



## DIR Est – Tunnels de la Voie des Mercureaux

### Renouvellement de la Gestion Technique Centralisée Spécifications techniques et architectures

CCTP – Livret 3

Juillet 2025

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



## SUIVI DES MODIFICATIONS

C	31/07/2025	Reprise suite retour service admin DIR	P. Peyret	C. Lemée	C. Lemée
B	24/06/2025	Reprises relectures CETU et DIR Est	P. Peyret Y. Gayet	C. Lemée	C. Lemée
A	05/05/2025	Version initiale	P. Peyret Y. Gayet	P. Peyret	C. Lemée
Version	Date	Modifications	Rédaction	Vérification	Approbation

## SOMMAIRE

<b>SUIVI DES MODIFICATIONS.....</b>	<b>1</b>
<b>SOMMAIRE.....</b>	<b>2</b>
<b>GLOSSAIRE ET TABLE DES ILLUSTRATIONS.....</b>	<b>4</b>
GLOSSAIRE.....	4
TABLES DES ILLUSTRATIONS.....	6
<b>I. OBJET DU DOCUMENT.....</b>	<b>7</b>
<b>II. SPÉCIFICATIONS GÉNÉRALES.....</b>	<b>8</b>
II.1. GÉNÉRALITÉS.....	8
II.2. CONTRAINTES ENVIRONNEMENTALES - INFLUENCES EXTERNES.....	8
II.3. RÉEMPLOI D'ÉQUIPEMENTS.....	11
II.4. FABRICATION.....	11
II.5. SÉCURITÉ – VERROUILLAGE.....	11
II.6. APTITUDE À LA MAINTENANCE.....	12
II.7. TRANSPORT – MANUTENTION – STOCKAGE.....	13
<b>III. SPÉCIFICATIONS TECHNIQUES.....</b>	<b>14</b>
III.1. GTC – SUPERVISION.....	14
III.2. MATÉRIELS RÉSEAUX.....	26
III.3. RÉSEAU ÉLECTRIQUE.....	30
III.4. REPÉRAGE.....	35
<b>IV. ARCHITECTURES.....</b>	<b>36</b>
IV.1. PRÉCONISATIONS GLOBALES.....	36
IV.2. ARCHITECTURE EXISTANTE.....	36
IV.3. ARCHITECTURE CIBLÉE.....	36
IV.4. CONSTITUTION ET HÉBERGEMENT DE PLATEFORMES.....	38
<b>V. INFRASTRUCTURE SYSTÈMES – VIRTUALISATION.....</b>	<b>42</b>
V.1. IMPLANTATION DU SYSTÈME D'INFORMATION.....	43
V.2. SYSTÈME DE VIRTUALISATION.....	44
<b>VI. COMPOSANTS COMMUNS D'ADMINISTRATION.....</b>	<b>46</b>
VI.1. COLLECTEUR DE LOGS.....	46
VI.2. SAUVEGARDE.....	46
VI.3. ADMINISTRATION ET SUPERVISION D'INFRASTRUCTURE.....	47
VI.4. SYNCHRONISATION HORAIRE – SERVEUR NTP.....	47
VI.5. AUTHENTIFICATION DES UTILISATEURS.....	48
VI.6. ANTIVIRUS.....	48
VI.7. SÉCURISATION DES FLUX RÉSEAU.....	48
VI.8. PATCH MANAGEMENT.....	48

---

<b>VII. CYBERSÉCURITÉ.....</b>	<b>50</b>
VII.1. EXIGENCES RELATIVES À L'ORGANISATION, AUX PRATIQUES ET MOYENS DU TITULAIRE DU MARCHÉ.....	51
VII.2. EXIGENCES CONCERNANT LES MATÉRIELS ET LOGICIELS LIVRÉS OU CONFIGURÉS.....	54
VII.3. DOCUMENTS ET FICHIERS RELATIFS À LA CYBERSÉCURITÉ À FOURNIR PAR LE TITULAIRE.....	58
VII.4. CONTRÔLE DES FLUX – SEGMENTATION DU RÉSEAU.....	61
VII.5. EXIGENCES CYBERSÉCURITÉ.....	61

## GLOSSAIRE ET TABLE DES ILLUSTRATIONS

### GLOSSAIRE

ABREVIATION	DEFINITION
AD	Active Directory
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API	Automate Programmable Industriel
CAES	Coffret Autonome d'Énergie Secourue
Cam	Caméra
CCTP	Cahier des Clauses Techniques Particulières
CEM	Compatibilité Électromagnétique
CISGT	Centre d'Ingénierie, de Sécurité et de Gestion du Trafic
CPU	Central Processing Unit (Unité Centrale de Traitement)
CSSI	Correspondant Sécurité des Systèmes d'Information
DAI	Détection Automatique d'Incidents
DALI	Digital Addressable Lighting Interface
DIR	Direction Interdépartementale des Routes
DMZ	Demilitarized Zone (Zone Démilitarisée réseau)
E/S	Entrée/Sortie
FO	Fibre Optique
FRP	Fibre Reinforced Plastic
FTP	File Transfer Protocol
Gbps	Gigabits par seconde
Go	Gigaoctet
GPO	Group Policy Object
GTC	Gestion Technique Centralisée
HTTP	HyperText Transfer Protocol
HTTPS	HTTP Secure
IHM	Interface Homme-Machine
IK	Indice de protection contre les chocs mécaniques
IP	Internet Protocol / Indice de Protection (selon contexte)
LED	Light Emitting Diode
LTS	Long Term Support
MAC	Media Access Control
MAB	MAC Authentication Bypass
Mbps	Megabits par seconde
MESD	Module d'Entrées/Sorties Déportées
MHz	Mégahertz
MOA	Maîtrise d'Ouvrage
MOE	Maîtrise d'œuvre
MTBF	Mean Time Between Failures
NIS2	Network and Information Security Directive (version 2)
NTP	Network Time Protocol

<b>OPC UA</b>	OPC Unified Architecture
<b>OS</b>	Operating System
<b>PAS</b>	Plan d'Assurance Qualité
<b>PASR</b>	Pôle Administration Systèmes et Réseaux
<b>PBO</b>	Point de Branchement Optique
<b>PC</b>	Personal Computer
<b>PID</b>	Proportionnel, Intégral, Dérivé
<b>RAU</b>	Réseau d'Appel d'Urgence
<b>RAM</b>	Random Access Memory
<b>RSTP</b>	Rapid Spanning Tree Protocol
<b>RTU</b>	Remote Terminal Unit
<b>SFP</b>	small form-factor pluggable
<b>SI</b>	Système d'Information
<b>SITOP</b>	Marque d'alimentations industrielles Siemens
<b>SNMP</b>	Simple Network Management Protocol
<b>SSH</b>	Secure Shell
<b>SSL/TLS</b>	Secure Sockets Layer / Transport Layer Security
<b>SSD</b>	Solid State Drive
<b>STP</b>	Shielded Twisted Pair (câble réseau blindé)
<b>TA</b>	Télé Alarmes
<b>TC</b>	Télé Commandes
<b>TCP</b>	Transmission Control Protocol / Internet Protocol
<b>TCP/IP</b>	Transmission Control Protocol / Transport Layer Security
<b>TCP/TLTGTS</b>	Tableau Général Basse Tension
<b>TD</b>	Temps Différé
<b>TELNET</b>	Telecommunication Network
<b>TM</b>	Télé Mesures
<b>TMA</b>	Tierce Maintenance Applicative
<b>TOR</b>	Tout ou Rien
<b>TR</b>	Télé Réglages ou Temps Réel (selon contexte)
<b>TS</b>	Télé Signalisations
<b>UC</b>	Unité Centrale
<b>UDP</b>	User Datagram Protocol
<b>URL</b>	Uniform Resource Locator
<b>USB</b>	Universal Serial Bus
<b>VM</b>	Virtual Machine
<b>VLAN</b>	Virtual Local Area Network
<b>VPN</b>	Virtual Private Network



## TABLES DES ILLUSTRATIONS

### Table des figures

Figure 1 - Illustration d'une baie 19''.....	14
Figure 2 : Visuel commutateur N2.....	25
Figure 1 - Illustration d'une baie 19''.....	14
Figure 2 : Visuel commutateur N2.....	25

### Table des tableaux

Tableau 1 : Liste des influences extérieures (tirée de l'annexe A de la norme CEI 60364-5-51).....	9
Tableau 2 - Configuration minimale pour serveurs.....	21
Tableau 3 - Configuration minimale pour poste opérateur.....	22
Tableau 4 - Dimensionnement des licences.....	24
Tableau 5 : Exigences d'infrastructure de virtualisation DIR Est.....	44
Tableau 6 - Exigences ou recommandations cyber à prévoir pour la rénovation GTC du CISGT.....	61
Tableau 1 : Liste des influences extérieures (tirée de l'annexe A de la norme CEI 60364-5-51).....	9
Tableau 2 - Configuration minimale pour serveurs.....	21
Tableau 3 - Configuration minimale pour poste opérateur.....	22
Tableau 4 - Dimensionnement des licences.....	24
Tableau 5 - Exigences ou recommandations cyber à prévoir pour la rénovation GTC du CISGT.....	61

## I. OBJET DU DOCUMENT

Le présent document constitue le 3<sup>ème</sup> livret du Cahier des Clauses Techniques et Particulières (CCTP) du marché relatif à l'opération de rénovation de la GTC de la DIR Est.

Ce CCTP est constitué de cinq livrets :

- Livret 1 : Généralités
- Livret 2 : Programme fonctionnel et Performances
- **Livret 3 (présent livret) : Spécifications matérielles et Architectures**
  - Spécifications générales
  - Spécifications techniques
  - Architectures
  - Infrastructure systèmes – Virtualisation
  - Composants communs d'administration
  - Cybersécurité
- Livret 4 : Planning et Migrations
- Livret 5 : Documentation confidentielle technique



**Le Livret 5 – Documentation confidentielle rassemble les documents et plans dont la diffusion est restreinte et soumise à la signature d'un accord de confidentialité.  
Se référer au Règlement de Consultation pour l'obtention de ce Livret.**



## II. SPÉCIFICATIONS GÉNÉRALES

### II.1. GÉNÉRALITÉS

Les produits fournis, ainsi que leur mise en œuvre, sont conformes aux prescriptions et recommandations des normes et textes réglementaires français/européens.

En cas de contradiction entre différentes normes et réglementations, c'est le texte le plus restrictif qui sera appliqué.

Si, pour un matériel déterminé, il n'existe pas de réglementation particulière et/ou avis technique français, le Titulaire soumettra à validation au Maître d'Ouvrage, le matériel qu'il jugera approprié et répondant aux normes européennes et/ou internationales et lui remettra toutes justifications, éventuellement associées à leur traduction en langue française, permettant d'apprécier la bonne qualité de ce matériel (procès-verbaux d'essais, références, etc.).

Tout changement de nature ou d'origine d'un produit demeure expressément subordonné à l'accord préalable du Maître d'Ouvrage. Ce visa ne pourra pas avoir pour effet de dégager le Titulaire de ses responsabilités.

Les matériaux et fournitures devront être de première qualité. Ils seront soumis avant leur approvisionnement et leur emploi à l'examen du Maître d'Ouvrage. Ceux qui seront jugés comme ne représentant pas les qualités requises ou comme n'étant pas convenablement façonnés devront être immédiatement déposés, enlevés, remplacés ou refaits sans que le Titulaire puisse prétendre à la moindre indemnité.

Les matériaux, métaux, appareils qui ne rempliraient pas rigoureusement les conditions stipulées au Cahier des Clauses Techniques Particulières (CCTP) seront refusés. Ils seront déposés par le Titulaire à ses frais. Les équipements refusés pourront être enlevés par le Titulaire et stockés dans un dépôt de son choix, à ses frais.

### II.2. CONTRAINTES ENVIRONNEMENTALES - INFLUENCES EXTERNES

Les performances des équipements, les conditions d'installation et la conservation des matériels devront satisfaire aux conditions suivantes (la codification est celle des normes internationales ou européennes).

Le présent chapitre a pour unique objectif d'attirer l'attention quant au choix des matériels – les contraintes ci-après doivent dans tous les cas avoir été prise en compte au niveau des spécifications des équipements et/ou de la mise en œuvre.

La conception et les matériels mis en œuvre doivent garantir un fonctionnement sûr et durable.

Les conditions d'environnement suivantes sont définies selon la classification de la norme NF C15-100-1 : *Les matériels électriques doivent être choisis et mis en œuvre conformément aux prescriptions du tableau 51A qui donne les caractéristiques des matériels nécessaires selon les influences externes auxquelles ils peuvent être soumis.*

Le tableau ci-dessous récapitule les principales influences externes à prendre en compte dans l'élaboration du projet.

Tableau 1 : Liste des influences extérieures (tirée de l'annexe A de la norme CEI 60364-5-51)

Influences externes	Locaux Techniques en (PCS, PS, Usines de ventilation...)	Issues de secours, niches de sécurité escaliers de transfert	Tunnels	Equipements en extérieur
Température ambiante	AA5 <i>Chaude</i> +5+40°C	AA5 <i>Chaude</i> +5+40°C	AA7 <i>Tempérée</i> -25 +50°C	AA8 <i>Ext non protégé</i> -50+40°C
Conditions climatiques (température/humidité)	AB4 <i>Chaude</i> +5+40°C 5% 95%	AB4 <i>Chaude</i> +5+40°C 5% 95%	AB4 <i>Chaude</i> +5+40°C 5% 95%	AB8 <i>Ext non protégé</i> -50+40°C 15%100%
Altitude	AC1 <i>Basse</i> ≤ 2000m	AC1 <i>Basse</i> ≤ 2000m	AC1 <i>Basse</i> ≤ 2000m	AC1 <i>Basse</i> ≤ 2000m
Présence d'eau (1)	AD1 <i>négligeable</i>	AD1 <i>négligeable</i>	AD5 <i>Jet d'eau</i>	AD5 <i>Jet d'eau</i>
Présence de corps solides (2)	AE2 <i>Petits objets</i>	AE5 <i>Poussières</i> <i>moyennes</i>	AE5 <i>Poussières</i> <i>moyennes</i>	AE5 <i>Poussières</i> <i>moyennes</i>
Présence de substances corrosives ou polluantes (3)	AF1 <i>négligeable</i>	AF4 <i>exposition</i> <i>continue</i>	AF4 <i>exposition</i> <i>continue</i>	AF4 <i>exposition</i> <i>continue</i>
Contraintes mécaniques aux chocs	AG2 <i>Moyens</i> ≤ 2J	AG2 <i>Moyens</i> ≤ 2J	AG4 <i>Très importants</i> ≤ 20J	AG4 <i>Très importants</i> ≤ 20J
Vibrations (4)	AH1 <i>Faibles</i>	AH2 <i>Moyennes</i>	AH2 <i>Moyennes</i>	AH2 <i>Moyennes</i>
Présence de flore ou moisissures (5)	AK1 <i>négligeable</i>	AK1 <i>négligeable</i>	AK1 <i>négligeable</i>	AK2 <i>Risques</i>
Présence de faune (6)	AL2 <i>Risques</i>	AL2 <i>Risques</i>	AL2 <i>Risques</i>	AL2 <i>Risques</i>
Influences électromagnétiques- statiques, ionisantes (7)	AM3 / AM5	AM3 / AM5	AM3 / AM5	AM3 / AM5
Rayonnements solaires	AN1 <i>Faibles</i>	AN1 <i>Faibles</i>	AN1 <i>Faibles</i>	AN3 <i>Significatifs</i>
Foudre	AQ2 <i>Indirecte</i>	AQ2 <i>Indirecte</i>	AQ2 <i>Indirecte</i>	AQ3 <i>Directe</i>
Mouvements de l'air / Vent (9)	AR1/ AS1 <i>Faibles</i>	AR1/ AS1 <i>Faibles</i>	AR2/ AS2 <i>Moyens</i>	AR3/ AS3 <i>Fort</i>
Compétence des personnes (10)	BA4/ BA5 <i>Averties</i> <i>qualifiées</i>	BA4/ BA5 <i>Averties</i> <i>qualifiées</i>	BA4/ BA5 <i>Averties</i> <i>qualifiées</i>	BA4/ BA5 <i>Averties</i> <i>qualifiées</i>

Influences externes	Locaux Techniques en (PCS, PS, Usines de ventilation...)	Issues de secours, niches de sécurité escaliers de transfert	Tunnels	Équipements en extérieur
Résistance électrique du corps humain (11)	BB1 <i>Normale</i>	BB1 <i>Normale</i>	BB2 <i>Normale</i>	BB2 <i>Faible</i>
Contacts de personnes avec le potentiel de terre	BC3 <i>Fréquents</i>	BC3 <i>Fréquents</i>	BC3 <i>Fréquents</i>	BC3 <i>Fréquents</i>
Evacuation des personnes en cas d'urgence	BD2 <i>Difficiles</i>	BD2 <i>Difficiles</i>	BD2 <i>Difficiles</i>	BD2 <i>Difficiles</i>
Nature des matières traitées ou entreposées	BE1 <i>Risques négligeable</i>	BE1 <i>Risques négligeable</i>	BE1 <i>Risques négligeable</i>	BE1 <i>Risques négligeable</i>
Matériaux de construction	CA1 <i>Non combustibles</i>	CA1 <i>Non combustibles</i>	CA1 <i>Non combustibles</i>	CA1 <i>Non combustibles</i>
Structure des bâtiments	CB1 <i>Risques négligeable</i>	CB2 <i>Propagation d'incendie</i>	CB2 <i>Propagation d'incendie</i>	CB1 <i>Risques négligeable</i>

(1) En tunnels, campagne de nettoyage par nettoyeur des piédroits et équipements par nettoyeur haute pression

(2) En tunnels, présence de suies (échappement) qui peut être présent en IS, NS et escaliers de Transfert

(3) En tunnels, sels de déneigement, gaz d'échappement, humidité pouvant être présent en IS, NS et Escaliers de transfert

(4) En tunnels, passage continu des véhicules provoquant des vibrations

(5) En extérieur, présence de pollen et végétation

(6) Présence de rongeurs

(7) Étendue des installations

(9) Courant d'air longitudinal selon scénario de ventilation / désenfumage

(10) Sauf en cas d'incendie, l'ensemble des locaux est réservé à un personnel averti ou qualifié

(11) BB2 en extérieur et en tunnel lors d'un lavage par exemple

L'ambiance extrêmement agressive, due aux gaz d'échappement des véhicules, qui règne dans les tunnels routiers nécessite la prise de certaines précautions dans le choix du matériel.

