CASAMBI

SECURITE DU RESEAU CASAMBI

LIVRET CASAMBI

TABLE DES MATIERES

INTRODUCTION 2
BLE ET VULNERABILITE 3
Qu'est-ce que le BLE ? 3
Types de cyberattaques auxquelles est confronté le BLE 4
Sécurité BLE 4
Topologie Casambi 5
Accessibilité du réseau 6
Canaux de communications et sécurité 7
Communication d'unité à unité dans un réseau maillé 7
Communication entre un appareil mobile et une unité 7
Communication entre la passerelle et le Cloud 7
Chiffrement complet 8
Préventions 8
Sécurité Cloud 9
.ioXt Certification 9
Engagement auprès de la communauté éthiques des hackers 10
Casambi dans les environnements hautement sensibles 10
Etude de cas 11
Hôpital Ulster 11
BBC 12
Aéroport d'Helsinki 13
Terminologie 14

INTRODUCTION

La technologie de Casambi permet aux concepteurs d'éclairage et aux fabricants de relier sans fil des appareils entre eux, ce qui permet de créer des réseaux d'éclairage intelligents personnalisables qui sont configurés et contrôlés à l'aide de l'application Casambi. La solution est basée sur Bluetooth Low Energy (BLE), une technologie sans fil conçue pour communiquer des données sur une courte portée.

Depuis son introduction sur le marché, le BLE a réussi à devenir une norme sans fil et peut être trouvé dans tous les smartphones et tablettes d'aujourd'hui. En fait, les prévisions de croissance indiquent que plus de six milliards d'appareils compatibles Bluetooth seront expédiés chaque année d'ici 2025 ; dont 96 % devraient inclure la technologie BLE d'ici la même année. Grâce à son mode basse consommation, le BLE est utilisé dans un large éventail d'applications telles que l'éclairage, les balises, les capteurs industriels, les dispositifs de fitness, les dispositifs médicaux et autres, où des informations sensibles sont transférées sur de courtes distances allant jusqu'à plusieurs centaines de mètres.

Lorsque nous parlons du transfert de données via des ondes radio, des questions de sécurité sans fil se posent rapidement. Les données sont précieuses et deviennent donc une cible pour des piratages coûteux et les dommages potentiels à la réputation qui en découlent.

Casambi est conscient de l'importance de la cybersécurité pour réussir en tant que fournisseur de solutions de contrôle d'éclairage et la place au centre de sa stratégie et de sa mentalité. Bien que Casambi bénéficie d'une solide réputation en renforçant continuellement sa posture de sécurité contre toute menace potentielle, le travail ne s'arrête jamais. La société reste vigilante et prête à s'adapter en cas de besoin.

