Socle de référence CYBERSÉCURITÉ du BACS Flex Ready®

GIMELEC

2025

Préambule

Le GIMELEC travaille avec ses partenaires de filière en vue de faciliter le déploiement des systèmes de pilotage des consommations d'électricité (BACS) dans les bâtiments tertiaires publics et privés de France, et ce, pour répondre aux objectifs nationaux de sobriété, de flexibilité électrique et de décarbonation.

Aujourd'hui, ces systèmes BACS sont de plus en plus souvent connectés pour pouvoir proposer de nouveau services et en particulier des services dit '*de flexibilité*' tels que le requiert le système électrique français à horizon 2030 (pour en savoir plus cliquer ici).

Ce socle de référence cyber sécurité du BACS Flex Ready® est une composante du Référentiel du BACS Flex Ready® du GIMELEC, reconnu par le cadre de référence de la marque Flex Ready®.

Ce socle de référence tient compte des normes et réglementations en vigueur et est recommandé comme prérequis minimal de cybersécurité.

Il est réalisé dans la perspective de l'application d'ici 2027 des réglementations CRA et NIS2.

Cette version pilote est destinée à être testée sur le terrain dans les mois qui viennent et s'enrichira des retours d'expérience autant que nécessaire.

Ce socle Cybersécurité du BACS Flex Ready® est le fruit d'une coopération entre le GIMELEC et Internet of Trust, expert en cybersécurité des systèmes embarqués et infrastructures.

Ce référentiel a été établi en coopération avec l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

L'ensemble de cette démarche est destiné à accompagner les concepteurs de ces systèmes, les opérateurs d'effacement mais aussi les prescripteurs et utilisateurs gestionnaires de bâtiments afin de faciliter l'élaboration des cahiers des charges et le déploiement des projets.

Le GIMELEC remercie l'ANSSI pour la coopération mise en œuvre dans le cadre de ce référentiel.

Le GIMELEC remercie également l'ensemble des sociétés ayant apporté leur soutien à ce travail : ABB France – aDvens – Distech-Controls – Hager – Legrand – Sauter Régulation – Schneider Electric – Siemens – Socomec – SPIE Facilities – Vinci Energies Building Solutions - Wallix

Table des matières

Liste des figures

Résumé

A travers le Baromètre des flexibilités de consommation publié en octobre 2024, la filière s'est projetée dans le passage à l'échelle nécessaire du pilotage énergétique des bâtiments, en lien avec le système électrique, pour atteindre les objectifs nationaux de sobriété et de flexibilité.

Pour les bâtiments tertiaires >70kVA, ce pilotage passe par le BACS (*Building automation and control system*), c'est ce qu'impose le Décret BACS depuis 2023.

Le BACS Flex Ready® est un BACS conforme au Décret BACS et connecté, capable donc de recevoir des demandes de flexibilité du système électrique ou de ses opérateurs et de mettre en œuvre une modulation de la consommation électrique en conséquence.

Il peut programmer des consommations électriques en fonction d'heures creuses et d'heures pleines, c'est la flexibilité régulière. Il peut aussi répondre à des demandes ponctuelles de modulation de la part d'opérateurs d'effacement, agrégateur/fournisseur d'énergie, c'est la flexibilité dynamique.

Le BACS Flex Ready® intègre une API standardisée qui lui permet de communiquer avec un opérateur d'effacement ou autre acteur du marché pour la mise en œuvre de modulations de consommation d'électricité. Il pourra ultérieurement inclure une API d'information tarifaire dynamique.

Ce document établit les exigences de sécurité applicables au BACS Flex Ready® et à son API. Il définit une analyse de risque générique et une architecture permettant d'élaborer un modèle de menace et un ensemble de contrôles de sécurité.

Ces spécifications de cybersécurité du BACS flexible sont utilisées dans la perspective de la marque Flex Ready® comme une grille de référence au travers de laquelle les acteurs présentent leur besoin et/ou démarche cybersécurité.

1 Introduction

Ce document identifie tout d'abord le champ d'application, les risques et les contrôles de sécurité du BACS Flex Ready® selon une architecture générique du BACS. Le document contient une analyse de risques et un ensemble minimal de contrôles de cybersécurité applicable à tous les BACS Flex Ready® opérationnels (équipement nouveau ou mis à niveau).

1.1 Contexte technique

Ce document vise à soutenir le passage à l'échelle en toute cybersécurité.

Le BACS Flex Ready® doit pouvoir recevoir et interpréter les signaux de flexibilité émis par les fournisseurs d'électricité (incitation tarifaire) et les opérateurs d'effacement (demande de modulation) et ainsi que les alertes de type EcoWatt du gestionnaire de réseau pour optimiser la consommation d'énergie en conséquence à l'échelle du bâtiment et des portefeuilles immobiliers.

La flexibilité nécessite des acteurs, des fonctionnalités et des connexions supplémentaires. Elle nécessite d'ouvrir les interfaces entre les gestionnaires de bâtiments, les exploitants, les opérateurs de réseaux et les acteurs de la flexibilité et de normaliser les échanges de données échangées.

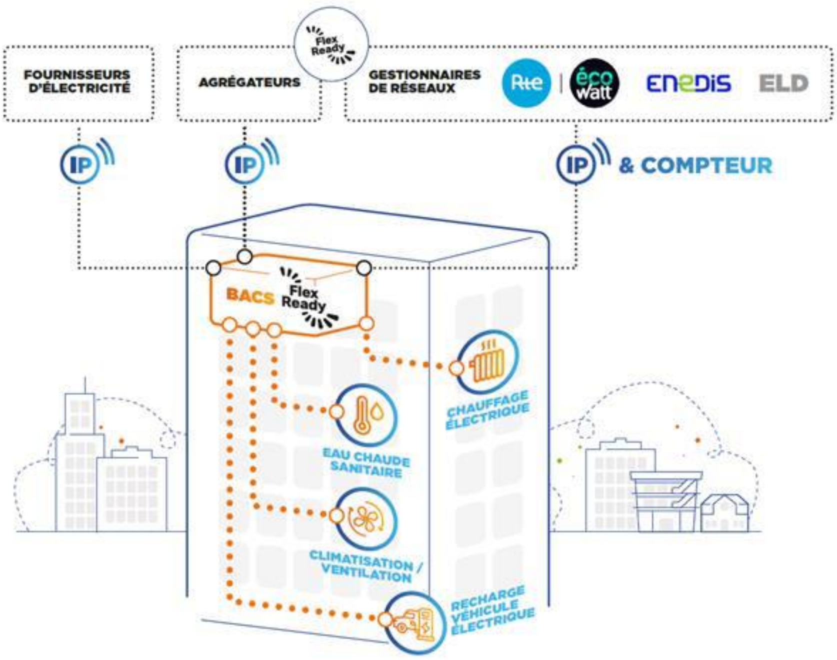

Figure1 : BACS Flex Ready®

Source : GIMELEC-RTE-ThinkSmartgrids-Ignes-Enedis-Plan-daction-flexibilites-de-consommation-octobre2024

Pour répondre à ce besoin, des travaux sont menés pour définir les normes techniques, opérationnelles et de cybersécurité afin d'assurer l'interopérabilité qui permet de relier les réseaux électriques et les bâtiments. Il s'agit notamment de :

- Une API standardisée pour permettre aux opérateurs et aux fournisseurs de communiquer des demandes de modulation ou des tarifs avec partir du BACS (voir annexe D).

- Un émulateur permettant aux BACS comme aux opérateurs d'effacement de tester la bonne intégration de cette API (voir annexe D).
- Les contrôles en matière de cybersécurité qui figurent dans ce document.

1.2 Motivation d'un référentiel de cybersécurité pour la phase pilote

Des projets pilotes ont lieu en 2025 pour tester la conformité des BACS au référentiel BACS Flex Ready® en vue d'un déploiement en 2026. Le référentiel de cybersécurité est intégré à cette phase pilote. Ce référentiel est centré sur la cybersécurité des fonctionnalités inhérentes à la flexibilité.

1.3 Audience

Ce document s'adresse à tous les acteurs impliqués dans le développement, le déploiement, l'installation, l'exploitation et le démantèlement (voir section 5). Et en premier lieu :

- Aux fournisseurs de BACS Flex Ready®, qui doivent mettre en œuvre les contrôles ;
- Aux opérateurs d'effacement, fournisseurs d'énergie ;
- Au comité de suivi de la marque Flex Ready®, aux gestionnaires de bâtiments à commande ou réception des travaux ou encore aux auditeurs qui vérifieront la mise en œuvre des contrôles.

1.4 Hypothèses

Dans cette version du document, les hypothèses suivantes ont été faites sur les cas d'utilisation envisagés et sur le champ d'application.

- Pris en compte dans la version "pilote" (ce document) :
  - Un seul BACS Flex Ready® pour chaque bâtiment.
  - Le réseau entre les opérateurs d'effacement et le système informatique du BACS Flex Ready® est réservé à la flexibilité et la modulation de l'énergie et l'API associée.
  - La passerelle réseau pour la gestion de l'énergie assure l'absence d'interférences entre la gestion de l'énergie et les autres opérations du bâtiment.
  - Les usages pilotés par les BACS sont considérés dans la zone de confiance car déjà existants pour les BACS non- Flex Ready®.
  - Seules les autorités de certification reconnues sont utilisées pour la gestion des certificats (PKI).
  - L'enregistrement des évènements (Log) et leur traitement sont gérés par les gestionnaires de risques de chaque acteur en fonction de son périmètre de responsabilité.
- À prendre en compte dans les versions futures
  - Un BACS pour plusieurs bâtiments et/ou plusieurs BACS dans un même bâtiment.
  - Un BACS Flex Ready® commandé/interfacé par plusieurs opérateurs d'effacement.
  - Les préconisations cybersécurité concernant le BACS au-delà de son option « flexibilité », telles que les connexions des utilisateurs du BACS, les mises à jour des microprogrammes des fonctions, la maintenance et les rapports.
  - Les usages pilotés par le BACS Flex Ready® dans le réseau de terrain seront à détailler. Considérer que les opérateurs d'effacement peuvent constituer une nouvelle menace car ils peuvent être utilisés pour mener des attaques coordonnées sur l'ensemble des BACS Flex Ready® (zone géographique).
  - Les sources de **temps** disponibles dans le bâtiment sont celles d'ENEDIS et d'autres. La responsabilité de la gestion du temps et le comportement à adopter en cas de divergence doivent être définis avant d'envisager des attaques de cybersécurité fondées sur des manipulations du temps (changements, dérivation, bruit, ...) et sur l'utilisation inappropriée de systèmes de récupération/urgence.