Au regard du tableau « choix et mise en œuvre des matériels en fonction de influences externes », tous les équipements du projet qui seront susceptibles d'être exposé à l'ambiance atmosphérique des voies circulées du tunnel devront faire l'objet d'une protection anticorrosion spécifique suivant leurs fonctions et leurs implantations.

Le Titulaire devra préciser pour chaque équipement concerné, le système anticorrosion retenu. En particulier, les procès-verbaux des essais au brouillard salin pour les durées d'exposition suivantes seront joints aux spécifications techniques d'achat.

Les valeurs indiquées dans le tableau sont données à titre indicatif. Il appartient au Titulaire de vérifier et d'ajuster les classifications (AA, AB, AF, etc.) aux conditions environnementales effectivement observées dans les tunnels, en s'appuyant sur des retours d'expérience récents et sur les recommandations des normes NF C 15-100-1 et IEC 60364-5-51. Une attention particulière devra être portée à l'exposition aux sels de déneigement, à la condensation et aux gaz corrosifs, afin de garantir un niveau de protection et de durabilité cohérent avec les contraintes en tunnel.

## II.3. RÉEMPLOI D'ÉQUIPEMENTS

Le réemploi d'équipements est interdit sauf pour ceux spécifiés au présent CCTP et appartenant au Maître d'Ouvrage. La responsabilité quant à la provenance et aux caractéristiques techniques des équipements réemployés incombe alors au Maître d'Ouvrage. Dans ce cas, il appartient au Titulaire de vérifier la compatibilité de ces équipements réemployés avec le reste des installations réalisées, et en cas de doute, de proposer des équipements neufs. Le Titulaire demeure néanmoins responsable des prestations prévues éventuellement au CCTP.

## II.4. FABRICATION

Le Titulaire devra garantir la qualité, la robustesse et l'homogénéité des équipements fournis dans le cadre du présent marché. Les matériels devront être neufs, de gamme professionnelle, issus de fabricants disposant d'un système qualité certifié ISO 9001. Tous les équipements d'une même nature (automates, MESD, serveurs, postes opérateurs, etc.) devront provenir du même fabricant ou d'une même gamme certifiée, sauf exception dûment justifiée. Les équipements devront être conformes à la réglementation CE, marquage visible et traçable.

Le Titulaire devra fournir pour chaque type de matériel :

- Une fiche technique constructeur (avec référence produit),
- Une attestation de conformité,
- Une preuve de pérennité de la gamme,
- Les boîtiers, coffrets, borniers et armoires devront respecter au minimum :
  - Indice de protection IP  $\geq$  IP54,
  - Indice IK  $\geq$  IK08 pour les armoires intérieures, IK10 pour les extérieures.

Le Titulaire indiquera la durée de vie attendue (en années ou en heures de fonctionnement) pour chaque équipement critique, et proposera un calendrier indicatif de remplacement préventif.

Le Titulaire devra garantir l'homogénéité des matériels fournis pour chaque catégorie fonctionnelle. Cela implique que tous les équipements de même type (automates, MESD, serveurs, postes opérateurs, etc.) doivent provenir d'un même fabricant ou d'une même gamme référencée, afin d'assurer la compatibilité logicielle, matérielle et de maintenance à long terme.

Toute exception à cette règle devra être préalablement justifiée et validée par la Maîtrise d'Ouvrage.

## II.5. SÉCURITÉ – VERROUILLAGE

Le Titulaire devra mettre en œuvre des dispositifs de sécurité physique et logique visant à prévenir toute utilisation non autorisée, tout accès inopiné ou toute manipulation risquant de perturber l'exploitation ou de compromettre l'intégrité du système. Chaque point de verrouillage fera l'objet d'une fiche d'inventaire (type de serrure, code clé, nombre de clés fournies).

Le Titulaire devra fournir :

- 2 jeux de clés complets par armoire ou baie livrée,
- Un plan de distribution des accès (DIR Est, mainteneur, etc.).

Toutes les interfaces d'accès (ports USB, ports de configuration, ports console) devront être désactivables par l'administrateur ou protégées par capuchon de sécurité plombable.

Sur les automates, postes et serveurs :

- Le BIOS/UEFI devra être verrouillé par mot de passe,
- Le démarrage sur supports externes devra être désactivé,
- Les ports inutilisés (USB, Wi-Fi, Bluetooth) devront être désactivés par défaut.

Les installations seront conçues et réalisées de façon à assurer la plus grande sécurité possible tant au personnel qu'au matériel et à permettre d'effectuer sans danger les visites et l'entretien des matériels.

## II.6. APTITUDE À LA MAINTENANCE

Le système dans son ensemble devra être conçu pour permettre une maintenance préventive et corrective aisée, rapide et traçable, sans interruption excessive de service. Les équipements devront permettre le remplacement de tout composant critique en moins de 30 minutes.

Tous les équipements (automates, cartes, disques, alimentations, batteries) devront être :

- Accessibles sans démontage complet,
- Identifiés par une sérigraphie ou étiquette persistante (référence, numéro de série),
- Remplaçables individuellement, sans dépendance à une configuration propriétaire.

Le Titulaire devra fournir :

- Une notice de maintenance par équipement,
- Un dossier de maintenance global incluant : plan de remplacement préventif, conditions de test, procédures de vérification post-remplacement.

Tous les réglages de configuration devront être :

- Traçables (fichiers de configuration exportables),
- Réversibles (possibilité de revenir à une configuration validée),
- Compatibles avec une restauration automatisée (image disque, export SCADA, etc.).

Une checklist de maintenance devra être remise, listant les contrôles périodiques à réaliser avec fréquence et seuils d'alerte. Le matériel et son installation devront être conçus pour permettre un entretien aisé et efficace. Le Titulaire devra répondre, pour chaque composant, aux exigences suivantes :

- Accessibilité commodité ;
- Modularité et interchangeabilité des éléments ;
- Possibilité de consignation ;
- Possibilité de manutention ;
- Utilisation d'outillage normalisé et approprié ;
- Facilité de câblage, de réglage.

Toutes les pièces soumises à usure seront interchangeables.

Le Titulaire doit indiquer et prévoir dans sa fourniture l'outillage spécial nécessaire et les différents niveaux d'intervention des opérations de maintenance appliquées aux systèmes proposés.

## II.7. TRANSPORT – MANUTENTION – STOCKAGE

Les approvisionnements sont à exécuter en temps utile et avec les plus grandes précautions, pour que le matériel posé soit et reste intact, en parfait état de conservation et de fonctionnement.

Les matériels seront livrés sous un emballage devant assurer une protection suffisante du matériel contre toutes les détériorations.

Les matériels seront réceptionnés à leur arrivée sur le chantier et avant leur montage par le Titulaire selon les modalités définies dans le Plan d'Assurance Qualité. Ces matériels resteront sous la responsabilité du Titulaire jusqu'à la réception du marché. Toute pièce reconnue défectueuse, détériorée ou volée jusqu'à cette date sera remplacée aux frais du Titulaire, dans les délais impartis par le Maître d'Œuvre. Le stockage provisoire et le gardiennage est à la charge du Titulaire durant cette phase d'exécution des travaux.

Aucun délai supplémentaire d'exécution des travaux ne sera accordé au Titulaire pour permettre le réapprovisionnement des matériels détruits ou volés.

Le Titulaire ne pourra présenter aucune réclamation ou frais supplémentaires, au titre des conditions d'accès aux différents lieux de stockage et à la réglementation des voies les desservant.

### III. SPÉCIFICATIONS TECHNIQUES



Outre les spécifications définies au présent chapitre, les matériels et logiciels fournis doivent respecter les exigences établies au §VII.

#### III.1. GTC – SUPERVISION

##### III.1.1. Baies (GTC, réseaux)

###### III.1.1.1. Principales caractéristiques

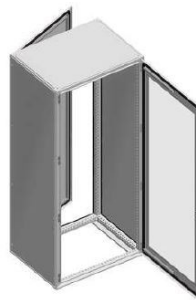


Figure 1 - Illustration d'une baie 19''

La baie 19" présente les principales caractéristiques suivantes :

- Enveloppe
  - Enveloppe en tôle d'acier pliée et soudée
  - Ossature : cadres inférieur et supérieur et montants verticaux assemblés mécaniquement par vis.
  - Toit en tôle d'acier peint.
  - Panneaux latéraux en tôle d'acier peint à fixation extérieure par vis imperdable.
- La baie sera constituée de panneaux qui auront les dimensions unitaires suivantes :
  - Hauteur : 2 000 mm ;
  - Largeur : 800 mm ;
  - Profondeur : 600 à 1000 mm (y compris poignée) ;
  - Socle : 100 mm ;
- Ouvertures
  - Porte avant en tôle d'acier peinte avec vitre collée en verre Securit.
  - Porte arrière pleine en tôle d'acier peinte.
  - Portes équipées de poignées, insert double-barre 5mm et serrures à clé en faces avant et arrière de chaque châssis.
  - Portes auront un débattement supérieur à 120° avec arrêtoir.
  - Serrure de sûreté à clé dont la marque et le numéro seront soumis à l'approbation de l'exploitant.
- Autres
  - Degré de protection : IP55 suivant norme IEC60529
  - Tenue aux impacts mécaniques externes : IK08 suivant norme IEC62262
  - Conforme à la directive RoHS, châssis 19'' suivant la norme IEC60297-1-4



- Peinture : poudre polyester-époxy
- La baie sera équipée de tous accessoires nécessaires à l'installation de la baie dans les règles de l'art : socle support, anneaux de manutention, goulotte, longerons techniques, colliers, plastrons, barre de blindage, tresse d'équipotentialité, ...
- Toutes les parties métalliques de la baie et des équipements qu'elle contient seront mises à la terre.

**L'implantation des équipements en baie sera validée par les équipes de maintenance de la DIR Est.**

### III.1.1.2. Éléments internes

- Alimentation(s)
  - Dans les baies, l'alimentation électrique sera double, réalisée en 230V monophasé, depuis un départ du TGBT Normal et un départ du TGBT Ondulé.
- Châssis 19''
  - Les équipements internes installés dans la baie seront montés sur un châssis 19'' fixe et solidaire de la baie supportant une charge statique de 400kg. Des rails de fixation devront être positionnés à l'intérieur de l'armoire facilitant ainsi le passage des câbles et la finition (linéarité des câbles).
- Ventilation mécanique
  - La baie dispose d'une ventilation mécanique forcée.
  - La mise en dépression des armoires sera préférée de façon à balayer plus facilement les matériels à refroidir : le ventilateur sera positionné en partie haute de l'armoire et les prises d'air en partie basse.
  - Les prises d'air devront être munies de cartouches filtrantes anti-poussière.
  - La ventilation permettra de maintenir une température inférieure à 35° C à l'intérieur de la baie pour une température ambiante dans le local de 30° C.
  - La ventilation sera commandée par un thermostat interne à la baie.
  - La ventilation sera arrêtée lors de l'ouverture des portes.
- Accessoires pour la maintenance
  - Les schémas de câblage de la baie seront disposés dans une pochette plastique fixée à l'intérieur du battant de porte.
  - Une tablette amovible sera fixée à l'intérieur du battant de porte afin de supporter l'ordinateur portable de maintenance (ou une tablette roulante, si le local est suffisamment grand).

### III.1.1.3. Implantation et fixation

Les baies seront posées au sol, soit sur réhausse métallique, soit sur une chaise (cas des faux-planchers) accessible par les faces avant et arrière, implantée dans les locaux techniques dans les ouvrages et aux locaux informatiques du CISGT.

Les câbles pénétreront par le dessous ou par le dessus, au travers d'un balai passe câble ou via un chemin de câble à prévoir.

### III.1.1.4. Réserves

Une baie dispose d'une réserve libre d'équipements et des servitudes de 30 % minimum.

### III.1.2. Automate Programmable Industriel (API)

L'architecture système est constituée de deux automates redondants qui devront être positionnés dans 2 baies séparées et constitués :

- Des modules d'alimentations redondantes des composants actifs,
- Un module processeur (CPU) ayant des capacités suffisantes au développement des nouvelles applications en termes d'E/S, de puissance CPU et de mémoire de programmes (réserve adaptée aux exigences du marché) ;
- Des fonctions de surveillance des applications et des matériels (chien de garde, voyant de défaut permettant un diagnostic rapide) assurant le contrôle du bon fonctionnement des automates et de leur redondance à chaud en cas de défaut,
- Des commutateurs externes de communication avec les unités d'entrées sorties déportés, avec une typologie en étoile avec double attachement sur fibres optiques et de protocole Ethernet/TCP-IP, Modbus/TCP-IP ou Profinet,
- Plusieurs modules de communication adaptés à la définition de la nouvelle architecture et à chacun des automates) et permettant de dissocier les communications avec les différents équipements et niveaux de l'architecture (Ethernet, Profinet, OPC UA, etc...).
- Des commutateurs externes de communication avec le système de supervision et autres équipements de la baie,
- Des modules de liaison avec les commutateurs,
- De modules de communication avec le bus interne à la baie,
- Une fonction de redondance duale à chaud native (Applicatif de redondance intégrée aux CPU ou aux matériels composants les anneaux de communication) – dont les performances sont décrites dans le Livret 2,
- D'éventuels modules de synchronisation.

L'automate disposera des équipements suivants :

- 1 rack fond de panier accueillant les différents éléments,
- 1 module de traitement CPU dont les performances seront dimensionnées pour le réseau de terrain supervisé. Ce module pourra :
  - Acquérir les informations en provenance des unités d'entrées / sorties déportés sur le terrain (TOR, analogiques et numériques, cartes contrôleurs DALI).
  - Traiter ces informations dans le cadre du fonctionnement spécifique de chaque installation,
- La CPU permettra de réaliser les fonctions :
  - Contrôle logique des équipements,
  - Fonctionnement séquentiel (démarrage/arrêt),
  - Régulations PID et asservissement des boucles,
  - Communication vers le réseau terrain métier dédié,
  - Transmission des états, alarmes détaillées ou de synthèse et le relayage des commandes avec les systèmes local et déportés de supervision,
- Une ou plusieurs liaisons Bus de terrain, intégrée à la CPU ou en rack CPU. La connectique utilisée permettra la connexion locale d'une console de programmation,
- Une interface de communication Ethernet TCP/IP pour la liaison au **réseau de fédération**,
- Une liaison de communication pour le raccordement au réseau de terrain E/S déportées,
- Modules de communication et d'acquisition analogiques ou tout ou rien des cartes d'entrées- sorties déportées,
- 2 modules d'alimentation présentant les caractéristiques suivantes :

- Tension nominale d'entrée 230V, fréquence 50Hz,
  - Tensions nominales de sortie 5Vcc et 24Vcc,
  - Puissance dimensionnée pour la consommation de l'unité,
  - Isolation galvanique entre primaire et secondaire,
  - Protection du primaire par fusibles,
  - Protection du secondaire contre les surcharges, les courts-circuits et les surtensions,
  - Limitation du courant d'appel,
  - Bornier à vis pour la liaison du boîtier au réseau d'alimentation,
  - Respect des normes relatives aux compatibilités électromagnétiques et à la pollution du réseau électrique,
- Degré de protection des éléments IP 20 minimum,
  - Borniers débrochables rendant le changement d'automate efficace et rapide afin que les opérations puissent reprendre rapidement en cas de défaillance,
  - Carte E/S de sécurité intrinsèque 24VCC,
  - MTBF supérieur à 100 000 heures,
  - Température de fonctionnement de 0 à 60°C,
  - Une carte de stockage des données,
  - 1 coupleur TCP/IP sur Ethernet pour la liaison au réseau de données de fédération,
  - Respect des normes relatives aux compatibilités électromagnétiques et à la pollution du réseau électrique,
  - Cartes E/S TOR et/ou analogiques.

Chaque carte d'interface doit comporter sur sa partie avant des LEDs indiquant l'état de la voie associée. De plus, chaque carte comporte un voyant d'état informant sur l'état de fonctionnement de la carte (autotests au moins jusqu'à la barrière d'isolement). Des détrompeurs mécaniques sur enfichage des modules permettant de faciliter le remplacement des modules.

Les API assureront le filtrage des entrées et permettront toutes les séquences de traitement. Ils posséderont leur propre horloge interne reliée à une horloge dite « mère », qui déterminera la base de temps, pour l'horodatage des événements.

L'API assurera le fonctionnement des automatismes au travers d'un langage de programmation simple et accessible à l'administrateur du système. La notion de programmation et de paramétrage recouvre :

- L'attribution des voies,
- La définition de traitement associé aux entrées-sorties,
- La définition des automatismes.

L'ensemble des programmes seront sauvegardés et téléchargés depuis le serveur de supervision.

En cas de défaillance, la reprise fonctionnelle s'effectuera automatiquement en assurant la continuité des fonctions et des états occupés avant la défaillance.

Lors de l'initialisation (ou après modification de certains paramètres), le programme API sera téléchargé (ou mis à jour) depuis le serveur de supervision.

L'accès aux paramètres de fonctionnement du système se fait localement via deux interfaces possibles :

- un terminal portable standard (PC) connecté localement à une application de surveillance de l'UC et des E/S déportées,
- et une IHM Web accessible à distance via un navigateur web.

Le choix de l'interface est laissé à l'appréciation de l'utilisateur. Cependant, l'utilisation d'une IHM Web est privilégiée pour sa facilité de maintenance, sa sécurité accrue, son accessibilité élargie et l'utilisation non soumise à l'achat d'une licence.

L'API sera équipé de dispositifs d'autodiagnostic permettant de signaler à la supervision l'absence ou la défaillance de l'un de ses composants :

- Absence carte,
- Défaut carte,
- Défaut d'alimentation,
- Défaut de communication,
- D'éventuels modules de synchronisation

Chaque ensemble est approvisionné avec l'ensemble du matériel externe nécessaire à sa mise en œuvre (pile de sauvegarde, connecteurs, carte mémoire, modules SFP, etc.). Pour chaque ouvrage, le titulaire doit prévoir un ensemble API en lot de rechange mis à disposition au niveau du local technique.