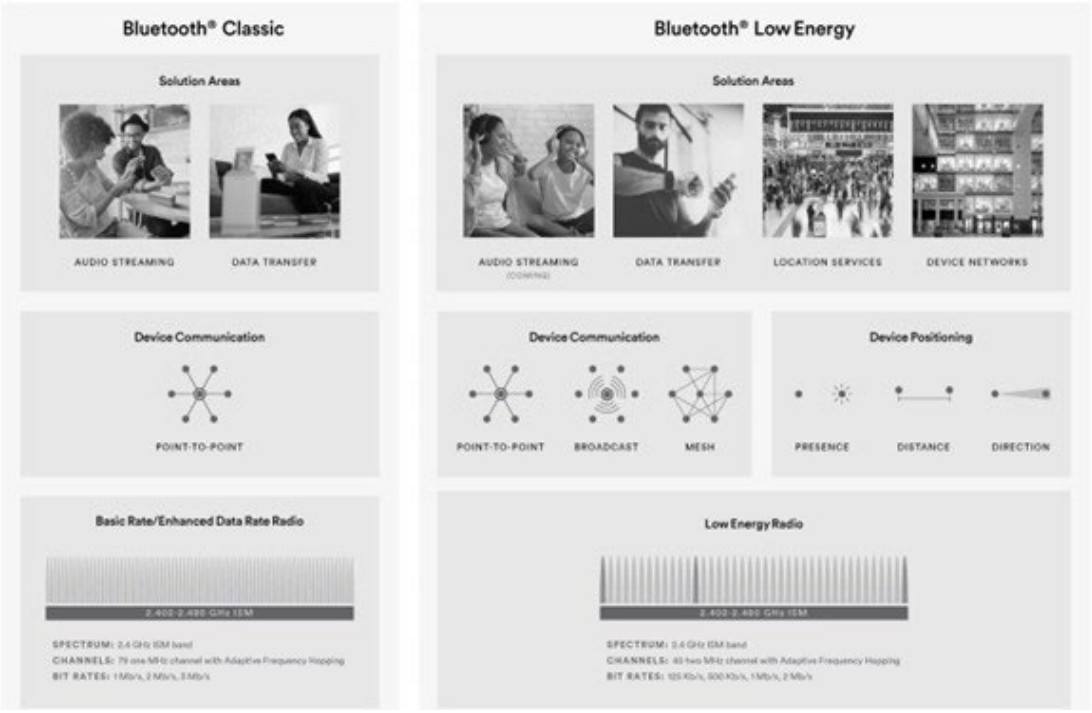
BLE ET VULNERABILITE

Qu’est-ce que le BLE ?

Le BLE (Bluetooth Low Energy) est une norme de technologie sans fil à courte portée qui fonctionne dans la bande ISM de 2,402 GHz à 2,480 GHz. Il existe deux types différents de technologies Bluetooth : Bluetooth Classic (Bluetooth BR/EDR) et Bluetooth Low Energy (BLE).

Le Bluetooth Classic est la technologie qui prend en charge la communication de périphérique à périphérique et est utilisée pour permettre la diffusion audio sans fil et le transfert de données sur des distances relativement courtes. Elle est couramment utilisée dans les enceintes sans fil, les claviers, les casques d'écoute et les systèmes de divertissement embarqués dans les voitures.

Le Bluetooth Low Energy (BLE) est conçu pour une consommation d'énergie très faible et pour transmettre de petits paquets de données sur 40 canaux. Le BLE prend en charge plusieurs topologies de communication telles que le point à point, la diffusion et le maillage.



Bluetooth classic vs. Bluetooth Low Energy. [Extrais du site nternet Bluetooth]

Les deux sont des technologies Bluetooth, cependant, ce sont des protocoles presque entièrement indépendants. Le document se concentre sur le maillage BLE, qui est la base de la solution de contrôle d'éclairage de Casambi. Le maillage BLE a été conçu pour les types d'applications que Casambi développe. Il est très robuste, éprouvé et est de loin le protocole radio de ce type le plus largement utilisé dans le monde. Il comprend des concepts avancés tels que le saut de fréquence afin de pouvoir utiliser plusieurs sous-fréquences où il y a moins d’interférences.

Mais Casambi va encore plus loin. Nous utilisons au sein de notre propre réseau maillé interne des sous-canaux différents de ceux du BLE standard. Cela signifie que nous n'avons pas d'interférences même des canaux BLE standard. Cependant, nous prenons également en charge les canaux BLE standard. Nous sommes donc entièrement compatibles avec la dernière norme BLE 5.3.

Types de cyberattaques auxquelles est confronté le BLE

Les principales façons dont les hackers peuvent exploiter un réseau BLE sont : l'écoute passive, les attaques "man in the middle" et le suivi d'identité.

L'écoute passive est une attaque par laquelle un troisième appareil écoute passivement les données qui sont transmises entre deux appareils appairés.

Une attaque "Man-in-the-middle" se produit lorsqu'un troisième appareil se fait passer pour un appareil légitime afin de tromper d'autres appareil et les inciter à se connecter à lui. De cette manière, l'attaquant peut prendre le contrôle de tout le réseau, intercepter toutes les données envoyées et injecter de fausses données dans la communication. Le suivi d'identité est lorsqu'un troisième appareil parvient ç associer l'adresse d'un appareil BLE à un utilisateur spécifique, puis à suivre physiquement cet utilisateur en se basant sur la présence de l'appareil BLE.

Sécurité BLE

Le Bluetooth Low Energy est un protocole de communication sans fil sécurisé, mais seulement s'il est spécifié et implémenté correctement. La définition du mode de sécurité, du niveau de sécurité et de la méthode d'appariement est cruciale pour garantir les propriétés de sécurité.

