# Rapport technique d'aménagement, d'interconnexion et de supervision du bâtiment de l'Autorité de Régulation des Transferts de Fonds du Congo (ARTF)

*Rédigé par Geolab*
*pour l'Autorité de Régulation des Transferts de Fonds du Congo (ARTF)*
Fait à Brazzaville — Novembre 2025

*Document interne – Diffusion restreinte à l'ARTF et à ses partenaires techniques agréés*

Geolab – Digital for all
Brazza Mall, Avenue de l'Intendance, Brazzaville, Congo
contact@geo-labtech.com

## Introduction institutionnelle

Ce rapport technique a été élaboré à la demande de l'Autorité de Régulation des Transferts de Fonds du Congo (ARTF) afin de définir les standards d'aménagement, d'interconnexion et de supervision de son nouveau bâtiment administratif. Il présente les exigences d'infrastructure, de connectivité, d'énergie et de sécurité nécessaires à l'exploitation du NOC, du Data Center, et du centre de contrôle du Smart Building, conformément aux besoins opérationnels de la plateforme FinTraX et aux bonnes pratiques internationales.

# 1. Objet du rapport

Le présent rapport fait suite à la visite effectuée le **18 octobre** sur le chantier du **bâtiment de l'ARTF**, actuellement en construction.
Son objectif est de formuler les **spécifications techniques** nécessaires à la préparation de l'infrastructure technologique et logistique du site.
Ces spécifications s'articulent autour de **trois axes principaux** :

1. **Aménagement du NOC et du Data Center** au **3e étage** du bâtiment.
2. **Rapatriement du CTI** au bâtiment de l'ARTF, tout en maintenant son rôle de **centre de relève active** du système **FinTraX**.
3. **Mise en place d'une logistique centralisée par un centre de contrôle et d'un système de gestion intelligente du bâtiment**, assurant la **surveillance et la sécurité** des installations 24h/24 et 7j/7.

Ce document décline l'ensemble des spécifications techniques: NOC/Data Center au 3e étage, rapatriement du CTI, centre de contrôle Smart Building, connectivité Internet/FAI et réseau gouvernemental, backbone Est/Ouest et Roof POP, énergie et continuité, et supervision centralisée par le Système de Contrôle et d'Alerte FBB.

## 1.1 Contexte général

Le bâtiment de l'ARTF est une construction de **neuf étages**.
Le **NOC (Network Operations Center)** et le **Data Center** seront aménagés au **3e étage**.
Il est également prévu d'y installer un **centre de gestion sécurisée** dédié à la **surveillance et au management intelligent** de l'ensemble du bâtiment.

Ce centre devra permettre :

- Une supervision en temps réel des systèmes critiques (électricité, climatisation, sécurité, connectivité, etc.) ;
- Un fonctionnement **en continu (24/7)** ;
- Une implantation dans un **espace central et sécurisé** avec accès restreint.

# 2. Aménagement du NOC et du Data Center (3e étage)

## 2.1 Objectifs et périmètre

Créer au 3e étage deux zones critiques et distinctes :

- une **salle serveurs (Data Center)** protégée, pour FinTraX + Smart Building (GTB/BMS) ;

- une **salle d'exploitation (NOC)** à accès restreint, avec mur d'écrans et postes opérateurs 24/7 ;
- un **vestibule / mini-réception** faisant office de **sas de sécurité** (mantrap) pour la **vérification des entrées** et le contrôle d'identité.

**Niveau de résilience visé :** équivalent **Tier III** (Uptime Institute – redondance N+1, maintenance sans arrêt), avec bonnes pratiques **ISO/IEC 27001** (sécurité de l'info), **ISO 22301** (continuité), **NFPA 75/76** (protection équipements info-télco), **ASHRAE TC9.9** (environnement).

---

## 2.2 Zoning & contrôle d'accès

### 2.2.1 Vestibule / Mantrap (mini-réception)

- **Sas à deux portes** interverrouillées (anti-passage en force) ; vitrage de sécurité si vue sur couloir.
- **Lecture badge + MFA** (badge + PIN/biométrie) **à chaque porte**, caméra dôme, interphone.
- **Poste agent de contrôle** : PC avec Système FBB (journal d'accès), tiroir sécurisé, casier visiteurs.
- **Politique visiteurs** : pré-enrôlement, badge temporaire, **accompagnement obligatoire**.

### 2.2.2 Séparation fonctionnelle

- **Zone NOC** (exploitation) et **Zone DC** (serveurs) **physiquement séparées**.
- Dans la zone DC : cloisonnement « **allée froide/allée chaude** » et **accès limité** aux personnels habilités DC.

### 2.2.3 Cloisons, portes et vitrages

- **Cloisons et portes coupe-feu** : **EI60** minimum (recommandé **EI90/EI120** pour le DC).
- **Vitrages** (si visibilité NOC ↔ DC) : **EI60** minimum, châssis métalliques, joints intumescents.
- **Seuils étanches fumées** (NF EN 1634), ferme-portes certifiés, fermeture automatique à l'alarme incendie.

---

## 2.3 Salle serveurs (Data Center)

### 2.3.1 Architecture & racks

- **Racks 42U** (600/800 × 1000/1200) avec **PDU A/B** mesurés, rails coulissants, verrouillage.
- **Segmentation physique par rangées :**
  - Rangée **FinTraX** (étiquetage vert)
  - Rangée **Smart Building/GTB** (étiquetage orange)
  - **Rangée réseau/ODF** (étiquetage bleu)
- **Équipements partagés** (pour optimisation coûts) : **hôtes de virtualisation** (cluster) et **SAN/NAS** communs ; **séparation logique stricte** (vSwitch, VLAN, VRF, RBAC, chiffrement).

### 2.3.2 Câblage & brassage

- **Cuivre** : Cat.6A F/UTP minimum, panneaux 24/48 ports ; chemins dédiés données/énergie.
- **Fibre** : OS2 (G.652.D) en **MTP/MPO** ou LC/UPC ; **ODF A/B** séparés ; **codes couleur** normalisés.
- **Repérage & DOE** : plan d'adressage, schémas L2/L3, **étiquetage** (ISO/IEC 14763), **OTDR/OLTS** en réception.

### 2.3.3 Refroidissement (ASHRAE TC9.9)

- **N+1** minimum (armoires de précision / in-row / CRAH), confinement **allée froide**.
- Température cible **18–27 °C** (idéal 22 ± 2 °C), humidité relative **40–60 %**.
- **Sondes T°/HR** en allées et retours, **détection fuite** sous plancher (si présent).

### 2.3.4 Alimentation & continuité

- **Chaînes électriques A/B** indépendantes : deux **UPS modulaires N+1** (double conversion on-line), **autonomie 30–60 min** à charge nominale **Tier 1**.
- **By-pass statique et de maintenance**, **para-foudre T1/T2**, terre **≤ 10 Ω**, liaisons équipotentielles (IEC 60364).
- **Groupes G1/G2** : voir chap. Énergie ; le **G2** maintient **Tier 1** la nuit/WE.
- **PDU intelligents** (commutation, mesure kWh), **seuils d'alarme** reportés au **FBB**.

### 2.3.5 Détection & extinction incendie

- **Détection précoce** type **VESDA** + détecteurs ponctuels.
- **Extinction propre** : **Novec 1230 / FM-200** (NFPA 2001 / EN 15004), scénarios d'arrêt clim/ventilation, **étanchéité pièce** (test Door Fan).
- Signalisation locale (sirènes/flash), **coupure d'urgence** (EPO) sous capot.

#### 2.3.6 Sécurité logique & supervision

- **NGFW multi-zones**, **VLAN/VRF** distincts (Prod/Mgmt/GOV/BMS), **authentification MFA** et **RBAC**.
- **Journalisation centralisée** (SIEM), horloge **NTP** commune.
- **Système FBB** : supervision **SNMPv3**, **API** ou **agents FBB** (Linux/Windows), tableaux de bord DC (énergie, T°/HR, ports, latence).

---

### 2.4 Salle d'exploitation (NOC)

#### 2.4.1 Ergonomie & norme

- Conception **ISO 11064** (postes de contrôle).
- **Mur d'écrans** (vidéo-wall) ≥ 3×2, redondant ; consoles opérateurs **24/7** (mobilier « sit-stand »).
- **Éclairage** anti-éblouissement (500 lx tâche / 300 lx ambiant), **acoustique** ≤ 45 dB(A).
- **Climatisation N+1** (confort + extraction mur d'écrans).

#### 2.4.2 Postes & réseaux

- **Double écrans** par opérateur + moniteur alerte ; **réseau filaire** (pas de Wi-Fi par défaut).
- **VLAN opérateurs**, **VLAN management**, **VLAN invités** isolé ; accès bastion.
- **UPSonline** 10–20 min pour consoles, KVM/IP, téléphonie, mur d'écrans.

#### 2.4.3 Procédures

- **SOP/MOP/EOP** (exploitation, maintenance, crise).
- **Journal 24/7**, **runbooks** incidents, **permutation d'équipes** ; **tests trimestriels** (bascule A/B, G2, perte WAN).

---

### 2.5 Intégration FinTraX & Smart Building

#### 2.5.1 Racks & logique

- **Racks FinTraX** : acquisition OneBox, API, analyse/corrélation, certification, bases HA.
- **Racks GTB/BMS** : SCADA, VMS (CCTV), contrôle d'accès, automates (BACnet/Modbus/KNX), **IoT gateways** (MQTT/OPC-UA).
- **Hôtes/Stockage partagés** : clusters hyperviseurs + SAN communs, **isolation stricte** (politiques, VLAN/VRF, micro-segmentation, chiffrement stockage/VM).

### 2.5.2 Connectivité

- Vers **sous-sol (-1)** : arrivées **FAI A/B** + **réseau gouvernemental** ; distribution via **colonnes Est/Ouest**.
- Vers **toit (Roof POP)** : fibres redondantes pour **satcom** futur.
- **ODF A/B** dans le DC ; brassage **propre** (cordons courts, velcro), **couleurs** par zone.