L'ensemble du matériel fournit dans ce marché devra se situer dans sa 1<sup>ère</sup> phase de vie, c'est-à-dire dans la période appelée « commercialisation active ». Le Titulaire remettra, avec la Spécification d'Achat Matériel de ces matériels, un engagement écrit du fournisseur garantissant à la DIR Est que les matériels auront une durée de commercialisation d'au moins 10 ans à compter de leur déploiement effectif (mise en service définitive).

Les API devront être alimentés par 2 sources différentes (normale, ondulée).

Une étude particulière devra être réalisée quant à l'emploi d'alimentations redondantes (type SITOP) dans les coffrets auxiliaires (CAES, armoires rd point, etc...). L'objectif étant d'assurer le maintien opérationnel des équipements les plus sensibles.

Le Titulaire devra présenter à l'agrément une gamme d'automates permettant de respecter les exigences de cybersécurité, identifiées au §III.2.

### III.1.3. Modules d'Entrée Sortie Déportées (MESD)

Les unités d'entrées/sorties déportées doivent être modulaires, extensibles, compatibles avec les API et les équipements de terrain, et répondre aux exigences de l'application en termes de nombre de voies, de types d'entrées/sorties et de communication. Elles permettent le regroupement local des informations de gestion technique centralisée des équipements situés dans leurs zones d'action respectives.

Les unités d'entrées sorties déportées sont constituées de modules montés sur rail DIN comprenant :

- Des modules de liaison avec les commutateurs du réseau de terrain,
- Des modules de distribution d'alimentation,
- Des modules d'entrées-sorties, tout ou rien, analogiques et les passerelles de communication avec les équipements disposant d'une intelligence embarquée,
- De plusieurs cartes d'entrées/sorties modulables dont le nombre sera défini en fonction des besoins des installations surveillées et majoré d'une réserve équipée de 30% :
  - Entrées Tout Ou Rien (TOR) de modularité 16, 32 ;
  - Sorties Tout Ou Rien (TOR) de modularité 16, 32 ;
  - Entrées analogiques équipées de module 4-20 mA, de modularité 4, 8 ;
  - ...

Ces unités pourront être simples ou multiples en cascade, avec modules d'extension de bus interne et câble de liaison, en cas de regroupement important de points comme au niveau du local technique.

Toutes les cartes devront être compatibles avec les équipements, capteurs existants ou à fournir.

Chaque carte d'E/S sera enfichée dans un rack qui lui permet de communiquer avec une unité centrale ou concentrateur par le bus intégré. Des modules paramétrables, voie par voie, en entrée ou en sortie pourront être mis en œuvre selon les capacités nécessaires. Le bornier possède des bornes sectionnables permettant le raccordement des câbles de l'installation en provenance des différents capteurs et actionneurs.

Le système sera modulaire et permet de retirer sous tension des cartes d'E/S sans perturber les autres modules. Les modules / racks et leurs borniers seront montés sur rails DIN dans les coffrets déportés. Ces modules seront pilotés au travers de l'API.

En résumé les caractéristiques :

- Coupleur de communication pour liaison vers réseau de terrain E/S déportées
- Classe de protection maximale pour la compatibilité électromagnétique CEM,
- Bornes sectionnables / débrochable à vis / ou équivalent,
- IP 20 minimum,
- 2 alimentations électriques présentant les caractéristiques suivantes :
  - Tension nominale d'entrée 230V, fréquence 50Hz
  - Tensions nominales de sortie 5Vcc et 24Vcc
  - Isolation galvanique entre primaire et secondaire
  - Protection du primaire par fusibles,
  - Protection du secondaire contre les surcharges, les courts-circuits et les surtensions,
  - Limitation du courant d'appel,
  - Bornier à vis pour la liaison du boîtier au réseau d'alimentation,
  - Respect des normes relatives aux compatibilités électromagnétiques et à la pollution du réseau électrique.
- Température de fonctionnement de 0 à 60°C,
- Prise de raccordement pour console de programmation,
- Cartes E/S TOR et/ou analogiques avec voyants indiquant l'état de chaque voie et de chaque carte.

Le Titulaire devra concevoir et configurer le système de manière à permettre l'intégration ultérieure de MESD supplémentaires, sans intervention lourde sur l'infrastructure existante.

À ce titre, il est exigé que :

- L'architecture logique et physique intègre une réserve minimale de 25 % sur la capacité totale du système en nombre de MESD raccordables, par rapport au périmètre initial du marché ;
- Les ports de communication terrain (RS-485, Ethernet, etc.) et les ports des automates ou switches soient dimensionnés avec cette réserve disponible à la mise en service ;
- Le plan d'adressage IP affecte des plages réservées (documentées) pour l'ajout ultérieur de MESD ;
- Les baies accueillant les MESD disposent de slots, rails et alimentation disponibles pour accueillir au moins 25 % de modules supplémentaires ;
- Le paramétrage des équipements de supervision, des automates et du SCADA prévoit des espaces de configuration libres (adresses, blocs de données, objets SCADA) permettant l'intégration de nouveaux modules sans recoder l'ensemble ;

- Une mise à jour des licences (si nécessaire) pour couvrir cette réserve soit explicitement documentée et budgétée.

Le Titulaire devra documenter précisément cette capacité de réserve dans son dossier de configuration initial, avec la cartographie physique et logique associée. Cette exigence fera l'objet d'une vérification en phase de recette.

### III.1.4. Serveurs physiques

#### III.1.4.1. Principe d'hébergement

Le Titulaire ne fournit pas l'infrastructure physique de virtualisation (serveurs hôtes, hyperviseurs, licences de virtualisation). Il devra en revanche exprimer précisément ses besoins en ressources (CPU, RAM, stockage, interfaces, tolérance de panne, architecture réseau virtuelle), ainsi que les contraintes logicielles.

Sur cette base, la DIR Est mettra à disposition l'infrastructure de virtualisation nécessaire (machines hôtes et licences associées), en environnement de production comme de préproduction.

L'infrastructure physique de virtualisation pour la plateforme de développement / TMA reste à la charge du Titulaire.

#### III.1.4.2. Principales dispositions

Les serveurs disposeront de plusieurs systèmes de tolérance de panne, garantissant ainsi un fonctionnement opérationnel :

- Le système de stockage pourra bénéficier d'une tolérance de panne d'un disque au minimum avec retour automatique en conditions nominales par mise en service d'un disque « de spare » préinstallé (RAID1E ou RAID5E) ;
- Les serveurs pourront être équipés d'une alimentation redondante échangeable à chaud permettant l'alimentation via un réseau ondulé et un réseau non ondulé dans les locaux techniques ;
- Chaque serveur pourra disposer d'un système autonome d'administration et de supervision du matériel indépendant du système d'exploitation installé et disposant d'une interface réseau dédiée ;
- Le dimensionnement des serveurs devra être adapté en fonction de l'architecture proposée ;
- A l'issue du déploiement, les consoles locales d'administration des systèmes seront désactivées. L'administration de ces équipements devra être effectuée via une console centrale. La mise en œuvre de droits spécifiques permettra d'offrir une granularité par sous-ensembles. Cela offrira la possibilité de déléguer l'administration d'un sous-ensemble à des tiers spécifiques.

Chaque serveur devra disposer d'une interface de management à distance (iLO, iDRAC...). Ces interfaces seront raccordées au réseau de management pour permettre aux équipes de maintenance de réaliser des opérations à distance.

Ces sous-systèmes devront être paramétrés pour être supervisés et/ou remonter des alertes (SNMP).

De manière générale, tout sous-système redondant devra disposer d'un mécanisme d'avertissement en cas de préalerte, alerte, panne ... de façon à informer les équipes de maintenance de la défaillance.

Les capacités de connexion Ethernet (nombre de ports) devront être suffisantes pour pouvoir faire de l'agrégation de lien à destination d'un switch ou d'un stack de switches 100 Mbps/1Gbps. Cette agrégation de lien sera mise en œuvre dans le présent marché.

Les applications doivent fonctionner sans nécessiter de droits d'administrations, sur les serveurs et sur les postes de travail.

Les configurations minimales des postes et serveurs proposées dans ce document sont fournies à titre indicatif. Le Titulaire devra, dans la phase de conception, réaliser une analyse de charge et de performance pour chaque rôle (supervision, simulation, jeu, maintenance, etc.) afin de proposer une configuration réellement adaptée aux usages opérationnels, aux durées de rétention et aux contraintes de disponibilité.

#### III.1.4.3. Serveur à vocation Temps Réel

Les serveurs à vocation Temps Réel sont des machines physiques dont le dimensionnement et la capacité de stockage sont étudiés par le Titulaire et répondront aux exigences formulées par les éditeurs des solutions proposées, a minima :

*Tableau 2 - Configuration minimale pour serveurs*

Composant	Descriptions
<b>CPU</b>	2 × processeurs multicœurs de gamme serveur, de type : – Intel® Xeon Scalable de 4 <sup>e</sup> génération (Sapphire Rapids) ou ultérieure, – ou AMD EPYC 7003 (Milan) / 9004 (Genoa) ou équivalent. Chaque processeur devra comporter au moins 16 cœurs physiques, avec une fréquence de base ≥ 2,4 GHz, et être compatible avec la plateforme de virtualisation retenue (VMware, Hyper-V, Proxmox).
<b>RAM</b>	128 Go DDR5 ECC RDIMM, extensible selon les besoins (jusqu'à 32 emplacements, 4 800 MT/s)
<b>Disque Dur</b>	2 x 1 To SAS/SATA 2,5" en RAID 1 pour l'OS + espace pour stockage secondaire et les sauvegarde
<b>SSD NVMe ou U.2 NVMe</b>	2 x 1,92 To NVMe U.2 pour les données applicatives, extensible selon la volumétrie attendue.
<b>Interfaces réseaux</b>	2 × ports 10 GbE SFP+ (ou RJ45 selon besoin) 2 × ports 1 GbE 1 × port dédié pour la gestion (iDRAC 9)

#### III.1.4.4. Serveur à vocation Temps Différé

Les serveurs à vocation Temps Différé sont des machines physiques dont le dimensionnement et la capacité de stockage sont étudiés par le Titulaire pour héberger les données et répondre aux exigences formulées par les éditeurs des solutions proposées, soit a minima une volumétrie de données :

- des applicatifs de deux tunnels ;
- sur une profondeur de deux ans ;
- avec une réserve libre de 30% (slots de disques et capacité).

Il s'agit ici de prévoir au moins deux serveurs physiques d'archivage et un ensemble de plusieurs machines virtualisées réparties sur ces deux machines de virtualisation, essentiellement pour les données issues :

- Des automates des ouvrages
  - Données « Terrain » :



- **TM** : Mesures des capteurs, DIRIS, etc.
- **TS** : Etats des équipements, etc.
- **TA** : alarmes
- De la traçabilité opérationnelle des utilisateurs (**TC**)
  - Commandes opérateur,
  - Changements des paramètres systèmes
  - Interactions avec le système
  - Mode d'exploitation
- Des alarmes techniques et alertes d'exploitation
  - Horodatage, détails, etc.
- Logs et suivi, des rapports, etc...

La réserve de la capacité de stockage devra être prête à l'emploi à la livraison.

De plus, le matériel devra avoir la capacité d'accueillir des disques supplémentaires (ou espace de stockage alloué) afin de pouvoir augmenter la capacité d'archivage en fonction des besoins.

### III.1.5. Poste opérateur

Afin de garantir et favoriser une gestion efficace, sécurisée et moderne des systèmes, il est souhaité de s'orienter vers une utilisation de machines virtualisées accessibles via des interfaces web.

Ces solutions permettent, entre autres :

- Une flexibilité accrue des prises de postes des opérateurs (et en cas de renfort),
- Une maintenance simplifiée,
- Une réduction des coûts matériels.

Ces postes seront installés et disponibles au CISGT.

#### III.1.5.1. Au CISGT

Les postes opérateurs du CISGT doivent disposer d'une configuration compatible avec les outils de supervision actuels, en garantissant une réactivité fluide, un double affichage ergonomique, et une longévité de maintenance sur 5 à 7 ans.

Le tableau suivant définit les caractéristiques minimales attendues à la date de livraison du matériel. Toute dégradation de performance observée en phase de recette pourra entraîner une demande d'ajustement.

Le matériel fourni devra être neuf, de gamme professionnelle (hors grand public), compatible avec les exigences SSI.

Les matériels constituant ces postes auront les caractéristiques minimales suivantes :

*Tableau 3 - Configuration minimale pour poste opérateur*

Composant	Descriptions
CPU	Intel® Core™ i5 de 12e génération ou supérieur (minimum 4 cœurs physiques / 8 threads, 2.5 GHz+)
RAM	16 Go DDR4 (fréquence ≥ 2666 MHz), extensible à 32 Go

Composant	Descriptions
Disque Dur	SSD NVMe PCIe 512 Go (minimum)
Interfaces réseaux	2 × ports Ethernet Gigabit (RJ-45)
Affichage	2 × ports DisplayPort 1.4 ou HDMI 2.0 (permettant double affichage 1080p ou supérieur)
Ports supplémentaires	4 × ports USB 3.1 Gen 1 ou Gen 2 (dont au moins 1 en façade)
Accessoires	2 × écrans 24" Full HD (1920 × 1080), support VESA : <i>selon retours ateliers ergonomie</i> Clavier/Souris

### III.1.5.2. En mode ultime secours

En mode ultime secours, c'est-à-dire lorsque les postes de surveillance principaux ou bien que les serveurs d'exploitation ne sont plus disponibles, des utilisateurs (opérateurs, techniciens de maintenance ou responsables CISGT), doivent pouvoir se connecter à distance ou depuis les locaux techniques, directement sur le serveur actif.

### III.1.5.3. Clients légers

Les retours d'expérience récents sur l'usage des clients légers dans des systèmes de supervision temps réel, notamment en environnement tunnel, mettent en évidence des limitations de performance, en particulier sur les temps de latence d'affichage des IHM. Le Titulaire devra réaliser une analyse technique détaillée des performances attendues pour les clients légers envisagés, incluant :

- la réactivité des interfaces en situation dégradée ou sous charge ;
- le délai de rafraîchissement des vues critiques (signalisation, alarmes, etc.) ;
- les impacts sur la supervision simultanée de plusieurs ouvrages ou scénarios.

Si cette évaluation révèle des latences incompatibles avec les exigences d'exploitation en temps réel, le Titulaire devra :

- proposer des clients lourds pour tout ou partie des postes opérateurs concernés ;
- en garantir l'intégration cohérente dans l'architecture globale (réseau, supervision, sécurité) ;
- s'assurer que la solution proposée respecte les critères de disponibilité et de maintenabilité exigés pour le poste opérateur.

Cette disposition vise à garantir une expérience fluide et fiable pour les opérateurs, en toute circonstance.

## III.1.6. Logiciel de supervision SCADA

### III.1.6.1. Architecture cible

La supervision est basée sur une architecture serveur / client. L'installation de supervision est composée de deux serveurs virtuels (hébergés sur deux serveurs physiques distincts) avec redondance à chaud.

Par son architecture virtualisée, il est possible d'assurer un double niveau de redondance :

- Une redondance « à chaud » offerte par le système de supervision ;
- Une redondance « à froid » offerte par le système de virtualisation.

Le protocole de communication entre les automates et la supervision doit être un protocole normalisé, type OPC UA.

### III.1.6.2. Nombres d'entrées / sorties et licences associées

La plateforme de supervision devra être dimensionnée pour acquérir un volume maximum d'entrées/sorties validé par le maître d'œuvre et le maître d'ouvrage lors des études préalables à l'exécution.

A titre indicatif, voici les ordres de grandeurs des installations actuelles :

*Tableau 4 - Dimensionnement des licences*

Licence	Nombre de postes	Nombre de points SCADA
<b>Serveurs</b>	2	10 000
<b>Postes client</b>	3	100

### III.1.6.3. Licences

Les licences fournies sont adaptées à la volumétrie des utilisateurs et points E/S surveillés, illimitées dans le temps.

Une licence de développement est également fournie pour permettre aux équipes maintenance de la DIR Est d'effectuer diagnostics et correctifs légers, sans compromettre les licences souscrites.

Les licences à prévoir, pour le système de supervision sont :

- Serveurs de supervision
- Serveurs d'historisation
- Serveurs de traitement de données (Rapports / TR / TD)
- Postes légers, clients opérateurs (légers ou lourds, au choix du Titulaire sur justification de l'atteinte des performances exigées)
- Poste de Maintenance

Les licences au format « dongle » sont interdites (voir §VII.2.2.2).

Le dimensionnement des licences devra prendre en compte les besoins en exploitation, maintenance et formation, y compris pour les postes de test, de développement et de jeu, afin d'éviter toute restriction bloquante en phase de vie du système. Le Titulaire proposera un scénario d'utilisation type (jour ouvré, formation, maintenance planifiée, situation de crise) pour valider ce dimensionnement.



A titre indicatif, les licences SCADA actuellement en exploitation sont communiquées au Livret 5 – Documentation confidentielle.

Se référer au Règlement de Consultation pour l'obtention de ce Livret.

### III.1.7. Systèmes d'exploitation

Il est attendu que l'ensemble des systèmes d'exploitation déployés sur les machines soit homogène. Ceci pour standardiser leur sécurisation et faciliter leur maintenance par les personnels de la DIR Est.

Ces systèmes d'exploitation sont fournis dans la dernière version LTS, avec disponibilité des mises à jour de sécurité pour au moins dix ans (par exemple Windows 11 pas 10).

Cette exigence doit être respectée pour l'ensemble des machines et systèmes prévus dans ce marché :

- Postes opérateurs
- Serveurs de virtualisation
- Serveurs virtualisés

## III.2. MATÉRIELS RÉSEAUX

### III.2.1. Routage N3

Le routage N3 est prévu par la DIR Est. Il est géré par les clusters pare-feu existants. Pour information, ces équipements sont certifiés ANSSI.



Les pare-feu sont précisés au Livret 5 – Documentation confidentielle technique.  
Se référer au Règlement de Consultation pour l'obtention de ce Livret.

Le Titulaire doit la fourniture de toute information (matrice de flux...) nécessaire à la réalisation de la configuration et mise en service de ces matériels par les équipes de la DIR Est.

