



DIR Est – Tunnels de la Voie des Mercureaux

Renouvellement de la Gestion Technique Centralisée Documentation technique

CCTP – Livret 5

Juillet 2025

LOMBARDI Ingénierie
70 rue de la Villette
69425 LYON CEDEX 03
+33 (0)4 26 84 26 10
info@LOMBARDI-ing.fr



SUIVI DES MODIFICATIONS

C	31/07/2025	Passage du document en accès public	P. Peyret	P. Peyret	C. Lemée
B	20/06/2025	Reprises relectures DIR Est et CETU	P. Peyret Y. Gayet	P. Peyret	C. Lemée
A	05/05/2025	Version initiale	P. Peyret Y. Gayet	P. Peyret	C. Lemée
Version	Date	Modifications	Rédaction	Vérification	Approbation

SOMMAIRE

SUIVI DES MODIFICATIONS.....	2
SOMMAIRE.....	3
I. OBJET DU DOCUMENT.....	4
II. SYSTÈMES.....	5
II.1. AUTOMATISMES.....	5
II.2. SCADA.....	8
II.3. ARCHITECTURE RÉSEAUX ET RÉSEAU FIBRE OPTIQUE.....	9

I. OBJET DU DOCUMENT

Le présent document constitue le 5^{ème} livret du Cahier des Clauses Techniques et Particulières (CCTP) du marché relatif à l'opération de rénovation de la GTC de la DIR Est.

Le CCTP est constitué de cinq livrets :

- Livret 1 : Généralités
- Livret 2 : Programme fonctionnel et Performances
- Livret 3 : Spécifications matérielles et Architectures
- Livret 4 : Planning et Migrations
- **Livret 5 (présent livret) : Documentation technique**

II. SYSTÈMES

II.1. Automatismes

II.1.1. Architecture

L'architecture de la couche basse de la GTC, à savoir la partie API comporte une spécificité notable, à savoir celle d'être raccordée à la fois à la supervision/SCADA ainsi qu'au SAGT. C'est notamment ce double attachement qui garantit la redondance ; un seul serveur GTC étant pour l'instant disponible sur l'infrastructure des tunnels de la Voie des Mercureaux.

Ces deux systèmes sont donc en mesure de disposer de remontées d'états ou même d'agir sur les équipements terrain raccordés au système automate.

- La GTC dans son ensemble comporte 3 niveaux de décision :
- Niveau 0 : Systèmes d'acquisition (capteurs et actionneurs),
 - Niveau 1 : Automatisme (API),
 - Niveau 2 : Supervision,
 - Niveau 3 : SAGT (Système d'Aide à la gestion du trafic),

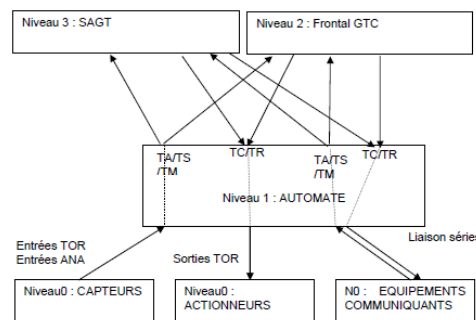


Figure 1 : Synoptique du dispositif de surveillance des systèmes de Bois de Peu et Fontain

