

# Fiche de liaison

## Gestion Technique Centralisée

CHAUFFAGE, VENTILATION, CLIMATISATION

Version 3.3 du 14 juin 2024

Tableau de versions		
04/03/16	Version 1	Eric Gindre : extraction et re-formulation à partir du document de travail CCTP du 14/11/14
07/03/16	Version 1.1	Eric Gindre : ajout parties sur la journalisation.
26/09/16	Version 1.2	Eric Gindre : ajout services export fichiers / serveurs de temps
21/03/17	Version 1.3	Eric Gindre : Précision chapitre 4.2 Archives et journalisation
05/02/19	Version 2.0	Eric Gindre : refonte idée générale
06/04/21	Version 2.1	Eric Gindre : refonte avec nouvelles évolutions
09/04/21	Version 2.2	Eric Gindre : ajouts des annexes
18/01/22	Version 2.3	Eric Gindre : adaptation Nantes Université et évolutions mineures
26/01/22	Version 2.4	Eric Gindre : ajout memento des livrables, amendement paragraphe sécurité et corrections mineures
04/02/22	Version 2.5	Eric Gindre : amendement contraintes non négociables
24/06/22	Version 2.6	Eric Gindre : complément focus sur la sécurité

04/01/2023	Version 2.7	Emmanuel Bas : relecture et ajout exigences DAT et MCO/MCS
23/01/23	Version 2.8	Eric GINDRE : Mise en forme et fusion amendement RSSI (E. BAS)
09/02/23	Version 2.9	Eric Gindre : ajout précisions sur le protocole Bacnet. Relecture Thomas Boudard
03/03/23	Version 3.0	Eric Gindre : apport chapitre 7.3 (Tangui Gourvennec)
16/03/23	Version 3.1	Eric Gindre : amendement pré-requis fichier de télé-re-lève de comptage.
26/10/23	Version 3.2	Eric Gindre & Jérémy De rochefort : ajout Spécificité protocole LoRa
14/06/24	Version 3.3	Eric Pénot : Adaptation aux évolutions contextuelles.

# 1. Sommaire

2. Liste des acronymes .....	6
3. Contexte et Enjeux .....	8
4. Architecture, constitution du système.....	8
4.1. Dossier d'architecture technique.....	8
4.2. Accès en HTTP - Accès local et à distance .....	8
4.2. Logiciel de supervision .....	9
4.3. Protocoles de communication et réseau informatique .....	9
4.4. Équipements tiers.....	11
4.5. Maintenance.....	11
4.6. Sécurité .....	12
4.7. Intégration dans l'existant.....	13
5. Serveur de supervision .....	13
5.1. Matériel.....	13
5.2. Archivage et journalisation.....	14
5.3. Accès.....	15
6. Supervision .....	16
6.1. Niveaux d'accès .....	16
6.2. Synoptiques .....	16
6.3. Protocoles .....	16
6.4. Notifications / alertes .....	17
6.5. Base de données .....	17
6.6. Solution logicielle .....	18
6.7. Journalisation .....	18
6.8. Accès clients .....	18
7. Pilotage Efficacité énergétique .....	19
7.1. Outil en production.....	19
7.2. Procédure de liaison .....	19
7.3. Modèle et format du fichier .....	20
8. Service de temps.....	20
9. Prestation.....	21

9.1. Analyse technique.....	21
9.2. Mise en service .....	21
9.3. Formation/Manuel d'utilisation .....	21
9.4. Sécurité.....	21
9.5. Livrables .....	22
10. Annexe.....	24
10.1 Schéma de principe de l'architecture GTC type .....	24
10.2 Tableau de correspondance objet Ethernet.....	24
10.3 Modèle de fichier d'index de consommation .....	25
10.4 Mémento des livrables.....	25
10.5 Exigences intangibles .....	27

## 2. Liste des acronymes

Annuaire LDAP	Lightweight Directory Access Protocol : norme pour les systèmes d'annuaires, incluant une structure de modèle de données, basé sur le protocole LDAP, Un annuaire LDAP respecte généralement le modèle X.500 édicté par l'UIT-T.
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information : <a href="http://www.ssi.gouv.fr/">http://www.ssi.gouv.fr/</a>
BBMD	BACnet/IP Broadcast Management Device La notion de BBMD correspond à une fonction de <i>propagation dirigée</i> des messages broadcast. Une fonction BBMD doit être présente sur chacun des segments de réseau qui doit être relié à un autre segment au travers d'un dispositif qui filtre les messages broadcast.
broadcast	Un broadcast dans un réseau informatique est un message qui est transmis à tous les participants d'un réseau et qui ne nécessite pas de réponse. Un élément actif du réseau envoie simultanément un paquet de données à tous les autres participants du réseau sans indication particulière d'adresses des destinataires.
CERT	Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques <a href="https://www.cert.ssi.gouv.fr/">https://www.cert.ssi.gouv.fr/</a>
Code RUS	Référentiel Universitaire des Surfaces. Référentiel unique de nomenclature des locaux et des surfaces élaboré en interne. Celui-ci décrit l'ensemble des éléments du SIP de Nantes Université.