- Le service Strate 1 NTP, ainsi que les services Strate 2, ne doivent être accessibles qu'à partir du BACS/SI du bâtiment.
- Des recommandations pourraient être ajoutées dans la prochaine version du référentiel pour des questions d'interopérabilité, comme le choix de protocoles sécurisés ou d'autorités de certification pour les PKI.
- A l'occasion de la prochaine version, un chapitre sur la traçabilité avec les régulations applicables (CRA et NIS2), les schémas d'évaluation (Audit, 62443, CC, FITCEM) et les standards de présomption de conformité pourra être développé.

Ce travail est mené en parallèle de référentiels complémentaires tels que le "**Cadre bâtimentaire du BACS Flex Ready® de la SBA**", travail en cours.

Il tient compte :

- Des recommandations de l'ANSSI.
- Des régulations de l'Union Européenne notamment le Cyber Resilience Act (CRA) qui s'appliquent aux produits, la Directive NIS2 applicable aux Infrastructures critiques et opérateurs essentiels.
- Des systèmes de certification/normes 303645, 62443, CSPN, audit.

Une cartographie et une coordination des différents référentiels pourront être intégrés dans une prochaine version.

La nouvelle version sera aussi l'occasion de faire une synthèse de toutes les bonnes pratiques à mettre en œuvre pour assurer le maintien des installations en condition de sécurité.

2 Description et caractéristiques du produit

2.1 Les BACS

Les systèmes d'automatisation et de contrôle des bâtiments sont des systèmes plus vastes conçus pour automatiser et gérer diverses fonctions des bâtiments, notamment le chauffage, la ventilation et la climatisation, l'éclairage, la sécurité et d'autres infrastructures essentielles. Les principaux objectifs sont d'améliorer la gestion énergétique globale du bâtiment et le confort des occupants, d'éviter le gaspillage énergétique et de réduire les coûts.

Les BACS sont généralement installés dans des bâtiments commerciaux ou logistiques, des bureaux, des bâtiments de santé, ou encore d'enseignement etc.

Les composants de base sont des capteurs, des contrôleurs, des actionneurs et des réseaux de communication qui permettent une gestion complète du bâtiment.

Les BACS ont trois fonctions principales :

- La régulation des différents usages énergétiques du bâtiment.
- La gestion technique centralisée de ces usages, au travers de consignes, ainsi que la supervision et la gestion des données associée (on parle de Energy Management System EMS).
- La communication et l'interopérabilité avec les différents systèmes techniques du bâtiment (chauffage, climatisation, traitement de l'air, etc.).

2.2 Les BACS Flex Ready®

Le BACS Flex Ready® est un BACS intégrant les fonctions complémentaires suivantes :

- Accès à internet pour les échanges concernant la flexibilité
- Une API d'échange entre les Opérateurs d'effacement et les Fournisseurs de BACS
- Une API permettant de gérer les commandes ÉcoWatt du Gestionnaire de réseau
- Des propositions de spécifications Cybersécurité du BACS Flex Ready® basée sur ce document et la liste de contrôles annexée.
- Des fonctionnalités optionnelles de communication vers le compteur telles que spécifiées par le distributeur d'électricité.

3 Architecture Flex Ready® BACS

3.1 BACS & BEMS

Un système d'automatisation et de contrôle des bâtiments (BACS) est un système centralisé conçu pour automatiser et contrôler diverses fonctions d'un bâtiment, telles que le chauffage, la ventilation, la climatisation (HVAC), l'éclairage, le chargement des véhicules électriques et le stockage de l'énergie dans des cellules photovoltaïques (PVC). Le système de gestion de l'énergie des bâtiments (BEMS) est un sous-ensemble du BACS qui se concentre spécifiquement sur la surveillance, le contrôle et l'optimisation de l'utilisation de l'énergie dans un bâtiment. (voir l'annexe A pour un schéma d'architecture détaillé).

3.2 Interfaces FLEX

Cette architecture permet d'identifier le périmètre appelé "Périmètre du BACS Flex Ready®" (PBF), qui comprend le BACS Flex Ready® et ses interfaces connectées aux zones et réseaux externes. En plus des interfaces BACS non-Flex Ready®, il existe trois types d'interfaces spécifiques à la gestion de la flexibilité : l'interface FLEX API, l'interface Time Sync et “l'interface Usages pilotés” pour assurer la modulation des usages.

3.2.1 Interface API (#1)

L'interface API est l'interface du réseau internet/intranet où les opérateurs d’effacement et le réseau informatique du système BACS Flex Ready® sont connectés pour échanger des données de contrôle et de surveillance de l'énergie pour la flexibilité.

Le BACS Flex Ready® :

- reçoit des requêtes de modulation, des points de consigne énergétiques et des commandes de réponse à la demande et d'urgence dans ce réseau à travers l’API ;
- envoie un retour d'information sur les demandes de contrôles, les données en temps réel et les données de consommation d'énergie aux opérateurs d’effacement par l'intermédiaire de l’API.

L'installation de l'API peut être configurée de deux manières, à savoir :

- **Implémentation interne**, l’API est conçue pour être utilisées au sein du réseau BACS pour la surveillance et le contrôle de l'énergie. L’API fonctionne dans un environnement contrôlé et est limitée aux réseaux internes. Le paysage des menaces est moins risqué et sujet à des menaces internes ou à une exposition accidentelle.
- Implémentation de l’API dans un cloud externe accessible via internet par les opérateurs d’effacement et le BACS. Dans ce cas l’API est plus exposée aux attaques et nécessite des mesures de sécurité strictes.

3.2.2 Interface de synchronisation temporelle (#2)

Les commandes et les données de consommation sont échangées et exécutées en temps réel. Leur pertinence repose sur l’utilisation d’une heure de référence fiable commune aux agrégateurs et aux dispositifs BACS Flex Ready® fiable (GPS). Les contrôleurs et les appareils BACS sont donc configurés pour synchroniser leurs horloges et horloges maîtresses avec le GPS. Les protocoles de synchronisation du temps (TSP) à utiliser sont par exemple SNTP, NTP, PTP, etc.

3.2.3 Interface vers les usages pilotés (#3)

Les usages pilotés par les BACS Flex Ready® sont la CVC, l'éclairage, le véhicule électrique. Il s'agit d'équipements qui consomment de l'énergie. Ces équipements sont installés dans les réseaux de terrain des BACS Flex Ready® par l'intermédiaire des interfaces BAP via leur équipement ou leurs contrôleurs locaux. Cette interface est utilisée pour collecter les données des capteurs et les données opérationnelles, les données de consommation d'énergie provenant des utilisations. Ces données sont transmises à l'EMS qui applique les algorithmes de modulation de l'énergie et envoi les consignes de l'automatisation à l'équipement via cette interface.

Dans ce référentiel, nous considérons principalement les interfaces API (#1) et Time Sync Interface (#2) pour la modélisation des menaces et pour es contrôles. Ces interfaces font partie de la surface d'attaque. L'interface vers les usages pilotés (#3) est fournie avec des recommandations générales, puisque l'analyse des menaces sur les usages pilotés est considérée comme partie intégrante des usages non- Flex Ready® supposés pris en compte dans la conception des caractéristiques d'automatisation des BACS non Flex Ready®.

4 Périmètre du BACS Flex Ready® (PBF)

La figure 2 présente une vue simplifiée de l'architecture de BACS Flex Ready® de l'architecture détaillée en annexe A. Elle représente le PBF et ses interfaces Flex #1 avec les opérateurs d'effacement, Flex #2 avec les serveurs de temps et Flex #3 avec les usages pilotés.

