



**1<sup>er</sup> RTP Quartier EDME**

**à Toulouse (31)**

**Construction d'un Magasin à munitions**



**Objet :**

**ANNEXE CYBERSECURITE DES SYSTEMES applicables au  
Système de supervision CADIVS  
Contrôle d'accès - détection intrusion - vidéosurveillance.**



**Architecture des systèmes de sécurité  
Système de supervision CADIVS  
Contrôle d'accès - détection intrusion - vidéosurveillance.**

Octobre 2024

Nombre de pages : 66

Edition du : 17 octobre 2024

1	INTRODUCTION .....	7
1.1	OBJET DU DOCUMENT.....	7
1.2	SYNTHESE DU BESOIN.....	8
1.3	ATTENDUS TECHNIQUES – EN RESUME .....	8
1.4	POINT D’ATTENTION .....	11
1.5	REMARQUES .....	11
2	PRESCRIPTIONS PRINCIPALES.....	12
2.1	DOSSIER D’OUVRAGE EXECUTE - DOE.....	12
2.2	ECHANGES ET MESSAGERIE ELECTRONIQUE .....	12
3	EXIGENCES APPLICABLES EN MATIERE DE CYBERSECURITE : REGLES GENERIQUES.....	13
3.1	INSTALLATION DES SYSTEMES .....	13
3.1.1	Stabilisation de l’exploitation .....	13
3.1.2	Compétences des intervenants.....	14
3.1.3	Certification des Editeurs de logiciel (CADIVS).....	15
3.2	ORGANISATION.....	15
3.3	PROPRIETE INTELLECTUELLE .....	15
3.4	DEVELOPPEMENT /INTEGRATION .....	16
3.5	TRAÇABILITE ET LIVRAISON .....	16
3.6	VEILLE .....	17
3.7	EXIGENCES RELATIVES AUX OUTILS ET A L'ENVIRONNEMENT DE DEVELOPPEMENT .....	17
3.8	MAQUETTES .....	17
3.9	INTERVENTION ET MISE EN OEUVRE .....	18
3.9.1	Moyens utilisés lors de la mise en œuvre .....	18
4	PERIMETRE TECHNIQUE CADIVS .....	19
4.1	PRESTATIONS ATTENDUES.....	19
4.1.1	Pour le système de CADIVS .....	19
4.1.2	Le système de protection Contrôle d’accès et Détection Intrusion (Synchronic).....	19
4.1.3	Supervision des alarmes et Gestion des catégories de variables.....	20
4.1.3.1	Précautions : .....	20
4.1.4	Le contrat de service .....	20
4.1.5	La cérémonie des clés : CADIVS – système et réseau .....	21
4.1.6	Serveur de Temps.....	21
4.1.7	Normes et règlements applicables.....	21
5	SPECIFICATIONS TECHNIQUES CADIVS.....	23

5.1	VIDEO SURVEILLANCE.....	23
5.1.1	Mode de fonctionnement attendu .....	23
5.1.1.1	Proposition des fonctions potentielles :.....	23
5.1.2	Centralisation du système.....	23
5.1.3	Fonctionnalités du système.....	23
5.1.4	Licences des logiciels utilisés.....	24
5.1.5	Stockeurs numériques.....	24
5.1.6	Capacité d'enregistrement.....	25
5.1.7	Scénario de pré-alarme .....	25
5.1.8	Exploitation.....	25
5.1.8.1	Dimensionnement serveur vidéosurveillance.....	25
5.1.8.2	Dimensionnement postes clients .....	25
5.1.8.3	Gestion de l'affichage .....	25
5.1.8.4	Ecrans de visualisation 42" .....	26
5.1.8.5	Supports d'écrans.....	26
5.1.8.6	Mosaïques préprogrammées .....	26
5.1.8.7	Joystick .....	26
5.1.8.8	Recherche synchronisée.....	27
5.1.9	Gestion graphique .....	27
5.1.9.1	Niveaux de plans .....	27
5.1.9.2	Etats des symboles dynamiques.....	27
5.1.9.3	Bandeau d'alarmes.....	27
5.1.10	Droits utilisateurs .....	27
5.1.10.1	Matrice de droits utilisateurs .....	27
5.1.11	Implantation des caméras.....	28
5.1.11.1	Emplacement des caméras.....	28
5.1.11.2	Pose sur mâts .....	28
5.1.11.3	VRD .....	29
5.1.12	Politique de sécurisation des connexions IP .....	29
5.1.12.1	Contraintes .....	29
5.1.12.2	Cérémonie des clés.....	30
5.2	DETECTION INTRUSION .....	30
5.2.1	Centralisation et supervision.....	30
5.2.1.1	Centralisation .....	30