	Il s'agit d'une suite de chiffres et de caractères normées ww_xx_yy_zzzz ww = code site géographique - xx = code bâtiment - yy = code niveau - zzzz code surface/local
DHCP	Dynamic Host Configuration Protocol ou protocole de configuration dynamique des hôtes, est un protocole réseau chargé d'assurer la configuration automatique d'un matériel communicant.
DPO	Délégué à la Protection des Données : responsable de l'application et du respect de la protection des données selon le <b>RGPD</b> .
DPIL	Direction du Patrimoine Immobilier et de la Logistique
DSIN	Direction des Systèmes d'Information et du Numérique
FQDN	Fully Qualified Domain Name ou nom de domaine pleinement qualifié est un nom de domaine complet qui désigne une machine déclarée sur un domaine informatique et permettant la correspondance (résolution) entre adresse IP et nom exprimé.
GTB / GTC	Gestion Technique du Bâtiment / Gestion Technique Centralisée
HTTP(S)	HyperText Transfer Protocol(Secure) ou protocole de transfert hypertexte (sécurisé) est un protocole de communication client – serveur développé pour le WEB. Https est la combinaison de <b>http</b> avec une couche de chiffrement afin de garantir la confidentialité et l'intégrité de la donnée dans les échanges client-serveur WEB. Les ports standards sont 80 pour le http et 443 pour le https.
LTS	Long Term Support : Terme générique pour indiquer qu'une version sera maintenue pendant un laps de temps assez long, gage de pérennité d'une solution sans mise à jour lourde.
MCO / MCS	Maintien en Condition Opérationnelle / Maintien en Condition de Sécurité
PSSIE, PSSI	Politique de Sécurité des Systèmes d'Information de l'État, Politique de Sécurité des Systèmes d'Information de l'université lié à la PSSIE
RGPD	Le règlement européen sur la protection des données ( <b>GDPR</b> en abréviation anglaise ou <b>RGPD</b> en abréviation française) impose depuis mai 2018 de nouvelles directives concernant le traitement des données à caractère personnel.
RSSI	Responsable de la Sécurité des Systèmes d'Information. Expert qui garantit la sécurité, l'intégrité et la disponibilité du système d'information d'une organisation
SGBD	Systèmes de Gestion de Bases de Données : solutions logicielles de gestion de bases de données informatiques.
SI	Système d'Information
SIP	Système d'Information Patrimonial.

SSH	Secure Shell est à la fois un programme informatique et un protocole de communication sécurisé.
TSE	Terminal Server Edition ou désormais RDS (Remote Desktop Service) est un composant de Microsoft Windows (dans les versions clientes et serveur) qui permet à un utilisateur d'accéder à des applications et des données sur un ordinateur distant, via n'importe quel type de réseau.
VLAN	Virtual Local Area Network : couche réseau abstraite permettant le transport étanche d'une plage réseau informatique au travers d'un même élément matériel actif.
VPN	Virtual Private Area Network. Le réseau privé virtuel est une technique d'interconnexion réseau permettant de relier deux réseaux locaux différents par un protocole sécurisé étanche à travers un réseau public (on parle de tunnel) .

### 3. Contexte et Enjeux

La mise en place d'un modèle d'infrastructure permet d'offrir une qualité de service et une rationalisation de l'exploitation des systèmes de GTB tout en respectant les règles de sécurité des systèmes d'information de Nantes Université .

Cette fiche recense les pré-requis techniques des solutions. Elle précise le cadre de fonctionnement et d'interopérabilité avec les infrastructures et les Systèmes d'Information de Nantes Université.

Cette fiche permet également de décrire les spécifications techniques permettant aux nouveaux systèmes installés de s'intégrer dans l'existant.

Elle ne couvre que les aspects techniques informatiques.

## 4. Architecture, constitution du système

### 4.1. Dossier d'architecture technique.

Un dossier d'architecture technique doit être fourni. Il contiendra, a minima, une description des systèmes mis en œuvre, leur rôle, ainsi que le détail des interconnexions réseau entre tous les équipements.

Les configurations et prérequis techniques seront également précisés dans ce dossier.

## 4.2. Accès en HTTP local et à distance

L'architecture mise en place permettra une exploitation (consultation et action) sur site et à distance de la GTB.

Les automates pourront être de type serveur HTTP avec accès par interface locale filaire (RJ45) sur le réseau local assigné (VLAN) afin de faciliter diverses opérations de maintenance, mais devront dans tous les cas être connectés à un serveur superviseur disponible en HTTP, à l'exclusion de tout autre protocole de communication notamment le bureau à distance (RDP), par l'intermédiaire d'un accès réseau sécurisé disponible à partir du réseau général de Nantes Université.

Les pages fournies par le superviseur seront de type HTML, à l'exclusion de tout type de technologie susceptible de faire exécuter du code sur le poste utilisateur (java, etc...), multi-utilisateurs simultanés et multi-postes, de préférence avec le navigateur Firefox dernière version (ou de moins d'un an) à la livraison **sans restrictions ni extensions propriétaires**. L'usage de cet accès pourra s'effectuer dans un environnement de services mandataires (proxy).

Le détail des interconnexions réseau devra impérativement être intégrée au Dossier d'Architecture Technique.

## 5.4.2. Logiciel de supervision

Il est fortement conseillé la mise en place d'un logiciel de supervision sur un serveur dédié qui, seul, permettra la mise à disposition de l'ensemble des données du système de gestion technique du bâtiment, ainsi que son suivi et son éventuelle modification de fonctionnement, auprès des utilisateurs identifiés et autorisés à y accéder.

De ce fait, et en prenant compte comme indiqué au point précédent, que ce superviseur fournira des pages HTML servies par un serveur répondant au protocole HTTP, un poste dédié sur site ne sera pas nécessaire, l'accès au superviseur pouvant s'effectuer à partir du réseau de Nantes Université par toute personnes possédant les droits requis.

A noter que si serveur de supervision il y a, ce serveur sera obligatoirement **hébergé au Datacenter** de Nantes Université.