### III.2.2. Commutateurs N2

Les commutateurs sont implantés en baie courant faible et dans les coffrets, ils seront de type industriel et présenteront les caractéristiques suivantes :

- Format compact monté sur rail DIN,
- Administrable,
- Support de VLANs, SNMP
- 2 ports SFP Gigabit, équipés des modules SFP/SFP+ adaptés aux débits et médias ;
- 8 à 16 ports RJ45 Ethernet selon les coffrets, pour respecter une réserve libre de 20% de ports ;
- Température de fonctionnement étendue (-40°C / +70°C)
- MTBF > 350.000 heures

Ces commutateurs seront de marque Allied Telesis ou équivalente pour être intégrés à la supervision technique. Les commutateurs seront alimentés via des alimentations redondées.

Les commutateurs supporteront les protocoles nécessaires à la communication de l'ensemble des équipements repris sur les réseaux de terrain, notamment les automatismes (automate et MESD via protocole définis au §III.1.2) et les équipements (PAU, caméras, PMV... via Ethernet/TCP-IP...).

Un port sera réservé aux usages internes DIR Est (maintenance, DISI, etc.), décompté séparément de la réserve de ports libres.



Figure 2 : Visuel commutateur N2

### III.2.3. Fibre optique



Il n'est pas spécifiquement identifié de travaux de tirage, mise en place de nouveaux câbles fibres optiques, le réemploi des câbles existants étant privilégié. Ces spécifications s'appliqueront le cas échéant. L'ensemble de la documentation relative au réseau fibre optique est disponible en annexe.

#### III.2.3.1. Connecteurs

Les connecteurs optiques servant à raccorder les fibres aux équipements d'extrémités devront être :

- de type adapté aux points de connexion physique existants, le cas échéant ;
- de type validé par la DIR Est pour les autres cas.

La conception des connecteurs et des férules devra assurer l'alignement latéral et angulaire précis des fibres optiques pour limiter au maximum les pertes d'insertion. Pour ces raisons, les fiches, les traversées, les pigtails et les jarretières seront issues du même fabricant.

L'affaiblissement maximal autorisé pour un connecteur devra être inférieur ou égal à 0,35 dB.

#### III.2.3.2. Câbles à fibres optiques

Les fibres optiques utilisées dans le câble devront répondre aux conditions techniques relatives aux fibres optiques monomodes de l'avis G652 de l'UIT-T. Ils respectent les caractéristiques suivantes :

- Monomode OS2
- Répartition en tube de 6 fibres
- Renfort central du câble non métallique (FRP)
- Armé
- Tube de protection
- Ruban synthétique entre les tubes et la protection anti-rongeurs
- Protection anti-rongeur en fibres de verre
- Gaine extérieure en polyéthylène HD noir

Les câbles cheminant en espace tunnel seront de type Cca s1, d1, a1 selon NF EN 50575.

Pour ce marché, les câbles peuvent être de modularité :

- 72FO ;
- 36FO ;
- 12FO.

#### III.2.3.3. Rangement des fibres et raccords

Le rangement des fibres et raccord sera réalisé sur des plateaux de rangement. Chaque plateau devra être équipé d'au moins six dispositifs permettant chacun la fixation des raccords de groupe de six fibres.

Il devra être possible de refaire des raccords après mise en ordre de marche de la liaison. Le nombre de réintervention encore possible sur toute fibre raccordée sera au moins égal à trois.

Le rangement des fibres et raccords protégés devra en conséquence être réalisé en respectant les règles suivantes :

- La réserve de fibres sera d'une longueur suffisante lors de la réalisation d'un troisième raccord, pour accéder à la machine de raccordement (soudeuse) et à la prise de l'information de flux lumineux nécessaire au centrage dynamique des cœurs de fibres ;
- Le stockage de la fibre sous un rayon minimal de 37,5 mm ;

Il faudra prévoir 15 mètres de love de fibre optique dans les chambres de tirages et locaux techniques pour s'assurer un confort de travail et une qualité d'intervention.

En cas de réintervention, il sera possible d'accéder à un raccord, sans altération du trafic sur les autres raccords.

#### III.2.3.4. Tiroirs optiques

Le raccordement des fibres optiques doit s'effectuer dans des tiroirs optiques compacts au moyen de dispositifs d'épanouissement. La capacité doit correspondre à la capacité des câbles optiques utilisés. Ces tiroirs optiques sont communs avec les autres systèmes ayant vocation à utiliser des fibres optiques.

Ils sont de type rackable 19". Ils sont facilement accessibles grâce à un plateau coulissant. Un kit de lovage et cassette d'épissurage permet l'organisation interne des brins optiques. Une plaque en face avant permet d'identifier les ports : repérage des connecteurs, zone d'étiquetage.

Pour ce marché, les tiroirs peuvent être de modularité de 12 FO à 144 FO.

#### III.2.3.5. Boîtes de dérivation optique

Les boîtes de dérivation optiques utilisées dans le cadre du marché seront toutes identiques.

Les boîtes seront mises en œuvre à proximité directe du cheminement principal de la tranchée couverte. Les boîtes de dérivation devront permettre de dériver certaines fibres optiques d'un câble en laissant en continuité et sans coupure d'autres fibres optiques de ce même câble (technique de piquage).

Les boîtes de raccordement devront :

- Assurer la protection des systèmes de rangement dans lesquels sont raccordées les fibres optiques ;
- Assurer l'étanchéité entre les gaines des différents câbles ;
- Être compatible avec les produits entrant dans la composition des câbles ;
- Assurer la réalisation des configurations suivantes :
  - Raccordement d'un câble de passage (technique de piquage) ;
  - Raccord droit ;
  - Division en deux câbles ;
  - Division en trois câbles ;
- Permettre la pénétration des câbles et le rangement des fibres raccordées et en réserve, à l'intérieur de la boîte de raccordement ;
- Permettre l'obturation des entrées de câbles non utilisées, avec des obturateurs présentant des caractéristiques mécaniques au minimum identiques à celles de la boîte de raccordement ;
- Maintenir et bloquer mécaniquement les câbles par arrimage du porteur central non métallique ;
- Assurer l'éclatement des fibres optiques du câble vers les dispositifs de rangement ;
- Résister aux sollicitations mécaniques (vibration, choc, écrasement, etc....) ;
- Résister aux sollicitations physico-chimiques (attaque chimique, pollution, etc....) ;
- Résister aux agressions des rongeurs, insectes et larves ;
- Ne pas nécessiter l'usage de flamme lors des travaux de confection.

Les boîtes de dérivation posséderont 18 entrées de câbles au moins, et auront une capacité suffisante de nombres soudures optiques.

Les boîtes de raccordement devront :



- Supporter le test d'étanchéité correspondant à 80 mb de pression en continu et 500 mb en flash test 15 mn (IP68) ;
- Supporter les chocs à 20 Joules (IK10) ;
- Permettre la réintervention sans destruction de la boîte de raccordement et des dispositifs de rangement des fibres ;
- Permettre d'accéder facilement aux raccords des fibres lors de réintervention, sans avoir à toucher à l'étanchéité des câbles déjà raccordés ;
- Permettre le contrôle d'étanchéité à chaque intervention ;
- Permettre le remplacement des câbles et l'installation de nouveaux câbles supplémentaires ;
- Se démonter totalement sans détérioration du contenu ni des câbles.

Le seul type de raccordement qu'il est permis d'utiliser dans les boîtes de raccordement est la soudure des fibres.

Il est également possible, que le Titulaire ait la nécessité de raccorder ses équipements sur une boîte de dérivation existante. Dans ce cas, il devra se référer aux plans de répartitions des soudures sur chacune des cassettes précâblées ou déjà câblées.

### III.2.3.6. Points de Branchement Optique (PBO)

Les PBO utilisés dans le cadre du marché seront tous identiques.

Les boîtiers seront mis en œuvre à l'intérieur d'un coffret ou armoire.

Les boîtiers PBO devront :

- Assurer la protection des systèmes de rangement dans lesquels sont raccordées les fibres optiques ;
- Être compatible avec les produits entrant dans la composition des câbles ;
  - Permettre la pénétration des câbles et le rangement des fibres raccordées et en réserve, à l'intérieur du boîtier ;
  - Permettre l'obturation des entrées de câbles non utilisées, avec des obturateurs présentant des caractéristiques mécaniques au minimum identiques à celles du boîtier ;
  - Maintenir et bloquer mécaniquement les câbles par arrimage du porteur central non métallique ;
- Assurer l'éclatement des fibres optiques du câble vers les dispositifs de rangement ;
- Résister aux sollicitations mécaniques (vibration, choc, écrasement, etc....) ;
- Résister aux sollicitations physico-chimiques (attaque chimique, pollution, etc....) ;
- Résister aux agressions des rongeurs, insectes et larves ;
- Ne pas nécessiter l'usage de flamme lors des travaux de confection.

Les boîtiers PBO posséderont 2 entrées de câbles au moins, et auront une capacité suffisante de nombres soudures optiques.

Les boîtiers PBO devront :

- Supporter le test d'étanchéité correspondant à 80 mb de pression en continu et 500 mb en flash test 15 mn (IP 68) ;
- Supporter les chocs à 20 Joules (IK10) ;
- Permettre la réintervention sans destruction de la boîte de raccordement et des dispositifs de rangement des fibres ;
- Permettre d'accéder facilement aux raccords des fibres lors de réintervention, sans avoir à toucher à l'étanchéité des câbles déjà raccordés ;
- Permettre le contrôle d'étanchéité à chaque intervention ;
- Permettre le remplacement des câbles et l'installation de nouveaux câbles supplémentaires ;

- Se démonter totalement sans détérioration du contenu ni des câbles.

Le seul type de raccordement qu'il est permis d'utiliser dans les boîtiers de raccordement est la soudure des fibres.

### III.2.3.7. Essais des fibres optiques – Réflectométries

Le Titulaire devra les tests de réflectométrie décrit ci-après pour tout câble à fibre optique déployé dans le cadre du projet ou sur les fibres existantes utilisées.

Le Titulaire devra proposer une topologie de réseau physique documentée, incluant les dispositifs de redondance et de segmentation (VLAN), ainsi que le plan de câblage optique redondé entre tous les éléments critiques du système (baies, automates, serveurs, postes opérateurs). Les performances et protections mécaniques des câbles et boîtiers seront conformes aux prescriptions renforcées. Les essais (réflectométrie, affaiblissement, raccordements) devront être systématiquement vérifiés, y compris sur les tronçons redondants.

#### III.2.3.7.1. Épissures

Les épissures et montages sur connectique devront être validés par des mesures d'insertion et de réflectométries dans les deux sens. Le niveau de qualité exigé est le suivant :

- Affaiblissement maximal d'une épissure : 0.1 dB à 1300 et 1500 mm
- Affaiblissement maximal d'un connecteur : 0.5 dB à 1300 et 1500 mm (un connecteur = deux fiches et une embase à raccord)

#### III.2.3.7.2. Contrôles de pose et raccordement – Mesures optiques monomodes

Tous les brins des câbles optiques seront systématiquement testés aux deux longueurs d'onde (1300 et 1500 m) :

- Selon le plan de contrôle du Titulaire :
  - Sur touret avant déroulage du câble ;
  - Après pose du câble et avant raccordement ;
- Obligatoirement :
  - Après raccordement.

Les tests de réflectométrie seront effectués :

- Tests brin par brin dans les 2 sens, en local et par tronçon ;
- Tests par brin dans les 2 sens, sur tout l'ouvrage ;
- Tests d'ensembles.

Tous les résultats des tests de réflectométrie seront compilés dans un dossier complet et organisé permettant une recherche aisée des résultats de chaque mesure effectuée.

## III.3. RÉSEAU ÉLECTRIQUE

### III.3.1. Câbles d'alimentation

#### III.3.1.1. Généralités

Le nombre de conducteurs, la section et la tension à employer dépendront de l'équipement terminal et de sa distance par rapport au point d'alimentation.

Les câbles de distribution basse tension seront calculés selon les règles de la norme NFC 15-100.

Le Titulaire fournira une note de calcul pour chaque câble issu du poste électrique (ou du point de service) alimentant un équipement. Cette note de calcul justifiera le choix des borniers et disjoncteurs sélectionnés.

#### III.3.1.2. Câbles rigides basse tension de norme européenne (Cca s1 d1 a1)

Tous les câbles soumis aux effets de l'incendie selon l'IT§4.1 devront être classé Cca, s1, d1, a1 selon la norme NF EN 50575. Les câbles employés pour la distribution basse tension dans les zones de sécurité nécessitant une bonne résistance à la propagation de l'incendie et des degrés de toxicité réduits sont conformes aux normes citées.

Ces câbles seront constitués :

- De conducteurs à âme en cuivre ou en aluminium à enveloppe isolante en polyéthylène réticulé.
- D'un assemblage avec ruban ou gaine de bourrage en matériau ignifuge sans halogène.
- D'une gaine extérieure en matériau thermoplastique ignifuge sans halogène.
- D'une gaine extérieure en matériau PVC de couleur noire.
- Repérage des conducteurs conforme à la norme NFC 32.081.
- Les câbles seront de types FR-N1 X1G1 ou équivalent.
- Les câbles cheminant directement en voûte où piédroit seront armés.
- Les câbles cheminant en multitubulaire disposeront d'une protection anti-rongeur.

#### III.3.1.3. Fils de câblages

Les fils de câblage seront utilisés pour le câblage des armoires, baies et coffrets :

- De type HO 7 VK et Eca dans la classification Européenne,
- Conformité à la norme UTE NFC 32 201,
- Conçus tension nominale 750 V,
- De section 1,5 mm<sup>2</sup> minimum ou filerie dédiée pour équipement spécifique.

### III.3.2. Câbles de transmission

#### III.3.2.1. Câbles multipaires SYT 2 / Euroclasse (Cca-s1-d1-a1)

Les câbles de contrôle-commande des équipements qui seront utilisés pour le raccordement sur les cartes d'entrées sorties des MESD seront de type SYT2. Ces câbles auront les caractéristiques suivantes :

- Âme cuivre
- Section minimale 0,5 mm<sup>2</sup>
- Isolation polyéthylène coloré
- Câblage en paires et assemblage en couches concentriques ou en faisceaux
- Revêtement sur assemblage par rubans plastiques
- Fil de continuité en cuivre
- Écran de protection électromagnétique par ruban polyester-aluminium sur l'ensemble des paires,
- Armure 2 feuillards acier disposés en hélice.

Les câbles mis en œuvre en tunnel et dans les issues de secours, pour le câblage des équipements d'exploitation ou de sécurité seront impérativement Euroclasse Cca s1 d1 a1. Aussi :

- Pour ces câbles, la gaine extérieure doit être sans halogène / Cca s1 d1 a1 (norme Européenne) ;

- Pour les autres câbles, la gaine extérieure doit être sans plomb.

### III.3.2.2. Câbles et jarretières Ethernet cuivre

Les caractéristiques des câbles et jarretières Ethernet seront les suivants :

- Câblage de catégorie 6, spécifié par la norme ISO/IEC 11801-2002 qui est relative au câblage de type Ethernet, permettant la transmission de données à des débits allant jusqu'à 10 Gbits/s et à des fréquences ne dépassant pas 600 MHz.
- Câble catégorie 6 présente quatre (4) paires torsadées individuellement et collectivement blindées afin de réduire les phénomènes parasites. Le blindage est au minimum constitué d'un écran rubané en aluminium (F/FTP).
- Ce type de câble s'associera avec les connecteurs GG45 compatible avec RJ45 utilisés de manière spécifique pour les applications où les exigences de sécurité sont importantes.
- Gaine « durcie » adaptée à un tirage en conduite pour les câbles empruntant de tels cheminements.

Pour chacune des nouvelles liaisons réalisées, le Titulaire devra tester la qualité de ses câbles. Cela comprend :

- Inspection visuelle
- Test de continuité
- Test de performances (débit, perte ou retard des paquets de données transmis)

### III.3.3. Cheminements

#### III.3.3.1. Principe

Autant que possible, les cheminements existants (réseaux secs enterrés, chemins de câble) seront employés.

#### III.3.3.2. Fourniture et pose de chemins de câbles

Les chemins de câbles à installer seront :

- en acier galvanisé à chaud, pour les cheminements intérieurs des locaux techniques ;
- en inox 316L, pour les cheminements en espace tunnel.

Les longueurs seront fixées entre elles bout à bout et sans chevauchement. Pour les dérivations de câbles, les chemins de câbles devront être pourvus de déversoirs.

Toutes les pièces fournies seront réalisées dans un matériau ayant reçu un traitement efficace contre la corrosion correspondant aux conditions d'ambiance, d'environnement et d'utilisation ; ce traitement devra être précisé par le titulaire et agréé par le Maître d'Œuvre.

Les produits finis seront galvanisés à chaud conformément à la norme NF A 91-121. L'épaisseur de galvanisation sera de 80 microns. Cette galvanisation ne sera exécutée qu'après tout découpage, pliage, soudage et perçage des différents éléments. Toute reprise de découpe sera recouverte d'une galvanisation à froid.

Ils devront être usinés afin d'éviter tout risque de blessure au montage et permettront d'assurer le maintien de la qualité de la gaine du câble lors du tirage.

Le titulaire établira le type et le nombre de chemins de câbles à mettre en œuvre, y compris les caractéristiques des supports et fixations (nature, pas de mise en œuvre) au cas par cas lors de ses études d'exécution, en fonction des câbles à installer. Il présentera les notes de calculs correspondantes. A minima il y aura 2 chemins de câbles, le premier de largeur 300mm pour les

courants forts et le second de largeur de 100mm pour les courants faibles. La hauteur d'aile sera au minimum de 48mm. Le titulaire devra prévoir 20% de réserve dans chaque chemin de câbles.

L'espace entre supports sera défini en fonction d'une flèche maximale de 1/200ème de la portée.

En intérieur, les chemins de câbles à installer seront en fils d'acier galvanisé à chaud d'une longueur de 2 à 3m en fonction de la charge à supporter et du pas des supports permettant la fixation des consoles murales/pendards des chemins de câbles.

Les chemins de câbles seront accrochés en plafond ou en piedroit. Le type de fixation dépendra de la nature de la paroi (béton armé, parpaing, poutre métallique...).