Il existe de nombreuses mesures de sécurité qui peuvent être utilisées contre les menaces potentielles : plusieurs schémas d'appariement de périphériques, le chiffrement, l'authentification des connexions et la randomisation des adresses.

TOPOLOGIE CASAMBI

La technologie de Casambi forme un réseau maillé (« Casambi Mesh ») qui permet la communication de nœud à nœud au sein d'un réseau d'éclairage. Le protocole Bluetooth Low Energy permet la communication entre un appareil mobile (ou l'appareil de contrôle) et la plateforme Casambi. La topologie en maillage est autonome, ce qui signifie que si un appareil échoue, le flux de signal est automatiquement rerouté à travers d'autres appareils, garantissant ainsi que les données disposent de plusieurs itinéraires vers leur destination. Cela augmente la fiabilité grâce à plusieurs nœuds et à la redondance des nœuds. Par conséquent, il n'y a pas de point de défaillance unique car aucun élément critique unique n'est nécessaire pour le bon fonctionnement du réseau ou d'une partie de celui-ci.

Aucun câblage spécial pour les commandes d'éclairage n'est nécessaire et toute la complexité matérielle est réduite au minimum car aucune unité centrale telle que des routeurs, des contrôleurs ou des passerelles n'est nécessaire pour le fonctionnement d'un réseau Casambi. Un réseau Casambi peut contenir jusqu'à 250 appareils et chacun est indépendant et dispose d'une sauvegarde de l'ensemble du réseau, c'est-à-dire que tous les nœuds du réseau maillé portent l'intelligence du système complet.

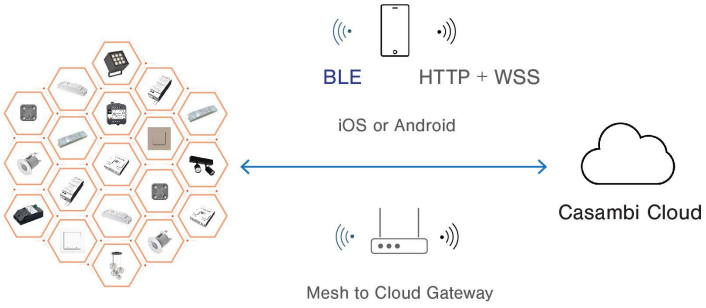
Jusqu'à 250 nœuds en fonction du monde réseau sélectionné
Casambi Stand-alone mesh network

Toutes les configurations du système et les contrôles des utilisateurs finaux sont gérés via l'application Casambi sur les appareils mobiles. Aucune connectivité réseau supplémentaire n'est nécessaire pendant le fonctionnement normal ; un réseau Casambi peut fonctionner sans être connecté à Internet.

Les appareils Casambi et le réseau maillé Casambi qu'ils forment ne sont pas accessibles depuis Internet. Ils n'ont pas d'adresses IP. Casambi utilise un protocole propriétaire grâce auquel les nœuds Casambi peuvent communiquer via la bande passante Bluetooth.

Un portail Internet peut être utilisé s'il est nécessaire d'avoir un contrôle à distance sur le réseau ou d'interfacer des systèmes de gestion de bâtiments via une connexion cloud. Étant donné que cela est accessible depuis Internet, une grande attention est accordée pour maintenir la configuration de sécurité de Casambi à jour.

Jusqu'à 250 nœuds en fonction du mode réseau sélectionné
Le réseau maillé dans fil de Casambi avec une passerelle Internet



ACCESSIBILITÉ DU RÉSEAU

Avec Casambi, il est possible de contrôler les droits d'accès à votre réseau et de définir qui interagit avec les lumières. Le réseau maillé dispose de 4 niveaux de sécurité qui peuvent être choisis et modifiés directement depuis l'application :

- Ouvert- accès libre ouvert à tous sans nécessiter de mot de passe. Les modifications nécessitent un mot de passe administrateur.
- Non partagé - les détails du réseau sont stockés uniquement sur l'appareil utilisé pour créer le réseau. Les autres appareils ne peuvent pas accéder au réseau.
- Protégé par mot de passe - il est possible d'utiliser et de modifier le réseau avec un mot de passe visiteur, à l'exception des paramètres de partage.
- Uniquement pour l'administrateur-seuls l'administrateur ou les administrateurs peuvent y accéder en utilisant un e-mail et un mot de passe d'administrateur.