5.2.1.1.1	Centrale de détection intrusion .....	30
5.2.1.1.2	Claviers de commande .....	30
5.2.1.1.3	Alimentations complémentaires .....	31
5.2.1.1.4	Fonctionnalités .....	31
5.2.1.2	Supervision .....	32
5.2.1.2.1	Interfaces homme/machine .....	32
5.2.1.2.2	Matrice des droits .....	32
5.2.1.2.3	Serveur d'exploitation (logiciel CADIVS principal) .....	33
5.2.1.2.4	Serveur de servitudes .....	33
5.2.1.2.5	Postes clients .....	33
5.2.1.2.6	Disque dur externe .....	33
5.2.1.3	Interface avec le système de vidéosurveillance .....	33
5.2.2	Détection bâtiminaire .....	34
5.2.2.1	Avant-propos .....	34
5.2.2.2	Implantation des équipements .....	34
5.2.2.3	Politique générique d'implantation des détecteurs .....	34
5.2.2.4	Implantation des équipements de centralisation .....	34
5.2.2.5	Détecteurs bi-technologie circulaire .....	34
5.2.2.6	Détecteurs infrarouge linéaire .....	35
5.2.2.7	Détecteurs bi-technologie linéaire .....	35
5.2.2.8	Détecteurs d'ouverture .....	35
5.2.2.9	Marquage des câbles et codes couleurs .....	36
5.2.2.10	Chemins de câbles .....	36
5.3	LE CONTROLE D'ACCES .....	36
5.3.1	Les accès au réseau : paramétrage des switchs .....	36
5.3.2	Procédures et responsabilités liées à l'exploitation .....	37
5.4	RESEAU SURETE .....	37
5.4.1	Architecture technique .....	37
5.4.1.1.1	Architecture attendue .....	37
5.4.1.1.2	Liens entre les locaux .....	37
5.5	ALIMENTATION .....	38
5.5.1	Alimentation régulée – Source d'alimentation .....	38
6	SECURISATION DU CŒUR DE SYSTEME .....	39
6.1	ANNUAIRE CENTRALISE : AD+ GPO .....	39

6.1.1	Protection centralisée du système CADIVS - comptes et accès .....	39
6.1.1.1	Rappel de mise en œuvre .....	39
6.1.2	Les sauvegardes.....	40
6.1.3	Les restaurations .....	40
6.2	LA PLATEFORME D'HEBERGEMENT .....	41
6.2.1	Les serveurs d'application et d'administration .....	41
6.3	L'ARCHITECTURE RESEAU .....	42
6.3.1	Internet.....	42
6.3.2	Interfaçage autres systèmes .....	42
6.3.3	Les switches ou commutateurs réseau .....	42
6.3.3.1	La liste des équipements (Carte d'identité) .....	43
6.3.3.2	Les VlanS .....	43
6.3.3.3	Les fonctionnalités .....	44
6.3.3.3.1	Fonctionnalités de sécurité nécessaires.....	44
6.3.3.3.2	Fonctionnalités de redondance.....	44
6.3.3.3.3	QoS « Quality of Service » .....	44
6.3.3.3.4	Fonctionnalités supplémentaires .....	44
6.3.3.3.5	Fonctionnalités de management de la consommation.....	45
6.3.3.4	Qualification de l'infrastructure de câblage.....	45
6.3.3.5	Surveillance des switches .....	45
6.3.3.6	Les MacAdress .....	45
6.4	LA LIAISON FIBRES OPTIQUES .....	45
6.4.1.1	Les Têtes optiques : soudées.....	46
6.4.1.1.1	La soudure fibre optique ou épissurage par fusion .....	46
6.4.2	Caractérisation des liaisons Fibres optiques .....	46
6.4.3	Spécifications des têtes de câbles optiques .....	47
6.4.3.1	Spécifications des connecteurs optiques et épissures .....	48
6.4.3.2	Spécifications des jarretières optiques .....	48
6.4.4	Qualification de l'infrastructure de câblage.....	49
6.4.4.1	Validation du réseau fibres optiques .....	49
6.5	LA BAIE D'HEBERGEMENT SERVEURS ET RESEAU .....	49
6.5.1	Équipement électrique des baies et coffrets .....	50
6.5.2	Sécurisation des liaisons.....	51
6.6	REPORTS DES ALARMES ET GESTION DE CONFIGURATION.....	51