Le conducteur de protection isolant sera relié au chemin de câble par bornes laiton bi-métal de 35mm<sup>2</sup>. Ces bornes seront implantées avec un pas de 3m. La fixation par collier plastique est proscrite.

En local technique, pour rejoindre les équipements terminaux, les câbles devront circuler dans des conduits répondant au minimum à la spécification NF-USE XX IRL 3321. Il ne sera admis qu'un seul câble par conduit. Le diamètre sera fonction du câble qui y chemine.

Le rayon de courbure d'un conduit doit être tel que le câble ne soit pas endommagé.

Les conduits seront fixés à l'aide de pattes, colliers ou étriers appropriés. Pour un conduit de type rigide, la distance entre les points de fixation ne devra pas dépasser 0.8 m.

En local technique, dans le cas où les cheminements existants sont exploitables (nombre suffisant et qualité satisfaisante), ils devront être utilisés en respectant les principes de cheminement de câble.

En traversée d'un accès circulaire, les chemins de câble ne devront pas entamer le gabarit réglementaire de circulation des personnes de 2 m.

Au niveau des pénétrations et jusqu'à la hauteur d'homme de 2 m, les chemins de câbles doivent être capotés par une dalle pleine.

Le titulaire devra réaliser pour chaque cheminement une vue en travers et en élévation avec un gabarit humain.

En aérien, sur les portiques principalement, les câbles devront transiter dans des gaines types TPC annelé, ils ne devront en aucun cas être apparents et fixés correctement à la structure en particulier lors de leur remontée vers les équipements.

### III.3.4. Protection anticorrosion

En raison d'une atmosphère agressive (gaz d'échappement des véhicules ou salages), toutes les pièces fournies par l'entreprise doivent être réalisées dans un matériau inoxydable ou ayant reçu un traitement de protection efficace contre la corrosion.

Le type de traitement proposé doit être précisé dans les demandes d'agrément matériel et agréé par le Maître d'Œuvre.

L'attention du titulaire est particulièrement attirée sur l'importance de cette protection, notamment pour les chemins de câbles et pièces de fixation.

La boulonnerie et la visserie utilisées pour la réalisation, l'assemblage et la fixation des pièces doivent être en acier inoxydable de qualité minimale définie par la nuance 316L. Tout contact entre matériaux de potentiels galvaniques différents doit être évité par l'interposition d'éléments isolants de pérennité éprouvée : plaquettes, rondelles, entretoises, etc.

Les peintures éventuelles seront soumises à l'agrément du Maître d'Œuvre et doivent être sous forme de poudrage thermodurcissable et comporter :

- un traitement de surface par décapage chimique et rinçage,
- une couche primaire d'accrochage,
- une couche de finition, par poudrage électrostatique d'épaisseur 80 à 100 microns, avec polymérisation à 200°.

### III.3.5. Compatibilité électromagnétique et mise à la terre

Toutes les dispositions seront prises pour prévenir tous risques de dysfonctionnement provenant de perturbations électromagnétiques, par une étude et une mise en œuvre conforme aux règles de l'art en matière de câblages, blindages, liaisons équipotentielles.

De manière générale, toutes les masses métalliques susceptibles d'être mises accidentellement sous tension, devront être reliées à la terre des masses.

L'ensemble des équipements électromécaniques, des chemins de câbles, des armoires électriques, les carcasses métalliques des appareils, les huisseries métalliques et de manière générale toutes les masses métalliques susceptibles d'être mises accidentellement sous tension, devront être reliées à la terre des masses.

La mise à la terre de l'ensemble des portiques et mâts devra être raccordée à un puits de terre.

La mise à la terre devra être réalisée conformément à la norme NF C 13-100 et NF C 15-100.

### III.3.6. Protection contre les surtensions électriques et atmosphériques

La protection contre la foudre et les surtensions repose sur un ensemble de normes techniques couvrant à la fois les installations électriques, l'analyse du risque et la conception des dispositifs de protection. Les principales références normatives applicables en la matière sont présentées ci-après.

Normes relatives aux réseaux électriques et intégrant des dispositions spécifiques à la protection contre la foudre :

- NF C 15-100-1 (août 2024) – Installations électriques à basse tension – Partie 1 : exigences générales
- NF C 17-200 (septembre 2016) – Installations électriques extérieures

Norme sur l'évaluation du risque et des mesures de protections :

- Série des normes NF EN 62 305 (édition 2) – Protection contre la foudre – Parties 1 à 4

Normes sur la conception des systèmes de protection associés :

- IEC / EN 61 643-11 et 61 643-12 – Parafoudres pour systèmes basse tension
- IEC / EN 61 643-21 et 61 643-22 – Parafoudres pour réseaux de signaux et de télécommunications
- NF C 17-102 (septembre 2011) – Protection contre la foudre – Systèmes de protection à dispositif d'amorçage (PDA)
- Série des normes NF EN / IEC 62 561 – Composants des systèmes de protection contre la foudre (CSP) – Parties 1 à 7

Un soin particulier sera apporté à la protection foudre de tous les équipements.

Une protection associant parafoudres et varistances valables en fonctionnement commun et fonctionnement différentiel sera utilisée pour le matériel BT (borne). Pour les autres matériels, des protections associant parafoudres et diodes en parallèle seront mises en œuvre pour les départs vers les caméras.

En cas d'ajout de parafoudres, ceux-ci devront être fournis avec une fiche technique stipulant clairement leur conformité aux normes en vigueur. À défaut, l'installation pourrait être refusée.

Une étude spécifique de coordination avec les systèmes de protection contre la foudre existants devra également être fournie.

### III.4. REPÉRAGE

Les repères (forme, contenu) doivent être soumis à l'agrément du MOE avant mise en place sur site.

Les règles de nommage pourront être imposés par le MOA, pour homogénéisation de son patrimoine.

#### III.4.1. Repérage des câbles

Tous les câbles devront être étiquetés a minima à leur tenant, aboutissant, à chaque chambre de tirage traversée, de part et d'autre des traversées de cloisons, à chaque changement de direction.

La codification des câbles sera validée en phase exécution avec la MOE et la MOA.

#### III.4.2. Repérage des équipements

Tous les équipements, baies et armoires doivent être étiquetés avec des étiquettes rigides sérigraphiées, en respectant les mêmes codes couleur.

La codification des équipements sera validée en phase exécution avec la MOE et la MOA.



## IV. ARCHITECTURES

### IV.1. PRÉCONISATIONS GLOBALES

Le Titulaire devra respecter les règles de l'art et celles de l'ANSSI dans les études puis la configuration des systèmes dont il sera en charge au travers de la réalisation de ce projet.

La DIR Est se réserve la possibilité de faire un audit du système à l'issue de la mise en service.

Il est important de considérer qu'une réserve de 30% sera systématiquement requise. Cette réserve concernera le stockage, la CPU, la RAM, les ports disponibles sur les équipements réseau.

### IV.2. ARCHITECTURE EXISTANTE



Ce chapitre est disponible au Livret 5 – Documentation confidentielle technique.  
Se référer au Règlement de Consultation pour l'obtention de ce Livret.

### IV.3. ARCHITECTURE CIBLÉE



Ce chapitre est disponible au Livret 5 – Documentation technique. Ce chapitre est disponible au Livret 5 – Documentation confidentielle.  
Se référer au Règlement de Consultation pour l'obtention de ce Livret.

#### IV.3.1. Architecture à haute disponibilité

Les ouvrages sont supervisés :

- Par un applicatif maître, exécuté sur une machine virtuelle hébergé sur un 1<sup>er</sup> serveur de virtualisation ;
- Par un applicatif redondant, exécuté sur une 2<sup>ème</sup> machine virtuelle hébergé sur un serveur de virtualisation distinct.

La distribution des serveurs physiques de virtualisation, des machines virtuelles dans l'infrastructure virtualisée est proposée par le Titulaire, et soumis à validation du Maître d'Ouvrage. Le Titulaire fournit une étude des modes dégradés (pertes matérielles, pertes de lien réseau) pour justifier de la distribution.

Les architectures cibles proposées au §IV.3.3 répondent à ces exigences.

#### IV.3.2. Réseau global – Backbone



Ce chapitre est disponible au Livret 5 – Documentation technique. Ce réseau global est décrit au Livret 5 – Documentation confidentielle.  
Se référer au Règlement de Consultation pour l'obtention de ce Livret.

### IV.3.3. Ouvrages

Le réseau local/terrain assure la communication entre les différents équipements qui le composent. Ses caractéristiques principales sont les suivantes :

- Liaisons terminales SFP+ 10 Gigabits/seconde
- Liaisons de stack SFP+ 10 Gigabits/seconde
- Liaisons entre équipements actifs 1 Gigabits/seconde
- Cloisonnement des flux de données (VLANs), avec a minima (l'organisation cible du découpage réseau est en cours d'élaboration/validation) :
  - VLAN vidéo/cam extérieures Mercureaux
  - VLAN DAI montantes
  - VLAN DAI descendantes
  - VLAN switches
  - VLAN RAU
  - VLAN équipements dynamiques
  - VLAN GTC
  - VLAN d'administration

Les réseaux sous-jacents devront être sécurisés par la mise en place de boucles réseau. Ces boucles seront instanciées selon les protocoles propriétaire des équipements choisis.

Il est important de noter que des postes virtuels dédiés à la supervision seront hébergés et mis à disposition des opérateurs à partir du CISGT Vauban.

### IV.3.4. Accès à distance

Les accès distants pour la maintenance seront fournis et gérés par les équipes techniques de la DIR Est.

Pour garantir la sécurité, l'accès est accordé par compte individuel et nominatif. Le partage de comptes (nom d'utilisateur/mot de passe), ou l'utilisation à plusieurs d'un même compte générique sont strictement interdits. Toute nouvelle ressource nécessitant un accès doit faire l'objet d'une demande d'ouverture de compte à la DIR Est.

Par ailleurs, les postes qui seront utilisés pour ces opérations devront être dédiées au projet et ne devront pas héberger d'autres données que celles du projet et ne pas avoir d'autres solutions logicielles que celles validées par la DIR Est et indispensable à la maintenance de l'architecture cible.

Tout accès de télémaintenance devra :

- être initié par la DIR Est via un VPN maîtrisé ;
- être temporaire, tracé, journalisé, avec demande préalable ;
- exclure toute connexion directe depuis l'extérieur vers les plateformes ou équipements.

## IV.4. CONSTITUTION ET HÉBERGEMENT DE PLATEFORMES

### IV.4.1. Besoins projet

Dans le cadre du projet, plusieurs plateformes informatiques sont prévues afin d'assurer les fonctions d'exploitation, de formation, de développement, de test et de maintenance. Ces plateformes ont des rôles complémentaires tout au long du cycle de vie du système.

Trois plateformes sont prévues :

Plateforme	Vocation	Hébergement
<b>Plateforme n°1 PRODUCTION</b>	Supervision opérationnelle des ouvrages	CISGT
<b>Plateforme n°2 PRÉ-PRODUCTION</b>	Essais d'intégration et de validation logicielle	CISGT
	<i>Tranche Optionnelle n°1 : Formation des agents et rejeu de scénarios</i>	
<b>Plateforme n°3 TMA</b>	Développements, correctifs, préparation des recettes plateforme, Tierce Maintenance Applicative (TMA)	Titulaire

Les rôles attribués à chaque plateforme peuvent évoluer dans le temps, sous réserve de l'approbation du Maître d'Ouvrage.

Toutes les plateformes devront être dimensionnées pour permettre une utilisation simultanée par plusieurs utilisateurs (exploitation, maintenance, formation). Chaque environnement devra refléter fidèlement l'architecture fonctionnelle et logicielle du système cible. Le Titulaire devra garantir la continuité des services (redondance, supervision des machines via Zabbix, sauvegardes compatibles VEEAM, etc.). Les plateformes doivent permettre l'accès distant sécurisé pour les équipes de la DIR Est et répondre aux exigences cybersécurité du projet.

Le Maintien en Conditions Opérationnelles (MCO) et le Maintien en Conditions de Sécurité (MCS) de ces plateformes est à la charge du Titulaire, durant les périodes projet, de garantie puis maintenance annuelle (Tranche Optionnelle n°2).

#### IV.4.1.1.1. Plateforme d'exploitation

Plateforme principale destinée à l'exploitation opérationnelle du système GTC rénové, hébergeant les applicatifs de supervision, les bases de données et les services associés. Elle comprend :

- Les serveurs virtualisés ou physiques en haute disponibilité,
- Les postes opérateurs du CISGT,
- L'environnement réseau sécurisé d'exploitation.

La plateforme d'exploitation est hébergée dans les locaux de la DIR Est, assurant ainsi un accès centralisé et sécurisé. Elle est maintenue à jour avec la dernière version de la solution.

Elle doit offrir une vue d'ensemble unifiée en temps réel de toutes les infrastructures, permettant la surveillance, la gestion des ouvrages et garantissant à tout moment, l'unicité de commande. Son interface intuitive et personnalisable répond aux besoins spécifiques de chaque utilisateur, favorisant la collaboration entre les services. Elle facilite l'identification proactive des anomalies et la prise de décision éclairée.

#### IV.4.1.1.2. Plateforme de préproduction

Cette plateforme est hébergée dans les locaux de la DIR Est (le lieu précis restant à préciser).

Plateforme miroir de la plateforme d'exploitation, utilisée pour les opérations de :

- validation des mises à jour,
- tests de non-régression,
- configuration préalable,

Lors de son démarrage, il doit être possible de :

- Démarrer la GTC en mode « intégration & développement »  
Il doit être possible pour les équipes de développement (Titulaire) et/ou les administrateurs fonctionnels de la DIR Est de :
  - Mettre à jour la GTC dans sa dernière version ;
  - Installer des correctifs (patch) ;
  - Paramétrer le système.

Elle doit permettre la validation complète de toute évolution logicielle ou configuration avant déploiement en production.

#### IV.4.1.1.3. Plateforme de simulation (tranche optionnelle n°1)

Cette plateforme permettant la simulation complète de scénarios d'exploitation et de gestion de crise, destinée à la formation des opérateurs. Elle est équipée d'un orchestrateur virtualisé permettant une simulation autonome sans intervention constante d'un formateur.

Cette plateforme fait l'objet d'une tranche optionnelle. En cas d'affermissement, le Titulaire pourra mutualiser tout ou partie des ressources matérielles avec la plateforme de préproduction, sous réserve de garantir une isolation fonctionnelle suffisante pour permettre des usages simultanés.

Cette plateforme doit être totalement indépendante de l'environnement réel d'exploitation, conformément aux exigences du Livret 2 – Programme fonctionnel, notamment en matière de sécurité, de non-connexion aux équipements terrain et de gestion d'interface simulée.

Elle devra notamment respecter les principes suivants :

- Aucun lien physique ou logique ne doit permettre de piloter, d'interroger ou de perturber les équipements réels du système GTC.
- La supervision, les IHM et les simulateurs déployés sur cette plateforme doivent utiliser des bases de données, des variables et des flux de données isolés, strictement séparés de ceux de la plateforme d'exploitation.
- Le simulateur sera doté d'un orchestrateur permettant l'exécution de scénarios prédéfinis sans dépendance à un environnement opérationnel actif.
- Cette plateforme pourra être mutualisée avec celle de préproduction uniquement si cette mutualisation n'engendre aucune perte d'isolation fonctionnelle ou logique.

Ce poste doit rester indépendant et isolé de l'exploitation des ouvrages et de leurs opérations. Cependant, il peut être autorisé à avoir un lien sécurisé avec le serveur d'administration unique, permettant le déploiement des versions validées les plus récentes sur les postes opérateurs en cours d'utilisation, ainsi que les mises à jour OS, antivirus, ...

Le Titulaire devra démontrer dans son mémoire technique que la solution proposée respecte cette indépendance.

Lors de son démarrage, il doit être possible de :

- Démarrer le simulateur de rejeu et de formation

- Dans ce mode, la version logicielle et le paramétrage du système doivent être les mêmes que ceux installés sur la plateforme d'exploitation.
- Il doit être possible pour l'ensemble des utilisateurs connectés d'exécuter l'ensemble des « briques » logicielles (ou matérielles) associées au simulateur. Cela signifie que le formateur doit pouvoir, au même titre que l'opérateur connecté, agir sur l'interface.
- Elle doit permettre la formation des opérateurs sur n'importe quel ouvrage.

Par défaut, cette plateforme sera utilisée pour la formation. Elle devra donc toujours être disponible pour un usage interne DIR Est.

#### IV.4.1.1.4. Plateforme de développement et TMA

Cette plateforme est hébergée dans les locaux du Titulaire.

Le Titulaire constitue la plateforme en ses locaux, à compter de la validation des spécifications matérielles de ses composants. Celle-ci est composée de baies accueillant les matériels (routeurs, serveurs, automates et MESD). La configuration effective est définie par le Titulaire avec au moins :

- Un poste opérateur ;
- Un réseau « haut » d'interconnexion CISGT / Ouvrages ;
- Un réseau « bas » terrain pour les ouvrages ;
- Une paire de serveurs physiques de virtualisation ;
- Une paire d'automates redondants ;
- Deux MESD, comportant au moins une carte de chaque référence déployée sur le terrain ;
- La capacité à contrôler les mécanismes de redondance ;
- Les éventuels programmes / matériels « bouchons » pour simuler les capteurs / actionneurs terminaux.

Cette plateforme doit offrir au Titulaire la possibilité de concevoir les différentes vues et interfaces pour chaque ouvrage, permettant ainsi la validation des étapes de recette plateforme. La configuration d'un ouvrage est ainsi chargée **à la demande** avant chaque modification.

Enfin, une fois le contrat de renouvellement des GTC et des API achevé, et selon le Titulaire en charge de la maintenance et de l'assistance (TMA) pour l'ensemble des GTC, cette plateforme pourra être démontée et transférée au nouveau Titulaire du marché de la TMA (prestation de réversibilité).

#### IV.4.2. Études d'intégration

Les environnements de production et de préproduction seront hébergés sur l'infrastructure de virtualisation fournie par la DIR Est.

Le Titulaire devra définir pour chaque machine virtuelle (serveur applicatif, base de données, SCADA, etc.) :

- les ressources nécessaires (vCPU, RAM, disques, adaptateurs réseau),
- les caractéristiques techniques spécifiques (redondance, système d'exploitation, dépendances logicielles),
- le plan de déploiement des VM (arborescence, dépendances, adressage IP).