Lorsque le réseau est en mode "Non partagé", il n'y a aucune communication avec le cloud. Lorsque le réseau est en mode "Uniquement pour l'administrateur", "Protégé par mot de passe" ou "Ouvert", l'application mobile Casambi enverra une copie (de sauvegarde) de la configuration du réseau vers le cloud Casambi.

La sécurité repose sur le principe du travail en couches - il s'agit d'ajouter des barrières supplémentaires. L'architecture du système de Casambi a été conçue pour maximiser la résilience contre les attaques. Dans la plupart des cas, la sécurité du système se résume essentiellement aux informations d'identification des utilisateurs. La seule façon d'accéder aux données est si vous disposez des informations d'identification appropriées.
En tant que mesure supplémentaire pour gérer la sécurité et l'intégrité des données, Casambi propose différents niveaux d'accès pour les utilisateurs :

- **Admin** : Possède un contrôle total sur tous les aspects du réseau
- **Manager :** Peut configurer le réseau (c'est-à-dire modifier la programmation), mais ne peut pas créer de nouveaux comptes utilisateur.
- **User** : Peut seulement utiliser le réseau mais ne peut effectuer aucune modification de programmation.

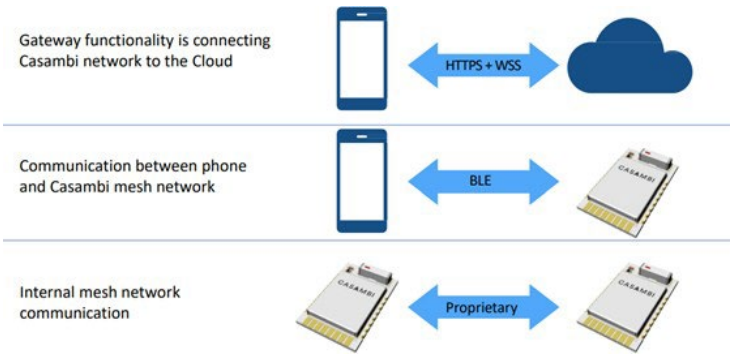
Jusqu'à 10 jetons d'accès peuvent être configurés pour les rôles d'utilisateur, de gestionnaire ou d'administrateur.

- Au niveau du réseau, d'autres possibilités d'accès sont également fournies :
- Verrouillage de l'appareil pour empêcher la désassociation (sans accès administrateur).
- La mise à jour du micrologiciel peut également être désactivée pour empêcher toute modification au niveau du micrologiciel.
- La configuration du réseau peut être sauvegardée dans le cloud via une application mobile.
- Le réseau peut être masqué aux autres utilisateurs.

CANAUX DE COMMUNICATIONS ET SECURITE

Chaque réseau Casambi comprend 3 canaux de communication principaux :

- Communication d'unité à unité dans le réseau maillé
- Communication entre les appareils mobiles et les unités/réseaux maillés.
- Communication entre la passerelle et le Cloud (seulement si la connexion au cloud est nécessaire)



Canaux de communication de Casambi

Communication d'unité à unité dans un réseau maillé

La communication d'unité à unité dans un réseau maillé utilise uniquement des paquets chiffrés, et le vecteur d'initialisation pour chaque message est composé de l'ID du réseau, de l'ID de l'unité et d'un code roulant.

Pour prévenir les attaques par rejeu (lorsqu'un attaquant intercepte et renvoie frauduleusement des paquets de données réseau qui ne lui appartiennent pas), chaque unité effectue une authentification bidirectionnelle par défi/réponse avec toutes les unités voisines.

Communication entre un appareil mobile et une unité

Bien que la connectivité standard Bluetooth Low Energy soit utilisée, les mécanismes de cryptage utilisés par Casambi sont propriétaires. Un chiffrement complet est assuré entre l'appareil mobile et les unités, où les deux côtés (mobile et unité) génèrent une nouvelle paire de clés publique/privée pour chaque connexion.