## 5.1. Protocoles de communication et réseau informatique

**Les automates et autres contrôleurs seront communicants selon des protocoles dit « ouvert »** (donnés ci-dessous), et pourront être multi-protocoles. **L'installation ne comprendra aucun protocole dit « propriétaire ».**

Le système de régulation sera constitué d'un ou plusieurs automates reliés au réseau Ethernet TCP/IP présent sur le site. Ce réseau est de type **VLAN**. Il est dédié à l'usage spécifique de ces équipements. Les automates communiqueront entre eux par le réseau Ethernet et / ou par une liaison de type BUS terrain.

Le serveur de supervision ne se trouvant pas sur le même sous-réseau que les automates. Une opération de routage est mise en place par Nantes Université pour assurer la connectivité. Ce routage bloquant les trames de type **broadcast**, cela peut imposer quelques contraintes avec certains protocoles métier. Il est nécessaire de garder à l'esprit cette limitation technique légitime notamment pour le protocole BACnet, afin d'envisager des relais **BBMD**.

Les paramètres de configuration réseau seront fournis par Nantes Université en retour de la liste complète des adresses MAC des systèmes installés (voir annexe 10.2 ). Le principe retenu s'appuie obligatoirement sur le service **DHCP** avec réservation d'adresse fixe.

Le système installé permettra la consultation et éventuellement la modification de l'ensemble des données des différents automates depuis une unique ressource centralisatrice, serveur HTTP fournissant les pages HTML nécessaires à cet effet.

L'ensemble des automates et autres contrôleurs devront conserver en mémoire la totalité des paramètres et données de régulation dont ils ont besoin (calendrier, consignes...), afin qu'ils puissent continuer à fonctionner en autonomie, y compris la mise en archive des collectes d'information, en cas d'interruption des liaisons entre eux et/ou les interfaces centralisatrices.

La réalisation du câblage des automates et le raccord au réseau informatique sera à la charge de l'installateur de la **GTC**. Les points d'accès normalisés seront de type RJ45 Ethernet catégorie 6.

Les technologies par courant porteur ne sont pas admises pour l'ensemble des applications.

Les technologies de communication par point d'accès WIFI indépendant sont également proscrites.

L'ajout d'éléments actifs intermédiaires sont proscrits si ils ont vocation à être raccordés aux réseaux de l'université (micro-switches...).

Les automates devront pouvoir communiquer à minima avec les protocoles suivants :

- BACnet
- LonTalk
- Ethernet
- TCP/IP
- Modbus
- KNX (si gestion éclairage)



- LoRa

### Particularité du protocole radio LoRa

L'utilisation du **protocole LoRa** est acceptée dans le cas où cela résout une installation contraignante (coût, particularité domaniale, de contractualisation...) de câbles physiques dans les bâtiments. Toutefois, l'utilisation de **LoRa** doit être limitée aux capteurs, la partie contrôle (notamment les automates) devant rester connectée par liaison physique.

La DSIN attire toutefois l'attention sur le fait qu'aucune activité de support ne sera assurée sur les émetteurs LoRa et leurs liaisons avec le récepteurs.

Par ailleurs, chaque récepteur sera interconnecté au reste du réseau par le biais d'un automate « passerelle », disposant de deux ports Ethernet, afin d'être connecté d'une part au réseau **GTB/GTC** du site et d'autre part au récepteur avec lequel il communiquera par **Bacnet/IP** ou **Modbus/IP**.

L'utilisation de services « cloud » pour le traitement des données remontées par les capteurs **LoRa** sera proscrite.

L'implémentation de l'infrastructure LoRa devra respecter en matière de sécurité les recommandations de LoRa Alliance :

[https://lora-alliance.org/resource\\_hub/lorawan-security-faq/](https://lora-alliance.org/resource_hub/lorawan-security-faq/)

## 5.2. Équipements tiers

Certains équipements (centrale de traitement d'air, groupe froid,...) ont leur propre automatisation embarquée et mettent à disposition une liaison de type **ModBus/JBus**. Ces équipements tiers devront pouvoir être reliés via une interface entièrement intégrée aux automates.

## 5.3. Maintenance

Le système devra permettre aux équipes exploitantes de la **DSIN** ou de la **DPIL** de sauvegarder (sous la forme d'un fichier informatique) à n'importe quel moment les programmes des automates et de la supervision sans utilisation de logiciels ou programmes spécifiques, afin de pouvoir restaurer le système, sans matériel ni logiciel propriétaires, en cas de défaillance d'un élément ou de perte de données.

Les mises à jours évolutives et de sécurité devront également faire l'objet d'une livraison avec ressource et documentation ainsi que d'un plan détaillé et chiffré de maintenance. La maintenance du

logiciel de supervision ne sera pas effectuée par la DSIN et devra être planifiée dès le départ par le prestataire du marché.

L'opération d'installation initiale sera dans tous les cas effectuée par l'installateur.

## 5.4. Sécurité

L'infrastructure réseau et l'architecture matérielle et logicielle du système d'information de l'université sont conçues et déployées en respectant les préconisations de l'**ANSSI** en général et de la **Politique de sécurité d'information de l'État (PSSIE)** de Nantes Université en particulier.

Chaque solution envisagée devra se conformer obligatoirement à ces directives. L'offre sera analysée en ce sens afin d'être validée par la **DSIN** avant réalisation par le prestataire.

Notamment :

Les réseaux de l'Université font l'objet d'une segmentation, d'une supervision et d'une surveillance adaptées à leur destination. L'accès à ces réseaux est contrôlé. Les interconnexions de réseaux sont limitées au strict nécessaire et parfaitement maîtrisées.