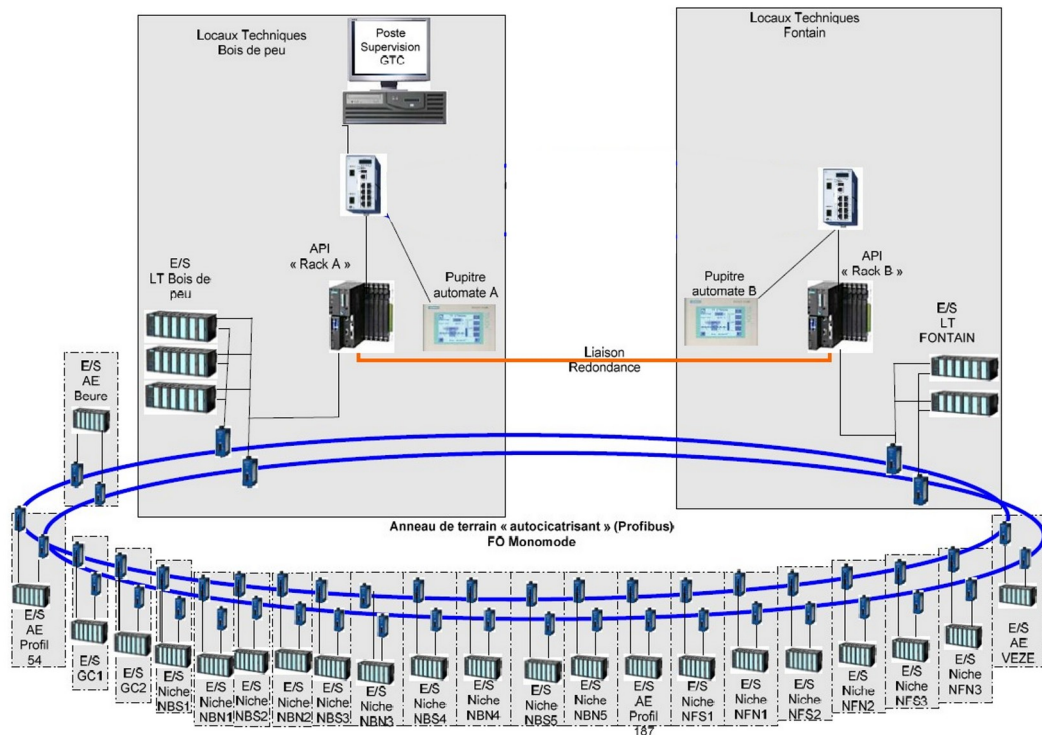


Figure 2 : Architecture générale des automatismes

II.1.2. Niveau terrain

Au niveau terrain, les **modules d'entrées-sorties déportées**, regroupés dans des racks, assurent l'acquisition des informations issues des équipements locaux et leur remontée vers les automates. Des **modules de communication MODBUS** permettent des échanges directs entre les automates et des équipements spécifiques tels que les centrales de mesures ou les onduleurs.

▪ Pupitres de commande

Chaque automate est associé à un pupitre de commande, permettant une supervision locale de l'état et des fonctions du système. Ces pupitres facilitent l'interaction directe avec le système et l'affichage des informations critiques pour les opérateurs, en complément des postes de supervision principaux du CSIGT.

▪ Armoires Électriques et coffrets

Ces armoires et coffrets, contiennent les modules déportés ET200M, utilisés pour la collecte des informations et le contrôle des dispositifs sur le terrain. Ils contiennent également des modules de communication série pour l'interfaçage avec divers équipements de sécurité, de fermeture, de mesures, etc.

▪ Centrales de mesures et informations onduleurs

Des modules de communication sont déployés pour interfacer les automates avec les centrales de mesures et les onduleurs. Ces modules de communication MODBUS permettent un échange de données en temps réel avec les automates, garantissant ainsi la réactivité du système. Tous les équipements sont connectés en série, au même réseau de communication MODBUS.

▪ Stations de périphérie décentralisées ET 200M

Il s'agit de stations modulaires esclaves sur le réseau Profibus. Elles peuvent accueillir 8 modules d'E/S ainsi que des processeurs de communication. En utilisant des modules de bus actifs, il est possible de remplacer ou d'ajouter des modules en fonctionnement. Les cartes d'entrées-sorties installées dans les modules ET 200M peuvent comporter de 8 à 32 voies TOR, et de 2 à 8 voies analogiques. La solution de connexion retenue est le système avec bornes à vis. Pour raccorder les modules ET 200M au Profibus, on dispose de coupleurs IM153 en tant qu'esclaves et de convertisseur FO/Cu OLM G12.