---

## 2.6 Construction & aménagement

- **Plancher technique** (si retenu) 300 mm min, lame d'air, caillebotis haute charge ; sinon **goulottes** et **chemins aériens** séparés (data/énergie).
- **Finition antistatique** (ESD), **jointoiement** anti-poussière.
- **Étanchéité fumées** (pénétrations coupe-feu), **capteurs fuite** aux points d'eau proches.
- **Local batteries** dédié si VRLA (ventilation, rétention) ; **$LiFePO_4$** recommandé (densité/autonomie/maintenance).

---

## 2.7 Sécurité & accès

- **Contrôle d'accès** centralisé (badge + MFA), profils : **Visiteur escorté / Opérateur NOC / Admin DC / Énergie**.
- **CCTV** (ONVIF) : sas, portes DC, allées racks, baie ODF, mur d'écrans ; **rétention ≥ 90 jours**.
- **Détecteurs intrusion** : ouvrants, bris de glace, **tamper** baies.

---

## 2.8 Essais, réception & DOE

- **Vérifications** : OTDR/OLTS fibre, mesure cuivre, test charge **UPS/PDU**, essais **EPO**, déclenchement **gaz**, **Door Fan Test**, montée en charge **clim**, tests **FBB** (métriques/alertes/commandes).
- **Scénarios** : perte **WAN A/B**, bascule **G2** nocturne, panne clim, coupure UPS A/B.
- **DOE** : plans « as built », schémas unifilaires, plan d'adressage, inventaires (numéros de série, racks/U, IP/VLAN), licences/garanties, procédures MOP/SOP/EOP, **modèles FBB** par équipement.

---

## 2.9 Exigences CCTP opposables (extrait)

1. **Coupe-feu** : cloison/portes/vitres **EI60** min (EI90/120 recommandé DC).
2. **Clim** : **N+1**, consignes **ASHRAE TC9.9**, sondes multiples, confinement allées.
3. **Énergie** : **double chaîne A/B**, **UPS N+1**, PDU mesurés, terre ≤ 10 Ω, TGBT sélectif, **para-foudre T1/T2**.
4. **Détection/Extinction** : **VESDA** + **Novec/FM200**, scénarios sûreté, étanchéité.
5. **Câblage** : OS2 LC/UPC, Cat.6A, **ODF A/B**, essais **OTDR/OLTS**, étiquetage ISO/IEC.
6. **Sécurité** : contrôle d'accès **MFA**, **CCTV** 24/7, journalisation **SIEM**.
7. **FBB** : tous équipements **TCP/IP** via **SNMPv3 / API / agent FBB**, modèles & pièges d'alarme fournis, dashboards DC & NOC livrés.
8. **Réception** : procès-verbaux d'essais, check-list conformité, formation opérateurs, **plan de maintien en conditions opérationnelles**.

---

## 2.10 Implantation suggérée (selon le plan du 3e étage)

- La **grande zone centrale** reste divisée en deux espaces distincts :
  - **Zone Ouest /Nord : Data Center** (racks FinTraX, Smart Building, ODF A/B).
  - **Zone Ouest/Sud : NOC**.

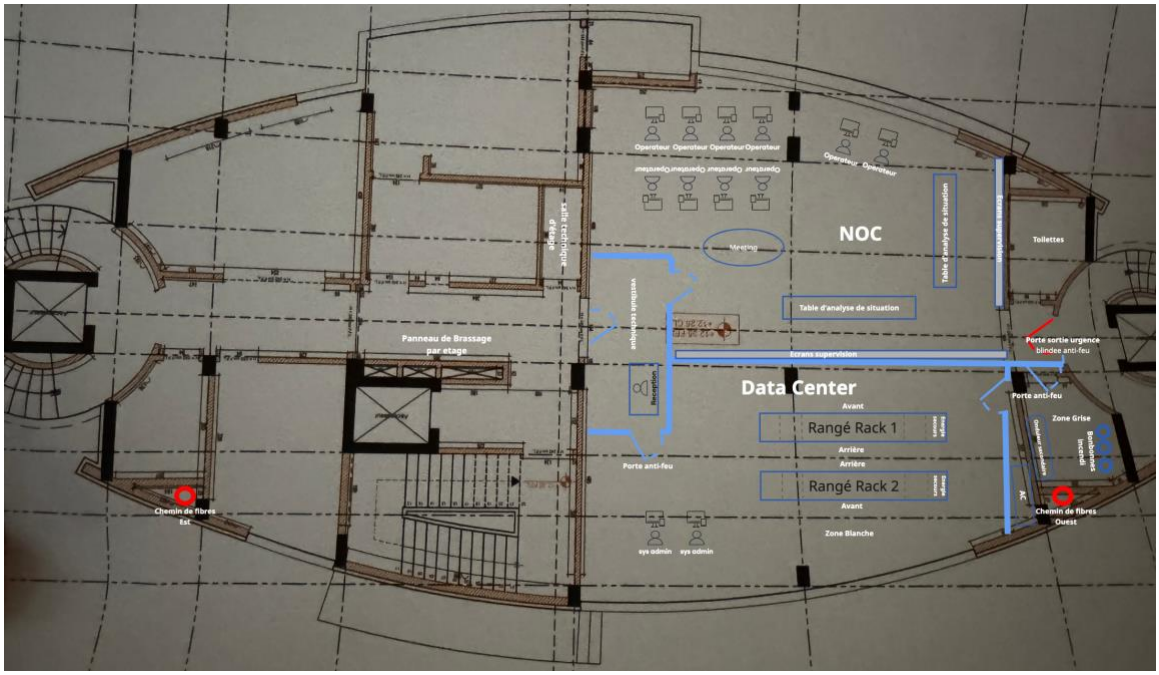
- Dans la **salle NOC** :
  - Les **10 postes opérateurs** sont alignés en arc de cercle face au **mur d'écrans**.
  - Les **deux tables d'analyse (war room)** sont positionnées latéralement, à proximité des écrans, pour les réunions de crise ou diagnostics collaboratifs.
  - La **table de conférence** se situe en retrait, à l'arrière du NOC, permettant d'accueillir 6 à 8 personnes sans interférer avec la supervision en cours.
  - Accès au **vestibule/mantrap** par une porte sécurisée à double badge, puis distribution vers le NOC ou le DC.
  - Cloisons vitrées coupe-feu EI60 entre NOC et DC assurant visibilité partielle.
  - Les chemins câbles data/énergie sont séparés ; l'éclairage et la climatisation sont indépendants.

---

### Résultat attendu

Un **3e étage** conforme aux normes de **sûreté**, **disponibilité** et **efficacité énergétique**, où :

- le **NOC** exploite 24/7 l'infrastructure,
- le **Data Center** héberge FinTraX et le Smart Building de façon **segmentée**,
- et le **sas de sécurité** garantit une **traçabilité stricte** des accès.




## 3. Rapatriement du CTI

# 3.1 Contexte et objectifs

Le **Centre de Traitement et d'Intégration (CTI)**, actuellement en exploitation à **Brazza Mall, Brazzaville (coord. 4.23881° S, 15.29080° E)**, constitue à ce jour le **site de production principal** de la plateforme **FinTraX**.
Conformément à la planification stratégique de l'ARTF, son rôle évoluera dans le cadre du **rapatriement de l'infrastructure FinTraX** vers le nouveau **bâtiment administratif de l'ARTF (coord. 4.27347° S, 15.27840° E)**.

L'objectif est de :

- transférer progressivement les fonctions critiques (serveurs, bases, outils d'analyse et monitoring) vers le **Data Center du bâtiment ARTF** ;
- transformer le **CTI** en **site secondaire actif (Hot Standby)** assurant la **continuité de service**, la **résilience**, et la **reprise automatique en cas d'incident majeur**.

Ce basculement s'effectuera par étapes, en garantissant la redondance fonctionnelle et la sécurité des données à chaque phase.

---

# 3.2 Architecture et interconnexion

### 3.2.1 Principe général

Le **CTI** et le **Data Center ARTF** formeront un **ensemble à haute disponibilité géo-distribuée**, relié par :

- **Deux fournisseurs Internet (FAI A et FAI B)** indépendants, chacun disposant de **deux points d'entrée** physiques dans le bâtiment ARTF (avant/arrière) pour assurer la redondance ;
- Un **réseau VPN TLS 1.3** sécurisé reliant les deux sites via ces FAI, avec tunnels chiffrés, authentification mutuelle par certificats X.509 et algorithmes AES-256/GCM + SHA-384.

Le **réseau gouvernemental privé** reste disponible pour la transmission sécurisée des données **KYC** et interconnexions avec les institutions (ONI, NIU, DGI, Passeports, etc.), sans transiter par Internet public.

### 3.2.2 Localisation et points de convergence

Toutes les fibres optiques convergent vers le **local technique central (niveau -1)** du bâtiment ARTF, avant d'être distribuées verticalement vers le 3e étage (Data Center FinTraX).
Les connexions sortantes du CTI suivent le même principe, via ses propres chambres de tirage optique.

---

## 3.3 Étapes de migration

### Phase 1 – Préparation de l'environnement ARTF

- Mise en service de la **nouvelle infrastructure serveurs FinTraX** (analyse, agrégation, corrélation, bases de données) au Data Center ARTF.
- Configuration des **liens VPN TLS 1.3 redondants** entre CTI et ARTF.
- Synchronisation initiale des bases, fichiers journaux et configurations via réplication sécurisée (rsync, PostgreSQL streaming replication, Elasticsearch cluster mirror).
- Vérification de la **connectivité bidirectionnelle** et de la **latence réseau inter-sites** (< 50 ms).

### Phase 2 – Réplication et synchronisation

- Activation d'une **réplication asynchrone contrôlée** entre le CTI (source) et le site ARTF (destination).
- Synchronisation des données FinTraX en flux continu, tout en maintenant la production au CTI.

- Mise en place du **monitoring FBB étendu** sur l'ensemble des équipements : serveurs, VPN, liens, performances réseau, synchronisation, alertes applicatives.