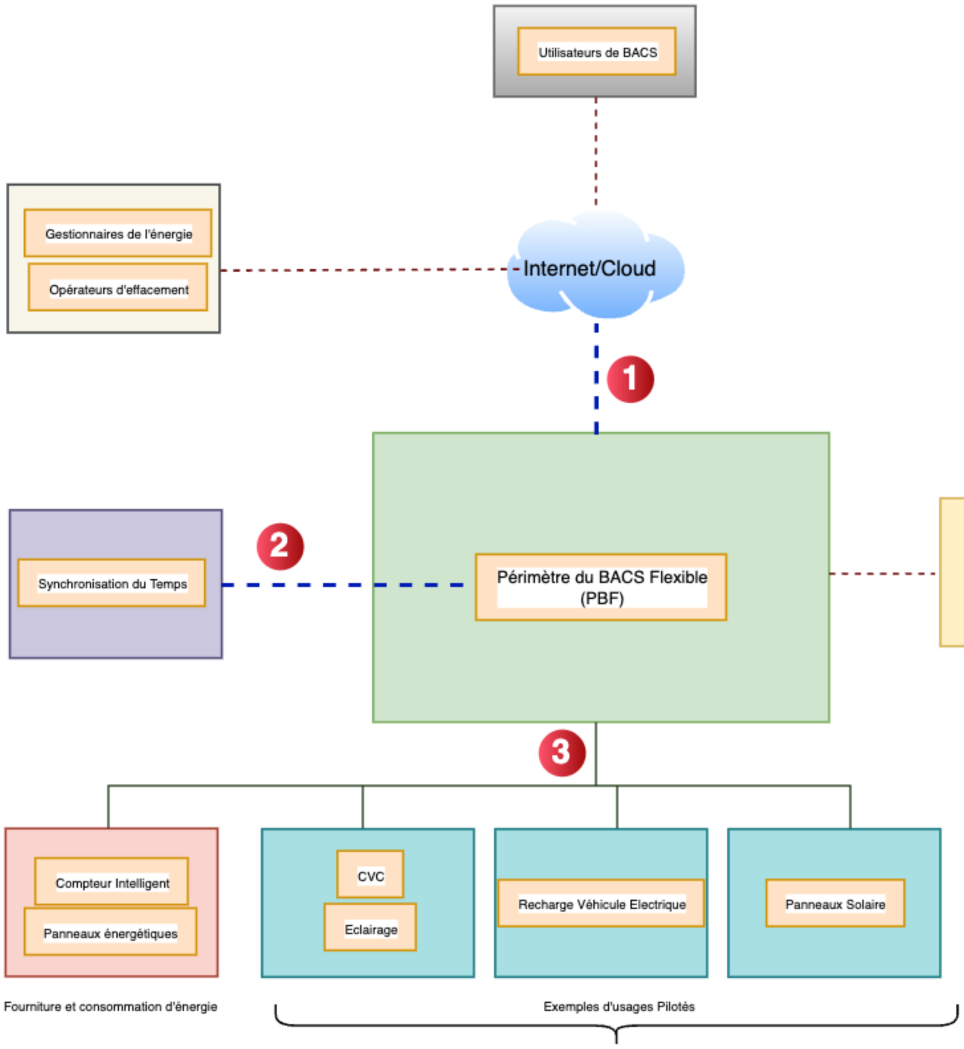

Figure2 : Le "PBF" et ses 3 interfaces

5 Biens à protéger

Les biens à protéger sont les suivants : les interfaces du PBF, les données et les flux d'informations entre le PBF et les parties externes. Les interfaces numérotées et étudiées dans ce document sont les 3 interfaces liées à la flexibilité. Les autres interfaces notamment celle vers les fonctionnalités de sécurité et sûreté du bâtiment font partie des BACS non Flex Ready®. Elles sont couvertes par les exigences de cybersécurité des BACS non Flex Ready®.

5.1 Interfaces

Nous présentons ici les protocoles qui prennent en charge les trois interfaces de PBF :

- Flex #1 : PBF <-> Opérateurs
- Flex #2 : PBF <-> Source de temps
- Flex #3 : PBF <-> Usages pilotés

Interface	Protocole d'interface	Type d'interface	Protocoles répertoriés
#1	Protocole Internet (IP)	Réseau Internet	HTTPS, TLS, MQTTS
#2	Protocole de synchronisation du temps (TSP)	Réseau Time Sync	SNTP, NTP, PTP, etc.
#3	Protocole d'automatisation des bâtiments (BAP)	Utilisations - Dispositifs de fonctionnement, de modulation et de consommation.	BACnet, Modbus, KNx, Lon Works, LoRa WAN, MQTT, MQTTS et leurs versions sécurisées, etc.

5.2 Données sensibles

Nous dressons ici la liste de toutes les données à protéger avec leur sensibilité en termes de :

- Confidentialité (**C**),
- Intégrité (**I**) et
- Disponibilité (**A**).

ID	Données	Description des données	C	I	A
D-01	Capteurs et données opérationnelles des services publics (CVC et éclairage, VE et PVC)	**CVC** : température (intérieure et extérieure), taux d'humidité, pression (air et eau), débit (air et eau), taux de CO2, qualité de l'air et prévisions météorologiques, vitesse et direction du vent, position des clapets, vitesse des ventilateurs et des moteurs, position des vannes, états de fonctionnement (marche/arrêt), mesures de performance, journaux de maintenance et diagnostic des défaillances). **Éclairage** : Intensité de l'éclairage, détecteurs de – mouvements, d'occupation, données sur la lumière ambiante provenant de capteurs de lumière du jour États de fonctionnement (marche/arrêt), niveaux d'éclairage, données de contrôle de l'intensité de l'éclairage. . **VE** : état de charge de la batterie (SOC), données relatives à la localisation du véhicule, données relatives à l'état et à la température de la batterie, données relatives au temps de charge, État de charge, taux de charge (kW), durée de charge, données sur l'utilisation de la station de charge, mode de charge, données sur la source d'énergie (réseau ou énergie renouvelable). **PVC :** niveaux de rayonnement solaire, données sur la production d'électricité, données sur les performances de l'onduleur, rapport sur les performances du système photovoltaïque, SOC, données sur le stockage de l'énergie, données sur l'état et l'entretien de la batterie, données sur la batterie et le courant, données sur la charge et la décharge, données sur la source d'énergie (réseau ou énergie renouvelable).		X	X
D-02	Modulation de la gestion de l'énergie (CVC et éclairage, VE et PVC)	**HVAC** : modulation du point de consigne de la température, signaux de réponse à la demande, instructions de délestage, programmes d'exploitation, points de consigne du débit d'air, modulation de la vitesse des ventilateurs, modulation VRF, ajustements du débit de réfrigérant et commandes basées sur l'occupation. **Éclairage** : Commandes de contrôle de l'éclairage en fonction de l'occupation et du mouvement, commandes de récupération de la lumière du jour, contrôle basé sur le temps, commandes de réponse à la demande, modulation du niveau d'éclairage, modes de contrôle de l'éclairage (manuel, automatique ou gradué). **VE** : limitation de la puissance de charge (kW), programmation des sessions de charge, réponse à la demande, priorisation de la charge, ajustement des modes de charge, intégration des énergies		X	X

ID	Données	Description des données	C	I	A
		renouvelables, arrêt ou refus de la charge, ajustement du taux de charge, délestage et écrêtement des pointes. **PVC :** contrôle de l'onduleur, commandes de charge et de décharge de la batterie, déplacement de la charge et réponse à la demande, interaction avec le réseau et commandes d'échange d'énergie, contrôle de la température de la batterie, contrôle de la synergie de la batterie, priorisation de la charge, équilibrage des cellules, suivi de la puissance maximale.			
D-03	Données sur la consommation d'énergie des services publics (kWh)	**Consommation d'électricité** : Données horaires, journalières et mensuelles provenant des compteurs d'électricité ou des compteurs intelligents (kWh), puissance de pointe (kW)		X	X
D-04	Contrat de distribution d'énergie (Pourcentage, kW, kWh, objectif, date et heure de référence, priorité)	**Points de consigne pour le contrôle de la charge** : Réduire la consommation d'énergie du chauffage, de la ventilation et de la climatisation (par ex de 20 %) pendant les heures de pointe. **Commandes de répartition de la production** : Décharge du système de stockage par batterie en cas de forte demande **Signaux de réponse à la demande** : Signal de tarification dynamique pour réduire la consommation lorsque les coûts de l'électricité augmentent. **Demandes de suivi et de rapport** : Il est demandé à l' EMS de fournir un rapport sur l'utilisation de l'énergie au cours des dernières 24 heures. **Commandes de stabilité du réseau** : Demande à l'EMS d'activer la puissance réactive pour stabiliser la tension. **Commande en cas d'urgence ou événement** sur le réseau : réduction des charges non essentielles. **Requêtes de modulation** envoyées par un opérateur d'effacement selon API Flex Ready **Prévision énergétique** : Prévision du niveau de charge pour le CVC pour les 10 prochaines heures en utilisant les tendances.		X	X
D-05	Données de validation et de règlement (contrôle de réalisation)	**Retour d'information sur l'ajustement de la charge** : Réduction réelle de la charge, confirmation du transfert de charge, durée et temps de réponse. **Performance de la réponse à la demande :** Modulation de l'économie d'énergie, réalisation de la demande de pointe et état de la participation à l'événement		X	X
D-06	Données de référence sur le profil de consommation	Tarifs des services publics, cycles de facturation et données historiques sur les coûts, analyse coûts-avantages des mesures d'économie d'énergie	X	X	X

ID	Données	Description des données	C	I	A
D-07	Données sur la consommation d'énergie en temps réel	Consommation totale d'énergie, consommation d'énergie par zone ou secteur, données de sous-comptage ou consommation d'énergie spécifique au système		X	X
D-08	Données historiques sur la consommation d'énergie	Historique des schémas de consommation d'énergie, des périodes de consommation de pointe, des schémas d'utilisation de l'énergie et des profils de charge		X	X
D-09	Données sur la production d'énergie	Énergie produite par des systèmes d'énergie renouvelable et données relatives au stockage de l'énergie dans des batteries et autres dispositifs de stockage		X	X
D-10	Données d'interaction de la grille	Stabilité du réseau et quantité d'énergie exportée vers le réseau à partir du bâtiment et détails sur l'énergie excédentaire		X	X
D-11	Données des journaux et des événements du BEMS	État du système, dysfonctionnements, événements, diagnostics de défaillance, pannes de données sur le chauffage, la ventilation et la climatisation, l'éclairage et la maintenance		X	X
D-12	Données sur l'occupation et le comportement	Modèles d'occupation, préférences des utilisateurs en matière de confort, tendances de l'utilisation de l'énergie sur la base de modèles historiques et/ou modèles prévisionnels		X	X
D-13	Données sur la durabilité environnementale	Émissions de carbone, utilisation des énergies renouvelables et économies d'énergie		X	X
D-14	Données sur l'infrastructure des bâtiments	Plans d'architecture, implantations, localisation, cartographie des capteurs, surface, typologie et caractéristiques de l'enveloppe		X	X
D-15	Données sur les actifs de gestion de l'énergie	Les détails des dispositifs de contrôle de l'énergie, tels que les marques, modèles et versions des capteurs, les détails des microprogrammes, etc.	X	X	X
D-16	Données de synchronisation du temps	Synchronisation horaire des contrôleurs et serveurs BACS avec le GPS		X	X
D-17	Données d'authentification du serveur BEMS	Clés secrètes, jetons d'accès, certificats, jetons web, listes de contrôle d'accès, noms d'utilisateur et mots de passe pour accéder au serveur lors du transfert de données vers et depuis les agrégateurs par l'intermédiaire de l'API.	X	X	X

5.3 Flux de données

Ce tableau décrit les échanges de données entre le PBF et les trois interfaces.