▪ Entrées/sorties déportées

Les équipements d'automatismes distribués assurent l'acquisition des données provenant des dispositifs situés le long de l'ouvrage et à ses abords. Ces automatismes s'appuient sur des stations ET200M, équipées d'une paire de modules de communication redondants pour garantir leur fiabilité. Les E/S déportées sont regroupés dans ces racks Simatic ET200M. Ces racks sont composés de :

- Têtes de Communication : Simatic IM153-2HF
- Modules 32 entrées TOR : Simatic SM321
- Modules 32 sorties TOR : Simatic SM322
- Modules 24 entrées TOR SIL : Simatic SM326
- Modules 10 sorties TOR SIL : Simatic SM326
- Modules 8 entrées ANA : Simatic SM321
- Modules de communication liaison série : Simatic CP341

▪ Focus sur les modules SIL2

Ces modules sont intégrés aux racks ET200M et utilisent le même canal de communication que les cartes standard (Protocole Profibus/Profisafe). En cas de défaillance d'une CPU, d'un IM 153-2 ou d'une ligne PROFIBUS, l'automate reste disponible. Par contre, en cas de défaillance de modules E/S de sécurité ou de l'ET200M, le périphérique n'est plus disponible, et les modules d'E/S de sécurité sont passivés.

Les équipements pilotés par des modules SIL2 et cas d'utilisation dans l'architecture existante sont :

- 6 feux à éclat situés aux entrées des sas : sur-signalétique variable pour les sas de Bois de Peu ;
- Barrières, feux R2 associés aux barrières et feux R24 : dispositifs de fermeture tunnel
- 2 ventilateurs de surpression avec registres et 2 clapets de décharge : surpression des sas
- Capteurs d'ouverture de porte des inter-tubes : détection de présence

En phase de conception, a été confirmé l'absence de besoin de maintenir ce niveau de sécurité SIL2 sur l'installation. L'existence de ces modules est donnée à titre indicatif.

II.1.3. Annexes

- API_TAB.xlsx
- systeme_automatisme.pdf

II.2. SCADA

II.2.1. Solution existante SCADA

ControlMaestro est la solution SCADA qui a succédé à Wizcon SCADA proposée par Elutions, dont dispose le CISGT Vauban. Elle permet aux opérateurs de visualiser l'ensemble des informations issues des ouvrages, d'interagir avec les systèmes et de garantir l'exploitation en mode nominal ou dégradé en cas d'indisponibilité du SAGT

Le CISGT dispose de plusieurs licences de ControlMaestro :

- 1 clé Runtime 10000 variables version 2008 (logiciel de supervision : RT10000)
- 3 clés Runtime 100 variables (logiciel de supervision : RT100)

Le frontal de supervision est équipé d'une carte de communication Ethernet Siemens. ControlMaestro dispose lui d'un driver « client OPC » qui envoie des requêtes vers le serveur OPC de la carte en fonction des besoins de rafraîchissement des écrans, des alarmes ou des courbes.

II.2.2. L'architecture existante SCADA

L'architecture se compose d'un poste serveur, 2 postes clients fixes et un poste client situé sur un portable de maintenance, actuellement inutilisé et entreposé dans les locaux du SeSyR.

L'OS du serveur est Microsoft Windows Server 2003 R2. La communication avec la supervision s'effectue en protocole OPC, tandis que le système REDCONNECT de Siemens gère automatiquement la redondance des automates et les basculements nécessaires. Un déport écran/clavier/souris (KVM) est intégré pour permettre le pilotage de l'application via un écran au format 16/10.