Communication entre la passerelle et le Cloud

La connexion entre un appareil mobile/une passerelle et le cloud est sécurisée par TLS (Transport Layer Security).
Toutes les communications sont effectuées via HTTPS (Hyper Text Transport Protocol Secure), qui est un processus de communication de bout en bout de confiance. Cela empêche les hackers d'intercepter les mots de passe et de pirater les comptes utilisateur.

Chiffrement complet

Tous les canaux de communication sont chiffrés, ce qui signifie que les informations sont converties en un code secret qui masque la véritable signification des données, empêchant ainsi les tiers non autorisés d'y accéder.

Étant donné que Casambi dispose de différents canaux de communication et propose une multitude de solutions, des API aux applications mobiles en passant par différentes solutions participant à la fabrication des appareils, l'entreprise utilise différents algorithmes de chiffrement et techniques pour sécuriser les données :

- 128-bit AES : chiffrement symétrique par blocs.
- AES-CMAC : algorithme d'authentification de message pour l'intégrité des données.
- ECDH : échange de clés sur courbes elliptiques.
- ECDSA : algorithme de signature numérique sur courbes elliptiques....
- Chiffrement complet entre l'appareil mobile et les unités. Une nouvelle clé de chiffrement est utilisée pour chaque connexion, dérivée avec ECDH.
- 10 mots de passe modifiables.

Les mises à jour over-the-air permettent à Casambi de diffuser de nouvelles fonctionnalités de sécurité et des correctifs logiciels à l'ensemble des appareils installés en une seule fois.

Préventions

Différentes méthodes sont utilisées pour prévenir différents types de cyber-attaque :

- **Prévention des attaques par rejeu** : utilisation de codes roulants pour les paquets de données et d'une authentification bidirectionnelle entre les unités pour valider les codes roulants initiaux.
- **Prévention de l'écoute indiscrète :** communication entièrement chiffrée. Même les administrateurs réseau ne peuvent pas décrypter la communication d'unité à unité.
- **Prévention des attaques de "Men in the middle"** : authentification bidirectionnelle entre l'appareil mobile et l'unité, ainsi qu'entre les unités elles-mêmes**.**
- **Prévention des attaques " trash-can"** : l'appareil mobile vérifie l'authenticité de l'unité avant de l'ajouter au réseau.
- **Prévention de la manipulation** : vérifications fortes de l'intégrité des messages.

SECURITE CLOUD

Les serveurs Casambi, situés en Europe, sont protégés par un pare-feu et surveillés 24h/24 et 7j/7. Ils sont régulièrement mis à jour avec des correctifs de sécurité, sont accessibles uniquement par un personnel limité et toutes les informations stockées sont chiffrées.

Le cloud nécessite un nom d'utilisateur et un mot de passe, ce qui permet d'obtenir un jeton d'accès à un "réseau Bluetooth" local. Les mots de passe sont stockés à l'aide d'algorithmes de hachage unidirectionnels. Avec un jeton d'accès, seul un réseau local peut être accédé. Un jeton d'accès est un identifiant de session qui permet l'accès au réseau, soit en tant qu'invité, soit en tant que gestionnaire, à partir d'un appareil mobile. Lorsque les mots de passe du réseau sont modifiés, tous les jetons d'accès existants sont invalidés.

Seules les informations liées aux configurations de réseau et aux performances du système sont stockées dans le cloud Casambi. Ces données ne peuvent être consultées que par Casambi dans le cadre du dépannage, du débogage du système ou de l'optimisation des performances du système. Cette analyse est toujours effectuée sous forme agrégée. L'agrégation des données est le processus de collecte de données sur l'utilisation et les performances du logiciel afin d'analyser et d'améliorer les performances du système. Au cours de ce processus, toutes les données personnelles sont anonymisées et aucune partie des informations n'est partagée avec d'autres tiers. Casambi s'engage à protéger la confidentialité des données de ses clients en utilisant des mesures de sécurité de premier ordre dans l'industrie.