Les serveurs et les postes de travail fournis par NU sont maintenus en conditions opérationnelles et de sécurité. A ce titre, ils sont assujettis à la politique d'application des mises à jour de sécurité. Les solutions logicielles seront compatibles avec ce principe. Ainsi, en cas d'évolution majeure du système d'exploitation, le soumissionnaire devra prévoir dès l'installation un plan de maintenance et d'intervention pour garantir la compatibilité ascendante de la solution fournie, pendant toute la durée de son exploitation.

Une procédure et/ou une offre de service pour la maintenance et l'application des mises à jour de sécurité devra être clairement décrite par le soumissionnaire. Cette proposition veillera à préciser les engagements de délai quant à la livraison et l'application des correctifs de sécurité les plus critiques.

Les firmwares ou micrologiciels des systèmes déployés ainsi que les solutions logicielles de traitement et de supervision devront être installés dans leur dernière version stable disponible au moment de l'installation et ne comporteront pas de failles de sécurité connues à cette date (responsabilité de l'éditeur).

Nantes Université se réserve le droit d'isoler les matériels voire de les arrêter en cas de vulnérabilité ou de compromission. Ils ne seront remis en fonctionnement qu'avec l'accord du Responsable de la Sécurité des Systèmes d'Information (RSSI).

## 5.5. Intégration dans l'existant

Afin de s'imbriquer dans les installations existantes, les automates pourront intégrer de préférence le protocole de communication BACnet conçu spécialement pour les applications de contrôle et d'automatisation des bâtiments. Adopté à la fois en tant que norme ISO et européenne, il constitue un langage commun permettant l'intégration des systèmes proposés par différents fabricants.

Un système BACnet peut échanger des données avec tout contrôleur BACnet compatible fourni par un autre fabricant et peut être surveillé et géré depuis un superviseur tiers. Le superviseur peut afficher des programmations, alarmes et données en temps réel d'un périphérique tiers et ajuster les paramètres.

La configuration d'un système, afin de permettre l'échange de données avec un autre périphérique BACnet sera effectuée via des modules de communication standard et ne nécessitera aucune connaissance sur le fonctionnement des autres équipements. La configuration du superviseur afin de gérer/surveiller un périphérique tiers sera simple.

Dans le cas d'une rénovation partielle d'un bâtiment ou d'un site possédant déjà un système de **GTC** avec une supervision et qui n'est pas totalement renouvelé dans le cadre de la rénovation, **le nouveau système installé devra s'interfacer / se fusionner avec l'existant** (c.à.d. les éléments restants non renouvelés). Si cela entraîne des modifications sur l'existant (changement de supervision, remise à niveau des automates existants,...), ces modifications seront à la charge du titulaire.

## 6. Serveur de supervision

### 6.1. Matériel

#### - Serveur hébergé.

La ressource logicielle (superviseur) sera hébergée sur un serveur - compatible Linux Debian 64 bits (version stable ou **LTS** à la livraison) ou Redhat/Centos 64 bits (version en cours à la livraison) ou Windows Pro/Windows serveur dernière version à la date d'installation, en version 64 bits.

Dans ce cas, cette infrastructure ne nécessitera **aucun poste informatique pas plus que de terminal dédié** ni de partie cliente à installer sur des postes de travail.

Ce matériel en environnement virtualisé sera fourni et hébergé par Nantes Université dans son Datacenter.

Nantes Université assurera le maintien en condition opérationnelle de cette machine qui sera intégrée au plan de continuité et de reprise d'activité (PCA et PRA). Elle sera donc régulièrement mise à jour avec les correctifs de sécurité recommandés, sous réserve des préconisations de compatibilité fournies par le prestataire en charge de la maintenance, si possible par la DSIN, sinon, directement par le prestataire de maintenance.

#### - Poste de travail local dans un contexte très particulier

Cas de figure le plus simple mais non conseillé.

Cette solution n'est à retenir qu'après une étude argumentée.

Il permet de cadrer au plus près des besoins des exploitants locaux pour un chantier léger non raccordé à une centrale de supervision existante.

A l'heure actuelle le système d'exploitation éprouvé sera soit Windows 10 Pro minimum soit Linux (Ubuntu, Debian version stable ou LTS). Un client ou un logiciel tiers pourra être éventuellement installé sur ce matériel après échange et accord de la DSIN.

La machine sera fournie par le prestataire de l'installation. Un plan de maintenance spécifique devra alors être proposé, qui prendra en charge la maintenance logicielle et matérielle de la machine, ainsi que les montées de version ou corrections de dysfonctionnements du logiciel spécifique installé.

La DSIN n'engage pas sa responsabilité sur la maintenance des accès à distance simultanés en raison des limitations techniques imposées par ce type d'implantation.

Dans les 2 cas de figure, le matériel sera raccordé au VLAN GTB du secteur.

S'agissant du serveur hébergé, une liste des caractéristiques techniques doit également être fournie afin de dimensionner les ressources matérielles de la machine virtuelle ou physique (système d'exploitation, espace disque, mémoire et processeurs).

Les VLAN des serveurs hébergés et des réseaux de terrain étant étanches, il est important de fournir lors de la présentation du plan d'architecture technique, le plan d'interconnexions réseau afin de mettre en place dès l'installation, les règles adéquates de filtrage.

## 6.2. Archivage et journalisation

La sauvegarde générale du système hôte est effectuée par la DSIN. La prise en charge des processus de journalisation système selon les préconisations de la PSSIE est également pris en charge par Nantes Université.