Le Titulaire n'administre pas l'infrastructure hôte, mais doit coordonner le déploiement de ses machines virtuelles avec les équipes techniques de la DIR Est.

#### IV.4.3. Constitution

Le Titulaire constitue les plateformes, dans les locaux DIR Est d'une part et en ses locaux d'autre part, à compter de la validation des spécifications matérielles de ses composants.

L'ensemble des plateformes devront être disponibles lors de la mise en ordre de marche de l'ouvrage. A compter de la mise en production de la supervision, les versions logicielles déployées sur chaque plateforme devront être identiques.

#### IV.4.4. Hébergement

La plateforme de développement et TMA est hébergée par le Titulaire. Les exigences suivantes sont applicables pour les conditions d'hébergement de cette plateforme :

- Climatisation : salle serveur existante est climatisée ; le Titulaire devra s'assurer que ses équipements s'intègrent dans les plages de température et hygrométrie prévues ;
- Sécurité anti-incendie : un système de détection faisant l'objet de tests réguliers doit prévenir et contenir tout départ de feu ;
- Cybersécurité : voir chapitre consacré à cette exigence sécuritaire spécifié et décrit dans le chapitre idoine
- Contrôle d'accès : l'accès à la salle d'hébergement doit être soumis à authentification afin de prévenir de l'intrusion de personnes non-habilitées ;
- Liaison fibre : la salle doit disposer d'un accès point à point en haut débit, de type fibre optique, pour permettre aux utilisateurs distants l'accès aux plateformes ;
- Assurance : la salle doit également être assurée contre tout type d'incident (vol, incendie, catastrophe naturelle, etc.). Le Titulaire doit fournir une attestation d'assurance valide pour la durée de l'accord-cadre.

## V. INFRASTRUCTURE SYSTÈMES – VIRTUALISATION

Dans le but de garantir des infrastructures informatiques résilientes et à haute disponibilité, d'augmenter le taux de disponibilité, de garantir l'évolutivité, de simplifier l'administration et la maintenance, le SI devra être porté par plusieurs systèmes de virtualisation répartis sur les différents ouvrages.

Ces systèmes de virtualisation compacts devront être déployés sur des architectures robustes hyperconvergées. La convergence de matériels standards au niveau stockage et calcul (x86) est entendue sur une seule plate-forme distribuée avec toute l'intelligence apportée par le logiciel.

Ces équipements informatiques respectent les exigences / objectifs suivants :

- Garantir la continuité des services critiques,
- Assurer un temps de reprise d'activité conforme aux exigences métiers,
- Garantir la disponibilité de la solution 24h/24-7j/7 avec une garantie de temps de rétablissement global inférieur à 4h ouvrées,
- Limiter les risques liés au trop grand nombre d'équipements,
- Avoir un environnement technique pérenne lié aux serveurs et au stockage pour accroître les performances,
- Garantir la sécurité des données critiques,
- Anticiper l'évolution du système informatique :
  - Croissance de la capacité de stockage des données
  - Ajout de nouveaux serveurs liés au déploiement de nouvelles applications ou services
- La solution installée devra être dimensionnée sans ajout de capacité de calcul ou de stockage pour une durée de 5 années.

L'infrastructure système proposée par le Titulaire, devra répondre aux différents enjeux de sécurisation opérationnelle, de cicatrization réseau, assurant ainsi un haut niveau service :

- Préférentiellement au niveau « haut », au CISGT :
  - Le serveur maître d'administration, d'historisation, de traitement des données, etc...
- Préférentiellement au niveau « bas », en local technique
  - Les serveurs d'exploitation principaux (maîtres et esclaves) des ouvrages ;
  - Le serveur esclave d'administration, d'historisation, de traitement des données, etc...



Le Candidat doit présenter dans son offre l'infrastructure de virtualisation :

- Implantation des éléments physiques ;
- Implantation des éléments logiques ;

tenant compte des impératifs de redondance et préconisations/fonctionnalités du progiciel de supervision qu'il intègre.



Le système de virtualisation dimensionné par le Titulaire doit supporter :

- l'ensemble des machines virtuelles nécessaires à sa solution de supervision des ouvrages ;
- l'ensemble des machines virtuelles nécessaires aux composants communs d'administration décrits ci-après.

## V.1. IMPLANTATION DU SYSTÈME D'INFORMATION

Le système d'information sera réparti entre les différents ouvrages concernés par le présent marché. Des serveurs physiques et virtuels seront prévus sur l'ensemble de ces sites.

### V.1.1. Implantation des éléments physiques

L'infrastructure globale est composée de plusieurs sous-ensembles, pouvant être répartis comme suit :

- Bois de Peu : 1 serveur physique de virtualisation en LT ;
- Fontain : 2 serveurs physiques de virtualisation en LT ;
- CISGT : 1 serveur physique de virtualisation en salle informatique.

### V.1.2. Implantation des éléments logiques

L'infrastructure globale est composée de plusieurs sous-ensembles, et ce, pour chacun des ouvrages :

- Bois de Peu :
  - 1 serveur virtuel GTC Maître ;
- Fontain :
  - 1 serveur virtuel GTC Esclave ;
  - 1 serveur virtuel d'historisation Esclave ;
- CISGT :
  - 1 serveur virtuel d'historisation Maître ;
  - 1 serveur d'administration SCADA, si la solution le nécessite ;
  - n serveurs de composants communs d'administration ;



## V.2. SYSTÈME DE VIRTUALISATION

### V.2.1. Composants fonctionnels

Un système de virtualisation peut intégrer les fonctionnalités suivantes :

#### V.2.1.1. Fonctionnalités d'exécution

- **FV1 – Hyperviseur :**

Ce composant gère les ressources matérielles et permet l'exécution de plusieurs machines virtuelles (VM) sur un même serveur physique ; Des solutions commercialisées sont par exemple : ESXi (VMWare), Proxmox VE (Proxmox), ...

- **FV2 – Réseau virtuel :**

Ce composant gère les connexions réseau entre les machines virtuelles et les réseaux physiques ; Des solutions commercialisées sont par exemple : vSwitch, NSX, Distributed vSwitch (VMWare), Open vSwitch, Linux Bridge (Proxmox), ...

- **FV3 – Gestion des clusters / Haute disponibilité :**

Ce composant permet de gérer plusieurs hôtes en cluster, assure la continuité de service en redémarrant automatiquement les machines virtuelles sur un autre hôte en cas de défaillance ; Des solutions commercialisées sont par exemple : vSphere HA (VMWare), Proxmox HA (Proxmox), ...

- **FV4 – Migration à chaud :**

Ce composant permet de déplacer une machine virtuelle d'un hôte à un autre sans interruption de service ; Des solutions commercialisées sont par exemple : vMotion (VMWare), Live Migration (Proxmox), ...

- **FV5 – Stockage partagé (utile à la migration et HA) :**

Ce composant permet de stocker les images des machines virtuelles et de les rendre accessibles à plusieurs hôtes ; Des solutions commercialisées sont par exemple : vSAN (VMWare), Proxmox Storage (avec Ceph, ZFS) (Proxmox), ...

#### V.2.1.2. Fonctionnalités d'administration

- **FV6 – Interface de gestion centralisée :**

Ce composant offre une console d'administration permettant de créer, configurer et gérer les machines virtuelles ; Des solutions commercialisées sont par exemple : vSphere Client (VMWare), Proxmox Web GUI (Proxmox), ...

- **FV7 – Sauvegarde et restauration :**

Ce composant permet de sauvegarder les machines virtuelles et de les restaurer en cas de besoin ; Des solutions commercialisées sont par exemple : vSphere Data Protection (VMWare), Proxmox Backup Server (Proxmox), Veeam...

- **FV8 – Surveillance et analyse :**

Ce composant permet de monitorer les performances et de l'état du système ; Des solutions commercialisées sont par exemple : vRealize Operations (VMWare), Integrated Monitoring (Proxmox), ...

▪ **FV9 – Gestion des templates et provisionnement :**

Ce composant permet de créer et déployer rapidement de nouvelles machines virtuelles ; Des solutions commercialisées sont par exemple : vSphere Templates et Content Library (VMWare), Templates et Clones (Proxmox), ...

## V.2.2. Exigences DIR Est

L'infrastructure de virtualisation déployée par le Titulaire pour la plateforme DEV/TMA comportera les composants fonctionnels suivants :

*Tableau 5 : Exigences d'infrastructure de virtualisation DIR Est*

Composant fonctionnel	Inclus au marché	Commentaires
FV1 – Hyperviseur	✓	
FV2 – Réseau virtuel	✓	Voir §IV.3.3
FV3 – Gestion des clusters / Haute disponibilité	✗	La redondance entre les serveurs TR est réalisée par des dispositifs applicatifs natifs de la solution SCADA. La redondance entre les bases de données TD est réalisée par des dispositifs applicatifs natifs de la solution de BDD
FV4 – Migration à chaud	✗	Conséquence du FV3
FV5 – Stockage partagé	✗	Conséquence du FV3
FV6 – Interface de gestion centralisée	✗	
FV7 – Sauvegarde et restauration	✓	
FV8 – Surveillance et analyse	✗	Voir §VI.1 et VI.3
FV9 – Gestion des templates et provisionnement	✗	VM spécifiques, pas de déploiements massifs

## VI. COMPOSANTS COMMUNS D'ADMINISTRATION

Le socle logique de l'infrastructure système est composé de serveurs physiques :

- système de sauvegarde des VM ;
- système de supervision technique de l'infrastructure ;
- horloge réseau NTP ;
- service d'authentification des utilisateurs ;
- antivirus
- DMZ...

### VI.1. COLLECTEUR DE LOGS

Actuellement, la DIR Est ne possède pas de collecteur de logs, mais a exprimé le besoin de mettre en place un serveur de logs pour la traçabilité des accès et des actions sur le réseau.

Il est demandé au Titulaire de fournir des machines capables de générer des logs pour assurer la traçabilité.

Le PASR prendra en charge l'installation et l'hébergement du serveur de logs. Le collecteur sera proposé par le Titulaire.

Le collecteur sera compatible avec le standard SYSLOG. En revanche, l'ensemble des machines déployées devront être configurées par le Titulaire pour transmettre leurs logs via des protocoles réseau sécurisés (SSL/TLS).

Tous les équipements seront néanmoins configurés pour retransmettre leur log via le protocole syslog. Ces transmissions devront être sécurisées. (TCP / TLS)

Le prestataire se coordonnera avec les équipes PASR DIR Est afin de configurer son environnement pour être compatible.

Le Titulaire devra mettre en œuvre le paramétrage de chaque machine (serveurs, postes, automates, MESD) pour générer des logs complets, selon les exigences de la DIR Est (événements système, connexions, incidents, modifications...). Il devra également prévoir un journal d'exploitation clair permettant l'analyse par la MOA (exploitation + cybersécurité). Le collecteur de logs proposé devra être documenté dans le Plan d'Assurance Sécurité. Il devra répondre à l'ensemble des exigences NIS2.

### VI.2. SAUVEGARDE

#### VI.2.1. Sauvegarde des données opérationnelles

L'archivage de restauration doit permettre la restauration des données système à un état antérieur en cas de défaillance ou de corruption des données (panne matérielle, cybersécurité), et ainsi garantir la continuité des opérations de surveillance et de service d'exploitation du CISGT.

Il devra donc être mis en place un système de sauvegarde complète, et automatique, assurant une redondance du stockage des données (RAID1E ou RAID5E), Tous les serveurs doivent assurer un niveau élevé de tolérance aux pannes matérielles.

Le Titulaire devra donc :

- Établir une procédure d'archivage des données (métier et paramétrage) et des systèmes en précisant les :
  - Format d'archivage,
  - Type de support de stockage,
  - Sécurisation des données,
  - Fréquence,
  - ...
- Établir une méthodologie de restauration système (dans son manuel d'installation ou de maintenance)
- Mettre en œuvre ces procédures, sur site, en présence des personnels DIR Est

La DIR Est prendra en charge :

- La réalisation des actions de sauvegardes régulières, selon les procédures ainsi éprouvées.

## VI.2.2. Sauvegarde des machines virtuelles (replica)

Le système de gestion des sauvegardes sera fourni et déployé par la DIR Est.

## VI.3. ADMINISTRATION ET SUPERVISION D'INFRASTRUCTURE

L'outil de surveillance devra être de type outil de gestion des événements et de monitoring réseau, compatible avec le protocole SNMP, et être utilisable par les techniciens et ingénieurs système pour la supervision infrastructure.

Le Titulaire fournira les modèles et toute information nécessaire pour permettre au PASR l'intégration des nouvelles machines dans la supervision technique Zabbix mise en place à la DIR Est. Cette solution logicielle est distincte de « l'autosupervision technique » réalisée par la GTC. Elle effectue la supervision technique de l'ensemble des infrastructures systèmes et réseaux de la DIR Est.

Cette surveillance permet de diagnostiquer :

- la perte, la défaillance matérielle ou logicielle des serveurs internes ou externes ;
- l'état des bases de données, des systèmes automatiques de gestion de logs / transactions, des sauvegardes de bases de données ;
- les défaillances de performances ou de fonctionnement en fonction de seuils (CPU / RAM / Espace disque / Charge réseau / Taux d'erreur Ethernet...) et disposer d'une capacité de stockage + visualisation a posteriori (pendant quelques jours) des valeurs ;
- l'état de l'infrastructure hébergeant les systèmes (serveurs physiques, hyperviseurs, systèmes de stockages éventuels) ;
- état des sauvegardes des systèmes (physiques et virtuel) gérée par le système (Veeam) déjà en exploitation à la DIR Est.

## VI.4. SYNCHRONISATION HORAIRE – SERVEUR NTP

Le service de synchronisation de l'heure a pour objectif de synchroniser l'horloge de toutes les machines (serveurs, postes de travail, automatismes) pour obtenir une base de temps cohérente sur le réseau de contrôle-commande. Le réseau Contrôle-Commande dispose d'une mise à l'heure

automatique des machines par le protocole NTP. Toutes les machines raccordées au réseau CC doivent supporter le protocole NTP.

Le serveur NTP primaire sera mis à disposition par la DIR Est.

## VI.5. AUTHENTIFICATION DES UTILISATEURS

Le Titulaire doit la fourniture de toute information (utilisateurs, groupes de sécurité, GPOs...) nécessaire à la réalisation de la configuration et mise en service de ce composant d'authentification des utilisateurs par les équipes de la DIR Est.

Il est demandé au titulaire concernant l'authentification des utilisateurs de la supervision des ouvrages de la Voie des Mercureaux (SCADA) que celle-ci soit possible de deux manières :

- Authentification sur la solution d'authentification des utilisateurs,
- Authentification par module logiciel propre au SCADA.

## VI.6. ANTIVIRUS

Les postes sur lesquels la solution SCADA sera installée devront être munis d'antivirus dernière génération type EDR.

La solution choisie devra pouvoir être mise à jour sans connexion à internet.

Cette solution devra être validée par la DIR Est et être compatible du système SCADA mis en œuvre.

## VI.7. SÉCURISATION DES FLUX RÉSEAU

Les certificats WEB ou autres nécessaires à la sécurisation des différents flux seront fournis par la DIR Est.

Ces certificats auto signés et/ou fournis par l'autorité DIR Est seront à déployer sur les différents serveurs les nécessitant.

Les flux inter sous-ensembles seront chiffrés et/ou sécurisés par les firewalls et par les principes déployés par la DIR Est pour leurs interconnexions.

## VI.8. PATCH MANAGEMENT

Aucun système de patch management ne sera déployé sur cette infrastructure.

Les mises à jour seront réalisées régulièrement et manuellement dans le cadre des prestations de la maintenance de ces systèmes. Les instances virtualisées devront être conçues de manière à être indépendantes les unes des autres, afin de pouvoir appliquer les mises à jour systèmes obligatoires sans perte d'exploitation. Cela signifie que :

- Les mises à jour devront dans un 1<sup>er</sup> temps être déployées sur les plateformes de développement / TMA (chez le Titulaire)

- 
- Des essais doivent être réalisés afin de confirmer qu'aucun conflit logiciel ou matériel n'est apparu
  - Déployer ensuite les mises à jour sur les plateformes DIR Est lors des nuits de fermetures d'ouvrages

## VII. CYBERSÉCURITÉ

Les exigences de cybersécurité indiquées dans ce chapitre ont pour origine principale le cadre légal et réglementaire impactant la DIR Est à savoir :

- **Comme marché public de nature technologique, l'arrêté du 18 sep 2018 « [Clauses simplifiées de cybersécurité](#) »,** dont les points clés sont rappelés ci-dessous mais il est recommandé de consulter le document à sa source :
  - Les sociétés titulaires du marché et leurs sous-traitants doivent connaître et appliquer les clauses les concernant de la politique de sécurité de la DIR Est : ces règles ont été extraites et sont explicitées dans ce document
  - Les titulaires peuvent être audités sans préavis pour vérifier le respect des clauses de cyber sécurité
  - Les titulaires du marché devront cascader ces exigences auprès de leurs sous-traitants, y compris possibilité par leurs soins d'auditer les sous-traitants
  - Les livrables doivent respecter l'état de l'art notamment en ce qui concernant la documentation (mesure de sécurité, flux...), l'administration (console dédiées), les sauvegardes (3-2-1 : 3 copies, 2 technologies, 1 exemplaire hors site principal avec chiffrement).
  - Les livrables ne doivent pas comporter de faille de sécurité connue et pouvoir être mis à jour
  - Peut être complété par un PAS (Plan d'Assurance Sécurité) sur le périmètre du projet, ce qui est le cas présentement. Le PAS vise notamment à définir les principes de classification des documents, leur protection (stockage, transfert, diffusion), les responsabilités et moyens à mettre en œuvre
  - Le constat de manquements à toutes les phases du projet peut entraîner le rejet d'une candidature, des pénalités, voire la suspension du marché.
  - Les dispositions d'aide à la gestion de crise sur l'installation fournie au marché.
- **La directive NIS2** dont la transposition en droit français est en cours : DIR Est sera selon les critères NIS2 « Entité Essentielle ». Les mesures de sécurité que l'on peut anticiper et qu'il serait coûteux de réaliser après livraison du projet de rénovation GTC sont prises en considération dans les exigences détaillées dans les paragraphes qui suivent
  - Dans l'attente de la transposition en droit français de la directive NIS2, l'ANSSI recommande de se baser sur les mesures [d'hygiène informatique](#) dont les points clés sont repris dans les chapitres suivants
- **Des consignes et recommandations du ministère de tutelle (Transports)** seront diffusées à toutes les directions régionales et ne sont pas encore connues : pour cette raison certaines mesures de sécurité sont pour l'instant repoussées
  - Par exemple : concernant la centralisation des logs, il est demandé dans le cadre du marché d'activer et configurer les systèmes de journalisation sur les systèmes livrés. En revanche, les solutions de collecte (WEF, syslog...) seront installées ultérieurement : Le titulaire devra rédiger des procédures applicables avec le déploiement de ces connecteurs centraux effectif.