6.6.1	Borniers d'interconnexion et de prise d'informations alarmes .....	51
6.6.2	Pré Requis au déroulement des reports d'alarmes.....	51
6.6.3	Tests unitaires .....	52
6.6.4	Essais transverses .....	52
6.6.5	Livrables attendus .....	53
6.7	CABLES MULTIPAIRES DE LIAISON .....	53
6.8	COMPATIBILITE ELECTROMAGNETIQUE « CEM » .....	54
6.9	LA FORMATION .....	55
7	DOCUMENTS A FOURNIR PAR LE TITULAIRE DU MARCHE.....	56
7.1	FOURNITURE DES FICHES TECHNIQUES.....	57
8	RECEPTION DES PRESTATIONS .....	59
9	ASSURANCE QUALITE .....	60
9.1	SYSTEME QUALITE .....	60
10	VERIFICATION DES INSTALLATIONS, ESSAIS ET MESURES.....	61
11	NETTOYAGE ET PROTECTION DES OUVRAGES .....	62
11.1	TRI ET EVACUATION DES DECHETS .....	62
12	DOCUMENTS APPLICABLES ET DOCUMENTS DE REFERENCE .....	63
12.1	DOCUMENTS TECHNIQUES APPLICABLES AU MARCHE .....	63
12.2	LIVRABLES ATTENDUS.....	63
13	ANNEXE 1 : MATRICE DE COMPETENCES .....	64
14	ANNEXE 2 : TAUX HORAIRES .....	66

# 1 INTRODUCTION

---

## 1.1 OBJET DU DOCUMENT

Ce document décrit les exigences techniques et organisationnelles liées à la fourniture et à l'installation des équipements matériels et logiciels pour le CADIVS<sup>1</sup>, les alarmes techniques diverses, ainsi que les principales mesures à mettre en œuvre dans le cadre du projet, afin de respecter les règles de la Cybersécurité et de l'hygiène informatique.

**NB :** *Le contrôle d'accès, en termes de lecteurs de badges de fourniture de badges, n'est pas à activer. Il n'est donc pas à prendre en compte au titre de ce cahier des charges.*

Le périmètre concerné intègre tous les équipements liés aux solutions techniques et informatiques installées au titre des systèmes de sécurisation du **Magasin à munitions** construit sur l'emprise du 1er régiment du train parachutiste - Quartier EDME à Toulouse (31).

En synthèse, tout équipement faisant appel à un système de gestion informatique, nécessitant une communication interne et/ou vers un système de remontée d'information ou une centralisation des alarmes, devra respecter les préconisations décrites au sein de l'annexe.

Sont concernés :

- Le contrôle des accès : (pas de lecteur supplémentaire au titre de ce marché)
- La détection intrusion,
- La vidéosurveillance,
- La Téléphonie et l'Interphonie
- La détection incendie : les reports d'alarmes sur l'hyperviseur des systèmes ci-dessus sont exclusivement en contacts secs

La liste n'est pas exhaustive

Ces installations sont liées au domaine technique et aux servitudes des bâtiments concernés par les travaux. Elles sont totalement indépendantes des prestations destinées à l'usage de l'informatique de la DIRISI.

**En cas de sujet évoqué doublement, dans le CCTP et dans la présente annexe, c'est la présente annexe qui devra être suivie. Les informations ne devraient jamais être contradictoires, toutefois, si cela était le cas, le candidat devra lever le doute en posant la question auprès du MOE/MOA. Les délais sont précisés dans le règlement de la consultation.**

---

<sup>1</sup> CADIVS : Contrôle d'accès, Détection Intrusion et vidéosurveillance. Hypervision incluse.