ID	Données	VERS LE PBF	DU PBF	Interface
D-01	Capteurs et données opérationnelles des services publics (CVC et éclairage, VE et PVC)	X		#3
D-02	Modulation de la gestion de l'énergie (CVC et éclairage, VE et PVC)		X	#3
D-03	Données sur la consommation d'énergie des services publics (kWh)	X		#3
D-04	Contrat de distribution d'énergie (Pourcentage, kW, kWh, objectif, date et heure de référence, priorité)	X		#1
D-05	Données de contrôle du réalisé		X	#1
D-06	Données de référence sur le profil de consommation		X	#1
D-07	Données sur la consommation d'énergie en temps réel		X	#1
D-08	Données historiques sur la consommation d'énergie		X	#1
D-09	Données sur la production d'énergie		X	#1
D-10	Données d'interaction avec le réseau électrique		X	#1
D-11	Données des journaux et des événements du BEMS		X	#1
D-12	Données sur l'occupation et le comportement		X	#1
D-13	Données sur la durabilité environnementale		X	#1
D-14	Données sur l'infrastructure des bâtiments		X	#1
D-15	Données sur les actifs de gestion de l'énergie		X	#1
D-16	Données de synchronisation du temps		X	#2
D-17	Données d'authentification du serveur BEMS	X		#1

6 Rôles et responsabilités

La section suivante liste les acteurs qui contribuent à la mise en œuvre de la cybersécurité des BACS Flex Ready®.

- Flexibilité
    - Opérateurs d'effacement
    - Gestionnaires de l'énergie
    - Fournisseurs d'énergie
    - Fournisseurs BACS
    - Fournisseurs de panneaux de contrôle de l'énergie
- Bâtiments
    - Propriétaires de bâtiment
    - Opérateurs de maintenance
    - Gestionnaire des installations
    - Gestionnaire de bâtiment
    - Intégrateur
- Services
    - Opérateur de point de charge (CPO)
    - Fournisseur de services énergétiques
- Occupants du bâtiment

Cette liste est donnée à titre indicatif, elle sera consolidée avec les autres parties du référentiel de BACS Flex Ready®. L'ensemble de ces acteurs devront s'organiser contractuellement afin de garantir la cybersécurité de l'ensemble du système.

Ce référentiel concerne les mesures techniques que le fournisseur de BACS Flex Ready® doit mettre en œuvre pour protéger le fonctionnement du BACS et pour garantir la sécurité des échanges avec les acteurs impliqués dans la Flexibilité, en particulier les opérateurs d'effacement.

Note : *Tous les rôles mentionnés ci-dessus sont responsables de :*

- *Générer, stocker et protéger les journaux afin de permettre la traçabilité de l'exécution de toute opération sensible sous son contrôle.*
- *Gérer leur PKI conformément aux politiques des autorités de certification reconnues.*
- *CF chapitre Hypothèse*

7 Événements redoutés et impacts

L'identification des événements redoutés est issue du guide de l'ANSSI *"EBIOS Risk Manager"*. Nous décrivons ci-dessous les conséquences et le type d'impact causés par l'atteinte aux biens identifiés dans la section 5 en termes de

- Intégrité
- Disponibilité
- Confidentialité
- Traçabilité
- Qualité du service

ID de l'événement	Evénement	Impact
FE-01	**Cause** : Indisponibilité du dispositif de contrôle du confort des occupants du bâtiment. **Conséquences possibles** : impossibilité de réguler les niveaux de température, humidité, CO2, d'éclairage...	Risques pour la santé et la sécurité des personnes Surconsommation
FE-02	**Cause** : Indisponibilité des services d'urgence du bâtiment **Conséquences possibles** : disfonctionnement de systèmes de détection d'incendie, d'effraction, ... et de réaction : extinction d'incendie, coupure de gaz, (de-)verrouillage de portes, ...	Risques pour la santé et la sécurité des personnes
FE-03	**Cause** : Indisponibilité des services de sécurité du bâtiment. **Conséquences possibles** : désactivation des systèmes de contrôle d'accès, des systèmes de surveillance, des alarmes anti-intrusion, des enregistrements permettant la traçabilité (Log).	Menaces pour la sécurité des bâtiments
FE-04	**Cause** : Indisponibilité des services aux occupants du bâtiment. **Conséquences possibles** : indisponibilité/disfonctionnement des stations de recharge, ascenseurs, alimentation en gaz, chauffage, ventilation et climatisation, alimentation électrique de secours.	Perturbations opérationnelles des services du bâtiment Pertes de revenus associées

ID de l'événement	Evénement	Impact
FE-05	**Cause** : Réseau électrique déséquilibré ou désactivation du système d'alimentation de secours **Conséquences possibles** : coupures de courant et temps d'arrêt du système BACS	Perturbations opérationnelles des services du bâtiment et pertes de revenus associées Risques pour la sécurité et la santé des personnes (patients dans les hôpitaux, les EHPAD)
FE-06	**Cause** : Les dysfonctionnements ou les altérations de la gestion et de la surveillance de l'énergie **Conséquences possibles** : chauffage ou refroidissement excessif des locaux, une mauvaise ventilation.	Perturbations opérationnelles Dommages aux équipements
FE-07	**Cause** : Connexion de dispositifs BACS/BEMS non autorisés et usurpation d'identité **Conséquences possibles** : perturbations de la gestion énergétique du bâtiment.	Perturbations opérationnelles intentionnelles des services du bâtiment et pertes de revenus associées
FE-08	**Cause** : Répartition inefficace de l'énergie à la suite de décisions erronées en matière de réponse à la demande, compteurs trafiqués **Conséquences possibles** : sur/sous facturation par les fournisseurs d'électricité,	Gaspillage d'énergie et perte de revenus associée Litiges
FE-09	**Cause** : accès non autorisé au système d'automatisation des bâtiments **Conséquences possibles** : extraction d'informations sensibles telles que les points de consigne des flexibles d'énergie, la consommation, les données personnelles des occupants, les données de contrôle d'accès au bâtiment. Corruption des données.	Vol de données Fraude Usurpation d'identité
FE-10	**Cause** : accès non autorisé au système de surveillance des bâtiments **Conséquences possibles** : Corruption des enregistrements d'événements, de changements	Litiges juridiques

ID de l'événement	Evénement	Impact
	de système, de dysfonctionnements ou de tentatives d’infractions.	
FE-11	**Cause** : Perte de qualité de service et de performance dans le contrôle du bâtiment, dégradation des contrôleurs **Conséquences possibles :** non-respect de la réglementation (normes)	Non-conformité Dommages à la réputation

8 Modèle de menace

Ce chapitre décrit les menaces déterminées sur les interfaces API (#1) et Time Sync (#2). Ces menaces sont dérivées en utilisant la méthodologie STRIDE. Les attaques visées se réfèrent aux attaques de MITRE.

La structure des menaces définit :

- L'identifiant de la menace,
- Les événements redoutés concernés,
- Les catégories STRIDE (voir annexe B),
- Les vulnérabilités typiques,
- Les données compromises,
- Les tactiques et techniques d'attaque de MITRE (voir annexe B).

8.1 Menaces spécifiques à l'interface API de (#1)

8.1.1 Attaques par injection

ID de la menace	T-API-001
FE ID	FE-06, FE-07, FE-08
Titre de la menace	Attaque par injection SQL
Description de la menace	Un attaquant manipule les entrées pour exécuter des requêtes SQL malveillantes contre la base de données sur le réseau via une API.
STRIDE	Usurpation d'identité, Sabotage
Vulnérabilités	Entrées utilisateur non validées, requêtes SQL dynamiques, pas d'instructions paramétrées pré-configurées, comptes de base de données sur-privilégiés, fuites d'erreurs, injection SQL aveugle et instructions SQL par lots.
Actifs de données affectés	D-04, D-05, D-06, D-07, D-08, D-09, D-10, D-11, D-12, D-13, D-14, D-15, D-17
Références MITRE Attack	Injection de contenu (T1659)

ID de la menace	T-API-002
FE ID	FE-06, FE-07, FE-08
Titre de la menace	Attaque par injection de commande
Description de la menace	Un attaquant cible l'API qui traite de manière incorrecte les données utilisateur, transmises à la ligne de commande du système d'exploitation ou à l'interpréteur de commandes.
STRIDE	Usurpation d'identité, Sabotage

Vulnérabilités	Entrées utilisateur non validées, exécution de commandes dynamiques, paramétrage inapproprié, confiance aveugle dans les entrées externes, accès à des commandes système sensibles, absence de validation des sorties, utilisation inappropriée du mode shell.
Actifs concernés	D-04, D-05, D-06, D-07, D-08, D-09, D-10, D-11, D-12, D-13, D-14, D-15, D-17
Références MITRE Attack	Injection de contenu (T1659)

ID de la menace	T-API-003
FE ID	FE-06, FE-07, FE-08
Titre de la menace	Attaque par injection NoSQL
Description de la menace	Un attaquant cible l'API pour manipuler des bases de données non relationnelles telles que MongoDB
STRIDE	Usurpation d'identité, Sabotage
Vulnérabilités	Entrées utilisateur non validées, construction de requêtes dynamiques, exploitation des opérateurs logiques, injection NOSQL aveugle.
Actifs de données affectés	D-04, D-05, D-06, D-07, D-08, D-09, D-10, D-11, D-12, D-13, D-14, D-15, D-17
Références MITRE Attack	Injection de contenu (T1659).