La solution SCADA tourne :

- Pour la **licence 10 000 variables** du CISGT Vauban : sur un serveur dédié HP ProLiant DL360 installé au LT BdP.
- Pour les 3 **licences 100 variables** : 2 sur des PC encastrables IPO TECHNOLOGIES dans les LT et 1 sur PC maintenance Panasonic

II.2.3. Annexes

- GT_601_C_DSG_SAGT.pdf
- GT_602_B_DA_SAGT.pdf
- GT_604_A_DSD_Communication_SAGT.pdf
- Table_echanges_SAGT.xlsx

II.3. Architecture réseaux et réseau fibre optique

II.3.1. Architecture existante

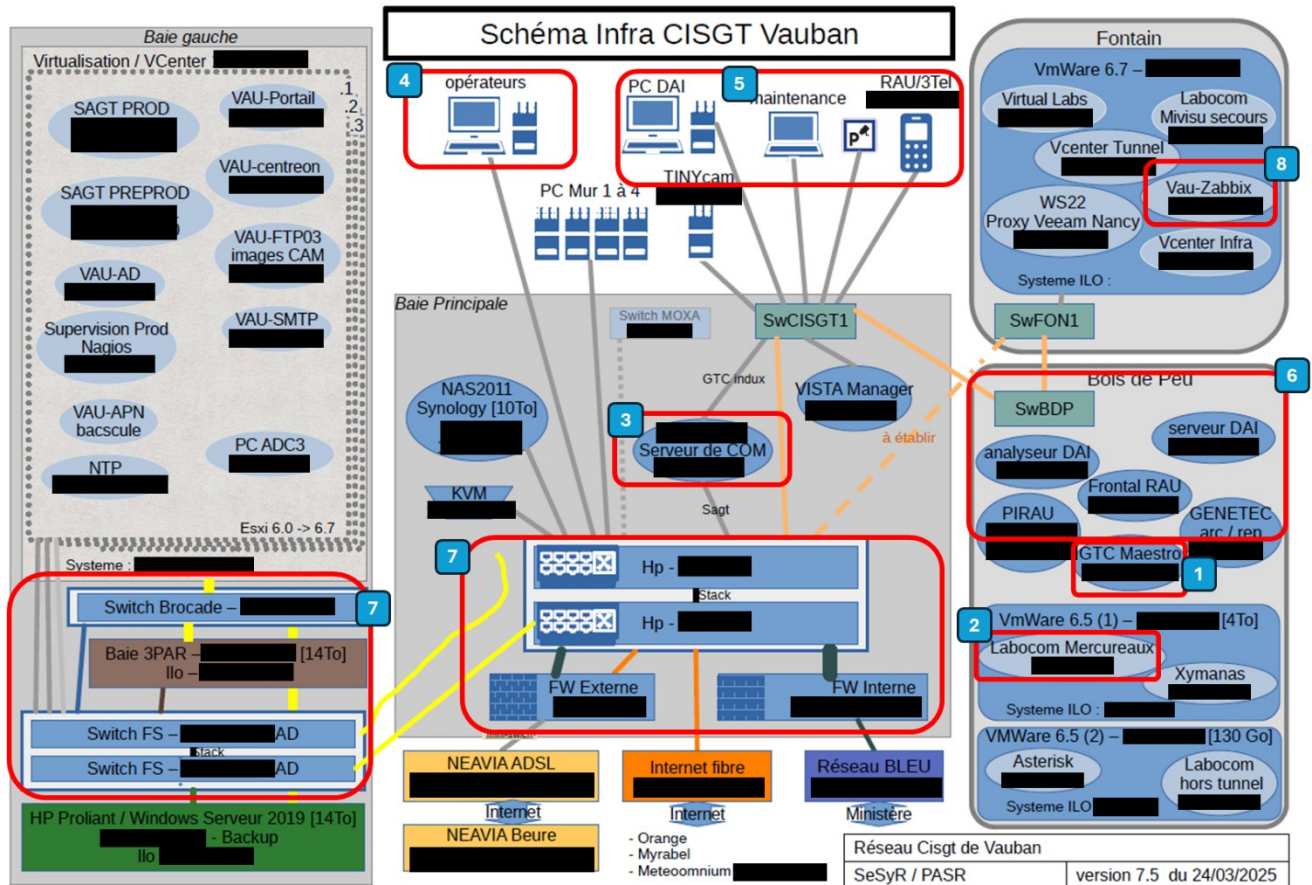


Figure 3 : schéma de l'infrastructure numérique du réseau CISGT Vauban

Les numéros évoqués sur ce schéma sont ceux mentionnés en livret 1 de ce CCTP.

