisme d'authentification.

VPN
Un réseau prive virtuel (Virtual Private Network) est un tunnel sécurisé à l'intérieur d'un réseau (Internet notamment). C'est un moyen d'échanger des informations de manière sécurisée.

WEB SERVICES
Ce sont des API, généralement RESTfull, exposées sur Internet, un intranet, ou sur un reseau comme le réseau «smart», permettant la communication et l'échange de données entre applications et systèmes hétérogènes dans des environnements distribués de manière synchrone ou asynchrone. Cela ne doit pas être confondu avec la notion de 'serveur web'.

WORLD WIDE WEB
Le Word Wide Web et le réseau mondial d'échange et de routage de données sur IP (Internet Protocole), généralement accessible par un navigateur Internet ou par des API RESTfull. Le World Wide Web est devenu le réseau mondial des autoroutes de l'information et des transactions sur Internet.



ANNEXE

Tableau des espaces OSCIMES

TYPES DE SURFACES PRIS EN COMPTE (D'APRÈS LA BASE OSCIMES)

ESPACES NON HOSPITALIERS
Archives
Hall d'entrée et sas d'accès (hall, ambulances)
Balcons, loggias ...
Toitures terrasses aménageables ou non
Circulations horizontales
Circulations verticales fermées (uniquement les niveaux servant d'emprise et les paliers)
Sanitaires
Espaces d'attentes intégrés aux circulations
Niveaux intermédiaire. (mezzanine, galeries, paliers des escaliers fermées)
Coursives et galeries fermées permettant l'accès à des locaux
Bureaux
Salles de réunion
Restauration Personnel (self et distribution)
Locaux techniques en combles, sous-sol, terrasses fermées
Locaux techniques en étage courant y c les gaines techniques et gaines d'ascenseur
Sous-sols (? Voir lignes supra) y compris les parkings
Combles ou sous-sols aménageables y c réserves foncières
Combles ou sous-sols non aménageables
HSP (hauteur sous plafond) < 1,80 m

SERVICES HOSPITALIERS
Consultation et Explorations fonctionnelles
Hospitalisation de jour (Médecine et Chirurgie Ambulatoire)
Urgences et SAU (Enfants, Adultes)
UHTCD (Unité d'Hospitalisation de Très Courte Durée)
Médecine
Chirurgie
Obstetrique
Pédiatrie
Psychiatrie
SSR
USLD – EHPAD
Réanimation (Enfants, Adultes) & Soins Intensifs
Réanimation (Enfants, Adultes) & Surveiallance Continue
Surveillance Continue
Néonatologie et SI Neonat
Bloc Opératoire (Activités interventionnelles) y/c SSCI
Bloc Obstetrical
Dyalise (toutes modalités)
Imagerie
Medecine Nucléaire – PetScan(et Gamma)
Radiothérapie
Laboratoires Biologies
Laboratoire Anatomopathologie
Pharmacie
Morgue
Stérilisation Centrale
Restauration – UCP – liaison froide
Vestiaires Centraux
Service Techniques y compris atelier biomedical

À PROPOS DE LA SBA

Créée en 2012, la Smart Buildings Alliance œuvre chaque jour à faire du smart building un atout au service des territoires, des entreprises et des occupants.

Unique en son genre par sa transversalité, son ouverture et la diversité des 450 entreprises et organisations membres qui la compose, la SBA structure ses actions autour de trois piliers: Smart Home (logement résidentiel collectif), Smart Building (bâtiment tertiaire) et Smart City (ville et territoire intelligents).

Revendiquant depuis plus de 10 ans un attachement fort pour un numérique responsable, la SBA prône la neutralité technologique tout en promouvant l'interopérabilité des systèmes, la mutualisation des équipements et des infrastructures, l'ouverture, la disponibilité, la qualité, la sécurité et la gouvernance des données.

Avec plus de trente commissions et groupes de travail, elle fédère l'ensemble des corps de métiers dans une démarche collaborative de construction de cadres de références, d'approches et de solutions innovantes.

La Smart Buildings Alliance est à l'origine du cadre de référence R2S (Ready 2 Service) et de ses déclinaisons (R2S Résidentiel, R2S 4Care, R2S Connect, R2S 4Grids, R2S 4Mobility...), ainsi que du référentiel BIM for Value.

L'alliance s'appuie sur des chapitres régionaux présents au plus près des territoires et rayonne également à l'international avec des SBA pays.

SMART HOME

SMART BUILDING

SMART CITY

DEVENEZ **MEMBRE**
DE LA SBA AU CÔTÉ DES
ACTEURS RÉFÉRENTS
DU SMART **BUILDING**,
DU SMART **HOME**
ET LA SMART **CITY**

Scannez ce QR Code pour plus d'informations sur l'adhésion à la SBA.