### Phase 3 – Bascule progressive des services

- Validation de la **complétude des synchronisations** et tests fonctionnels.
- Redirection contrôlée des **OneBox** des assujettis (opérateurs, banques, agrégateurs) vers la nouvelle adresse du **bâtiment ARTF**.
- Maintien temporaire d'un **mode actif/actif** entre les deux sites pour assurer le recouvrement transactionnel et la cohérence des flux.
- Surveillance étroite par le **Système FBB**, avec corrélation entre journaux CTI et ARTF.

### Phase 4 – Stabilisation et requalification du CTI

- Le CTI devient officiellement **site secondaire actif (Hot Standby)**.
- Activation de la **réplication bidirectionnelle** (asynchrone, bascule automatique).
- Maintien en conditions opérationnelles du CTI avec capacité d'hébergement minimale (≥ 30 % de la charge du site principal).
- Le CTI conserve ses accès VPN, pare-feux, systèmes de stockage et capacités d'analyse locales pour garantir la continuité en cas de sinistre sur le site ARTF.

---

# 3.4 Sécurité et supervision

## 3.4.1 Sécurité des communications

- **VPN TLS 1.3** avec chiffrement **AES-256/GCM**, **authentification mutuelle (mTLS)** et renouvellement automatique des certificats.
- Segmentation par **VLAN** et **VRF** dédiées (FinTraX, Monitoring, Admin).
- Pare-feux de nouvelle génération (NGFW) configurés en **règles de flux Est/Ouest** et **contrôle applicatif**.
- Politique **Zero Trust inter-sites**, avec authentification multi-facteurs pour les administrateurs.

## 3.4.2 Sécurité des données

- Données en transit : **chiffrées** (TLS 1.3, Perfect Forward Secrecy).
- Données au repos : **AES-256** sur volumes SAN/NAS, clés gérées via module HSM (Hardware Security Module).
- Sauvegardes : locales + distantes, avec plan **3-2-1** (3 copies, 2 supports, 1 hors site).
- Contrôle d'intégrité périodique (hash SHA-512).
- Test trimestriel de restauration.

### 3.4.3 Supervision FBB

L'ensemble des liens, serveurs et processus de synchronisation est **intégré au Système de Contrôle et d'Alerte FBB (SCAFBB)** :

- Suivi des **latences inter-sites**, **taux de réplication**, **alertes de désynchronisation** ;
- Corrélation automatique entre incidents applicatifs et performance réseau ;
- Génération d'alertes multi-canaux (mail, SMS, dashboard) ;
- Visualisation simultanée des statuts CTI / ARTF via un tableau comparatif.

---

## 3.5 Exigences techniques minimales

| Domaine | Exigence |
|---|---|
| **VPN & Réseau** | 2 FAI distincts, double entrée physique, tunnels TLS 1.3 mTLS AES-256, bande passante ≥ 500 Mbps symétrique, latence < 50 ms |
| **Bases de données** | Réplication PostgreSQL streaming / MongoDB / Elasticsearch mirror |
| **Stockage** | SAN/NAS redondé (RAID 6/10), synchronisation rsync + snapshots incrémentaux |
| **Supervision** | FBB avec sondes SNMPv3 + API + agents, corrélation ARTF/CTI |
| **Sécurité** | Certificats X.509, ACL inter-sites, Zero Trust, MFA admin |
| **Continuité** | CTI capable de reprendre la production ≤ 15 min après coupure ARTF |
| **Tests** | Bascule mensuelle simulée, DRP complet semestriel |

---

## 3.6 Résultat attendu

- Le **bâtiment ARTF** devient le **site primaire FinTraX**, hébergeant l'intégralité des serveurs, bases et outils d'analyse.
- Le **CTI** devient **site secondaire actif**, capable de **reprendre automatiquement** les opérations en cas d'incident sur le site principal.
- La **synchronisation bidirectionnelle** garantit la **cohérence des transactions** et des données KYC.
- La **supervision intégrée FBB** offre une **visibilité unifiée** sur les deux sites, les flux VPN, les serveurs et les alertes.
- La transition se fait **sans interruption de service**, dans le respect des normes de sécurité et de résilience.

## 4. Gestion intelligente du bâtiment (Smart Building)

# 4.1 Objectif général

Le bâtiment de l'ARTF doit intégrer une **infrastructure intelligente** permettant la **supervision, la commande et la maintenance proactive** de l'ensemble des systèmes techniques.
Cette gestion centralisée vise à :

- réduire les coûts d'exploitation et de maintenance ;
- améliorer l'efficacité énergétique et la sécurité ;
- assurer une **surveillance 24/7** à partir d'un **centre de contrôle centralisé (CCC)** connecté au **Système de Contrôle et d'Alerte FBB** ;
- et garantir la **résilience** du bâtiment face aux défaillances électriques, climatiques ou sécuritaires.

---

# 4.2 Architecture fonctionnelle

### 4.2.1 Systèmes supervisés

Le système de gestion intelligente (GTB/BMS) regroupe et surveille :

1. **Énergie et alimentation**
   - Réseau électrique principal et secours (G1, G2, UPS, PV)
   - Mesure des consommations (MID / PUE Data Center)
   - Surveillance tension/fréquence/température armoires électriques
2. **Climatisation et confort**
   - Centrales de traitement d'air (CTA), splits, ventilations
   - Capteurs T°/HR par zone, alertes défaillance
   - Régulation automatique selon occupation
3. **Sécurité & sûreté**
   - Contrôle d'accès (MFA, badges, biométrie)
   - Détection incendie (détecteurs, VESDA, FM200/Novec)
   - Vidéosurveillance (CCTV, enregistrement NVR, reconnaissance intrusion)
   - Détection intrusion et levée de doute audio/vidéo
4. **Infrastructure IT & réseaux**
   - Liens fibre (Internet / gouvernemental / interne)
   - Switches, routeurs, serveurs, PDU, UPS, clim Data Center
   - Corrélation des alertes via FBB
5. **Gestion environnementale et bâtiments annexes**
   - Éclairage (automatique, détection de présence, DALI/KNX)
   - Ascenseurs, pompes, réserves d'eau, alarmes techniques

- Capteurs IoT : $CO_2$, fuites, vibrations, fumées, mouvement

---

# 4.3 Centre de Contrôle Centralisé (CCC)

## 4.3.1 Emplacement et rôle

Le **Centre de Contrôle Centralisé (CCC)** constitue le **cœur opérationnel** du Smart Building de l'ARTF.
Il assure la **surveillance en temps réel**, la **corrélation des alarmes** et la **commande à distance** de tous les systèmes techniques du bâtiment, incluant énergie, climatisation, sécurité, réseaux, et équipements IoT.

Le CCC sera aménagé dans une **zone sécurisée et climatisée** du bâtiment, **distincte du NOC**, mais étroitement **interconnectée** avec celui-ci pour le partage des informations critiques.

---

## 4.3.2 Interconnexion et redondance

Le **Centre de Contrôle Centralisé** est relié au **Data Center du 3e étage** par **deux chemins optiques redondants** :

- **Backbone Est**,
- **Backbone Ouest**,
  chacun transportant une fibre dédiée à la gestion intelligente (Smart Building / GTB).

Ces fibres partent du **local technique central (niveau -1)** et longent chaque côté du bâtiment jusqu'au **3e étage**, avant de rejoindre le **Data Center**, garantissant ainsi :

- une **redondance physique complète** (itinéraires distincts, traversées de gaine séparées),
- une **tolérance aux pannes** (rupture fibre, maintenance, travaux extérieurs),
- et une **résilience logique** assurée par la **bascule automatique** sur le lien actif restant.

Chaque lien est configuré en **agrégation de liens (LACP)** avec **VRRP ou HSRP** au niveau IP, assurant la continuité du flux de données vers le Data Center.

---

## 4.3.3 Infrastructure technique du CCC

Le CCC héberge :

- un **mur d'écrans** multi-fenêtré pour la visualisation des flux vidéo, énergétiques, et climatiques ;
- **5 à 6 postes opérateurs** dédiés à la maintenance et à la supervision technique ;
- un **serveur GTB/BMS local**, connecté au cluster de virtualisation du Data Center via VLAN "SmartBuilding-Mgmt" ;
- des **postes d'intervention** (maintenance, sécurité) configurés avec des accès limités (RBAC) et authentification forte.

En cas de perte totale de liaison entre le CCC et le Data Center, le serveur GTB local est capable d'assurer une **autonomie de fonctionnement de 48 heures** avec stockage tampon des données et remontée différée vers le FBB à la reconnexion.