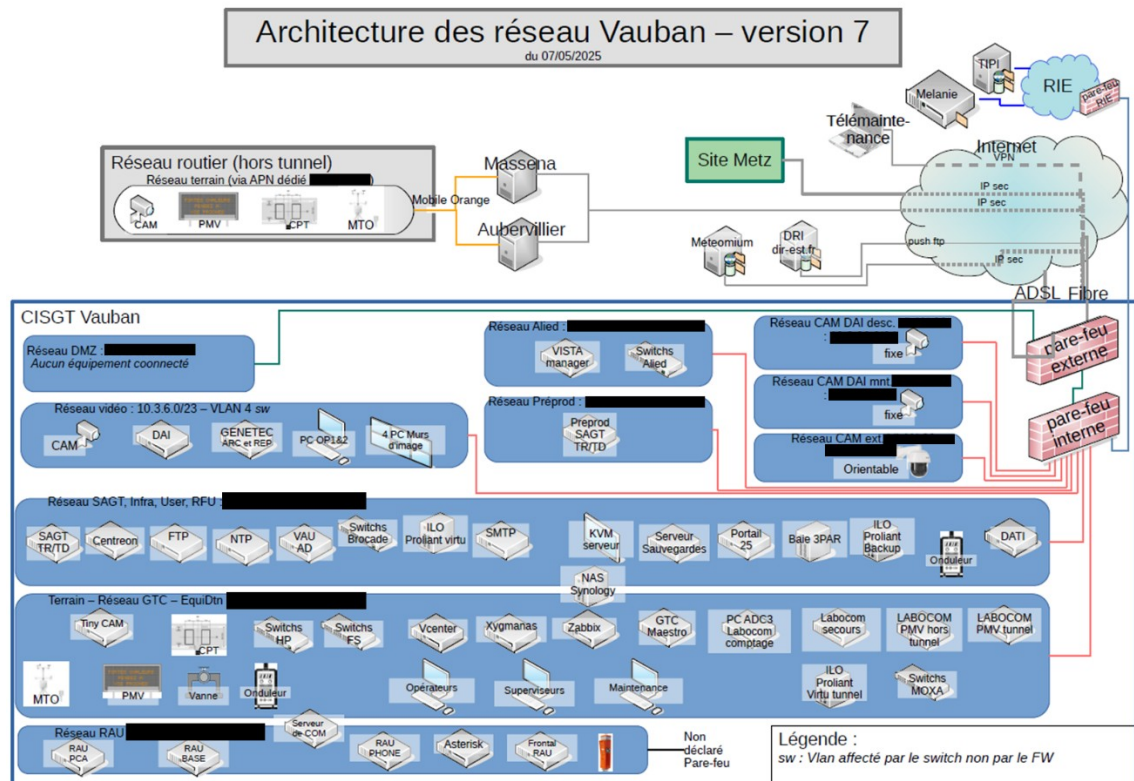


Figure 4 : architecture des réseaux Vauban

Le PASR, service dédié à l'administration des systèmes et réseaux de la DIR Est, s'appuie sur deux clusters de pare-feu "actif/passif" internes et externes (assurant la haute disponibilité). Les pare-feu actuels sont satisfaisants ; il n'y a pas de volonté de remplacer ces équipements. Même constat est fait pour le matériel réseau.