Dans le cadre des exigences de sécurité du système d'information, le Titulaire devra garantir, sur toute la durée du marché (chantier + TMA), une organisation sécurisée, stable et traçable, notamment vis-à-vis :

- De la télémaintenance :
  - Toute session de télémaintenance doit être initiée, contrôlée et tracée par la DIR Est, via un accès VPN chiffré dédié.
  - Aucune session distante non sollicitée, automatique ou permanente ne sera autorisée.
  - Un journal des sessions (identifiant, date/heure, durée, objet de la session, IP source) devra être automatiquement intégré dans le collecteur de logs du système.
  - Le Titulaire devra fournir une procédure de télémaintenance validée en recette et mise à jour en cas d'évolution du personnel ou des outils.
- Du maintien du niveau de compétence :
  - Le Titulaire doit désigner une équipe projet nominative et maintenir un registre des personnes habilitées à intervenir sur le système (nom, rôle, formation SSI, dates de validité).
  - Toute personne accédant aux plateformes devra être :
    - identifiée de manière nominative,
    - disposant d'un compte personnel et non partagé,
    - formée aux bonnes pratiques de sécurité (rappel de la politique de mots de passe, gestion des supports, comportement en télémaintenance, etc.).
- Du remplacement du personnel :
  - Tout remplacement d'un intervenant ayant un rôle sur le système devra être :
    - notifié à la MOA,
    - accompagné d'un dossier de validation (CV, certificat de compétence, délégation, etc.),
    - intégré dans le registre SSI mis à jour.

Ces éléments seront contrôlés lors des revues SSI régulières, avec obligation pour le Titulaire de démontrer la traçabilité et la conformité des pratiques organisationnelles.

## VII.1. EXIGENCES RELATIVES À L'ORGANISATION, AUX PRATIQUES ET MOYENS DU TITULAIRE DU MARCHÉ

Il est demandé aux prestataires de respecter les bonnes pratiques de cybersécurité listées ci-dessous. Il précisera **dans la réponse à l'appel d'offre s'il répond à ces exigences et détaillera comment elles sont respectées**.

Le titulaire du marché devra formaliser les mesures et assurer leur suivi (mesures, audits, corrections tracées) dans un **Plan d'Assurance de Sécurité (PAS) sur le périmètre du marché** (intervenants, moyens) qui sera partagé avec la DIR Est.

### VII.1.1. Données confidentielles

Toutes les données concernant les infrastructures de la DIR Est (équipements, réseaux) et les codes, plans, documentations générées lors de la réalisation des études, développement et installation sont considérées comme confidentielles, et doivent :



- Être stockées de manière sécurisée par le titulaire du marché et les sous-traitant (ex : pas sur clé USB non chiffrée, non accessible en cas de perte de PC portable etc...)

La diffusion et l'accès doivent être restreintes aux personnels ayant besoin d'y accéder (ex : contrôle des droits d'accès sur des serveurs de fichier, attention à la diffusion par email interne, utilisation de moyens sécurisés – chiffrement – pour la communication entre organisations (disques chiffrés, emails chiffrés, PJ Zed!, utilisation ACID, etc.))

### VII.1.2. Organisation de la cybersécurité chez le titulaire

Le titulaire du marché et les co-traitants doivent chacun désigner un Correspondant Sécurité du SI durant le projet (CSSI), qui sera le principal acteur garantissant la sécurité des informations au sein de son organisation et des éventuels sous-traitants, et sera l'interlocuteur des responsables sécurité de la DIR Est et de l'assistant à maître d'ouvrage.



Des certifications concernant l'organisation ou le CSSI seront un plus pris en considération pour la notation du Candidat, notamment :

- Certifications ISO/IEC 27005, CISSP, GISCIP, ISA/IEC 62443 pour les personnes physiques
- Certifications ISO/IEC 27001, ISA/IEC 62443-2-4, ISA/IEC 62443-4-1 pour les organisations

Le CSSI doit avoir une formation et une expérience en cybersécurité dont il peut faire état.

Le CSSI a la charge de préciser les règles et moyens de sécurisation des données durant le projet dans le PAS, en conformité avec les exigences figurant dans le CCTP et ses livrets.

Le CSSI décline au sein de son organisation les moyens, gère les accès aux documents dans le SI de son organisation, pour en assurer la confidentialité et limiter la diffusion aux personnels ayant besoin d'y avoir accès.

Le CSSI s'assure que les contrats de sous-traitance intègrent les mêmes exigences, éventuellement limitées à celles pertinentes suivant la nature de la prestation.

Le CSSI signale tout changement significatif au sein de son organisation et des sous-traitants éventuels, en particulier changement de personnes / départs, ainsi que tout incident de sécurité (ex : vol d'un PC avec données projets, email envoyé à un destinataire erroné etc...).

### VII.1.3. Charte ou engagement utilisateurs du SI intervenant sur le projet

Le titulaire du marché et les sous-traitants doivent avoir un charte informatique valide (appliquée via règlement intérieur ou contrats de travail), permettant d'encadrer l'utilisation du SI en général et des équipements utilisés pour les projets en particulier, afin de protéger la confidentialité des données du projet en les responsabilisant en cas de négligence voire de malveillance.

A défaut un engagement écrit reprenant les exigences du présent document et concernant les intervenants sera à effectuer.

#### VII.1.4. Sensibilisation des intervenants

Il est de la responsabilité du CSSI de s'assurer que tous les intervenants sur le projet ayant à utiliser ou générer des informations confidentielles ont été sensibilisés :

- A la réalité du risque de cybersécurité sur les infrastructures critiques, pour cela [les fiches incidents mises à disposition par le CLUSIF](#) peuvent être utilisés
- Aux règles applicables dans le projet, en particulier la gestion des documents confidentiels. Ces règles peuvent être déclinées selon les fonctions par le CSSI
- Au fait qu'un audit est possible sans préavis et que les clauses techniques seront vérifiées durant les tests de recette
- Le CSSI et éventuelles autres personnes gérant les droits d'accès comme indiqué dans le chapitre "Organisation" doivent avoir été formées à la cybersécurité et sont présumées comprendre et savoir faire appliquer toutes les clauses de cybersécurité

En sus des points mentionnés, la sensibilisation s'étendra à la sûreté informatique. Cette démarche d'ensemble vise à inculquer une culture de cybersécurité robuste et proactive chez tous les intervenants, garantissant la protection optimale des informations confidentielles.

Un registre des formations et sensibilisation cyber doit être maintenu à jour afin de pouvoir vérifier pour chaque intervenant la date et durée de la formation ou sensibilisation.

#### VII.1.5. Sécurité du SI utilisé par les prestataires pour le projet

##### VII.1.5.1. Postes de travail et serveurs utilisés par le prestataire

Les règles suivantes doivent être appliquées aux postes d'administration, de conception, développement utilisant ou générant des données confidentielles dans le cadre du projet :

- **Poste dédié** : des postes dédiés aux activités d'administration, de conception ou de développement doivent être utilisés pour le projet
  - Ces postes doivent être autorisés à réaliser les actions suivantes :
    - Programmation des automates,
    - Gestion des accès,
    - Installation et mise à jour d'équipements,
    - Gestion des systèmes.
  - Ces postes ne doivent pas être utilisés pour des activités de bureautique, notamment courriel professionnel général, accès internet généralisé hors ressources nécessaires pour le projet, et a fortiori aucune utilisation personnelle n'est autorisée
  - Ces postes doivent être durcis. En particulier, le disque dur des postes portables doit être chiffré et les applications non pertinentes pour l'utilisation ne doivent pas être présents (ludique, logiciels sans rapport avec le métier...).
- **Moindres privilèges** : le principe de moindre privilège doit être appliqué pour tous les comptes d'administration. Seuls les droits strictement nécessaires doivent être octroyés.
  - En l'absence d'une gestion des postes via AD et GPO, les comptes utilisés pour le projet en conception, développement etc... doivent être de type « utilisateur invité » (et non administrateur)

- **Opérations d'administration** : les comptes d'administration doivent être utilisés uniquement pour réaliser des opérations d'administration.
- **Politique de mots de passe** : une politique de mots de passe doit être appliquée. Elle doit respecter à minima les exigences suivantes :
  - 12 caractères minimal, mélange de 3 types de caractères (minuscules, majuscules, chiffres, caractères spéciaux)
  - 16 caractères minimal pouvant être une passphrase (mots sans rapports)
- **Système à jour** : tous les composants logiciels (système d'exploitation, anti-virus, logiciels de développement, édition de documents, plans...) doivent disposer de mises à jour automatiques. Pour les autres logiciels ou applications, des notifications de mise à jour manuelle sont soumises aux administrateurs dans un délai maximum d'une semaine (navigateurs internet, outils...)
- **Pare-feu et anti-virus** : dans tous les cas un anti-virus doit être installé et à jour (Cf paragraphe ci-dessus), et si le poste est connecté à un réseau non dédié aux opérations (conception, développement...) tel qu'un réseau bureautique ou un réseau personnel (travail à domicile) il est obligatoire que le pare-feu intégré à l'OS soit activé.
- Les systèmes doivent être administrés et notamment les éventuelles alertes de sécurités doivent être journalisées et leur traitement suivi.

#### VII.1.5.2. Intervention sur les réseaux DIR Est (installation, maintenance)

Lors des interventions sur les sites DIR Est l'utilisation de postes tiers ou de médias amovibles n'est pas autorisé, les règles suivantes s'appliquent :

- Le CISGT doit être prévenu en amont et au moment de tout accès aux locaux techniques.
- Pour les phases d'installation, de mises en service, de tests, aucun PC prestataire ne doit être relié au réseau DIR Est.
- Un PC prestataire est autorisé pour l'usage HORS LIGNE de configuration d'un équipement ne disposant pas de stockage (équipements réseau tant qu'ils ne sont pas reliés au réseau par ex), mais pas pour un ordinateur. L'utilisation de clé USB est généralement à proscrire, surtout que d'autres possibilités d'échanges de documents, de fichiers, d'applications existent.
- Pour les autres cas, la DIR Est fournira un ordinateur portable et procédera si nécessaire à l'installation des logiciels requis par le prestataire.

## VII.2. EXIGENCES CONCERNANT LES MATÉRIELS ET LOGICIELS LIVRÉS OU CONFIGURÉS

### VII.2.1. Critères de sélection des composants matériels et logiciels

Les critères ci-dessous sont à prendre en considération pour choisir une solution ou un équipement plutôt qu'un autre à fonctionnalités équivalents en termes de performance. Ceci concerne tous les systèmes programmables ou configurables avec capacité de communication sur un réseau (Ethernet ou sans fil).

#### VII.2.1.1. Certification

Si pour une fonction ou équipement une certification existe, en particulier [CSPN](#) ou ISAsecure/IECEE, l'équipement sera privilégié.

En l'absence de certification, les propriétés ci-dessous seront vérifiées (propriétés issues du modèle de cible de sécurité automate de l'ANSSI).

#### VII.2.1.2. Possibilité de désactiver les interfaces non utiles en exploitation

La plupart des équipements connectés disposent d'un serveur web permettant de les configurer (HTTP, HTTPS), ainsi qu'un ou plusieurs services de prise de main à distance (TELNET, SSH), ainsi que d'autres services standards (FTP...) ou propriétaire.

Lors de tests unitaires d'équipements dans la phase d'étude, les tests suivants doivent être effectués. Les résultats sont consignés dans des rapports. En cas d'échec à procéder à ces vérifications l'équipement ne pourra être utilisé sans dérogation de la DIR Est : toute exception doit être validée et fera l'objet d'une évaluation du risque et d'une décision d'accepter un risque résiduel ou pas.

- En cas de connectivité IP d'un poste non déclaré : vérification par scan de tous les ports ouverts par défaut (TCP, UDP) et identification des protocoles. En cas de port ouvert / protocole inconnu (hors matrice des flux), le fournisseur doit être sollicité pour apporter une réponse.
- Tous les services non directement liés à l'exploitation doivent pouvoir être désactivés sauf un accès de maintenance. Cet accès doit pouvoir être sécurisé de manière adéquate :
  - Certificat
  - Mot de passe de complexité suffisante (voir "Politique de mots de passe")
  - Communication chiffrée entre le client et l'équipement (ex : plutôt SSH que Telnet)
  - Mécanisme empêchant les attaques de force brute

#### VII.2.1.3. Autres fonctions de durcissement

Vérifier que les systèmes (notamment PC / serveurs) et systèmes d'exploitation supportent l'activation des fonctions de sécurité décrites dans la section « Durcissement » ci-dessous.

#### VII.2.1.4. Disponibilité du support et de mises à jour de sécurité

Afin de s'assurer qu'en cas de divulgation d'une faille de sécurité sur un équipement, le fournisseur doit avoir des procédures de déploiement d'une mise à jour du micrologiciel (firmware) et/ou d'un composant (ex : service SSH) et de diffusion sécurisée (a minima avec empreinte vérifiable sur leur site internet). La durée de ce support doit être de dix ans.

On s'assurera que la mise à jour du firmware repose sur un mécanisme sécurisé.

La mise à jour doit pouvoir se faire sans qu'il y ait un besoin de connexion directe entre l'équipement et un serveur du fournisseur sur internet (accès à disque ou connecteur réseau distant par exemple)

#### VII.2.1.5. Absence de vulnérabilité connue

Une vérification sur les bases de vulnérabilité (MITRE, ICS-CERT, CERT FR) sera effectuée pour vérifier l'absence de vulnérabilité de l'équipement, ainsi que de l'OS embarqué (ex : VxWorks) et du serveur web embarqué sur la base de sa version (ex: nginx).

#### VII.2.1.6. Fonctions de journalisation distante

- La journalisation doit être configurée sur les équipements suivants (liste limitée aux équipements pertinents dans le cadre du projet) :
  - Postes et serveurs SCADA,

- Sur les postes et serveurs Windows, la taille des journaux doit être augmentée à minimum 1Go (au lieu de 20Mo) avec rotation.
- Les événements à journaliser sont ceux recommandés par l'ANSSI [dans le guide d'hygiène](#) (voir chapitre 36) ainsi que les alertes de tous les services ou règles de sécurité configurées (Cf partie « Durcissement » ci-dessous).
  - Postes d'administration,
  - Composants applicatifs (web, base de données),
  - Equipements réseaux manageables.
- Les équipements terrain (API, RTU...) pourront être protégés contre les accès non autorisés, les manipulations malveillantes et les intrusions par l'application d'un système tel que Nanolocksec.
- L'équipement doit pouvoir envoyer via un mécanisme standard (SNMP, syslog) des événements à une station de collecte qui sera configurée ultérieurement.

## VII.2.2. Critères fonctionnels pour le choix des équipements

### VII.2.2.1. Commutateurs Ethernet

Le remplacement des équipements communiquant via des bus ou solutions point à point impose d'installer des commutateurs (switches).

Les équipements devront être compatibles avec les switches du backbone notamment concernant les connexions RSTP, et doivent pouvoir être administrés via la HP IMC utilisée par DIR Est.

Les équipements devront permettre les fonctions suivantes :

- Fonction routage niveau 3
- Gestion par SNMPv2 ou v3 (désactiver SNMPv1)
- Emission d'événement au format syslog
- Fonction MAB : restriction des accès par adresse MAC
- Fonction SPAN (ou mirroring, ou audit) : possibilité de répliquer le trafic de plusieurs ou tous les ports, ou par VLAN, pour a minima le trafic entrant (Rx) en sortie sur un port choisi
- LAPS possible pour les uplinks notamment.

### VII.2.2.2. Fonctionnement sans média USB

La DIR Est ne souhaite pas que soit utilisé des « dongles » pour la gestion des licences. Pour des raisons liées à la cybersécurité, et d'une manière générale, l'utilisation des clés USB (stockage) ne sera pas autorisée sur l'ensemble du réseau.

Cela sera contrôlé par le serveur de sécurité qui inventoriara les médias utilisables sur les différents sites.

## VII.2.3. Configuration – Durcissement

Les actions de configuration suivantes devront être effectuées avant la phase de mise au point et feront partie des tests des équipements. Si elles ne sont pas réalisables ou causent des problèmes fonctionnels alors une justification sera apportée.

- Mise à jour avec la dernière version de firmware/logiciel disponible
- Configuration de différents utilisateurs selon capacité de l'équipement, configuration d'informations d'identification

- Configuration des règles de complexité des mots de passe
- Modification des mots de passe par défaut et positionnement de mots de passe de complexité suffisante et différents pour chaque système (12 caractères aléatoires ou passphrase de 20 caractères)
- Désactivation des services obsolètes et protocoles non nécessaires : désactivation des protocoles Netbios, NTLMv1, SMBv1 et v2, de IPv6, LLMNR, mDNS, découverte et annonces réseau. Fonction serveur et partage de fichiers si non utilisés.
- Activation du pare-feu et configuration pour interdire toutes les connexions entrantes sauf celles nécessaires
  - A cet effet une matrice des flux entrants et sortants des serveurs et postes sera documentée : tous les autres flux doivent être interdits. La matrice des flux fait partie des livrables (voir chapitre « Documents et fichiers relatifs à la cybersécurité »)
- Désinstallation des logiciels non nécessaires (notamment sur Windows : jeux, Microsoft Store, Xbox...)
- Configuration si l'équipement le permet de la sécurité des communications (ex : certificats pour OPC-UA, filtre par IP/Mac...)
- Désactivation du support de medias amovibles (USB)
- Activation du chiffrement des disques (pour les équipements hors CISGT) et activation / vérification de la configuration de démarrage sécurisé (secure boot)
- Concernant les API, RTU (E/S déportées), variateurs, ASI :
  - section programme et Bloc Fonction Dérivé sont protégés par mot de passe,
  - L'accès aux applications des équipements et Firmware sont protégés par mot de passe,
  - Chaque équipement peut autoriser la ou les adresses IP à entrer en communication,
- Les protocoles de communication inutilisés sont désactivés (ex : FTP / ...).