La sauvegarde du serveur virtuel ou physique est pris en charge selon les directives à fournir et les documents d'installation et d'exploitation :

- sauvegarde du système d'exploitation ou non
- sauvegarde de l'environnement logiciel individualisé ou non

La description de la stratégie de sauvegarde devra être fournie dès la projection du chantier.

La valeur de rétention devra également être indiquée si c'est un critère important. Sinon la politique locale sera appliquée : une sauvegarde complète une fois par semaine pendant quatre semaines, puis une sauvegarde complète une fois par mois.

## 6.3. Accès

Les accès à aux serveurs sont prévus à partir des réseaux privés de l'université mais également depuis l'extérieur par mise en place d'un accès à distance sécurisé de type **VPN** (client riche).

**Les accès vers Internet sont exclus.** Si la supervision nécessite des requêtes réseau de quelque type que ce soit, vers l'extérieur du périmètre de Nantes Université, cela devra être mentionnées dans l'architecture des interconnexions réseau afin d'être prises en compte (fonctionnement liste blanche) .

**La DSIN gardera obligatoirement un accès administrateur** système du serveur sur lequel sera installé la supervision. Des comptes (avec possibilité d'administration) pourront être ajoutés sur demande.

Les types d'accès système seront soit des consoles **SSH** pour les environnements Linux soit des connexions **TSE** pour les serveurs Windows soit un bureau à distance dans le cas du poste de travail isolé.

Le cadrage de ces accès potentiels sera effectué dès les premières phases du projet.

Il est nécessaire de fournir le plus tôt possible la liste des intervenants afin de pouvoir créer leur comptes d'accès. Selon notre politique de sécurité (respectant la **PSSIE**) les comptes créés doivent être nominatifs et l'activation assujettie à un bornage de dates (début et fin de validité).

Les différentes parties intervenantes devront également signaler tout changement de situation afin que les comptes d'accès soient modifiés en conséquence (suppression, création...)

Nantes Université respecte le **RGPD**. Le nom du **DPO** peut être fourni sur demande.

## 7. Supervision

### 7.1. Niveaux d'accès

L'accès se fera par un **identifiant / mot de passe**. Il sera possible de créer des groupes d'utilisateurs, associés à des droits en visualisation, modification, suppression, administration. Il sera possible de créer des groupes d'utilisateurs ayant accès uniquement à une partie des équipements, suivant par exemple un critère géographique (un bâtiment uniquement, un site uniquement, ...), fonctionnel (uniquement les équipements relatif au chauffage, à la ventilation...).

A minima trois niveaux d'accès seront possibles :

- un niveau d'accès qui autorisera seulement la visualisation.
- un niveau d'accès intermédiaire ajustable pour la conduite des installations.
- un niveau d'accès à tous les paramètres sans restriction (administrateur) qui permettra également de configurer les différents niveaux d'accès

**Il est vivement souhaité** que ce module de comptes soit **interfaçable avec un annuaire externe de type LDAP ou ActiveDirectory**, au moins pour la partie authentification.

### 7.2. Synoptiques

Le nommage des éléments patrimoniaux, la numérotation devront correspondre au plus près à la nomenclature en vigueur à Nantes Université (**code RUS** et nom d'usage). Elle sera fournie par la DPIL.

### 7.3. Protocoles

Les interfaces d'exploitation (y compris la supervision) utiliseront classiquement le protocole de communication **https en priorité, à défaut le protocole http**, qui fourniront des pages de type HTML exclusivement, en utilisant des **ports fixes et non aléatoires** . Le synoptique des différentes connexions réseau associé à leur protocole de communication devra être fournie avec l'offre.

En cas d'exposition de la ressource sur une zone de nommage privée de l'université – de type \*.univ-nantes.prive, un certificat auto-signé sera toléré. La **DSIN** fournira le nom complet (**FQDN**) des ressources à atteindre.

Il est possible également de mettre en place un nommage avec certification valide. Dans ce cas, la **DSIN** fournira

- le **FQDN** sur la zone intra.univ-nantes.fr
- le certificat valide de la zone

L'accès WEB sécurisé **https** est fortement recommandé, selon la **PSSIE**. Dans certains cas qui demanderont une étude de la **DSIN**, il sera possible de n'avoir que le protocole **http**.

La déclaration d'un nom associé à un domaine (**FQDN**) sera systématique pour ces ressources lorsque il y aura affectation d'une adresse IP.

**La requête par adresse IP directe est à proscrire.** La déclaration de liens en @IP dans le mécanisme du logiciel est également à proscrire.

## 7.4. Notifications / alertes

Une fonction de transmission de notification et d'alerte devra être possible par envoi de courriers électroniques, voire de télé-versement par FTP d'informations sur le collecteur d'informations central (données télémétriques de consommations) installé à l'université.

Nantes Université possède son propre relai de messagerie interne. Les caractéristiques seront fournies au moment du paramétrage.

## 7.5. Base de données

Si une base de données est requise hors intégration logicielle, celle-ci pourra être fournie par la **DSIN** notamment pour les **SGBD** suivants :

- Oracle
- MySQL / MariaDB
- MS-SQL Server

(version courante au jour de la prestation)

Pour Oracle et MS-SQL Server, ce sera de préférence en environnement partagé (contrainte de licences).

Ce besoin fera l'objet d'une étude préliminaire systématique de faisabilité par la **DSIN** afin que ses équipes puissent l'intégrer dans leur périmètre d'exploitation.

Les autres types pourront faire l'objet d'une étude de potentialité d'exploitation sans engagement de résultat ni d'exploitation par la **DSIN**.