8.1.2 Menaces sur l'authentification et l'autorisation

ID de la menace	T-API-004
FE ID	FE-07, FE-09
Titre de la menace	Authentification ou autorisation défaillante
Description de la menace	Un attaquant cible les API avec une authentification incorrecte ou des mécanismes de contrôle d'accès manquants.
STRIDE	Usurpation d'identité, Élévation des privilèges.
Vulnérabilités	Jetons de session faibles, informations d'identification faibles, absence de contrôle d'accès basé sur les rôles (RBAC).
Actifs de données affectés	D-04, D-05, D-06, D-07, D-08, D-09, D-10, D-11, D-12, D-13, D-14, D-15, D-17
Références MITRE Attack	Protocole de la couche application (T1071), Comptes valides (T1078), Déversement de données d'identification (T1003).

8.1.3 *Falsification de requêtes intersites (CSRF)*

ID de la menace	T-API-005
FE ID	FE-06, FE-07, FE-08, FE-09
Titre de la menace	Falsification des requêtes intersites (CSRF).
Description de la menace	Les attaques CSRF peuvent être réalisées lorsque les API gèrent mal l'authentification de l'utilisateur et ne mettent pas en œuvre les protections anti-CSRF.
STRIDE	Usurpation d'identité, Sabotage, Divulgation d'informations.
Vulnérabilités	Les API s'appuient sur les cookies pour la gestion de la session, sans validation de l'origine.
Actifs concernés	D-04, D-05, D-06, D-07, D-08, D-09, D-10, D-11, D-12, D-13, D-14, D-15, D-17
Références MITRE Attack	Protocole de la couche application (T1071).

8.1.4 *Scripts intersites (XSS)*

ID de la menace	T-API-006
FE ID	FE-06, FE-07, FE-08, FE-09
Titre de la menace	Scripts intersites (XSS)
Description de la menace	Un attaquant injecte des scripts malveillants dans les données stockées par l'API ou envoie une charge utile malveillante dans le cadre de la demande d'API.
STRIDE	Usurpation d'identité, Sabotage, Divulgation d'informations
Vulnérabilités	Absence de validation des entrées, Reflected XSS, Stored XSS et DOM-Based XSS
Actifs concernés	D-04, D-05, D-06, D-07, D-08, D-09, D-10, D-11, D-12, D-13, D-14, D-15, D-17
Références MITRE Attack	Protocole de la couche application (T1071)

8.1.5 *Transmission de données non sécurisée*

ID de la menace	T-API-007
FE ID	FE-06, FE-08, FE-09
Titre de la menace	Transmission de données non sécurisée
Description de la menace	Un attaquant intercepte les données entre les agrégateurs et le réseau informatique du BACS en raison de l'absence de chiffrement.
STRIDE	Sabotage, Divulgation d'informations

Vulnérabilités	Absence de chiffrement, protocoles cryptographiques faibles, validation incorrecte des certificats, exposition des données dans la mémoire cache, clés API ou jetons exposés, pas de TLS pour les sockets web, configuration non sécurisée de TLS, exposition aux attaques par canal latéral, messages d'erreur révélant des données sensibles.
Actifs concernés	D-04, D-05, D-06, D-07, D-08, D-09, D-10, D-11, D-12, D-13, D-14, D-15, D-17
Références MITRE Attack	Adversaire au milieu (T1557)

8.1.6 Limitation du débit et épuisement des ressources

ID de la menace	T-API-008
FE ID	FE-01, FE-02, FE-03, FE-04, FE-05
Titre de la menace	Attaques DoS ou DDoS
Description de la menace	Un attaquant cible l'API avec des demandes excessives conduisant à des attaques par déni de service ou par déni de service distribué.
STRIDE	Déni de service
Vulnérabilités	Appels d'API non restreints, traitement inefficace, charges utiles volumineuses, absence d'authentification et d'autorisation, réseaux non sécurisés, mémoire tampon mal configurée.
Actifs concernés	D-04, D-05, D-06, D-07, D-08, D-09, D-10, D-11, D-12, D-13, D-14, D-15, D-17
Références MITRE Attack	Arrêt du service (T1489), Déni de service au niveau du terminal (T1499), Déni de service au niveau du réseau (T1498).

8.1.7 Points d'accès non sécurisés

ID de la menace	T-API-009
FE ID	FE-07, FE-09
Titre de la menace	Points d'accès non sécurisés
Description de la menace	Points d'extrémité Flex BACS et points d'extrémité agrégateurs exposant des fonctionnalités sensibles sans contrôles appropriés, par exemple des points d'extrémité de débogage ou des API d'administration.
STRIDE	Usurpation d'identité, Divulgation d'informations
Vulnérabilités	Manque d'authentification, manque d'autorisation, exposition excessive des données, absence de chiffrement, validation incorrecte des données.
Actifs concernés	D-04, D-05, D-06, D-07, D-08, D-09, D-10, D-11, D-12, D-13, D-14, D-15, D-17
Références MITRE Attack	Exploitation d'une application publique (T1190), Exploitation pour l'exécution d'un client (T1203), Protocole de la couche d'application (T1071), Exploitation pour l'escalade des privilèges (T1068), Exfiltration de commande et de contrôle (T1041).

8.1.8 Sabotage des paramètres

ID de la menace	T-API-010
FE ID	FE-06, FE-07, FE-08
Titre de la menace	Sabotage des paramètres de l'API
Description de la menace	Les attaquants modifient les paramètres de l'API pour manipuler les points de données de surveillance de l'énergie.
STRIDE	Usurpation d'identité, Sabotage
Vulnérabilités	Absence de validation des entrées, contrôles d'autorisation insuffisants, paramètres sensibles exposés, utilisation inappropriée de données côté client, liaison inappropriée des paramètres.
Actifs concernés	D-04, D-05, D-06, D-07, D-08, D-09, D-10, D-11, D-12, D-13, D-14, D-15, D-17
Références MITRE Attack	Exploitation d'une application publique (T1190), Exploitation pour l'exécution d'un client (T1203), Protocole de la couche d'application (T1071), Exploitation pour l'escalade des privilèges (T1068), Exfiltration de commande et de contrôle (T1041).

8.1.9 Falsification des requêtes côté serveur (SSRF)

ID de la menace	T-API-011
FE ID	FE-07, FE-09
Titre de la menace	Falsification des requêtes côté serveur (SSRF)
Description de la menace	Les attaquants exploitent les API pour envoyer des requêtes non autorisées à des services internes ou externes afin d'accéder aux réseaux internes et de voler des données sensibles.
STRIDE	Divulgation d'informations, Élévation des privilèges
Vulnérabilités	Accès aux services internes, exposition aux données sensibles, contournement des pares-feux et des contrôles d'accès
Actifs concernés	D-04, D-05, D-06, D-07, D-08, D-09, D-10, D-11, D-12, D-13, D-14, D-15, D-17
Références MITRE Attack	Exploitation d'une application publique (T1190), exploitation pour l'exécution d'un client (T1203), protocole de la couche application (T1071), exploitation pour l'escalade des privilèges (T1068), exfiltration de commande et de contrôle (T1041), découverte de fichiers et de répertoires (T1083), déni de service d'un point final (T1499).

8.1.10 Mauvaise configuration CORS

ID de la menace	T-API-012
FE ID	FE-07, FE-09
Titre de la menace	Mauvaise configuration CORS

Description de la menace	Les attaquants ciblent les API mal configurées pour permettre l'accès à partir d'origines non fiables.
STRIDE	Divulgation d’informations, Élévation des privilèges.
Vulnérabilités	Autoriser toutes les origines, exposer des données sensibles à des domaines non autorisés, autoriser des informations d'identification, autoriser des en-têtes de type "wild card", traitement inapproprié des demandes de contrôle en amont (preflight).
Actifs concernés	D-04, D-05, D-06, D-07, D-08, D-09, D-10, D-11, D-12, D-13, D-14, D-15, D-17
Références MITRE Attack	Exploitation d'une application publique (T1190), pour l'exécution d'un client (T1203), Exploitation pour l'escalade des privilèges (T1068), Exfiltration de commande et de contrôle (T1041).

8.1.11 Journalisation et surveillance non sécurisées

ID de la menace	T-API-013
FE ID	FE-10
Titre de la menace	Journalisation et surveillance non sécurisées.
Description de la menace	L'absence d'enregistrement adéquat permet aux activités malveillantes de passer inaperçues et d'être répudiées.
STRIDE	Répudiation.
Vulnérabilités	Journalisation insuffisante, journalisation excessive, sabotage des journaux, transmission et stockage des journaux en clair, accès non sécurisé aux journaux, manque d'intégrité des journaux, mauvaises politiques de conservation des journaux, manque de centralisation des journaux.
Actifs concernés	D-07, D-08, D-11,
Références MITRE Attack	Suppression d'indicateurs sur l'hôte (T1070), fichiers ou informations obscurcis (T0127), collecte d'informations sur l'identité de la victime (T1589), comptes valides (T1078), services système (T1569), données provenant du système local (T1005).