#### VII.2.3.1. Désactivation des services inutiles sur Windows

Le Titulaire devra procéder à une revue complète des services Windows sur chaque type de machine, en particulier les postes opérateurs et serveurs, afin de désactiver les fonctions non nécessaires à l'exploitation ou à la supervision. Cette désactivation devra être documentée, vérifiable, et testée pendant la recette technique.

Services : les ressources (liens) proposent les mesures de désactivation des services sur [Windows Server](#) et postes clients.

Sur Windows les services suivants peuvent être désactivés (source HS2 Secuwin)

- lmhosts : TCP/IP NetBIOS Helper
- WMPNetworkSvc : Media Player Network Sharing Service
- DiagTrack : Connected User Experiences and Telemetry
- Diagnostic Tracking Service : Lié à la télémétrie
- dmwappushservice : Lié à la télémétrie
- stisvc : Windows Image Acquisition (scanner)
- Spooler : Print Spooler (imprimante locale)
- DPS :Diagnostic Policy Service
- WerSvc :Windows Error Reporting Service
- iphlpsvc :IP Helper (IPv6)
- TabletInputService : Touch Keyboard and Handwriting Panel Service
- Services Xbox, Map...

#### VII.2.3.2. Activation de fonctions de sécurité sur Windows

Les postes et serveurs seront Windows version 11, dernière version (niveau de patch) disponible à date de l'intégration, sauf proposition alternative à valider par la DIR Est.

Les fonctions de sécurités suivantes seront activées à moins que des applications de sécurité tierces (EDR, anti-virus avec restriction d'exécution par white list...) soient installées. Les tests fonctionnels seront bien entendu réalisés avec ces fonctions activées.

- [installer AppLocker](#) et configuration la plus restrictive possible pour les applications installées (dont navigateurs sur les postes clients) et en particulier les applications SCADA (serveurs)
- Si une solution équivalente est proposée (verrouillage, scellement) elle peut être utilisée après accord DIR Est (vérification éditeur / recommandation ANSSI)
- Si le prestataire est habitué à utiliser [WD Application Control](#) (plus récent que AppLocker), WDAC peut être configuré en remplacement ou en plus de Applocker.
- Activer Windows Defender Exploit Guard : même recommandation (via GUI) – la configuration peut s'exporter entre postes. Activer a minima :
- Controlled folder access (dispositif d'accès contrôlé aux dossiers – via GUI) : restreindre l'écriture sur les répertoires métiers aux applications correspondantes
- Exploit protection
- Activer la journalisation des événements correspondants

Un test de vérification de l'efficacité de chacune des mesures sera fourni pour la recette (Cf « Documentation » ci-dessous), par exemple : impossibilité d'exécuter un exécutable .exe non autorisé, impossible de créer un fichier (avec notepad ou autre...) dans un répertoire protégé.

### VII.3. DOCUMENTS ET FICHIERS RELATIFS À LA CYBERSÉCURITÉ À FOURNIR PAR LE TITULAIRE

#### VII.3.1. Plan d'Assurance Sécurité Projet

Ce plan doit être réalisé au démarrage du projet et visé par la DIR Est. Il décline au niveau de l'organisation et des sous-traitants le plan de cybersécurité. Il doit être conforme aux exigences stipulées dans ce cahier des charges chapitre "Exigences relatives à l'organisation, aux pratiques et moyens du titulaire du marché", les écarts ou exceptions doivent être acceptées par la DIR Est.

La déclinaison des moyens de sécurisation des données (stockage, contrôle d'accès, communication) doit être indiquée.

La liste des personnes ayant accès aux documents confidentiels est précisée et mise à jour.

Les règles et informations (utilisateurs) sont susceptibles d'être auditées sans préavis par la maîtrise d'ouvrage, conformément à l'arrêté du 18 sep 2018, dont on rappelle les points clés :

##### *Article 3 - Contrôles et audits*

*3.1. Durant la préparation ou la réalisation du marché, l'acheteur peut conduire ou mandater des contrôles et audits de sécurité informatique des fournitures, prestations, moyens utilisés et services proposés par le candidat ou titulaire, et leurs sous-traitants.*

*3.2. Dans tous les cas, des audits légitimés par la sélection ou le suivi de titulaires de marchés peuvent être réalisés sans accord préalable dès lors que les tests et sondes respectent les conventions*



*techniques d'usage permettant de les identifier (par exemple, User-Agent référençant une URL d'explication, reverse-DNS permettant de donner une origine claire à une adresse IP, etc).*

### VII.3.2. Documentation des actions de configuration

Les actions nécessaires pour respecter les différentes règles de sécurité (durcissement, configuration...) doivent figurer soit dans la documentation générale soit dans un document spécifique.

Le document doit être exhaustif de manière à permettre le remplacement d'un équipement en panne sans perte de niveau de cybersécurité.

### VII.3.3. Procédures d'installation, sauvegarde et restauration

Le titulaire fournira les supports (ou sources sécurisées) et les procédures et/ou scripts nécessaires à la sauvegarde, installation à partir de postes et serveurs non configurés, et restauration à partir des sauvegardes ; Toutes ces procédures, supports, manuels devront être les plus descriptifs et détaillés possible. Pour certaines tâches spécifiques et complexes, un support « vidéo » pourra être demandé au Titulaire lors des formations.

### VII.3.4. Inventaire et cartographie des livrables

Les documents ci-dessous devront être mis à jour au fur et à mesure des évolutions des installations afin qu'ils correspondent à la réalité des systèmes en fonctionnement, permettant ainsi les audits.

Une description fonctionnelle des installations, comprenant en particulier :

- Les noms et les fonctions des applications,
- Les lieux d'installation des équipements.

Un inventaire des biens, comprenant notamment :

- La liste des plages d'adresses IP des sous réseaux et des points de sortie des sites,
- La liste des serveurs, des postes de travail, des automates,
- La liste des équipements réseau et sécurité (routeurs, switches, pare-feu, etc.),
- La liste des dispositifs d'administration (équipements dédiés).

La description des configurations de chacun des composants.

- Fournisseur, modèle, niveau de micrologiciel / firmware.
- Le cas échéant URL permettant de récupérer des mises à jour
- Confirmation de désactivation des services inutiles
- Activation des fonctions de journalisation, protocole et événements journalisées
- Les dates d'obsolescence (fin de mise à disposition de mises à jour)
- Le cas échéant : ports ouverts inconnus, désactivation de services impossible, avec trace de l'accord de la DIR Est pour accepter les risques résiduels liés
- Les règles de filtrage éventuels, ou autre solution de sécurisation des communications

Un schéma d'architecture physique, comprenant :

- Les réseaux locaux,
- Les accès distants,



- Les interconnexions avec le réseau bureautique, Internet ou des réseaux tiers,
- Les routeurs et commutateurs réseau,
- Les accès d'administration.

Un schéma d'architecture logique représentant les flux avec le détail des protocoles.

- De préférence réalisée avec un outillage permettant de capter les flux réels (sondes réseaux adaptées) afin de s'assurer de l'exactitude des flux
- Des tests et audits pourront être réalisés durant la phase de mise en régime pour vérifier l'exactitude du schéma et des flux

Un inventaire des comptes, comprenant notamment :

- La description des profils utilisateurs ainsi que la liste de leurs droits sur le réseau industriel,
- La liste des comptes utilisateurs par profil, y compris les comptes d'administration,
- La liste des comptes de service.

### VII.3.5. Risques résiduels

La liste des exceptions aux règles (firmware pas à jour, fonctions non désactivables etc.), leur justification et l'accord de la DIR Est sont consignés dans ce document.

### VII.3.6. Comptes et mots de passe configurés

La liste des comptes et mots de passes configurés est fournie dans un conteneur [Keepass2](#) et le mot de passe du conteneur communiqué directement au responsable projet DIR Est.

### VII.3.7. Cahier de recette des fonctions de sécurité

Le cahier de recette des fonctions de sécurité doit permettre de vérifier tous les éléments de configuration et moyens techniques mis en œuvre. La plupart des points de contrôles sont des actions manuelles, par exemple :

- Vérification de la désactivation de comptes génériques, du fonctionnement avec un compte non administrateur,
- Vérification et test des autres points de durcissement : services désactivés, pas de logiciel inutile etc...
- Vérification de l'inventaire (modèles, versions...) via audit d'au moins un composant par type

Certaines actions devront être outillées, le cahier de recette précisera les outils à utiliser, le titulaire du marché devra effectuer les actions durant la recette sous le contrôle de la maîtrise d'ouvrage, et donc disposer des licences, équipements et compétences nécessaires.

- Test de génération de logs (utilisation d'un collecteur ad-hoc avant configuration du collecteur DIR Est)
- Scan d'équipements et du réseau pour vérifier l'inventaire, la cartographie et les risques résiduels pour la partie "ports ouverts" sur les équipements

### VII.3.8. Maintien en conditions de sécurité

Des actions de maintenance seront nécessaires afin de maintenir le niveau de cybersécurité de l'installation, et sont à décrire dans un document de "Maintien en conditions de sécurité".

Le document précise les actions à mener par le mainteneur afin de :

- Actions de mettre en place les mises à jour régulières préventives (ex : mise à jour des signatures anti-virus, des systèmes d'exploitation...) hors limitations éventuelles consignées dans le document risques résiduels
- Vérifier régulièrement (période à préciser) le bon fonctionnement des configurations de sécurité : journalisation, filtrage d'accès (le cas échéant)
- Vérifier le non-engorgement (ressources mémoires, processeur, disque)
- Vérifier régulièrement l'absence de vulnérabilités
  - Soit par consultation de sources à indiquer
  - Soit par exécution d'un outil en phase de maintenance (à préciser également)
- Auditer les comptes configurés et autres éléments de configuration
- Vérifier la cartographie, l'inventaire (y compris niveaux de firmware), les flux
- Revoir le document des risques résiduels et identifier de possibles solutions (équipement équivalent pouvant remplacer à fonctionnalité identiques, solution technique additionnelle...)

Ces actions seront réalisées au moins une fois durant la période de garantie de parfait achèvement.

## VII.4. CONTRÔLE DES FLUX – SEGMENTATION DU RÉSEAU

Il est demandé de fournir un inventaire détaillé (y compris modèles, versions logicielles exactes et firmware, absence de vulnérabilité publiquement connue) et cartographie des flux (quel équipement communique avec quel(s) autre(s), sens de connexion, protocole).

Ces éléments seront vérifiés lors de la recette par des moyens à discrétion de DIR Est.

Le projet de mise à jour de la GTC permet d'intégrer les actions nécessaires à une segmentation et contrôle de flux sur le réseau GTC dans un premier temps via les commutateurs installés pour connecter les équipements (eux-mêmes connectés aux switches du backbone) :

- Définition d'un nouveau plan d'adressage
- Configuration des nouveaux équipements / reconfiguration de l'existant en conséquence
- Acquisition/Configuration/Installation/Test des équipements
- Le contrôle d'accès par MAB doit permettre la communication uniquement avec les équipements locaux identifiés dans l'inventaire.

## VII.5. EXIGENCES CYBERSÉCURITÉ

Dans le contexte actuel, où la cybersécurité est devenue un enjeu stratégique majeur pour les centres de gestion du trafic, en particulier ceux gérant des ouvrages à tunnels, et face à l'augmentation des cybermenaces, il est crucial de mettre en place des mesures de protection robustes pour garantir la sécurité et la continuité des opérations.

Les exigences en matière de cybersécurité pour ces systèmes critiques sont encadrées par des réglementations nationales et européennes, telles que la directive NIS2, PSSI-E, RGPD, etc.

Ces normes visent à assurer l'intégrité, la confidentialité et la disponibilité des données et des systèmes de contrôle, tout en prenant en compte les spécificités du secteur routier et des tunnels. L'objectif est de mettre en œuvre des solutions techniques et organisationnelles adaptées pour prévenir, détecter et répondre efficacement aux incidents de sécurité, tout en maintenant la fluidité et la sécurité du trafic routier.

L'analyse réalisée en phase de diagnostic nous renseigne sur les exigences ou recommandations à prévoir lors de la conception des solutions soumises pour la rénovation du système GTC du CISGT Vauban, dont voici la liste détaillée ci-dessous :

DOMAINE	EXIGENCE OU RECOMMANDATION	SOURCE	NATURE
Capacité du candidat	Nomination d'un responsable sur le projet pour les sujets de cybersécurité (formé, expérimenté, idéalement avec certification)	Arrêté 18 sep	Obligatoire
Capacité du candidat	Gestion sécurisée des données projet : Hébergement obligatoire des données sensibles en France, accès contrôlé et limité aux intervenants sur le projet, traçabilité	PSSI-E	Obligatoire
Capacité du candidat	Antécédents en termes de cybersécurité : expérience de gestion des exigences sur projet similaire, indication des incidents passés	NIS2	Obligatoire
Capacité du candidat	Eventuelles certifications en sécurité de l'information de l'organisation ou de participants au projet	NIS2	Optionnel
Capacité du candidat	Existence d'une charte de sécurité informatique et d'une sensibilisation à la cybersécurité pour tous les intervenants (employés et autres). Formation pour les développeurs, chefs de projets...	NIS2	Obligatoire
Chaîne d'approvisionnement	Engagement à donner visibilité sur la chaîne de sous-traitance et à répercuter et garantir le respect des exigences présentes	NIS2 Arrêté 18 sep	Obligatoire
Chaîne d'approvisionnement	Produits labélisés ou certifiés : préférence pour des équipements et logiciels conformes aux standards européens de cybersécurité	NIS2	Si possible
Chaîne d'approvisionnement	Sélection de produit avec une durée de vie > 5 ans a minima pour les mises à jour de sécurité. o Engagement à signaler toute vulnérabilité découverte post-livraison et à fournir des solutions dans des délais contractuellement définis	NIS2, CRA	Obligatoire
Chaîne d'approvisionnement	Documentation technique : incluant liste des logiciels inclus, analyse de risque cybersécurité, déclaration claire période de support et mises à jour	CRA	Si possible
Chaîne d'approvisionnement	Les livrables ne doivent pas comporter de faille de sécurité connue et pouvoir être mis à jour	Arrêté 18 sep	Obligatoire
Chaîne d'approvisionnement	Les équipements doivent pouvoir générer des événements journalisable (logs, format syslog ou Windows)	NIS2	Préférence
Chaîne d'approvisionnement	Les réseaux et systèmes utilisés dans le cadre du projet (développement, test, programmation...) sont dédiés au travail sur le projet et ne sont pas également utilisés pour des activités de bureautique. Ils sont à jour de sécurité et dispose d'une solution anti-virus à jour	Arrêté 18 sep	Obligatoire
Chaîne d'approvisionnement	L'utilisation éventuel de média amovibles (clés USB etc...) est faite selon des règles de sécurité à préciser	NIS2	Obligatoire
Documentation et livrables	Les livrables doivent respecter l'état de l'art notamment en ce qui concernant la documentation (mesure de sécurités, flux...),	Arrêté 18 sep	Obligatoire

DOMAINE	EXIGENCE OU RECOMMANDATION	SOURCE	NATURE
	l'administration (consoles dédiées), les sauvegardes (3-2-1 : 3 copies, 2 technologies, 1 exemplaire hors site principal avec chiffrement),		
<b>Documentation et livrables</b>	Une documentation décrit les moyens d'assurer le maintien en condition de sécurité des livrables	Arrêté 18 sep	Obligatoire
<b>Documentation et livrables</b>	Les livrables incluent les éléments logiciels et procédures permettant d'effectuer des sauvegardes, ré-installation et restauration à partir des sauvegardes	NIS2	Obligatoire
<b>Documentation et livrables</b>	Le cahier de recette explicite les tests de cybersécurité permettant de vérifier le respect des exigences	PSSI-E	Obligatoire
<b>Documentation et livrables</b>	Analyse de risques et registre des risques résiduels	PSSI-E NIS2	
<b>Documentation et livrables</b>	Les équipements munis de système d'exploitation standards sont durcis comme préconisé par les bonnes pratiques de l'ANSSI, et le fonctionnement nominal (logiciels IHM, SCADA...) doit utiliser un compte sans privilège d'administration	NIS2	Obligatoire
<b>Documentation et livrables</b>	Un inventaire détaillé des composants livrés et une cartographie des flux est fournie et vérifiée lors de la recette	NIS2 Arrêté 18 sep	Obligatoire
<b>Sécurité du projet</b>	Un plan d'assurance sécurité est développé et soumis au client par le titulaire, et respecte l'état de l'art	Arrêté 18 sep	Obligatoire
<b>Sécurité du projet</b>	Le titulaire signale immédiatement tout incident de sécurité vi le responsable sécurité à celui du client. Les sous-traitants ont la même obligation	PSSI-E	Obligatoire
<b>Sécurité du projet</b>	Les titulaires peuvent être audités sans préavis pour vérifier le respect des clauses de cyber sécurité	Arrêté 18 sep	Obligatoire

Tableau 6 - Exigences ou recommandations cyber à prévoir pour la rénovation GTC du CISGT

La Maîtrise d'Ouvrage (MOA) a déjà mis en œuvre plusieurs mesures de cybersécurité et poursuit actuellement ses efforts dans ce domaine.

Néanmoins, l'entrepreneur aura la responsabilité de mener des vérifications et des contrôles approfondis pour s'assurer que les exigences et recommandations en matière de cybersécurité sont effectivement appliquées.

Concernant les exigences non encore satisfaites, il incombe à l'entrepreneur d'en informer la MOA et de collaborer étroitement avec elle pour suivre la mise en œuvre de ces actions cruciales en termes de cybersécurité.

Cette approche proactive et collaborative vise à garantir une protection optimale des systèmes et des données sensibles du centre de gestion de trafic et des ouvrages à tunnels.