.IOXT CERTIFICATION

ioXt
internet of secure things

Casambi a obtenu la certification de cybersécurité de l'alliance ioXt pour son système, ce qui confirme son engagement continu envers la sécurité réseau pour ses clients et ses parties prenantes.

Le système de contrôle d'éclairage sans fil de Casambi a été testé positivement conformément aux huit principes directeurs de l'alliance :

- Aucun mot de passe universel - des informations d'identification de sécurité uniques sont requises pour l'opération.
- Interfaces sécurisées - les interfaces du produit sont correctement sécurisées.
- Cryptographie éprouvée - la sécurité du système utilise une cryptographie forte, éprouvée et mise à jour.
- Sécurité par défaut - la sécurité du système est activée par défaut de manière appropriée.
- Logiciels vérifiés - le système ne prend en charge que les mises à jour logicielles signées.
- Mises à jour de sécurité automatiques - une stratégie établie pour l'application de mises à jour de sécurité en temps opportun.
- Programme de signalement des vulnérabilités - des mesures encourageant le signalement responsable de vulnérabilités ou de faiblesses présumées dans le système.
- Date d'expiration de sécurité - transparence sur les politiques de fin de vie et la fourniture de mises à jour de sécurité.

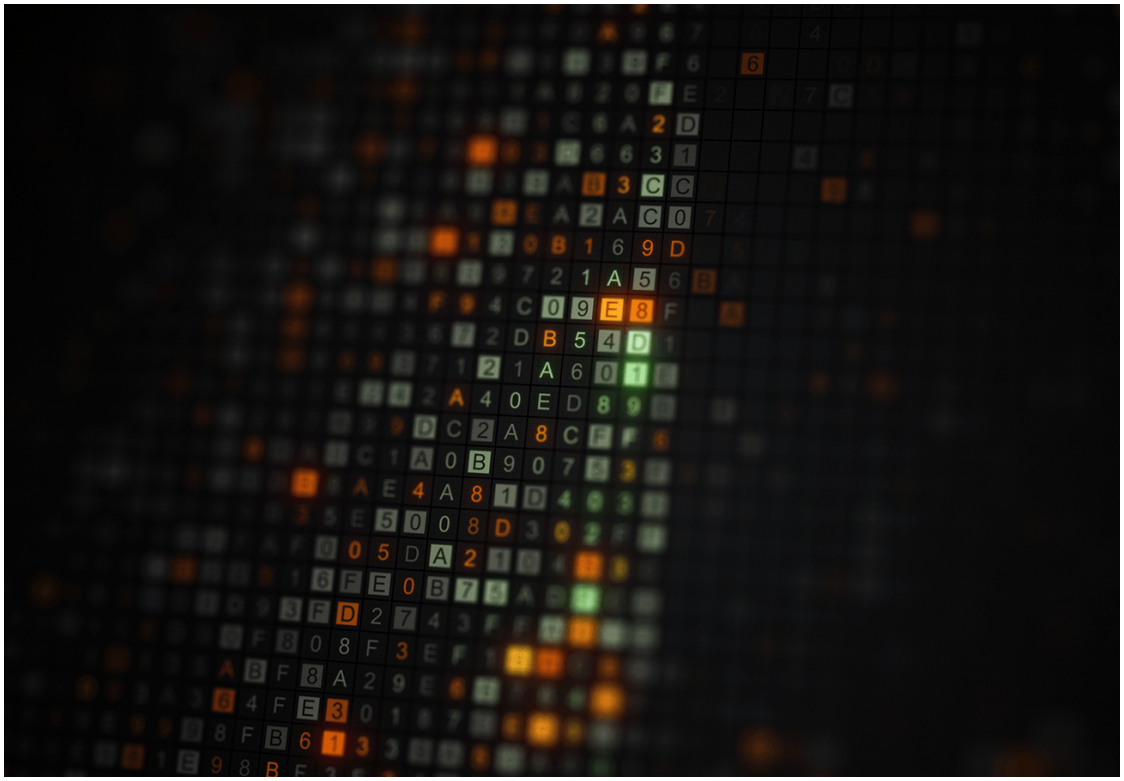
ENGAGEMENT AUPRES DE LA COMMUNAUTE ETHIQUES DES HACKERS

Casambi accorde une grande valeur au travail des chercheurs en sécurité et des hackers éthiques qui agissent de bonne foi pour sécuriser le monde numérique. Étant donné que la sécurité est une préoccupation majeure, Casambi dispose d'une politique de divulgation des vulnérabilités qui établit des lignes directrices claires pour mener des activités de découverte de vulnérabilités et pour le processus de signalement des vulnérabilités potentielles dans les systèmes Casambi.