## 7.6. Solution logicielle

Les services applicatifs déployés devront se conformer à la **PSSIE** et aux règles élémentaires de sécurité. Ils devront être compatibles avec le système d'exploitation pré-cité sans adaptation spécifique lourde.

Cette infrastructure ne nécessitera ni aucun poste informatique ni terminal dédié ni de partie cliente à installer sur des postes de travail.

Sauf cas très particulier elle sera installée sur la machine virtuelle dédiée, hébergée au data center de Nantes Université.

Les processus, voire les conditions de mises à jour correctives devront être exposées dans l'offre.

Cela devra faire l'objet d'un contrat de maintenance le cas échéant.

## 7.7. Journalisation

La **PSSIE** stipule une journalisation à plusieurs niveaux. Il est fortement recommandé que l'application puisse à minima journaliser les accès (comptes et date/heures). Il est souhaitable également que les processus dits « sensibles » soient également archivés.

De même il est souhaité que ces fichiers puissent être déportés sur la gestion centralisée des journaux mise en place à Nantes Université.

Le prestataire doit impérativement indiquer où sont ces fichiers traces et comment les manipuler et les archiver (rotation, archivage...)

## 7.8. Accès clients

L'accès au logiciel de supervision devra être **multi-postes** et **multi-utilisateurs**.

La technologie employée devra être si possible indépendante de tout environnement propriétaire tiers et également indépendante du système d'exploitation du poste client. L'usage de cet accès pourra s'effectuer dans un environnement de services mandataires type « proxy » depuis le poste de travail client.

Le nombre de clients simultanés devra être à minima de 10 personnes.

Il devra être compatible de préférence avec le navigateur Mozilla Firefox dernière version à la livraison (ou versions antérieures de moins d'un an).

**il est fortement recommandé que la solution cliente soit de type WEB** sans installation de partie cliente sur le poste de travail. Dans les autres cas, Nantes université décline toute responsabilité de dysfonctionnement.



Une documentation décrivant les caractéristiques techniques précises doit être fournie dès l'offre.

**Les ressources et les livrables devront être fournis à l'issue de la prestation.**

## 8. Pilotage Efficience énergétique

### 8.1. Outil en production

Nantes Université utilise **la solution Energisme** de l'éditeur du même nom pour **l'analyse et le pilotage décisionnel des consommations**.

Cette brique sera utilisée par défaut pour les tableaux de bord sauf demande particulière de la Maîtrise d'Ouvrage.

### 8.2. Procédure de liaison

Les compteurs et les automates collecteurs type concentrateur devront communiquer avec un service centralisateur par export de fichier normé **csv au travers d'un flux FTP**.

La ressource est fournie par l'université et la **DSIN** communiquera les paramètres d'accès.

Le cahier des charges fonctionnel définit le type d'export (index) et la fréquence (horaire)

### 8.3. Modèle et format du fichier

Le fichier exportable sera de type csv selon cette règle :

nom du fichier :  
Horodatage\_IDSite\_IDBatiment\_NomEmetteur.CSV  
format du contenu :  
"IdCompteur ; Horodatage ; Valeur index

#### Caractéristiques et directives

- Enregistrement des index toutes les 10 minutes.
- Limitation du nombre d'enregistrements à 144 par fichier journalier (1 index toutes les 10 minutes \* 6 \* 24 = 144).
- Utilisation de la virgule comme séparateur décimal
- Nombre de décimales max : 2

- Premier enregistrement à 23h10 J-1 & dernier enregistrement J+0 23h.
- Envoi du fichier de type csv au travers d'un flux de type FTP suite au dernier enregistrement (entre 23h et minuit).
- Horodatage au format "JJ/MM/AAAA HH:MM:SS"
- Affichage par ordre décroissant dans le fichier. Ligne 2 : Dernière enregistrement. Dernière ligne : premier enregistrement.
- Utilisation de la nomenclature UN pour le nom des compteurs. Une table d'échange sera fournie par UN.
- Première colonne nommée impérativement **DATE** en respectant la casse.

Un modèle est présenté en annexe 10.3

## 9. Service de temps

Nantes Université possède un service de synchronisation de temps basé sur le protocole NTP.

Il pourra être utilisé pour synchroniser les horloges des automates et des compteurs si ces derniers sont compatibles avec la norme.

## 10. Prestation

### 10.1. Analyse technique

Le dossier d'architecture Technique (DAT) sera fourni le plus tôt possible, en amont du chantier de réalisation. Celui-ci comportera les schémas des installations et des implantations, les synoptiques de connexion et les caractéristiques des matériels. Une description d'intégration de la solution logicielle prévue, ou l'intégration à un existant doit être également exposée pour validation de conformité. Cf. paragraphe Sécurité 10

## 10.2. Mise en service

La mission du prestataire comprend la phase de mise au point, d'ajustement et de corrections éventuelles du système pendant la phase de conception, de réalisation et durant toute la période ultérieure liant le prestataire au donneur d'ordre. Ces opérations seront effectuées en liaison avec la **DSIN**.

Les pré-requis système et réseaux seront fournis par la **DSIN** dès lors que l'analyse technique aura été validée.

L'ensemble des fonctions de la **GTC** seront mises en service en connaissance des besoins réels des usagers et des techniciens pour la maintenance et l'exploitation (permission d'accès, gestion des alarmes, suivis énergétiques, archivage...).

## 10.3. Formation/Manuel d'utilisation

Le prestataire devra dispenser une formation à l'emploi du nouveau matériel si demandée par la maîtrise d'ouvrage pour les exploitants fonctionnels.

Dans tous les cas **une restitution technique avec transfert de compétence et documentation** d'installation et d'exploitation devra être **effectuée entre le prestataire et la DSIN**.