LES ACTIONS DE LA SBA

- **RENCONTRES**
  - Fédérer la filière dans un esprit de transversalité
  - Événements SBA pour le partage d'expérience et la veille autour des thématiques du bâtiment intelligent dans la ville et le territoire durables.
- **PUBLICATIONS**
  - Partager notre vision et nos recommandations
  - Cadres de référence (R2S, R2S 4Mobility, R2S Résidentiel, R2S Connect, BIM4Value...), Thémas et livres blancs, baromètres, webinars.
- **COMMISSIONS**
  - Réflexions sur l'évolution du bâtiment dans la ville intelligente
  - Plus de 30 commissions spécifiques actives grâce à nos 450 membres.
- **RELATIONS INSTITUTIONNELLES**
  - Sensibiliser les décideurs publics
  - Ministères, institutions publiques, collectivités locales, syndicats professionnels...
- **COOPÉRATION INTERNATIONALE**
  - Rayonner au-delà des frontières
  - Échanges avec les organisations internationales. Ainsi qu'une présence nationale, régionale et européenne.

UNE QUESTION ? UN PROJET ?
CONTACTEZ-NOUS...

par mail : contact@ smartbuildingsalliance.org

par téléphone : 0820 712 720

www.smartbuildingsalliance.org

www.linkedin.com

twitter.com

youtube.com

LES MEMBRES

ABB • ACCENTA • ACOME • ACR • ACS2I • ACTIVUS GROUP • AD VANTAGE • AD-STOA • ADEUNIS RF • ADVIZEO BY SETEC • AESTRIA • AFPA - TOULOUSE • AIRELIOR FACILITY MANAGEMENT • AIRTHINGS • AIRZONE FRANCE SARL • ALCANTE • ALCATEL LUCENT ENTERPRISE • ALLIANCE DU BÂTIMENT • ALLIANZ REAL ESTATE • ALPHA RLH • ALTAREA COGEDIM • ALTERNET • AN2V • ANITEC • APILOG AUTOMATION • ARC INFORMATIQUE • ARISTOTE • ARP ASTRANCE • ARTELIA • ARUBA • ASCAUDIT ÉNERGIES & FLUIDES • ASSOCIATION BACNET FRANCE • ASSOCIATION FRANÇAISE DE L'ÉCLAIRAGE • ASSOCIATION HQE • ASSOCIATION PROJET LORIAS • ASSUR & SENS • AURA DIGITAL SOLAIRE • AUTOMATIQUE ET INDUSTRIE • AV USER CLUB • AVELIS GROUP • AVELTYS • AVIDSEN • AXIANS • AZUR SOFT • B ECO MANAGER • B27 • B2AI • BARBANEL • BCC • BIMSY • BIRDZ • BNP PARIBAS REAL ESTATE • BOUYGUES CONSTRUCTION • BOUYGUES ENERGIES & SERVICES • BOUYGUES IMMOBILIER • BUREAU VERITAS CERTIFICATION • C2S BOUYGUES • CABA • CAILLOU VERT CONSEIL • CAISSE DES DÉPÔTS • CAPENERGIES • CBRE • CCI NICE CÔTE D'AZUR • CCUBE EXPERTISE • CD2E • CDC HABITAT • CERTIVEA • CINOV • CIT RED • CNAM • CNOA • CNPP • CODRA • CONNECTING TECHNOLOGY • CONNEK+ CONSEIL • CONSEIL DE DÉVELOPPEMENT MÉTROPOLE DE LYON • CONTINENTAL AUTOMOTIVE • COVIVIO • CR SYSTEM • CRESTRON EUROPE BV • CSTB • CYBERREADY • CYRISEA • DATA SOLUCE • DECAYEUX • DECELECT • DEERNS FRANCE • DELTA DORE • DEMATHIEU & BARD • DESKAPAD • DIS INGÉNIERIE • DISTECH CONTROLS • DOMOCORE • DOVOP DÉVELOPPEMENT • DREES & SOMMER • DRYAS • DTO SOLUTIONS • E-T-A • E'NERGYS • ECM RENOVBAT • ÉCOLE DE MANAGEMENT DE NORMANDIE • ECONOMIE D'ENERGIE • EFFICACITY • EFICIA • EFUTURA • EGF BTP • EGIS CONSEIL BÂTIMENTS • EIFFAGE ÉNERGIE • EMBIX • EN ACT ARCHITECTURE • ENERBEE • ENERGIE IP • ENERGISME • ENGIE SOLUTIONS • ENJOY • ENLESS WIRELESS • ENSI POITIERS • EQUANS • EY • EURECAM • EVOLIS • EXEO INGÉNIERIE • F2A