8.2 Menaces spécifiques à l'interface Time Sync (#2)

ID de la menace	T-TS-001
FE ID	FE-06, FE-07, FE-08
Titre de la menace	Attaque par usurpation d'identité
Description de la menace	Un attaquant se fait passer pour un serveur de temps légitime et fournit des données temporelles incorrectes.
STRIDE	Usurpation d’identité

Vulnérabilités	Absence d'authentification dans les protocoles de synchronisation du temps (par exemple, NTP, PTP), absence de chiffrement ou de protection de l'intégrité dans les anciennes versions de NTP, validation faible ou inexistante des sources de temps par les clients, vulnérabilités de PTP, serveurs de temps publics non sécurisés.
Actifs de données affectés	D-16
Références MITRE Attack	Protocole de la couche d'application (T1071), Exfiltration par commande et contrôle (T1041)

ID de la menace	T-TS-002
FE ID	FE-06, FE-07, FE-08
Titre de la menace	Attaque de l'homme du milieu
Description de la menace	Un attaquant intercepte et manipule les messages de synchronisation temporelle entre le BEMS et le serveur de temps.
STRIDE	Sabotage
Vulnérabilités	Absence de chiffrement et d'authentification, absence de nonces ou d'horodatage, absence de contrôles d'intégrité.
Actifs de données affectés	D-16
Références MITRE Attack	Adversaire au milieu (T1557)

ID de la menace	T-TS-003
FE ID	FE-06, FE-07, FE-08
Titre de la menace	Rejeu
Description de la menace	Les messages de synchronisation temporelle légitimes sont capturés et rejoués ultérieurement.
STRIDE	Sabotage
Vulnérabilités	Absence d'authentification des messages, absence de nonces ou d'horodatage, absence de contrôle d'intégrité, absence d'expiration ou de fenêtre temporelle, absence de canaux de transmission sécurisés, absence de sécurité du réseau.
Actifs de données affectés	D-16
Références MITRE Attack	Adversaire au milieu (T1557)

ID de la menace	T-TS-004
FE ID	FE-01, FE-02, FE-03, FE-04, FE-05
Titre de la menace	Attaque d'amplification
Description de la menace	Le serveur de temps ou le réseau est surchargé de demandes, ce qui empêche la synchronisation de l'heure.
STRIDE	Déni de service.
Vulnérabilités	Absence de limitation de débit, absence de contrôle d'accès, serveurs de temps ouverts, vulnérabilités de la diffusion et de la multidiffusion.
Actifs de données affectés	D-16
Références MITRE Attack	Déni de service au niveau du terminal (T1499), Déni de service au niveau du réseau (T1498).

8.3 Menaces communes spécifiques à l'interface d'utilisation (#3)

Les utilisations sont les équipements locaux connectés dans les zones du bâtiment avec des contrôleurs d'équipement. Le contrôleur d'équipement interagit avec les capteurs et les dispositifs de contrôle (VAV, moteurs, etc.), qui sont supervisés par le contrôleur d'automatisation. Ainsi, pour le "PBF", les menaces communes sont identifiées, mais elles ne sont pas détaillées puisqu'elles existent pour les BACS non- Flex Ready®. Les menaces communes à toutes les utilisations (CVC, éclairage, PV et VE) sont les suivantes :

ID de la menace	T-US-001
FE ID	FE-01, FE-02, FE-03, FE-04, FE-05, FE-06, FE-07, FE-08, FE-09, FE-10, FE-11
Menaces	Accès non autorisé Attaques en réseau Logiciels malveillants et rançongiciels Menaces internes Attaques par usurpation d'identité Altération physique Attaques DDoS/DoS
Titre de la menace	Menaces courantes pour les usages pilotés
Description de la menace	
STRIDE	Usurpation d’identité, Sabotage, Répudiation, Divulgation d’informations, Déni de service, Élévation des privilèges
Actifs de données affectés	D-01, D-02 & D-03

9 Contrôles de sécurité et méthodologie d'évaluation

9.1 Introduction

Une liste de contrôles applicables à la phase Pilote a été établie pour éliminer ou de réduire l'impact des menaces identifiées au chapitre 8. Les contrôles sont regroupés dans les 9 catégories ci-dessous.

La liste des 51 contrôles est fournie séparément dans des fichiers Excel (voir en fin de ce chapitre).

Cette liste sert de base pour mesurer la cybersécurité de la solution en fonction du contexte (typologie, criticité du bâtiment concerné, ...).

Cette liste détaillée a pour but d'apporter de la transparence à l'ensemble des acteurs sur ce qui est réellement mis en œuvre. L'efficacité de ces contrôles s'appuie sur la contribution de l'ensemble des acteurs

- Le développeur de BACS a la responsabilité de fournir les fonctionnalités identifiées dans les contrôles (par exemple authentification des opérateurs d'effacement)
- Le gestionnaire de bâtiment a la responsabilité de sélectionner les contrôles à activer et les données à injecter par l'intégrateur, sur la base d'une analyse de risque. L'analyse de risque doit démontrer que les contrôles mis en œuvre sont suffisants pour protéger le bâtiment et ses équipements et les opérateurs d'effacement. Le gestionnaire de bâtiment a également la responsabilité de mettre en œuvre les contrôles organisationnels (Liste à jour d'équipements ou de personnes autorisées, organisation d'audit, ...).
- L'intégrateur a la responsabilité de configurer le BACS avec les informations pertinentes en suivant les instructions du gestionnaire du bâtiment et les procédures préconisées par le fournisseur de BACS.
- Le mainteneur a la responsabilité de maintenir le BACS en condition de sécurité en suivant les instructions du gestionnaire du bâtiment et les procédures préconisées par le fournisseur de BACS.

Le GIMELEC identifie dans cette liste un ensemble de contrôles qui constituent **le socle minimal qui s'impose quel que soit la topologie ou la criticité du bâtiment**. Il consiste à garantir à minima que seuls les acteurs autorisés peuvent se connecter au BACS (localement ou à distance).

Les contrôles encadrés constituent ce socle minimal et sont au nombre de 5.

Selon la typologie, les besoins et la criticité bâtiment, tout ou partie des **contrôles additionnels** devront être implémentés pour répondre aux risques identifiés dans **l'analyse de risque**. Ces contrôles concernent la sécurité, le fonctionnement correct et la disponibilité des services offerts par le BACS et utilisés dans les bâtiments.

9.2 Catégories de contrôles

1. **Authentification des dispositifs/hôtes et des données de communication entre le système BACS et les opérateurs externes**

- C-5 : Authentification du BACS auprès des hôtes externes
- C-6 : Expiration et révocation pour l'authentification du BACS et de ses hôtes externes
- C-14 : Utilisation de certificats émis par une autorité de certification de confiance pour assurer l'authentification des hôtes externes et de l'API BACS
- C-36 : Utiliser des mots de passe et une authentification multifactorielle
- C-39 : Utiliser des méthodes d'authentification des "usages pilotés". Comme les certificats numériques
- C-41 : Mettre en place un contrôle d'accès pour les "usages pilotés"
-

2. **<u>Chiffrement des données en transit et au repos</u>**
   - C-12 : Chiffrement de la couche application
   - C-13 : Chiffrement de la couche transport
   - C-15 : Protection des communications bidirectionnelles entre l'API BACS et les hôtes externes
   - C-26 : Protéger l'intégrité des logs entre l'API et les hôtes externes
   - C-27 : Déployer les versions sécurisées des protocoles de synchronisation du temps
   - C-28 : Activer les mécanismes de Chiffrement et d'authentification pour le trafic de synchronisation temporelle.
   - C-29 : Chiffrement de la communication entre le BEMS/BACS et les serveurs de temps
   - C-30 : Chiffrement et authentification des paquets IP en transit
   - C-37 : Désactiver les protocoles non sécurisés
   - C-38 : Chiffrer les communications entre les "usages pilotés" et les contrôleurs BACS

-

3. **<u>Assainissement et filtrage pour protéger des données</u>**
   - C-1 : Validation des entrées du BACS
   - C-2 : Filtrage des appareils et des hôtes se connectant à l'API
   - C-4 : Validation des sorties du BACS
   - C-18 : Surveiller et bloquer requêtes non autorisées et les requêtes répétées
   - C-23 : Définir des en-têtes "Access-Control-Allow-Origin" stricts
   - C-33 : Filtrage des appareils et des hôtes se connectant au serveur de temps
   - C-43 : Filtrage des connexions des "usages pilotés" aux contrôleurs BACS
   - C-44 : Restreindre l'accès physique aux "usages pilotés" et aux contrôleurs BACS critiques au seul personnel autorisé

4. **<u>Techniques de protection de la disponibilité</u>**
   - C-16 : Limitation du nombre de requêtes
   - C-17 : Rejet des requêtes ayant une charge utile supérieure surdimensionnée.
   - C-34 : Protection du serveur de temps.

   C-46 : Prévention des attaques DDos entre les "usages pilotés" et les contrôleurs BACS.

5. **<u>Autorisation</u>**
   - C-7 : Contrôle d'accès pour les hôtes externes lors de la communication avec l'API.
   - C-41 : Mettre en place un contrôle d'accès pour les "usages pilotés".
   - C-51 : Serveur proxy pour accéder au BACS (PAM)

6. **Journalisation sécurisée**
    - C-25 : Assurer une journalisation complète et éviter d'enregistrer des informations sensibles inutiles

    C-47 : Enregistrer tous les événements fonctionnels

7. **Contrôle d'intégrité**
    - C-40 : Validation/ intégrité des données des capteurs
    - C-45 : Détection d'altération physique ou de tentatives d'accès physique

-

8. **Techniques anti-rejeu**
    - C-31 : Protection contre le rejeu - Identifiants de paquets

    C-32 : Protection contre le rejeu - Serveur de temps multiples

9. **Les bonnes pratiques généralement applicables.**
    - C-3 : Ne pas utiliser les commandes Shell
    - C-8 : Utilisation de jetons anti-CSRF
    - C-9 : Empêcher les demandes d'origines croisée
    - C-10 : Encodage de la sortie
    - C-11 : Prévention des attaques XSS (Cross-site scripting)
    - C-19 : Éviter d'exposer les "Endpoint" sensibles en environnement ouvert.
    - C-20 : Audit des vulnérabilités des "Endpoint"
    - C-21 : Empêcher les accès aux adresses IP internes
    - C-22 : Mettre en place une liste blanche d'Url d'hôtes externes.
    - C-24 : Restreindre le partage des ressources entre origines multiples (politiques CORS)
    - C-35 : Désactiver la commande "monlist" si le protocole NTP est utilisé pour la synchronisation du temps
    - C-48 : Sécuriser les accès administrateurs
    - C-49 : Installation systématique des correctifs de sécurité approuvés
    - C-50 : Installation sécurisée des logiciels

9.3 Contrôles détaillés

Les contrôles détaillés sont fournis sous forme de fichiers Excel à destination
- des gestionnaires de bâtiments,
- des fournisseurs de BACS Flex Ready®,
- des opérateurs de flexibilité.