## 10.4. Sécurité

*Le socle des exigences en matière de sécurité est décrit dans le paragraphe 4.6*

### Automates

Les microprogrammes (firmwares) des automates seront à jour des derniers correctifs de sécurité au moment de la mise en production.

Une procédure de mise à jour régulière obligatoire devra être envisagée, idéalement incluse dans un contrat de maintenance.

### Serveur

La livraison du serveur hébergeur sera à jour des correctifs de sécurité et des correctifs du système d'exploitation. La **DSIN** maintient ce serveur en condition opérationnelle pendant la durée d'exploitation.

Elle avertira également de la fin de support du système d'exploitation et de la nécessité de projeter une évolution de la solution avec les acteurs concernés.

La DSIN sous autorité du RSSI se réserve le droit de couper les accès et d'arrêter le serveur en cas de vulnérabilité ou de compromission.

Le redémarrage se fera sur décision du RSSI de l'université.

### **Applicatifs**

Les mises à jour correctives des applicatifs (préconisées) seront à envisager, voire également prévues dans un contrat de maintenance.

Elles pourront être exécutées selon le cadre contractuel éventuellement par les équipes d'exploitation de l'université idéalement directement par l'intégrateur ou le titulaire du contrat de maintenance.

La DSIN se réserve également le droit de bloquer les accès en cas de découverte de failles de sécurité importantes. Sous le couvert du RSSI, Elle demandera également à l'intégrateur de fournir une solution corrective, voire d'engager sa responsabilité sur l'absence de correctif ou d'impact négatif.

### **Protection des données personnelles**

Le traitement des informations personnelles est assujéti au RGPD. Même si les données personnelles se résument aux prénom, nom et adresse électronique, Nantes Université se réserve le droit de demander si le cadre est respecté en cas de doute, ainsi qu'éventuellement **au délégué à la protection des données (DPO)** de l'éditeur/intégrateur. L'université respecte le RGPD et possède un DPO.

## **10.5. Livrables**

L'installateur fournira une liste des objets Ethernet avec leur nom, leur fonction, leur géolocalisation précise et leur adresse MAC.

Les fichiers de sauvegardes des configurations des automates seront mises à disposition sur un support numérique (dans un dossier sur le serveur de supervision par exemple).

L'installateur devra fournir un exemplaire du logiciel avec les différentes ressources d'installation ainsi que la sauvegarde du ou des paramétrages des automates et de la supervision sur un media numérique ou un espace dédié; ces ressources permettant de réinstaller le système, sans matériel ni logiciel spécifiques, en cas de défaillance d'un élément, de perte de données ou tout simplement de migration de système.

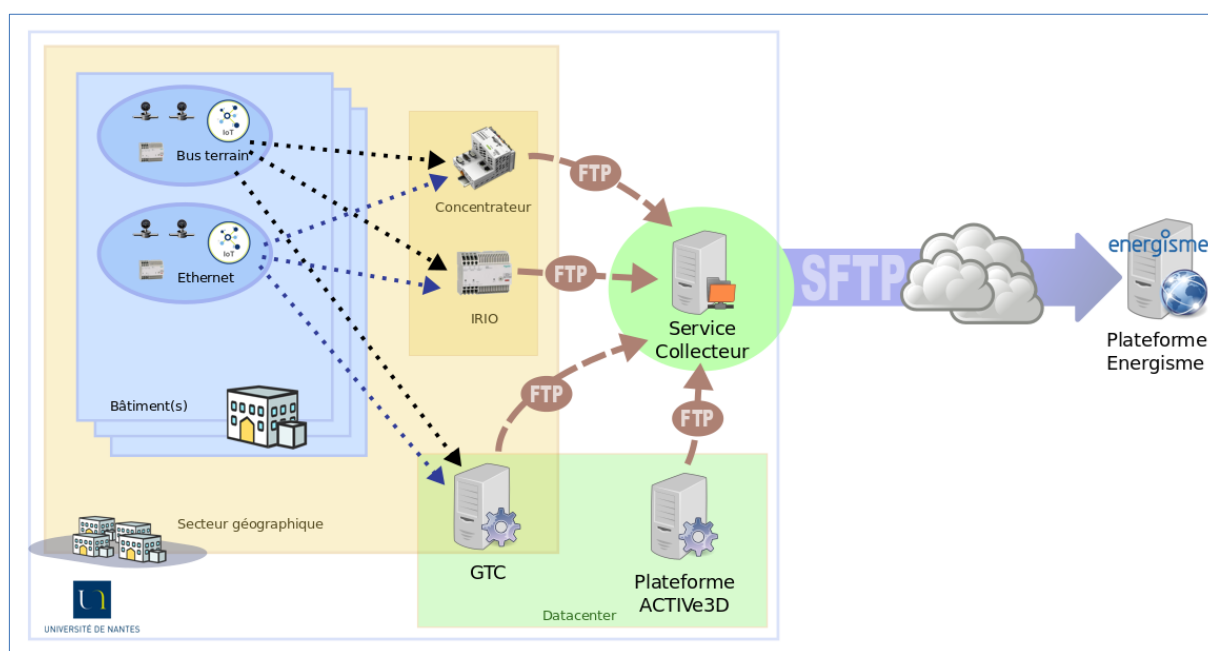
Il devra fournir aussi la documentation technique d'installation et de mise en route.

Un nouvel exemplaire comprenant la dernière version devra être fourni en cas d'intervention de remise à jour / à niveau...