---

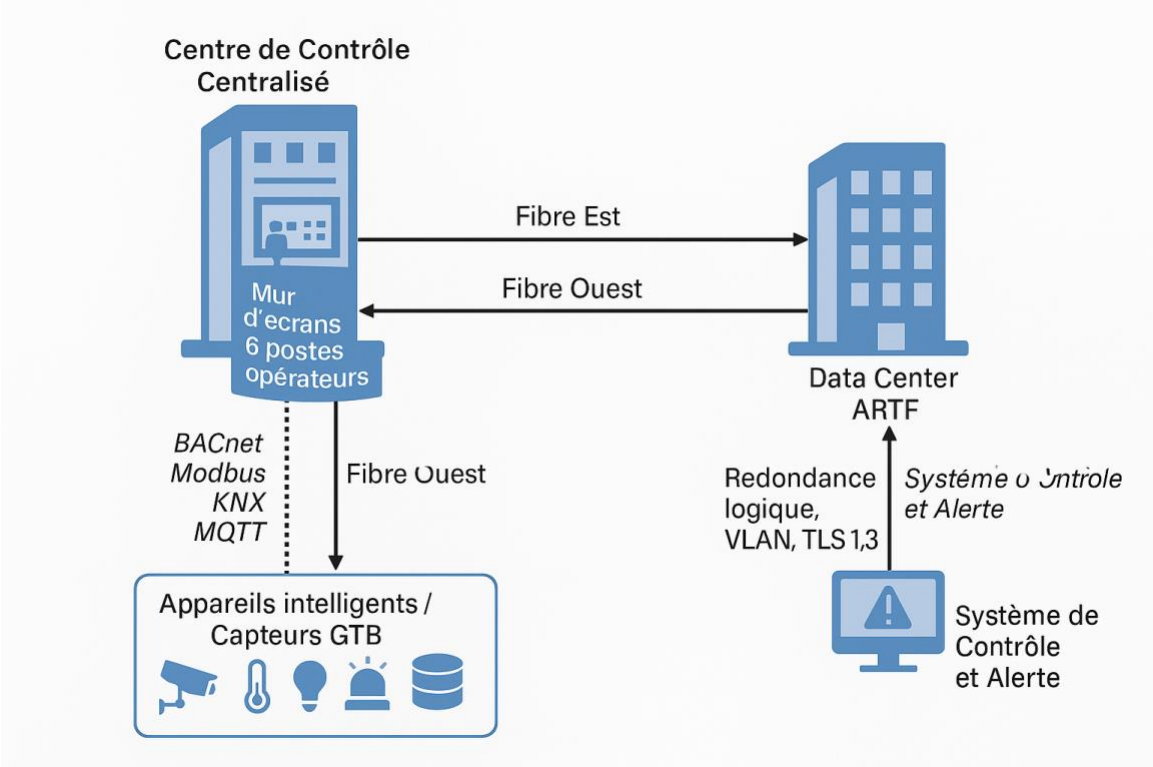
### 4.3.4 Sécurisation d'accès

- **Accès physique** : sas double porte avec interverrouillage, badges personnels et biométrie.
- **Accès logique** : authentification multifactorielle (MFA), segmentation VLAN/VRF dédiée "GTB", chiffrement TLS 1.3 interne.
- **Supervision vidéo** : caméras ONVIF couvrant tous les accès et consoles du CCC, stockage local ≥ 90 jours.
- **Contrôle d'ambiance** : climatisation N+1, humidité 45–60 %, alarme température/hygrométrie connectée au FBB.

---

### 4.3.5 Intégration réseau et supervision

- Le CCC communique avec les systèmes du Data Center (serveurs GTB, SCADA, FBB, stockage) via les **deux fibres Est/Ouest**.
- Les échanges sont encapsulés dans des **VLAN redondants** avec bascule automatique (L2 failover, LACP).
- Tous les flux sont **chiffrés** (IPsec + TLS 1.3) et supervisés via le **Système de Contrôle et d'Alerte FBB**, assurant la détection immédiate de toute rupture ou latence anormale sur les liens.
- Les **alertes de coupure**, **seuils de latence**, et **pertes de paquets** sont remontés au tableau de bord principal du FBB pour corrélation et notification automatique.




---

### 4.3.6 Résilience et exploitation

- Alimentation **A/B** séparée, redondée par **UPS online 15–30 min** et **G2**.
- Système **autonome 48h** en cas d'isolement du Data Center.
- Sauvegarde automatique de la configuration GTB et duplication vers le CTI.
- Surveillance FBB 24/7 : état des postes, température, latence, charge serveur, disponibilité des liens Est/Ouest.

---

## 4.4 Communication et interopérabilité

### 4.4.1 Protocoles supportés

Les équipements GTB (Gestion Technique de Bâtiment) doivent être compatibles avec au moins un des protocoles ouverts suivants :

- **BACnet/IP** (ASHRAE 135) pour climatisation, ventilation, énergie.
- **Modbus/TCP** pour armoires électriques, pompes, compteurs.
- **KNX/IP** pour éclairage, stores, capteurs.
- **MQTT / OPC-UA** pour capteurs IoT et intégrations cloud.
- **ONVIF / RTSP / SIP** pour vidéosurveillance et interphonie.

Les passerelles doivent permettre la **conversion multi-protocoles** et la **remontée normalisée** vers le FBB (via SNMPv3, API REST ou agent FBB).

### 4.4.2 Supervision unifiée via SCAFBB

Le système FBB agit comme **plateforme fédératrice**, intégrant toutes les données techniques, alarmes, événements et mesures :

- Acquisition SNMPv3 / API REST / MQTT / BACnet ;
- Tableaux de bord multi-niveaux (bâtiment, étage, équipement) ;
- Cartographie en temps réel (vue 3D ou plan 2D interactif) ;
- Alertes intelligentes (corrélation, priorisation, notifications multicanal).

---

## 4.5 Sécurité, résilience et disponibilité

### 4.5.1 Infrastructure

- Serveurs GTB virtualisés sur cluster ARTF (hyperviseurs partagés avec FinTraX, isolation logique).
- Stockage local sur SAN/NAS partagé, sauvegardes quotidiennes + répliquées vers CTI.
- Alimentation via double circuit A/B, UPS + G2.
- OS et logiciels GTB certifiés (Windows Server / Linux LTS / Base SQL/NoSQL redondée).

### 4.5.2 Continuité

- Fonctionnement autonome 48h sur batteries + G2 en cas de coupure réseau.
- Surveillance environnementale (T°, HR, tension, accès) du centre lui-même.
- Basculabilité automatique vers CTI si perte du site principal.

---

## 4.6 Tableau de bord FBB / GTB

Le **tableau de bord Smart Building FBB** regroupe :

| Domaine | Type de métrique | Seuils / Alertes |
|---|---|---|
| **Énergie** | PUE, consommation, tension, charge UPS | >90% = alerte jaune ; >95% = critique |
| **Climatisation** | T° ambiante / Data Center / NOC | >27°C = Alerte |
| **Sécurité** | Porte ouverte, intrusion, incendie | Temps réel |

| Domaine | Type de métrique | Seuils / Alertes |
|---|---|---|
| **Vidéo** | Perte flux, enregistrement, stockage | Automatique |
| **GTB IoT** | Température, Humidité, fuite, $CO_2$, mouvement | Programmable |
| **Réseau** | VPN, FAI, latence | Corrélé avec CTI |

---

# 4.7 Exploitation et maintenance

- Les opérateurs du CCC sont intégrés à la **cellule technique ARTF**, en coordination directe avec les équipes du NOC et du Data Center.
- Une **permanence 24/7** est assurée (astreinte technique).
- Les opérations GTB suivent la méthodologie **ITIL** (incidents, changements, problèmes).
- Tous les équipements sont recensés dans la **CMDB FBB** et suivis par des **tableaux d'indicateurs (KPI)**.
- **Maintenance préventive** : inspections mensuelles, nettoyage, recalibration des sondes, tests clim/alarme/incendie semestriels.

---

# 4.8 Résultat attendu

Le **bâtiment ARTF** devient un **bâtiment intelligent et résilient**, dont chaque sous-système est :

- **connecté, mesuré et supervisé** en temps réel,
- **corrélé** par le Système FBB,
- **pilotable à distance** avec droits et traçabilité,
- et **prévisible** grâce à la détection proactive des anomalies.

L'ensemble offre à la Direction de l'ARTF :

- un **contrôle centralisé total** de ses installations,
- une **sécurité accrue** (accès, énergie, incendie),
- et une **efficacité énergétique mesurable** et durable.

---

## 5. Architecture de connectivité externe

# 5.1 Objectifs

L'architecture de connectivité externe du bâtiment de l'ARTF vise à garantir :

- la **résilience** et la **redondance** des connexions réseau avec l'extérieur,
- la **sécurité cryptographique** des échanges (TLS 1.3, VPN IPsec, authentification mutuelle),
- la **continuité d'accès** aux flux des assujettis et aux plateformes gouvernementales,
- et l'**isolation fonctionnelle** entre les réseaux FinTraX, Smart Building et Administration interne.

---

# 5.2 Topologie générale

Le bâtiment de l'ARTF est relié à l'extérieur par **trois réseaux principaux**, chacun doté de sa propre infrastructure physique et logique :

| Réseau | Type | Description | Objectif |
|---|---|---|---|
| **Réseau Internet Public** | Double FAI A/B | Deux opérateurs indépendants, chacun avec double entrée (avant et arrière du bâtiment) | Flux FinTraX, communications CTI, accès OneBox, messagerie, supervision |
| **Réseau Gouvernemental Privé (RGN)** | Réseau IP MPLS privé national | Connexion directe aux institutions gouvernementales (NIU, ONI, DGI, DGAIC, etc.) | Transmission des données KYC et interopérabilité avec les registres nationaux |
| **Réseau de Gestion Intelligente (Smart Building)** | Réseau interne isolé | Relié uniquement au Centre de Contrôle Centralisé et au Data Center via fibres Est/Ouest | Gestion GTB, sécurité, énergie, IoT |

---

# 5.3 Entrées physiques et redondance

## 5.3.1 Double entrée fibre

Le bâtiment dispose de **deux chambres optiques indépendantes** :

- **Entrée avant (Sud)** : accès FAI A + Réseau Gouvernemental (tronc principal)
- **Entrée arrière (Nord)** : accès FAI B + Réseau Gouvernemental (tronc de secours)

Chaque fibre suit un trajet **physiquement distinct** jusqu'au **local technique central (niveau -1)**, où elles convergent vers :

- un **ODF A/B (Optical Distribution Frame)**,
- un **système de monitoring optique**,
- et un **patch panel redondant** (étiqueté selon le plan de câblage fibre).

### 5.3.2 Résilience des liens

Les deux FAI assurent une **connexion Internet symétrique ≥ 1 Gbps**, avec engagement de disponibilité (SLA ≥ 99,9 %).
Les liens sont configurés en **agrégation active/passive (BGP failover)**, avec :

- **BGP AS distincts**,
- **préfixes annoncés de manière indépendante**,
- et bascule automatique en cas de perte de route.

---

## 5.4 Réseau gouvernemental (RGN)

### 5.4.1 Accès et sécurité

Le **réseau gouvernemental privé** est une dorsale MPLS sécurisée, administrée par le **Ministère du Numérique et de l'Économie**.
L'accès du bâtiment ARTF se fait par **deux liens optiques redondants** (avant/arrière) aboutissant également au local technique central, puis remontant directement au **3e étage (Data Center)**.

Ces liens ne transitent pas par Internet et utilisent :

- **adresses IP privées** selon le plan national RGN,
- **firewall dédié (Zone Gouvernementale)** isolé du reste du réseau ARTF,
- **authentification forte (certificats PKI national)** pour tout échange de données.

### 5.4.2 Rôle fonctionnel

Ce réseau transporte exclusivement :

- les flux **KYC**, **identité**, **fiscalité** (NIU, ONI, DGI, Passeports, DGAIC) ;
- les échanges inter-ministériels ;
- les communications d'administration de confiance.