Pour plus d'information, veuillez accéder à *https://casambi.com/vulnerability-disclosure-policy/*

CASAMBI DANS LES ENVIRONNEMENTS HAUTEMENT SENSIBLES

Casambi est déployé dans des environnements hautement sensibles, tels que les hôpitaux et les aéroports, où la fiabilité et la sécurité des communications sont essentielles. Ces cas témoignent de la robustesse de la technologie et des services de soutien. Le système est conçu de manière robuste et a été certifié comme étant sécurisé contre les cybermenaces, conformément aux normes mondiales.



ETUDE DE CAS

Hôpital Ulster

La solution de contrôle Casambi couvre l'ensemble de l'éclairage de l'hôpital, notamment les chambres, les postes de soins infirmiers, les couloirs, les locaux techniques, les bureaux, ainsi que tous les éclairages extérieurs autour du périmètre et du toit.

Une fonctionnalité particulière que Casambi offre se trouve dans les chambres des patients, où plusieurs capteurs surveillent des éléments tels que "mouvement hors du lit" (alertant les infirmières si un patient sort du lit) et la lumière du jour, qui ajuste ensuite l'éclairage en conséquence. Les lumières des chambres peuvent également être contrôlées depuis le poste de soins infirmiers lors d'événements tels qu'une urgence. De plus, de nombreuses scènes des chambres, accessibles via un combiné de chevet, offrent différentes ambiances pour des activités telles que la lecture ou le visionnage de la télévision.

Site : Ulster Hospital, Acute Services Block

Localisation : Belfast, United Kingdom C

Nœuds Casambi : 9 000+

BBC

La diffusion de la BBC atteint plus de 400 millions de personnes dans le monde chaque semaine, et son service d'actualités télévisées 24/7 est le plus important au monde. En 2020, l'organisation a décidé d'adopter la même approche novatrice pour ses bâtiments, qui abritent de nombreux studios de télévision et de radio, des centres de données et des bureaux.

La BBC a installé le système de contrôle d'éclairage sans fil de Casambi dans neuf de ses bâtiments à travers le Royaume-Uni.

En choisissant Casambi, l'équipe de la BBC a eu accès à l'ensemble de l'écosystème Casambi Ready, comprenant des milliers de capteurs et dispositifs de contrôle interopérables. Des capteurs de Tridonic et Danlers ont été installés pour permettre la détection de présence/absence et le gradateur de lumière en fonction de la luminosité du jour, garantissant que les lumières ne sont allumées que lorsque cela est nécessaire. Des interrupteurs sans fil à récupération d'énergie d'EnOcean sont également utilisés, offrant une autre façon pratique au personnel de contrôler les lumières. Les interrupteurs sans fil d'EnOcean conviennent particulièrement bien à Casambi, car Casambi est le seul système de contrôle d'éclairage avec lequel ils peuvent être associés à l'ensemble du réseau, plutôt qu'au nœud individuel le plus proche, garantissant une mise en service et un fonctionnement fiable.

L'installation à Broadcasting House a été réalisée en fin de soirée, et chaque zone mise à niveau devait être prête le lendemain matin lorsque le personnel revenait à son poste de travail, afin d'éviter toute perturbation.

Site : New Broadcasting House (London), Wogan House (London), Energy Centre (London), Mailbox (Birmingham), Glasgow Pacific Quay (Belfast), Manchester Media Centre, BBC Oxford, and BBC Radio Nottingham.