SYSTÈMES • FACILITY DATA STANDARD • FARE PROPRETÉ • FEDENE • FÉDÉRATION DES ASCENSEURS • FEI • FEILO SYLVANIA • FFIE • FLOW • FORMAPELEC • G-ACTIV • GA SMART BUILDING • GA2B • GECINA • GETEO • GIMELEC • GPMSE-TN • GRIOT CONSEIL • GROUPE PROJEX • GROUPE QUALITEL • GROUPE SNEF • GROUPE TRACE • HABITAT76 • HAGER • HEINRICH ECLAIRAGE SAS • HELINK • HELVAR • HENT CONSULTING • HERVE THERMIQUE • HID GLOBAL • HOPPE FRANCE • HSBC • HUAWEI TECHNOLOGIES • HUB TEN • HXPERIENCE • HYDRAO • HYDRELIS • HYVILO • I-PORTA • ICADE • ICONICS • IDEX • IDTIQUE • IGNES • IKO REAL ESTATE • IMA PROTECT • IMMOBILIÈRE 3F • INGÉROP CONSEIL ET INDUSTRIE • INNES • INNESSENS - SCGI • INNOVATION PLASTURGIE COMPOSITES • INOVAYA • INSTALLUX • ISTA • J2 INNOVATIONS • JEEDOM • JIP CORPORATION • JOOXTER • KALIMA DB • KARDHAM DIGITAL • KIPSUM • KNX • KORUS • L'IMMOBILIÈRE IDF • LAKOUDIGITAL • LANCELOT CONSULTING • LD EXPERTISE • LE RÉSIDENTIEL NUMÉRIQUE • LEGRAND • LES COMPAGNONS DU DEVOIR • LEXCITY AVOCATS • LINKIO • LM INGENIERIE • LONMARK FRANCE • LUCIBEL • LUTRON ELECTRONICS • MAGMA • MBACITY • MEANWHILE • MEDIACONSTRUCT • MICROSENS • MOBILITY PLUS • MOBOTIX • MOVEWORK • MTCE CONSULTING • MUSEUM NATIONAL D'HISTOIRE NATURELLE • NAITWAYS • NCI • NET DISPLAY SYSTEM • NEODOMUS SOLUTIONS • NET AND YOU • NETSEENERGY • NEXITY • NOBATEK • NODON • NOVABUILD • NT CONSEIL • OCCITALINE • OKKOS • ONEPOINT • OPNA • ORANGE • ORIZON GROUP • ORLÉANS MÉTROPOLE • OVERKIZ • PALAMEDE TECHNIC EUROPE • PATRIARCHE UX • PBRAMAUD CONSEIL • PLAN BÂTIMENT DURABLE • PÔLE FIBRES - ENERGIVIE • PÔLE TES • POLESTAR • PRESTANTENNES • PRESTATERRE • PROLOGIS • PROTECT FRANCE • PULS • QWANDA • QWANZA • RABOT DUTILLEUL • RÉSEAU DEF • RÉSEAU DUCRETET • RESO • REUSITH • REXEL • ROBEAU • RT FLASH • S2E2 • S2T INGENIERIE • SAFE CLUSTER • SAINT-GOBAIN • SALTO SYSTEMS • SAMEA INNOVATION • SAS KINTSUGI-LOWCARBON (SETUR) • SATO ET ASSOCIÉS • SAUTER RÉGULATION • SBI CONSULTING • SCHNEIDER ELECTRIC • SE3M • SEDEA/HESTIA • SELUO • SERCE • SERELEC • SETEC BÂTIMENT • SIA PARTNERS • SIBCO • SIEA • SIEL 42- TERRITOIRE D ENERGIE LOIRE • SIEMENS ENERGY • SIG - SERVICES INDUSTRIELS DE GENÈVE • SIGNIFY • SIMONS VOSS TECHNOLOGIES • SLAT • SMALT • SMART BLUEDING • SMART HOME • SMART WORLD PARTNERS • SMARTHOME EUROPE • SMO VAL DE LOIRE NUMÉRIQUE • SOCOMEC • SOGEPROM • SOGETREL • SOMFY • SPAC • SPIE • SPINALCOM • SPL LYON CONFLUENCE • SQUARE SENSE • STID • SUPPLINNOV • SYLFEN • SYNOX • SYNTEC INGÉNIERIE • SYPEMI • SYS & COM • SYSTEMATIC PARIS-RÉGION • TACTIS • TECH FOR BUILDINGS • TECHNAL • TECHNILOG • TECXTEAM • TELEVES CORPORATION • TENNERDIS • TK ELEVATOR • TPF LUXEMBOURG • TRIGRR • TWYNSIS • UBIANT • ULIS • UNIVERS FIBRE • UNIVERSITÉ DE RENNES 1 • URBAN PRACTICES • URMET FRANCE • USGC • USING CITY • VAYANDATA • VELTYS • VERSPIEREN • VILOGIA • VINCI ÉNERGIES • WAGO • WAVESTONE • WEBDYN • WISE BUILDING • WIT • WITCO • WITTI • WIXALIA • WSP • XICATO • Z#BRE

LES MEMBRES **D'HONNEUR DE LA SBA**

SMART BUILDINGS ALLIANCE FOR SMART CITIES

www.smartbuildingsalliance.org