Une solution de Maintien en condition opérationnelle et/ou de sécurité MCO / MCS doit être fournie dans le document d'installation ou d'exploitation

## 11. Annexe

### 12. 10.1 Schéma de principe de l'architecture GTC type



### 13. 10.2 Tableau de correspondance objet Ethernet

Désignation(*)	Fonction principale	Géolocalisation	Adresse MAC

(\*) La désignation se rapprochera au plus près de la nomenclature de nommage du local dans lequel est installé l'automate. Elle reprendra notamment le **code RUS**.

## 14. 10.3 Modèle de fichier d'index de consommation

DATE ;03\_04-CEL ;03\_04-CEF ;03\_04-CCH001 ;03\_04-CCH002  
11/09/2022 23:00:00 ;7023705,11 ;2099334,00 ;2460721,20 ;967690,19  
... 142 enregistrements ...  
10/09/2022 23:10:00 ;7023705,11 ;2099334,00 ;2460721,20 ;967687,86  
...

## 15. 10.4 Mémento des livrables

Livrable	Résumé	Période
Analyse technique de la solution	Fourniture du Document d'Architecture Technique (DAT) présentant la solution dans son ensemble avec cartographie des implantations, schémas, type de solution matérielle et logicielle.	Dès les phases APD.
Caractéristiques du serveur	Description des caractéristiques techniques de la machine hébergeuse : <ul style="list-style-type: none"><li>- système d'exploitation</li><li>- taille disque</li><li>- processeurs</li><li>- services de base éventuels</li><li>- stratégie de sauvegarde</li></ul>	Le plus tôt possible
Solution collecteur/superviseur envisagée	Description de l'éditeur, des caractéristiques, des fonctions et de l'environnement fullweb et des technologies de construction associées (framework, .Net, Java, PHP...)	Le plus tôt possible
Matrice d'interconnexion réseau et protocoles de communication	Liste ou cartographie des échanges réseaux entre les sources et les services collecteur/superviseur (hébergés sur le serveur qui sera fourni) avec les ports et les protocoles	Le plus tôt possible

Listes des éléments de type Ethernet	Liste des éléments à raccorder sur les réseaux Ethernet en fournissant le lieu d'implantation et l'adresse MAC	Après les premières réunions de cadrage.
Listes des acteurs prestataires	Liste des intervenants pendant l'installation et l'intégration des éléments de la GTC. Cette liste doit comporter obligatoirement le prénom, nom, fonction et adresse mail.*	Pendant les opérations d'installation et avant la recette.
Copie ressources installées	Copie sur media numérique ou dépôt sur un espace du serveur des paquets d'installation du logiciel ainsi que le mode opératoire (dossier d'Installation ou dossier d'exploitation)	A la réception des travaux et avant la recette finale
Copie paramétrage des éléments ethernet	La fourniture sur media numérique ou dépôt sur le serveur des fichiers de sauvegarde des configurations des éléments ethernet.	A la réception des travaux et avant la recette finale
Procédure de MCO /MCS	La fourniture écrite des procédures de maintien en condition opérationnelle ou de reconstruction dans les documents d'installation ou d'exploitation	A la réception des travaux et avant la recette finale

\* Nantes Université respecte le RGPD. Le nom de son DPO peut être fourni.

## 16. 10.5 Exigences intangibles

Techniques / matériels	Description	Conséquence
Courant porteur	Les éléments de type CPL ne sont pas admis pour les raccordement Ethernet.	L'infrastructure installée ne sera pas raccordée aux réseaux de Nantes Université.

WIFI	Les éléments Wifi ou un réseau wifi pour le raccordement ne sont pas permis.	L'infrastructure installée ne pourra pas être raccordée aux réseaux de Nantes Université
Micro-switches	Les actifs réseaux intermédiaires de type micro-switch ne sont pas tolérés sur les réseaux de l'université.	L'infrastructure installée ne sera pas raccordée aux réseaux de Nantes Université.
Ordinateur ou poste de travail	Les machines physiques pour héberger localement les ressources numériques sont très fortement déconseillées.	L'infrastructure installée et ces matériels ne seront pas raccordés aux réseaux de Nantes Université.
Client riche	Les clients riches pour exploiter les solutions de supervision sont fortement déconseillés. S'ils nécessitent d'une part des contraintes techniques d'installation sur le postes de travail et que d'autre part ils obligent de mettre en place une gestion de flux et de protocole(s) complexe(s), ils ne sont pas compatibles avec la stratégie de sécurité informatique de Nantes Université.	Les clients ne seront pas installés sur les postes de travail des personnels exploitants de Nantes Université.
Non respect d'au moins une préconisation	Cette fiche de liaison technique comporte un ensemble de pré-requis ou de recommandation étudiées afin de permettre l'interfaçage avec l'infrastructure et les ressources informatiques de Nantes Université. Elles s'acceptent dans son intégralité et ne peut souffrir de dérogation.	La DSIN de Nantes Université, après analyse, se réserve le droit de ne pas accéder aux demandes particulières. Elle n'engagera pas non plus sa responsabilité pour le fonctionnement et le maintien en condition opérationnelle de la solution installée dans son ensemble.  L'infrastructure installée pourra ne pas être raccordée aux réseaux de Nantes Université
Bacnet	L'emploi du protocole Bacnet / IP utilisant le port 47808 en UDP doit obligatoirement prendre en compte la limitation du routage et la désactivation du broadcast. L'emploi de la solution BBMD peut être employée. La mise en place reste à la charge de l'intégrateur.	La DSIN ne sera en aucun cas responsable des dysfonctionnements et n'apportera aucune aide ni expertise en la matière.



Direction des Système d'Information et du Numérique  
Service Informatique de Gestion