Le trafic y est soumis à des politiques de sécurité **Zero Trust**, **IDS/IPS** gouvernemental et **chiffrement TLS 1.3 interne**.

---

# 5.5 Connectivité des assujettis

## 5.5.1 Accès OneBox

Chaque assujetti (banque, opérateur, fintech, agrégateur) est équipé d'un **boîtier OneBox** installé sur son site.
Ces équipements se connectent à la plateforme FinTraX du bâtiment ARTF via :

- le **réseau Internet public**,
- à travers un **tunnel VPN TLS 1.3** authentifié et chiffré (certificats émis par ARTF PKI),
- avec **filtrage IP et contrôle d'identité** (mTLS).

## 5.5.2 Gestion de la transition

Durant la période de migration :

- les OneBox continuent d'envoyer leurs transactions vers le **CTI (site primaire actuel)** ;
- puis, après la mise en service complète du Data Center ARTF, elles seront **progressivement réaiguillées** vers la nouvelle adresse IP publique du bâtiment. Un **plan d'adressage et de bascule contrôlée** sera mis en œuvre pour assurer la cohérence des flux.

---

# 5.6 Interconnexion ARTF ↔ CTI

La connectivité entre le **CTI** et le **bâtiment ARTF** repose sur :

- **Deux tunnels VPN TLS 1.3 redondants** passant par FAI A et FAI B ;
- **Chiffrement AES-256/GCM**, **authentification mutuelle mTLS**, **certificats X.509** ;
- **Monitoring FBB** : supervision des latences, pertes de paquets, disponibilité VPN, bande passante utilisée.
  La réplication des bases et des transactions FinTraX se fait de manière **asynchrone sécurisée**, avec **bascules automatiques** en cas de panne d'un lien.

---

# 5.7 Sécurité et supervision

## 5.7.1 Pare-feux et DMZ

Le bâtiment ARTF intègre :

- une **zone DMZ Internet**,
- une **zone DMZ gouvernementale**,
- et une **zone interne protégée**.
  Chaque zone est isolée par **firewalls de nouvelle génération (NGFW)** avec inspection applicative, IPS, et logs corrélés dans le FBB.

### 5.7.2 Système FBB (Supervision globale)

Tous les liens externes sont intégrés à la supervision **FBB (FinTraX Building Brain)** :

- surveillance en temps réel des **tunnels VPN**, **ports fibre**, **latence FAI**,
- corrélation avec les journaux de pare-feux et les alertes applicatives,
- génération d'alertes automatiques via dashboard, mail, WhatsApp, SMS, API.

---

## 5.8 Redondance énergétique et continuité

Les équipements de terminaison optique (ODF, routeurs, pare-feux, VPN gateways) du local technique sont :

- alimentés par **double circuit A/B**,
- protégés par **onduleurs Online**,
- et secourus par **génératrices G1/G2**.
  La **climatisation du local technique** est intégrée à la GTB, avec supervision FBB.

---

# 6. Backbone optique vertical & Roof POP

## 6.1 Objectif

Le backbone optique vertical du bâtiment de l'ARTF assure la **distribution et la redondance des connexions fibre** reliant :

- les **points d'entrée avant et arrière** du bâtiment,
- le **local technique central (niveau -1)**,
- les **étages techniques (notamment le 3e étage : Data Center & NOC)**,
- et le **toit (Roof POP)** destiné à accueillir les futurs liens **satellitaires** et **antennes de communication**.

Ce backbone constitue la **colonne vertébrale réseau** du bâtiment et garantit :

- la **continuité de service** en cas de rupture sur un trajet,
- la **capacité d'évolution future** (satellite, 5G, faisceaux hertziens),
- la **segmentation physique et logique** entre réseaux Internet, Gouvernemental, Smart Building et Interconnexion Interne.

---

# 6.2 Topologie générale

Le backbone se compose de **deux chemins optiques verticaux redondants**, situés sur les **faces Est et Ouest** du bâtiment.
Ces deux colonnes optiques :

- partent du **local technique central (niveau -1)**,
- montent dans des **gaines verticales sécurisées** jusqu'au **Roof POP**,
- traversent chaque étage avec **boîtes d'accès optiques** (interconnexion possible à chaque palier),
- et convergent au sommet dans une **baie d'interconnexion Roof POP**.

Chaque colonne transporte :

1. **Fibre Internet publique (FAI A/B)**
2. **Fibre Réseau Gouvernemental (RGN)**
3. **Fibre Smart Building / GTB**
4. **Fibre interne de secours (cross-link)**

---

# 6.3 Structure physique et normalisation

| Élément | Spécification |
|---|---|
| **Type de fibre** | Monomode OS2, 12 à 48 brins par colonne |
| **Connecteurs** | LC/APC ou SC/APC, identifiés par couleur (bleu : FAI, vert : RGN, jaune : Smart Building) |
| **Gainage** | Tube rigide FRP non propagateur de flamme (LSZH) |
| **Protection** | Gaine métallique dans les zones communes, étiquetage norme TIA-606-C |
| **Accessibilité** | Boîte d'accès optique à chaque étage (rack mural ou baie 6U) |
| **Redondance** | Colonne Est et colonne Ouest interconnectables au -1 et au Roof POP |
| **Supervision** | Modules SFP avec télémétrie FBB (dB, pertes, latence) |

| Élément | Spécification |
|---|---|
| **Sécurité physique** | Serrures à clé unique GTB, détecteurs d'ouverture reliés au FBB |

---

# 6.4 Local technique central (niveau -1)

Le **local technique** agit comme le **nœud de convergence primaire** :

- Accueil des **fibres d'entrée** (FAI A/B, RGN)
- Connexion aux **ODF A/B** pour distribution vers les colonnes Est/Ouest
- Présence de **switches optiques de monitoring**, **splitters**, et **convertisseurs opto-électriques**
- Liaisons montantes (uplinks) protégées par **UPS local** et **double alimentation**

Ce local est climatisé, équipé d'un système d'alarme incendie, et connecté au FBB pour la surveillance en continu.

---

# 6.5 Accès optique à chaque étage

## 6.5.1 Disposition générale

Chaque étage du bâtiment est équipé d'une **salle technique dédiée**, positionnée au **centre du plan d'étage**, permettant la **distribution horizontale** vers les zones de travail, les équipements réseau, les bornes Wi-Fi et les dispositifs Smart Building.

Les **Points d'Accès Optiques (PAO)** situés dans les colonnes **Est et Ouest** desservent cette salle via des **liaisons cuivre de catégorie 7** à haut débit (10 Gbps minimum), converties localement par des **modules transceivers fibre/ethernet**.

---

## 6.5.2 Architecture de connexion

Le cheminement est le suivant :

```
Fibre Backbone (Est/Ouest)
        │
        ▼
[Boîtier PAO de l'étage]
        │  (LC/APC - fibre OS2)
   Convertisseur Média
 (Fibre → Ethernet Cat 7)
        │
        ▼
```

```
[Panneau de brassage cuivre Cat7]
        |
        ▼
[Switch d'étage / équipements Smart Building / bornes Wi-Fi]
```

---

### 6.5.3 Équipements et interfaces

| Élément | Spécification |
|---|---|
| **PAO** | Boîtier mural ou rack 6U avec connecteurs LC/APC |
| **Convertisseur Média** | SFP 1G ou 10G compatible OS2, duplex LC, RJ45 cuivre, alimentation 48V POE ou 220V |
| **Câblage Cuivre** | Catégorie 7 S/FTP (blindage individuel + global), longueur ≤ 90 m |
| **Panneau de Brassage Cuivre** | 24 ports RJ45 blindés, norme ISO/IEC 11801 classe F |
| **Switch d'Étage** | 24/48 ports Gigabit ou 10GBase-T, POE+, redondance LACP, VLAN segmentés |
| **Alimentation** | UPS local + double circuit A/B, intégré GTB |
| **Repérage et documentation** | Étiquetage norme TIA-606-C, suivi dans CMDB FBB |

---

### 6.5.4 Sécurité et supervision

- Tous les convertisseurs média et panneaux de brassage sont **surveillés par le Système FBB** via sondes SNMPv3 ou agents propriétaires (tension, température, statut lien).
- Chaque salle technique d'étage est équipée :
  - d'un **capteur T°/humidité** connecté à la GTB,
  - d'un **détecteur d'ouverture de porte**,
  - et d'un **mini-UPS** assurant 15 à 30 minutes d'autonomie locale.
- Les liaisons Cat 7 sont testées et certifiées pour le **10GBase-T**, avec réflectométrie cuivre (Fluke DSX).

---

### 6.5.5 Résultat attendu

Cette architecture garantit :

- une **distribution horizontale performante et modulaire**,
- la **conversion transparente fibre ↔ cuivre** sans perte de débit,
- une **maintenance simplifiée** (panneaux de brassage centraux),

- une **supervision unifiée** par le système FBB,
- et une **prédisposition complète** pour les extensions futures (Wi-Fi 6E, IoT, vidéo IP, etc.).

---

# 6.6 Roof POP – Point Haut du Bâtiment

Le **Roof POP (Point of Presence)** constitue le **terminus supérieur** du backbone.
Il est conçu pour :

- accueillir des **antennes de communication** (5G, Wi-Fi longue portée, liaisons radio, faisceaux hertziens),
- intégrer un **modem satellite VSAT** ou **Starlink professionnel** pour redondance Internet,
- abriter une **baie d'interconnexion optique**, protégée et ventilée,
- et assurer une **connectivité directe** au Data Center (3e étage) via fibres Est/Ouest.

### Caractéristiques du Roof POP

| Élément | Spécification |
|---|---|
| **Localisation** | Toit technique, zone protégée et climatisée |
| **Équipement** | Baie 12U inox, panneaux optiques 24 ports LC/APC |
| **Protection** | IP65 / IK10, détection intrusion & fumée |
| **Alimentation** | Circuit A/B + panneaux solaires + UPS 2 kVA |
| **Surveillance** | Caméra IP + capteurs T°, HR, tension |
| **Accès** | Badge technique + verrouillage GTB + supervision FBB |

---

# 6.7 Supervision et maintenance

- Toutes les fibres backbone sont intégrées au **Système FBB** via modules SFP avec télémétrie :
  - perte optique (dB),
  - disponibilité du lien,
  - trafic, latence, erreurs CRC.
- Alertes automatiques en cas de coupure ou atténuation anormale.
- Maintenance préventive semestrielle : inspection des connecteurs, nettoyage, test de réflectométrie (OTDR).