Ces fichiers contiennent un identifiant unique pour chaque contrôle, une description, le caractère obligatoire ou optionnel du contrôle et les éléments à produire pour étayer l'auto-déclaration de respect des contrôles.

A chaque contrôle est associé une liste d'éléments de preuve qui pourront être utilisés pour étayer la déclaration de conformité au référentiel et ou servir dans le cadre d'une évaluation par un tiers.

Interface	ID de contrô	Categorie de contrô	Titre du contrôle	Explication	Menaces concernées	Références menaces dans le document	Obligatoire/Optionnel	Les preuves	Conforme / Non Conforme/ Non applic	
Interface #1 (OE - BACS)	C-1	Assainissement et filtrage	Validation des entrées du BACS	Validation des données d'entrée de l'API . Valider et assainir toutes les entrées de l'utilisateur et rejeter les caractères ou entrées inattendus - concerne le BACS	Attaque par injection SQL, attaque par injection de commandes, attaque par injection NoSQL, Cross Site Scripting (XSS)	T-API-001, T-API-002, T-API-003, T-API-006	Obligatoire	Vérifier si la validation des entrées exigée dans la spécification de l'API est suffisante et définir la méthodologie de test.		
Interface #1 (OE - BACS)	C-2	Assainissement et filtrage	Filtrage des appareils et des hôtes se connectant à l'API	Mettre en place un pare-feu d'application Web (WAF) pour utiliser la liste blanche des entrées plutôt que la liste noire.	Attaque par injection SQL, attaque par injection de commandes, attaque par injection NoSQL	T-API-001, T-API-002, T-API-003	Obligatoire	Démontrer la mise en place du parfeu et l'implementation de la liste blanche.		
Interface #1 (OE - BACS)	C-3	Bonnes pratiques	Ne pas utiliser les commandes Shell.	Utiliser uniquement les bibliothèques incluses dans langage de programmation sans exécution directe de commandes Shell sur le serveur de l'API.	Attaque par injection de commandes	T-API-002	Obligatoire	Démontrer l'absence de commande système.		
Interface #1 (OE - BACS)	C-4	Assainissement et filtrage	Validation des sorties du BACS.	Validation des données de sortie de l'API: restreindre et assainir les commandes de sortie avant de les renvoyer aux utilisateurs.	Attaque par injection de commandes	T-API-002	Obligatoire	Démontrer que le trafic de sortie de l'API est un message structuré pour la communication: l'unicité de l'instance, le format ou la cohérence des données.		
Interface #1 (OE - BACS)	C-5	Authentification	Authentification du BACS auprès des hôtes externes	Authentification forte de l'API BACS auprès des hôtes externes. Utiliser les protocoles d'authentification OAuth 2.0, OpenID Connect.	Accès non autorisé, altération des paramètres de l'API	T-API-004, T-API-010	Obligatoire	Fournir la spécification du mécanisme d'authentification utilisé par l'API		
Interface #1 (OE - BACS)	C-6	Authentification	Expiration et révocation pour l'authentification du BACS et de ses hôtes externes.	Authentifier l'API BACS auprès des hôtes externes. Utiliser des jetons sécurisés (JWT) avec mécanisme d'expiration et de révocation. Se référer au guide https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs	Accès non autorisé	T-API-004	Obligatoire	Démontrer que l'authentification de l'API est basée sur Secure JWT et qu'elle est mise en œuvre conformément aux recommandations.		
Interface #1 (OE - BACS)	C-7	Autorisation	Contrôle d'accès pour les hôtes externes lors de la communication avec l'API.	Mettre en œuvre un système RBAC et appliquer le principe du moindre privilège.	Accès non autorisé	T-API-004	Obligatoire	Liste des recommandations et des primitives disponible. Il est recommandé d'utiliser à moyen terme Oauth 2.0/ Active Directory.		
Interface #1 (OE - BACS)	C-8	Bonnes pratiques	Utilisation de jetons anti-CSRF	Utiliser des jetons anti-CSRF pour restreindre les requêtes utilisateurs aux sites légitimes. Générer et valider un jeton unique pour chaque session avec une demande de changement d'état envoyée via un en-tête personnalisé.	Falsification des requêtes intersites (CSRF)	T-API-005	Obligatoire	Démontrer la génération de jetons contenant les actions autorisées et leur insertion dans les demandes API pour empêcher les actions non autorisées.		
Interface #1 (OE - BACS)	C-9	Bonnes pratiques	Empêcher les demandes d'origines croisée	Utiliser SameSite, un mécanisme de sécurité du navigateur qui détermine si les cookies d'un site web sont inclus dans des requêtes provenant d'autres sites web. Configurer les cookies avec l'attribut SameSite=strict ou SameSite=Lax pour empêcher les demandes d'origine croisée. Se référer au guide https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs	Falsification des requêtes intersites (CSRF)	T-API-005	Optionnel	Démontrer que Samesite a été activé et qu'il limite les requêtes intersites conformément aux préconisations.		
Interface #1 (OE - BACS)	C-10	Bonnes pratiques	Encodage de la sortie	L'encodage des sorties transforme les caractères spéciaux de la balise script en leurs équivalents codés HTML, empêchant ainsi l'exécution du script dans le navigateur. Encoder toutes les entrées de l'utilisateur avant de les inclure dans une réponse de l'API.	Scripts intersites (XSS)	T-API-006	Obligatoire	Fournir des préconisations pour configurer le codage de sortie des requêtes API afin de s'assurer que les données sont traitées comme du texte en clair, ce qui permet d'éviter les attaques XSS.		
				Appliquer un en-tête de politique de sécurité du contenu strict pour						

Les fichiers sont disponibles en ligne sur le site du GIMELEC : https://gimelec.fr/flexready

Annexe A – Architecture détaillée

La figure ci-dessous représente le BACS Flex Ready® qui content les fonctionnalités du BEMS et du BACS non- Flex Ready®. Le BACS Flex Ready® surveille la consommation d'énergie en temps réel du chauffage, de la ventilation et de la climatisation, de l'éclairage, des véhicules électriques et du PVC.

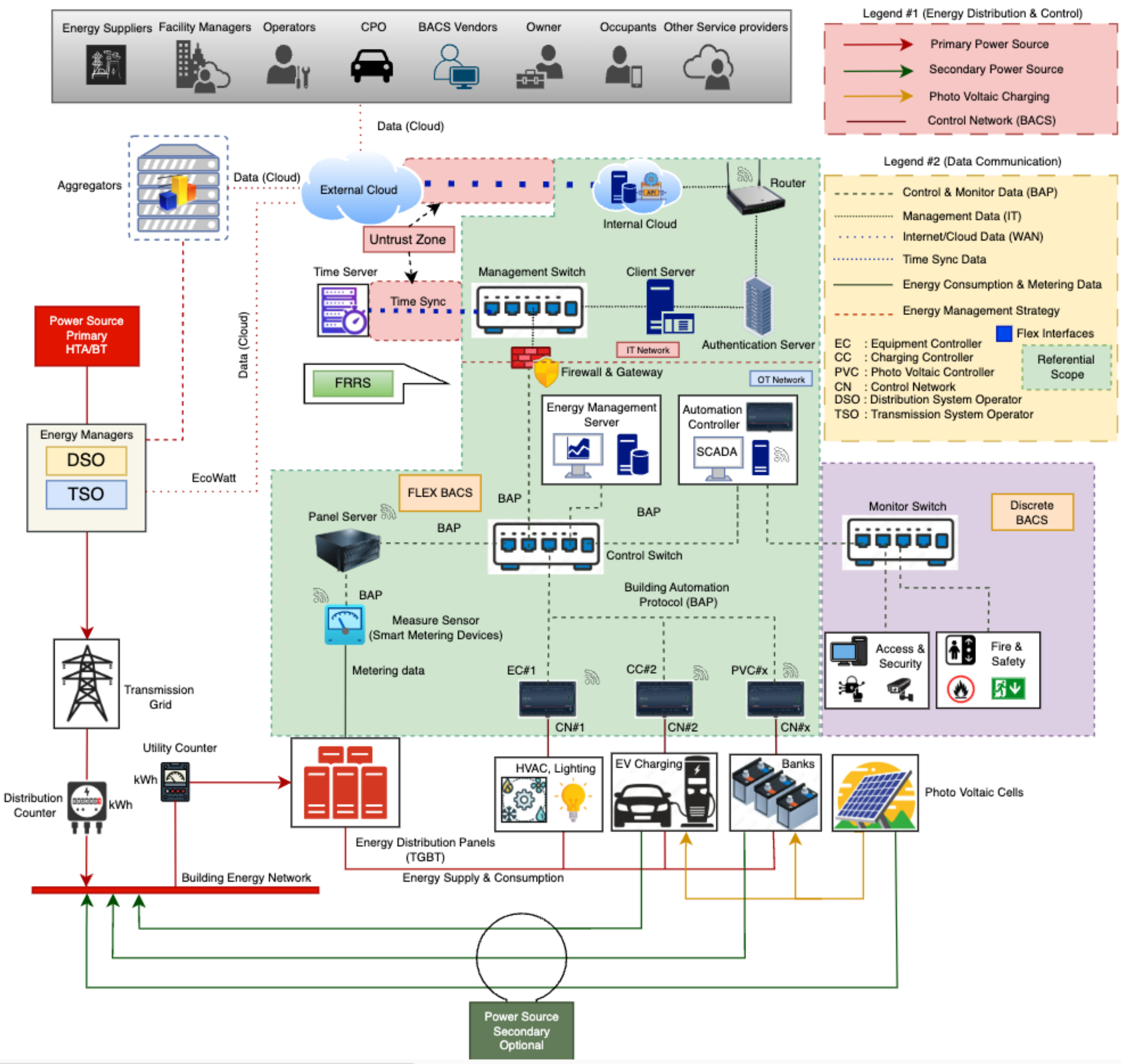

Figure3 : Architecture typique d'un BACS flexible

Annexe B – Méthodologies

STRIDE est un cadre de modélisation des menaces développé par Microsoft pour identifier et classer les menaces potentielles pour la sécurité d'un système. Il aide les organisations à comprendre et à atténuer les vulnérabilités des logiciels, des systèmes ou des processus en les classant par catégories.