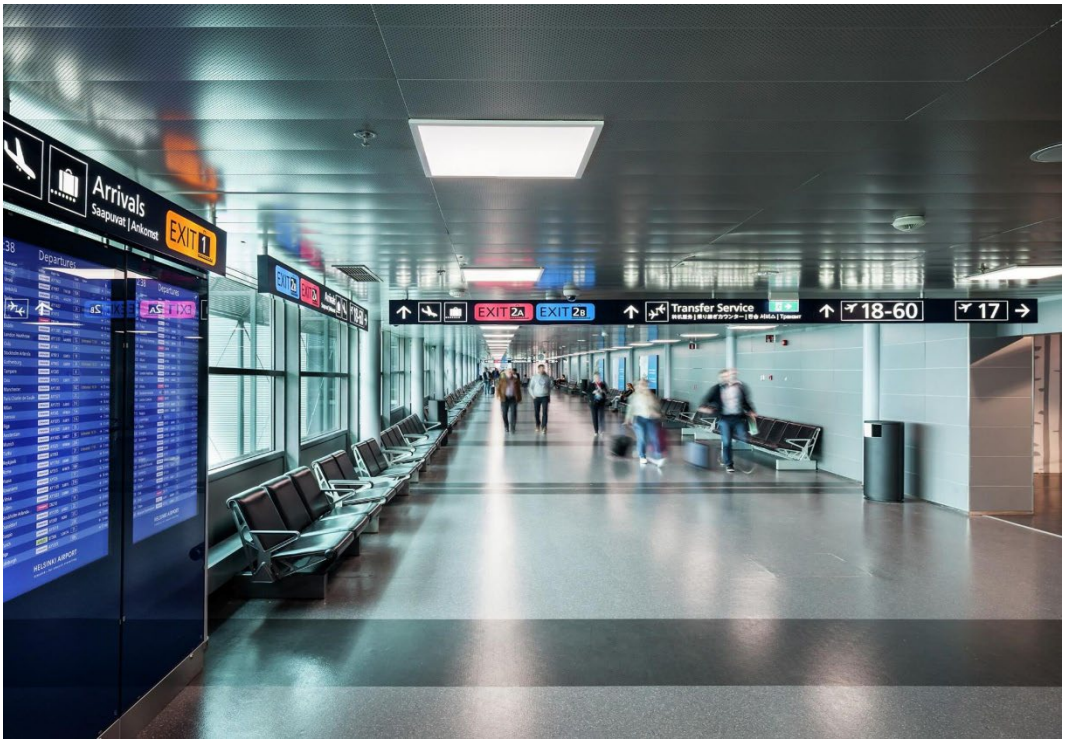
Location : United Kingdom

Nœuds Casambi : 10.000+ 10.000+

Aéroport d’Helsinki

Les objectifs du projet étaient de trouver une solution d'éclairage de haute qualité et durable, sans fil, pour les sections du Terminal 1, y compris les hauts plafonds, les couloirs de maintenance au rez-de-chaussée et les couloirs reliant les terminaux T1 et T2. De plus, des capacités de création de scènes uniques pour les différentes zones et une amélioration globale de l'efficacité énergétique étaient également considérées comme des priorités élevées.

Les terminaux d'aéroport nécessitent une illumination optimisée 24h/24, toute l'année. À l'aéroport d'Helsinki, cela a été réalisé grâce aux capteurs de lumière du jour Casambi Ready qui ajustent les niveaux d'éclairage en fonction de la quantité de lumière solaire traversant les grandes fenêtres du terminal. Un éclairage général a été attribué aux portes d'embarquement pour créer une atmosphère calme et chaleureuse. Les espaces commerciaux à proximité (chacun avec ses directives de marque) disposent également d'un éclairage plus adapté.



Site : Helsinki Airport
Location : Vantaa, Finlande
Nœuds Casambi : 2500

TERMINOLOGIE

- *AES - Symmetric encryption cipher*
- *AES - CMAC – AES Cipher based Message Authentication CodeAPI – Application Programming Interface*
- *BLE – Bluetooth Low Energy*
- *ECDH – Elliptic Curve Diffie-Hellman key exchange algorithmECDSA – Elliptic Curve Digital Signature Algorithm*
- *HTTPS - Hyper Text Transport Protocol SecureID - Identification*
- *ISM band – Industrial, Scientific, and Medical Radio BandMITM – Man in the midle*
- *TLS - Transport Layer Security*

casambi.com
Technologies Oy / Inc.