---

# 6.8 Résilience et continuité

Le backbone optique assure :

- **Redondance totale Est/Ouest** (niveau -1 ↔ Roof POP ↔ 3e étage)
- **Bascule automatique LACP / VRRP** entre les chemins en cas de rupture
- **Continuité de service** pour tous les flux :
  - Internet (FAI A/B)
  - Réseau Gouvernemental (RGN)
  - Smart Building (GTB)
  - Data Center ↔ Roof POP ↔ CTI

Cette configuration garantit une **résilience optique de niveau Tier III**, conforme aux meilleures pratiques **TIA-942-B / ISO 24764** pour infrastructures critiques.

## 7. Data Center – Nœud central FinTraX & Smart Building

# 7.1 Rôle et positionnement

Le **Data Center du 3e étage** du bâtiment de l'ARTF constitue le **nœud central** de l'écosystème numérique FinTraX et du Smart Building.
Il héberge :

- les **serveurs de production FinTraX**,
- les **bases de données KYC**,
- les **composants analytiques et de certification**,
- les **serveurs GTB/BMS** assurant la gestion intelligente du bâtiment,
- ainsi que les systèmes de **supervision et de corrélation FBB**.

Il est conçu selon les principes de **haute disponibilité (Tier III)** et de **sécurité multi-niveaux**, garantissant la continuité de service même en cas de défaillance d'un composant ou d'une alimentation.

---

# 7.2 Zonation et accès

Le Data Center est divisé en trois zones fonctionnelles distinctes :

| Zone | Fonction | Accès |
|---|---|---|
| **Zone blanche (salle serveurs)** | Racks FinTraX, GTB, stockage, virtualisation | Restreint – accès biométrique double facteur |
| **Zone grise (technique)** | UPS, PDU, tableaux, climatisation, câblage fibre/cuivre | Techniciens habilités uniquement |

| Zone | Fonction | Accès |
|---|---|---|
| **Zone NOC attenante** | Supervision, consoles d'exploitation, murs d'écrans | Opérateurs 24/7 – accès contrôlé |

Un **sas de sécurité** avec **porte coupe-feu EI90** et **contrôle d'accès biométrique + badge** sépare les zones.
Une **baie de réception (vestibule technique)** permet la validation des entrées/sorties de matériel sans compromettre l'intégrité de la salle.

---

# 7.3 Environnement et infrastructures critiques

| Élément | Spécification |
|---|---|
| **Plancher technique** | Plancher surélevé 600 mm, charge ≥ 1 000 kg/m², structure acier galvanisé |
| **Cloisons** | EI90 (résistance feu 90 min), vitrage sécurit pare-flammes pour visibilité NOC |
| **Climatisation** | Système redondant N+1 InRow / Split CRAC, gestion automatique via GTB |
| **Température/Humidité** | 22 °C ± 2 °C / HR 45–60 % |
| **Surpression d'air** | 2 Pa pour protection poussière |
| **Détection incendie** | Système VESDA + détection multi-capteurs, agent extincteur Novec 1230 |
| **Sol antistatique** | Revêtement ESD ≤ $2 \times 10^6$ Ω |
| **Éclairage** | LED 500 lux, déclenchement automatique + mode maintenance |

---

# 7.4 Architecture informatique

## 7.4.1 Infrastructure physique

- 8 à 10 **racks 42U**, répartis selon fonction :
  - **FinTraX (racks A1–A4)** : serveurs d'analyse, certification, base de données.
  - **Smart Building (racks B1–B2)** : serveurs GTB/BMS, SCADA, IoT.
  - **Infrastructure commune (racks C1–C2)** : virtualisation, stockage, firewall, FBB.
  - **Réseau (racks D1–D2)** : switchs cœur et distribution, ODF fibre, PDU intelligents.
- Racks ventilés avant/arrière, température contrôlée, monitoring SNMP.

### 7.4.2 Virtualisation et stockage

- Hyperviseurs **Proxmox VE** ou **VMware vSphere 8** (cluster 3 à 4 hôtes)
- Stockage centralisé **SAN/NAS 10/40 GbE** (RAID 10, redondance double contrôleur)
- Réplication asynchrone vers CTI (ZFS send/receive, rsync, snapshots incrémentaux)
- Sauvegardes quotidiennes + hebdomadaires sur stockage déporté chiffré (AES-256)

### 7.4.3 Réseau interne

- Double cœur 10 / 40 Gbps, commutation L3 (VRRP, LACP)
- VLAN segmentés : FinTraX, KYC, Smart Building, Management, Sécurité, Backup
- Pare-feux NGFW actifs/actifs, inspection SSL, IDS/IPS intégré
- Connectivité redondée vers backbone Est/Ouest et Roof POP
- Tunnels VPN TLS 1.3 avec CTI et institutions externes

---

## 7.5 Systèmes FinTraX

Le Data Center héberge les modules essentiels :

1. **Collecte des transactions** (OneBox Gateways, APIs REST sécurisées)
2. **Analyse et corrélation** (Elastic / Grafana / ML local)
3. **Certification et signature** (modules HSM, PKI ARTF)
4. **Base de données** (PostgreSQL HA, partitionnement logique, réplication CTI)
5. **Monitoring FBB intégré** : supervision réseau, applicatif, KYC, flux transactionnels.

Toutes les communications sont chiffrées **TLS 1.3 + mTLS**, avec authentification basée sur certificats X.509.

---

## 7.6 Systèmes Smart Building

Les serveurs **GTB/BMS** du Data Center gèrent :

- **Contrôle d'accès** (badges, biométrie, interphonie IP)
- **CCTV / VMS** (ONVIF, stockage NAS redondé)
- **Détection incendie / intrusion / environnementale**
- **Énergie** (mesure MID, UPS, groupes, PV, charge réseau)

- **Climatisation / ventilation / température**
- **Réseau IoT** (MQTT/OPC-UA, passerelles KNX/BACnet/Modbus)

Chaque sous-système est intégré dans le **Système FBB**, garantissant l'interopérabilité totale via SNMPv3, API REST ou agents FBB.

---

# 7.7 Sécurité et conformité

- **Surveillance physique 24/7**, caméras IP ONVIF, contrôle d'accès biométrique.
- **Audit de conformité ISO 27001** et **Uptime Tier III**.
- **Zéro Trust Architecture** interne (MFA, segmentation, micro-segmentation).
- **Protection contre surtension / foudre / EMI**.
- **Accès administrateurs journalisé** (Syslog sécurisé, traçabilité RGPD).
- **Plan de Reprise d'Activité (PRA)** et **Plan de Continuité (PCA)** testés semestriellement.

---

# 7.8 Supervision FBB

Tous les équipements du Data Center (serveurs, onduleurs, clim, PDU, réseau, sécurité) sont intégrés au **Système de Contrôle et d'Alerte FBB** :

- supervision centralisée,
- corrélation intelligente (IT + bâtiment),
- tableaux de bord dynamiques,
- alertes multicanaux (SMS, mail, webhook).

Le FBB mesure également :

- température par rack,
- consommation énergétique (PDU intelligents),
- disponibilité réseau,
- latence vers CTI,
- taux de synchronisation FinTraX.

---

# 7.9 Résilience énergétique

- Alimentation A/B séparée depuis tableau principal.
- UPS modulaires N+1 (autonomie 30–60 min).
- Génératrice G1 (bâtiment) + G2 (mode éco nuit/week-end).

- Panneaux solaires Roof POP dédiés Data Center.
- Système automatique de délestage et priorisation (via GTB).

---

# 7.10 Résultat attendu

Le **Data Center du 3e étage** devient le **cœur numérique souverain** de l'ARTF :

- hébergeant FinTraX et le Smart Building,
- assurant interconnexion CTI ↔ ARTF ↔ Gouvernement,
- garantissant sécurité, disponibilité et évolutivité.

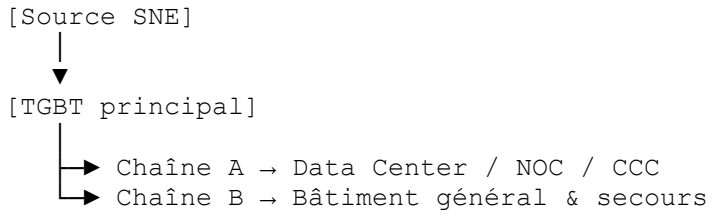
L'ensemble répond aux standards internationaux et confère à l'ARTF une **infrastructure de référence régionale**.

## 8. Énergie, continuité & efficacité

### 8.2.1 Alimentation principale

- Le bâtiment est alimenté en **triphasé 400 V / 50 Hz** depuis le réseau public de la **SNE (Société Nationale d'Électricité)**.
- Le point d'entrée principal se situe au **local technique du rez-de-chaussée**, équipé d'un **TGBT principal (Tableau Général Basse Tension)**.
- Deux **lignes montantes verticales indépendantes (A et B)** alimentent les étages via des **TD (Tableaux Divisionnaires)** dédiés.

### 8.2.2 Chaîne de distribution




Chaque étage dispose de :

- un **tableau divisionnaire A/B**,
- un **mini-UPS local** pour les charges sensibles,
- une **liaison GTB** pour la surveillance énergétique.

---

# 8.3 Groupes électrogènes et secours

## 8.3.1 Groupe principal G1

- **Puissance** : ≥ 250 kVA (capable d'alimenter 100 % du bâtiment).
- **D démarrage automatique (ATS)** ≤ 15 s après coupure secteur.
- **Carburant** : diesel, autonomie 48 h minimum.
- **Local insonorisé et ventilé**, avec système d'échappement extérieur.