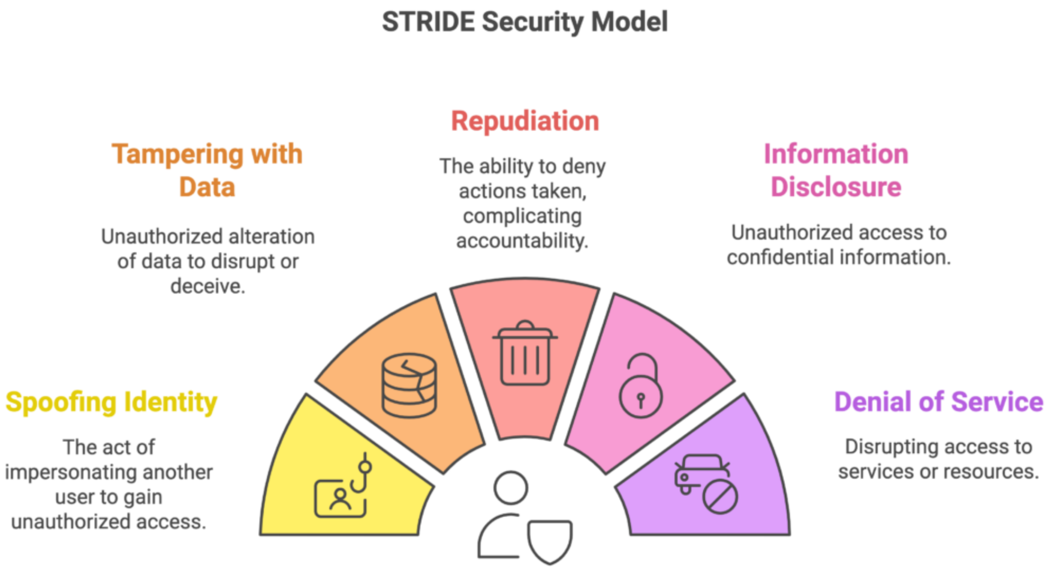

Figure4 : infographie STRIDE

Plus d'informations ici [: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats](https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats)

Le cadre **ATT&CK** de **MITRE** (Adversarial Tactics, Techniques, and Common Knowledge) est une base de connaissances complète et accessible dans le monde entier sur les tactiques et techniques des adversaires, basée sur des observations du monde réel. Développé par MITRE Corporation, il est largement utilisé dans le domaine de la cybersécurité pour comprendre, détecter et répondre aux cybermenaces. Plus d'informations ici.

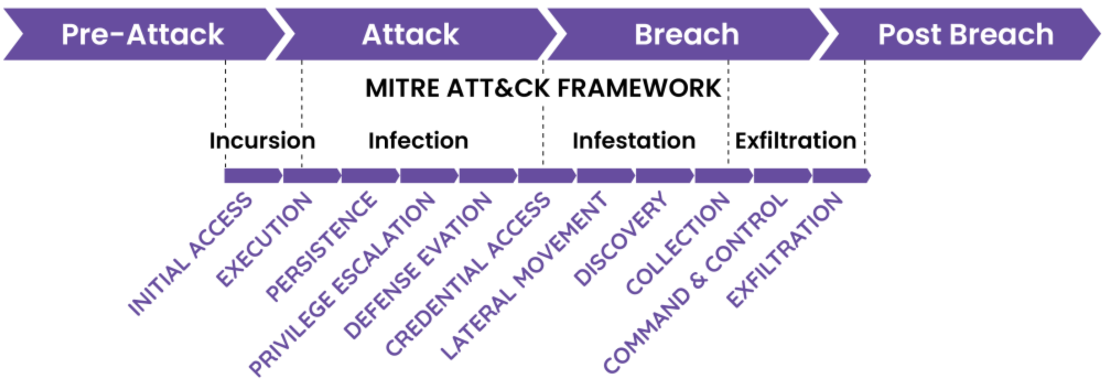

Figure5 : Infographie de MITRE

Annexe C – Abréviations

API ::	Interface de programmation d'applications
BACS :	Système d'automatisation et de contrôle des bâtiments
BAP :	Protocole d'automatisation des bâtiments
BMS :	Système de gestion des bâtiments
BEMS :	Système de gestion de l'énergie des bâtiments
CORS :	Partage de ressources inter-origines
CSRF :	Falsification des requêtes intersites
DoS :	Déni de service
DDoS :	Déni de service distribué
DSO :	Gestionnaire de réseau de distribution
EMS :	Système de gestion de l'énergie
VE :	Véhicule électrique
GPS :	Système de positionnement global
FE :	Événement redouté
IT :	Internet
JWT :	Jeton Web JSON
HSTS :	HTTP Strict Transport Security (sécurité stricte du transport)
HTTP :	Protocole de transfert de texte
HTTPS :	Hyper Text Transfer Protocol Secure (protocole de transfert de texte sécurisé)
CVC :	et refroidissement
IP :	Protocole Internet
LAN :	Réseau local
NTP :	Network Time Protocol (protocole de temps réseau)
NTS :	Network Time Security (sécurité du temps en réseau)
OAuth :	Autorisation ouverte
OS :	Système d'exploitation
PBF :	Périmètre du BACS Flex Ready® / Flex Ready® Referential Scope
PDL :	Charge de distribution d'énergie
PTP :	Precision Time Protocol (protocole de temps de précision)
PVC :	Photo Voltaic Charging/Cells
SBA :	Smart Building Alliance

SSRF :	Falsification des requêtes côté serveur
TLS :	Transport Layer Security (sécurité de la couche transport)
TSO :	Gestionnaire de réseau de transport
TSP :	Protocole de synchronisation du temps
VLAN :	Réseau local virtuel
WAF :	Web Application Firewall
WAN :	Réseau étendu (Wide Area Network)
XSS :	Cross-Site Scripting

Annexe D Sources d'information

9.4 Secteur du bâtiment

SBA

- FLEXENR-Cahier des Charges Fonctionnel Bâtiment

NG Bailey

- Systèmes de gestion des bâtiments (GTB) - Spécifications générales

RTE

- NEBEF 3.5-Règles pour la valorisation des effacements de consommation sur les marchés de l'énergie
- Baromètre des flexibilités de consommation d'électricité https://www.rte-france.com/analyses-tendances-et-prospectives/barometre-flexibilites-consommation-electricite

GIMELEC

- API FLEXReady® V-12Emulateur Opérateurs d'effacement
- REFERENTIEL BACS Flex Ready®

9.5 Recommandations et orientations

ANSSI

- Maitriser la SSI-La cybersécurité des systèmes industriels
- Audition du Directeur général de l'ANSSI au Sénat : Cybersécurité : audition de l'ANSSI
- Mesures préventives cyber prioritaires : Les Mesures Cyber Préventives Prioritaires | ANSSI
- Le guide d'hygiène informatique : Guide d'hygiène informatique | ANSSI (cyber.gouv.fr)
- Guide des rançongiciels : anssi-guide-attaques par rancongiciels tous concernes-v1.0.pdf (cyber.gouv.fr)
- Recommandation sur l'identification à double facteur et les mots de passe : anssi-guide-authentification multifacteur et mots de passe.pdf (cyber.gouv.fr)-
- Sauvegarde des systèmes d'information ; Sauvegarde des SI : L'essentiel

9.6 Textes juridiques nationaux

- Décret BACS https://www.legifrance.gouv.fr/download/pdf?id=GFAP7EBRI-ElnNFUXwSwMtAWhRDD8LWdMqRihxSDaKo=
- Dossiers législatifs - Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité-

9.7 Schémas d'évaluation

ETSI

- EN 303 645-EN 303 645 Cybersécurité pour l'Internet des objets grand public : Exigences de base (v2.1.1)

ISA/IEC

- 62443-ISA/IEC Norme de cybersécurité industrielle

9.8 Méthodologies

ANSSI

- EBIOS Risk Manager v1.0-ANSSI

Microsoft

- Méthodologie STRIDE-Microsoft STRIDE

Tactiques et techniques

- Références de MITRE en matière d'attaques pour les tactiques, les techniques et les mesures d'atténuation MITRE ATT&CK

9.9 Règlements de l'UE

- Directive relative aux équipements hertziens (RED),
- Loi sur la résilience cybernétique, https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
- NIS2 https://cyber.gouv.fr/la-directive-nis-

FIN DU DOCUMENT