Des clients vulnérables sont néanmoins présents dans les tunnels (IHM locales dans les locaux techniques) et donc exposés à des acteurs malveillants motivés (intrusion physique dans les locaux techniques). Les IHMs locales sous XP (« Panel PCs ») peuvent être utilisées en connexion locale (moyen de secours) mais l'utilisation nominale est d'accéder aux données centralisées (SCADA au CISGT) ce qui présente un risque de cybersécurité plus ou moins élevé selon les règles activées dans les pare-feux.

La redondance des accès extérieurs n'est pas assurée par la fonctionnalité SD WAN. La redondance des pare-feux assure les liaisons externes.

Il existe un cloisonnement des flux de données (VLANs) :

- VLAN vidéo/cam extérieures Mercureaux
- VLAN DAI montantes
- VLAN DAI descendantes
- VLAN switches
- VLAN RAU
- VLAN équipements dynamiques
- VLAN GTC

Les accès distants pour la maintenance sont gérés via un client OpenVPN ou StormShield connecté au pare-feu externe. L'authentification s'appuie sur des comptes AD, où les groupes déterminent les ressources accessibles. Le réseau SAGT dispose d'une VM AD qui réplique l'AD de Myrabal hébergé sur le site du même nom, soit à Moulins-lès-Metz. La connexion VPN utilise le protocole SSL.

L'ensemble des commutateurs réseaux constituant le réseau des tunnels est de marque Allied Telesys et les 3 modèles disposent tous de toutes les capacités nécessaires à la mise en œuvre de mesures de sécurité telles que figurant dans les exigences réglementaires, notamment :

- Emission de logs d'événements au format syslog
- Capacité de gestion de VLAN, filtrages
- Capacité de contrôle d'accès (contrôle des équipements autorisés à se connecter)
- Capacité d'audit / surveillance (« port mirroring »)