## 8.3.2 Groupe secondaire G2 (éco)

- **Puissance réduite** : 60–80 kVA.
- Utilisé la **nuit, week-end ou hors charges critiques**, pour limiter la consommation de carburant.
- Alimente uniquement : Data Center, NOC, CCC, sécurité, clim et éclairage technique.
- Gestion automatique via GTB selon plages horaires ou détection de charge.

## 8.3.3 Groupes et priorités

Les deux groupes sont synchronisés via **ATS double entrée** et **contrôleur intelligent** :

- bascule automatique sur **G2** lorsque la demande < 40 % de la charge nominale,
- priorisation automatique des charges critiques selon scénario GTB.

---

# 8.4 Onduleurs (UPS) et alimentation redondée

| Élément | Spécification |
|---|---|
| **UPS Data Center** | Double chaîne A/B, on-line double conversion, autonomie 30–60 min |
| **UPS NOC & CCC** | UPS 20 kVA N+1, autonomie 20 min |
| **UPS étage** | Mini-UPS 3–5 kVA pour équipements GTB et réseau |
| **Bypass** | Statique + manuel de maintenance |
| **Batteries** | $LiFePO_4$ (sécurité, densité, durée de vie 10–15 ans) |
| **Monitoring** | Tension, température, cycles, durée restante – supervision FBB |

L'ensemble des UPS est surveillé via **protocole SNMPv3**, avec intégration complète au **Système FBB** (alertes batterie faible, surcharge, température, défaut redresseur).

---

# 8.5 Énergie solaire (Roof POP)

Des **panneaux photovoltaïques** installés au niveau du **toit technique (Roof POP)** complètent la production énergétique :

- **Surface utile** : environ 80 m², orientation Nord-Est.
- **Puissance crête estimée** : 30–40 kWc.
- **Onduleurs solaires** redondants reliés au TGBT via convertisseurs hybrides.
- L'énergie produite alimente en priorité le **Data Center**, puis le **bâtiment général**.
- En cas de coupure prolongée, les panneaux maintiennent les systèmes essentiels (**GTB, FBB, clim, sécurité**) en fonctionnement réduit.

Suivi en temps réel via le **FBB** : tension DC, production instantanée, rendement, état onduleurs, PUE solaire.

---

# 8.6 Gestion et supervision énergétique

## 8.6.1 Intégration GTB / FBB

Tous les équipements énergétiques (UPS, groupes, TGBT, TD, onduleurs solaires, PDU) sont intégrés dans le **Système FBB** via la **GTB** :

- acquisition en **Modbus/TCP**, **SNMPv3** ou **BACnet/IP**,
- centralisation au **Centre de Contrôle Centralisé**,
- remontée dans le **tableau de bord énergétique** (PUE, consommation, état des chaînes A/B).

## 8.6.2 Indicateurs clés

| Indicateur | Objectif |
|---|---|
| **PUE global** (Power Usage Effectiveness) | ≤ 1.7 |
| **Disponibilité énergétique** | ≥ 99,982 % (Tier III) |
| **Taux de charge G2** | < 60 % en mode éco |
| **Rendement UPS** | ≥ 94 % |
| **Rendement solaire** | ≥ 85 % de la puissance nominale |
| **Temps de bascule secteur → G1** | < 15 s |

---

# 8.7 Sécurité électrique

- **Mise à la terre unique** (< 10 Ω), liaison équipotentielle sur tout le bâtiment.

- **Parafoudre** T1/T2 aux TGBT et TD selon **IEC 62305**.
- **Sectionnement clair** des circuits A/B, couleur et étiquetage normalisés.
- **Détection de défaut d'isolement** et **capteurs de température** dans chaque armoire.
- **Déclenchement différentiel** 30 mA dans zones sensibles.
- **Test de charge trimestriel** sur groupes et UPS.
- **Éclairage de secours** sur circuit dédié avec autonomie ≥ 2 h.

---

# 8.8 Efficacité énergétique et durabilité

- **Optimisation GTB** : délestage automatique, extinction des zones inoccupées.
- **Récupération de chaleur** des systèmes de climatisation pour préchauffage d'eau technique.
- **Climatisation Free-Cooling** (selon température extérieure).
- **Utilisation de LED basse consommation** et **détecteurs de présence**.
- **Surveillance continue de la consommation** par étage et par usage (GTB → FBB).
- **Rapports mensuels** d'efficacité énergétique et d'émissions $CO_2$ évitées.

---

# 8.9 Résultat attendu

L'architecture énergétique du bâtiment ARTF assure :

- une **continuité d'alimentation totale** (Tier III),
- une **bascule automatique multi-niveaux** (secteur → G1 → G2 → solaire),
- une **supervision centralisée** par le système **FBB**,
- et une **efficacité énergétique durable** mesurable en temps réel.

L'ensemble offre un **bâtiment autonome, sécurisé et optimisé**, garantissant le maintien opérationnel du système FinTraX et du Smart Building 24 h/24, 7 j/7 et conforme aux standards internationaux (TIA-942-B, IEC 60364, ISO 50001)

## 9. Système de Contrôle et d'Alerte FBB (SCAFBB)

# 9.1 Rôle et principe général

Le **Système de Contrôle et d'Alerte FBB** — *FinTraX Building Brain* — constitue la **plateforme centrale de supervision, de corrélation et d'alerte** de l'ensemble de l'écosystème du bâtiment ARTF.

Il unifie la **surveillance IT (serveurs, réseaux, applicatifs)** et **OT (énergie, climatisation, sécurité, GTB)** au sein d'une **interface unique**, permettant :

- la **visualisation en temps réel** des états, performances et alertes,
- la **corrélation automatisée** des incidents entre domaines (IT ↔ bâtiment ↔ sécurité),
- et la **réaction intelligente** (notifications, automatisation, actions correctives).

Le SCAFBB est conçu pour garantir une **interopérabilité complète**, une **extensibilité sans contrainte de fabricant**, et une **disponibilité continue 24/7**.

---

# 9.2 Architecture fonctionnelle

Le système repose sur une architecture **multi-couches** :

| Couche | Fonction principale | Exemple de composants |
|---|---|---|
| **Collecte (agents & sondes)** | Captation des métriques et statuts | SNMPv3, API REST, MQTT, BACnet, Modbus, agents FBB |
| **Transport & traitement** | Normalisation, filtrage, mise en file, stockage brut | Broker MQTT / API Gateway / Syslog / Collector |
| **Corrélation & analyse** | Fusion et hiérarchisation des événements | Moteur d'alertes, IA de corrélation, règles multi-domaines |
| **Visualisation & reporting** | Tableaux de bord dynamiques et historiques | Portail Web FBB, dashboards NOC/CCC, rapports automatiques |
| **Automatisation & réaction** | Actions automatiques ou manuelles sur alerte | Scripts API, notifications, commandes SNMP set, fermeture contact |

---

# 9.3 Collecte des données

## 9.3.1 Types de données supervisées

- **IT / Réseaux :** serveurs FinTraX, VM, hôtes, switches, VPN, liens fibre Est/Ouest, CTI, Internet FAI.
- **OT / Bâtiment :** énergie (UPS, G1, G2, solaire), climatisation, GTB, capteurs IoT, accès, vidéosurveillance.
- **Applicatif :** FinTraX (flux, transactions, bases KYC), GTB (états automates, charges électriques).
- **Environnement :** température, humidité, vibrations, intrusion, fumée, $CO_2$.

### 9.3.2 Protocoles supportés

- **SNMP v3 sécurisé (AES-256 + SHA-256)**
- **API REST / WebSocket** pour intégration applicative
- **MQTT / OPC-UA** pour IoT et GTB
- **Syslog sécurisé (TCP/TLS)** pour événements systèmes
- **Agent FBB natif** compatible Linux / Windows / équipements réseau

Tous les flux sont chiffrés via **TLS 1.3** et authentifiés par **certificats X.509** émis par la PKI ARTF.

---

## 9.4 Corrélation et analyse intelligente

Le SCAFBB intègre un **moteur de corrélation événementielle** basé sur un modèle de logique hybride :

- règles **déterministes (SI...ALORS...)** pour incidents connus,
- corrélation **temporelle** entre événements multiples,
- analyse **heuristique et IA légère** pour détection d'anomalies (séries temporelles, patterns anormaux).

Exemples :

- coupure d'un lien fibre + alerte d'un switch = incident "rupture optique colonne Est" ;
- surconsommation UPS + température rack > 30 °C = "risque surcharge thermique DC".

Les **alertes critiques** sont automatiquement priorisées selon leur impact (P1 à P4) et les **actions correctives** peuvent être déclenchées automatiquement (bascule lien, redémarrage service, notification opérateur).

---

## 9.5 Tableaux de bord et visualisation

### 9.5.1 Interfaces

- **Portail Web FBB** : accessible via HTTPS, authentification MFA, profils utilisateurs (Admin / NOC / CCC / Technique).
- **Dashboards dynamiques** :
  - Vue **Data Center** : énergie, température, serveurs, réseaux, stockage.
  - Vue **Smart Building** : climatisation, GTB, sécurité, caméras.

    - Vue **Connectivité externe** : VPN, CTI, FAI, RGN.
    - Vue **Énergie & efficacité** : PUE, rendement solaire, charge G2.
- **Carte topologique interactive** : représentation du bâtiment et des flux, mise à jour en temps réel.

### 9.5.2 Alertes et notifications

- Envoi automatique par **email, SMS, WhatsApp, Telegram, ou webhook API**.
- Gestion des escalades et relances automatiques selon SLA.
- Historique des alertes exportable (CSV/PDF).
- Journalisation conforme **ISO 27035 (gestion d'incidents)**.

---

# 9.6 Intégration multi-systèmes

| Domaine | Intégration | Type |
|---|---|---|
| **FinTraX** | API REST / agents / logs applicatifs | Analyse transactionnelle & certification |
| **Smart Building (GTB)** | BACnet/IP, Modbus/TCP, KNX, MQTT | États capteurs & automates |
| **Réseau / Télécoms** | SNMPv3, ICMP, NetFlow | Switches, routeurs, VPN, fibres |
| **Énergie** | Modbus/TCP, SNMP, SCADA GTB | UPS, G1, G2, PDU, onduleurs solaires |
| **Sécurité / Vidéo** | ONVIF, API NVR, SNMP | Caméras, enregistreurs, contrôle d'accès |
| **CTI / Externe** | VPN TLS 1.3 + API sécurisée | Synchronisation données et supervision inter-sites |

Le SCAFBB agit comme **bus d'intégration global**, garantissant la cohérence des flux et la compatibilité entre fabricants.

---

# 9.7 Résilience et sécurité du SCAFBB

- Architecture **redondée active/active** sur deux serveurs FBB dans le Data Center.
- Réplication asynchrone vers le CTI (base + configurations).
- Sauvegarde automatique toutes les 6 h.
- Authentification **MFA + RBAC** (rôles et sous-rôles).
- Journalisation complète des actions opérateurs (audit trail).
- Système **haute résilience** avec bascule automatique en cas de perte d'un nœud.

---

# 9.8 Maintenance et exploitation

- Supervision **24/7** par l'équipe NOC.
- Mises à jour mensuelles des modules FBB.
- Test trimestriel des alertes critiques.
- **Documentation** : fiches d'équipement, MIBs, API, schémas d'intégration.
- **Formation opérateurs et techniciens** : niveau 1 (exploitation), niveau 2 (intégration), niveau 3 (administration).
- **Support évolutif** : ajout de nouveaux équipements ou protocoles via modules FBB.

---

# 9.9 Résultat attendu

Le **Système FBB (SCAFBB)** devient le **noyau de pilotage unifié** du bâtiment et du système FinTraX :

- garantissant **une supervision globale, proactive et interopérable**,
- assurant **la corrélation automatisée** entre les domaines IT, énergie, sécurité et Smart Building,
- et permettant à l'ARTF d'exploiter un **bâtiment totalement intelligent, prédictif et résilient**.

Le FBB fait du site ARTF un **modèle de gestion intégrée** des infrastructures critiques — combinant **supervision, analyse, efficacité et souveraineté numérique**.

## 10. CCTP Interopérabilité et Intégration FBB

### 10.1 Objet

Le présent addendum définit les **exigences minimales d'interopérabilité, d'intégration et de conformité** que devront respecter **tous les équipements, logiciels et systèmes techniques** installés dans le bâtiment de l'Autorité de Régulation des Transferts de Fonds du Congo (ARTF).

Ces exigences s'appliquent à :

- l'ensemble des systèmes **électriques, énergétiques, climatiques, de sécurité, GTB, IoT et IT**,
- les infrastructures du **Data Center, NOC et CCC**,

- et toutes les solutions tierces destinées à être **supervisées ou intégrées** dans le **Système de Contrôle et d'Alerte FBB (SCAFBB)**.

---

## 10.2 Objectif de l'intégration FBB

L'objectif est de garantir que tous les équipements installés :

1. puissent **communiquer** avec le système FBB via des protocoles standards ouverts ;
2. exposent des **métriques et états** lisibles et normalisés ;
3. permettent une **supervision unifiée** au sein du tableau de bord FBB ;
4. supportent des **actions de commande ou de contrôle à distance** ;
5. respectent les principes de **sécurité, redondance et traçabilité** définis par l'ARTF.

---

## 10.3 Normes et protocoles exigés

Tout équipement fourni et installé doit, selon sa catégorie, être **nativement compatible** avec au moins un des protocoles suivants :

| Domaine | Protocoles minimum requis |
|---|---|
| **Réseau / IT** | SNMP v3, ICMP, Syslog, API REST, NetFlow |
| **Énergie / Électrique** | Modbus/TCP, BACnet/IP, SNMP v3 |
| **GTB / Smart Building** | KNX/IP, Modbus/TCP, BACnet/IP, MQTT |
| **Vidéo / Sécurité / Accès** | ONVIF, SIP, HTTPS, API REST |
| **IoT / Capteurs** | MQTT, OPC-UA, CoAP, HTTP(S) |
| **Supervision logicielle / Applications** | API REST JSON, SNMP, Webhooks, Syslog |

Les équipements fermés (protocoles propriétaires) sont **strictement interdits** sauf si un **connecteur ou passerelle ouverte** est fournie par le constructeur ou intégrée par le maître d'œuvre sous validation FBB.

---

## 10.4 Données et supervision

Chaque équipement doit pouvoir transmettre au minimum :

- **État d'alimentation / disponibilité**
- **Statut de communication / alarme**
- **Mesures principales (tension, température, charge, débit, etc.)**

- **Alertes et codes d'erreurs normalisés (OID, API ou JSON)**
- **Historique local ou tampon** en cas de coupure réseau

L'intégration au FBB se fera via **agent FBB** ou **passerelle compatible**, fournis par l'intégrateur.

---

## 10.5 Agents et connecteurs FBB

### 10.5.1 Agents logiciels

Les agents FBB sont disponibles pour les environnements :

- **Linux (Debian/Ubuntu/RHEL)**
- **Windows Server**
- **Appliances réseau (via Docker / API)**

Ils permettent la collecte locale et la remontée sécurisée via TLS 1.3.

### 10.5.2 Connecteurs FBB

Des connecteurs standards sont fournis pour :

- **Modbus/TCP** (énergie)
- **BACnet/IP** (GTB)
- **ONVIF / SIP** (sécurité)
- **MQTT / OPC-UA** (IoT)
- **API REST** (applications externes)

L'intégrateur doit valider la compatibilité de chaque équipement avant installation.

---

## 10.6 Sécurité et conformité

Tous les échanges entre équipements et le FBB doivent :

- être **chiffrés** (TLS 1.3, AES-256, SSHv2) ;
- être **authentifiés** (certificats X.509, clé API ou signature HMAC) ;
- être **journalisés** pour audit (Syslog sécurisé, logs horodatés) ;
- respecter la **segmentation réseau** (VLAN dédiés IT / OT / Administration).

Chaque fournisseur devra fournir :

- le **plan d'adressage IP** de ses équipements,
- la **liste des ports et protocoles utilisés**,

- et la **documentation d'intégration** FBB correspondante.

---

## 10.7 Exigences de test et validation

Avant toute mise en production :

1. chaque équipement sera **testé en environnement isolé** (sandbox FBB),
2. un **rapport d'intégration FBB** sera produit, incluant :
   - l'état de communication,
   - la liste des métriques remontées,
   - les codes d'alerte normalisés,
   - les éventuelles limitations.
3. l'équipement ne sera **accepté définitivement** qu'après validation par la **cellule technique ARTF / Geolab**.

---

## 10.8 Maintenance et évolutivité

- Les équipements intégrés doivent supporter les **mises à jour sans rupture de service**.
- Le maître d'œuvre doit garantir la **fourniture des MIBs, APIs, et clés d'accès** pendant toute la durée d'exploitation.
- Les mises à jour ou ajouts de périphériques devront être documentés et validés par la **cellule FBB**.
- Une **formation intégration FBB** doit être dispensée à chaque nouvelle équipe technique.

---

## 10.9 Responsabilité de conformité

Tout équipement ou système non compatible avec le FBB :

- sera considéré comme **non conforme** au CCTP ;
- pourra être **refusé ou désactivé** du système global ;
- entraînera, le cas échéant, une **retenue de garantie** jusqu'à mise en conformité complète.

---

## 10.10 Résultat attendu

L'application du présent addendum garantit :

- une **interopérabilité totale** entre les sous-systèmes IT, OT, énergie, sécurité et GTB,
- une **supervision centralisée et cohérente** dans le Système FBB,
- une **traçabilité complète** des événements et alarmes,
- une **extensibilité maîtrisée** du bâtiment pour les évolutions futures (5G, IA, Edge Computing).

L'ensemble de ces clauses assure la pérennité technique du projet et confère au bâtiment ARTF un **niveau d'intégration et de résilience exemplaire**, conforme aux standards internationaux de gestion des infrastructures critiques.

# Conclusion et Validation du Rapport Technique

## Bâtiment de l'Autorité de Régulation des Transferts de Fonds du Congo (ARTF)

**Rapport technique d'aménagement, d'interconnexion et de supervision**
**Rédigé par Geolab – Brazzaville, République du Congo**

---

## Synthèse du projet

Le présent rapport établit la **conception technique complète** du bâtiment de l'ARTF, actuellement en construction, et définit les standards d'**aménagement, d'interconnexion, d'énergie, de supervision et de sécurité** nécessaires à sa mise en exploitation.

Les études menées visent à :

- **héberger le NOC et le Data Center FinTraX** au 3e étage dans des conditions de sécurité et de performance conformes aux standards **TIA-942-B / Tier III** ;
- **rapatrier le CTI** vers le bâtiment ARTF, assurant une **redondance active** et une synchronisation continue des données ;
- **implémenter un Smart Building complet**, supervisé par le **Centre de Contrôle Centralisé (CCC)** ;
- et **unifier la supervision IT/OT** à travers le **Système de Contrôle et d'Alerte FBB (SCAFBB)**, garantissant une interopérabilité totale entre tous les systèmes énergétiques, numériques et environnementaux.

Ce rapport tient compte des impératifs d'**efficacité énergétique**, de **résilience**, et de **sécurité nationale**, en conformité avec les orientations stratégiques de l'Autorité de Régulation des Transferts de Fonds du Congo.

---

## Livrables et conformité

Les livrables techniques comprennent :

- les **plans d'aménagement du NOC et Data Center**,
- la **topologie de connectivité externe**,
- le **backbone optique vertical et Roof POP**,
- la **distribution énergétique redondée (G1/G2/solaire)**,
- la **conception du Smart Building et du CCC**,
- et le **CCTP d'interopérabilité FBB**.

L’ensemble des spécifications, schémas et protocoles a été défini selon les normes internationales applicables (ISO, IEC, TIA, ITU, ASHRAE).

---

## Résultat attendu

À l’issue de la mise en œuvre :

- le **bâtiment ARTF** deviendra le **centre névralgique souverain** du système FinTraX et de la supervision nationale des transferts de fonds ;
- il disposera d’un **écosystème totalement intégré**, sécurisé, et supervisé ;
- et constituera une **référence régionale** en matière de bâtiment intelligent, de souveraineté numérique et d’efficacité énergétique.