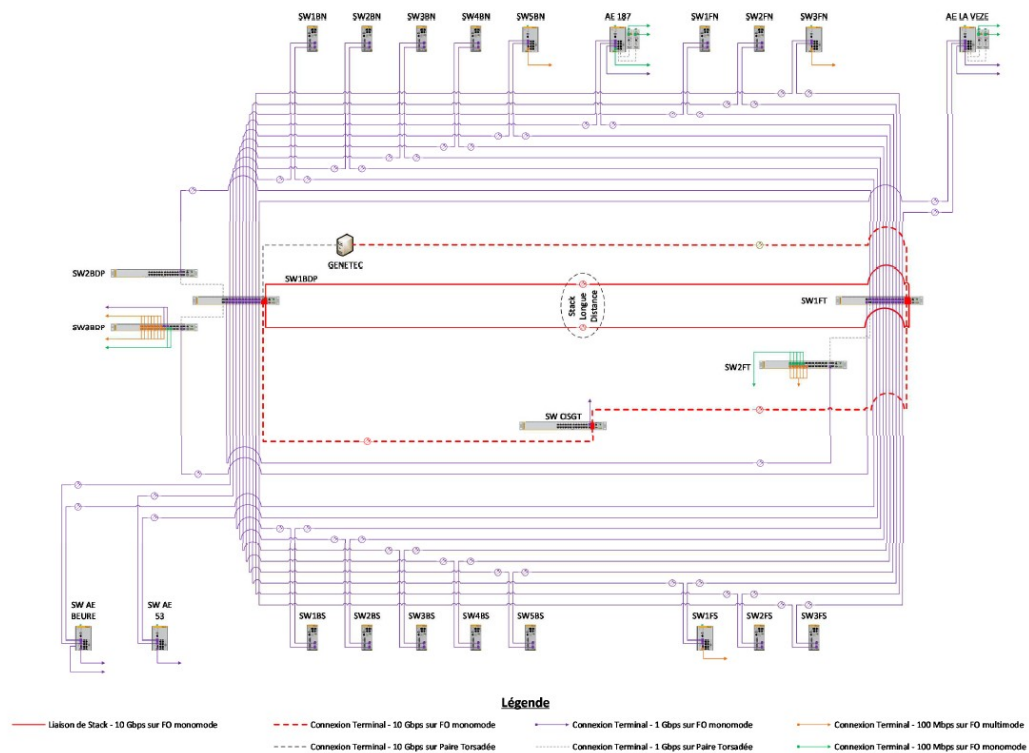


Figure 5 : Architecture réseau du CISGT

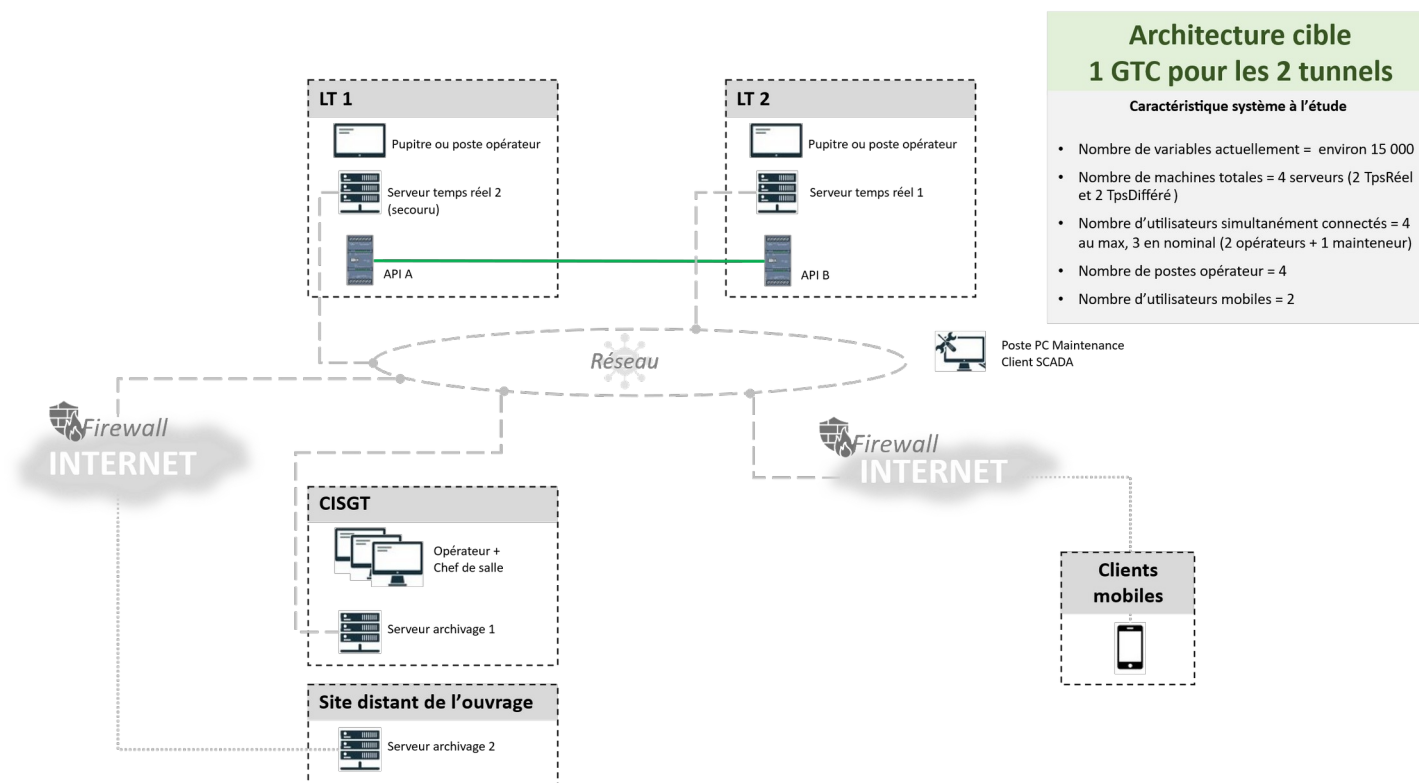
À Vauban, les accès extérieurs se font via VPN SSL via les pare-feux externes, mais sans limitation de temps.

La DIR Est réfléchi à améliorer cette gestion des droits des accès extérieurs pour les contrôler via une procédure simple avec une limitation du temps de connexion (VPN) à 4h avec accès autorisés via pare-feu comme cela est le cas pour les accès extérieurs vers le réseau du CISGT Myrabel.

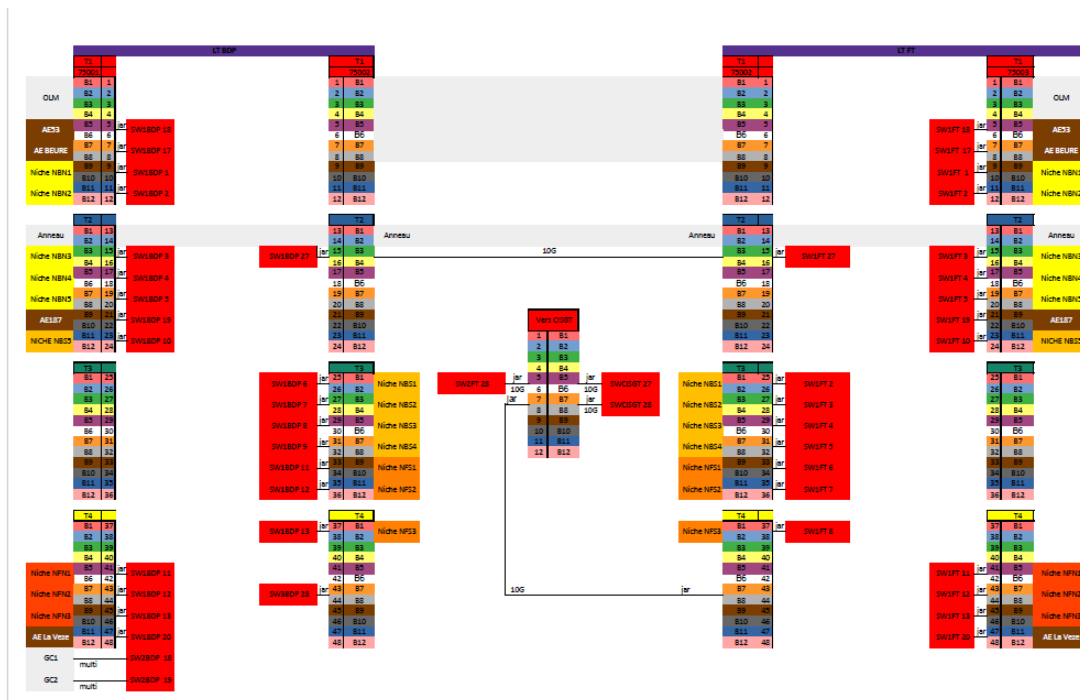
Aucun contrôle d'activité / surveillance n'est en place ni d'exigence concernant le poste utilisé pour accéder aux ressources DIR Est une fois l'accès distant établi.

II.3.2. Architecture ciblée

Ci-dessous est une illustration de l'architecture ciblée transmise en phase de conception à plusieurs fournisseurs pour illustrer le besoin de la DIR Est :



II.3.3. Réseau FO



II.3.4. Annexes

Architecture :

- Architecture_cible.pdf

Réseau FO :

- Anneau_FO_Réseau.pdf
- Tableau_cablage_FO.pdf
- Architectures_Réseaux.pdf
- Baie_reseau_FO_BDP.pdf
- Baie_automate_Réseau_FO_Fontain
- Coffret_AE_BEURE.pdf
- Coffret_NBN1.pdf
- Coffret_NBN2.pdf
- Coffret_NFN1.pdf
- Coffret_NFN2.pdf
- Synoptique_reseau_FO_video.pdf