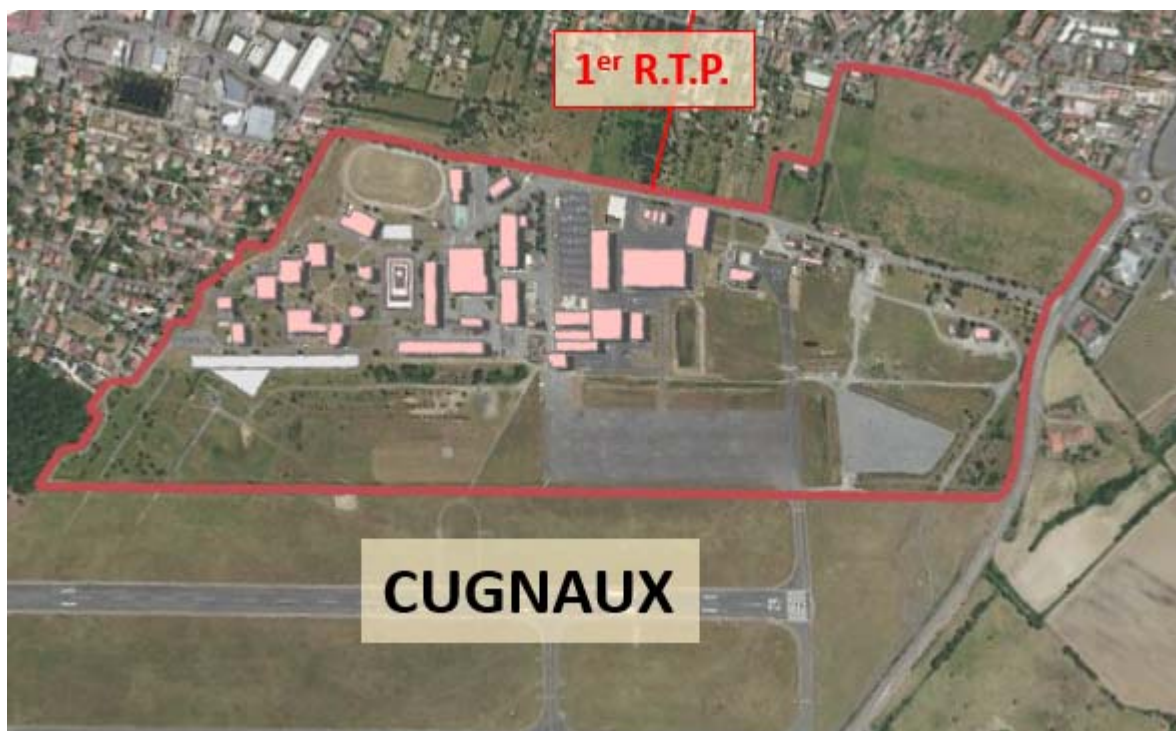
## 1.2 SYNTHÈSE DU BESOIN

Le Magasin à munitions devra être équipé de détection intrusion :

- La **détection intrusion** devra être raccordée au système de supervision existant (SYNCHRONIC), mais ce la solution logicielle devra avoir été mise-à-jour et réorganisée au préalable.
- Le système gère actuellement l'ensemble du contrôle d'accès et de la détection intrusion du site, la supervision Horizon (SYNCHRONIC) gère l'ensemble.

Le Magasin à munitions devra être équipé de vidéo surveillance.

En revanche, la vidéo surveillance existante ne doit pas être modifiée, les nouvelles caméras ne devront pas être ajoutée à ce système. C'est donc, un tout nouveau système qui devra être installé dans les règles de l'ANSSI.



## 1.3 ATTENDUS TECHNIQUES – EN RESUME

Dans le cadre de la construction du magasin à munitions, un nouveau système est à fournir pour la VS, et le système CADI existant doit être mis à jour et réorganisé selon le bref résumé ci-dessous :

- 1 système de vidéo surveillance :
  - Ce système et son environnement complet (réseau – caméra – cœur de système, etc) sont à fournir, installer et paramétrer dans son intégralité
  - Aucune liaison ne doit être effectuée avec le VMS actuellement en exploitation, pas de liaison physique ou logicielle ou de réseau. Le nouveau système de vidéosurveillance doit être autonome, totalement indépendant de l'ancien.



- Cependant, et si nécessaire, les câbles (optiques ou Ethernet) pourront cheminer dans les mêmes fourreaux ou chemins de câbles, mais sans connexion commune.
- Fourniture et installation d'un serveur et son unité de stockage et d'un PC client, dédiés au nouveau VMS
  - 1 mise à jour du système de Contrôle d'accès, Détection intrusion et sa supervision graphique de centralisation des alarmes.
    - Mise à jour Logicielle des logiciels Horizon et PC PASS – SYNCHRONIC (version actuelle mise en jour en 2022).
    - Fourniture et installation d'un serveur dédié SYNCHRONIC (CADI + supervision)
    - Bascule des licences d'exploitation, des données depuis la machine actuelle (ancien PC) et réinstallation sur le nouveau serveur d'exploitation à fournir (DC1).
    - Migration de l'ensemble des données et alarmes Synchronic sur le nouveau serveur. *Attention, la cartographie de l'hyperviseur devra être mise à jour, le fond de plan actuel modifié avec l'ajout du Magasin à munitions et toutes les alarmes activées (+/- 2500 opérationnelles)*
    - Fourniture et installation d'un second serveur (DC2) pour Active Directory – Antivirus Server – Sauvegarde -- (AD/AV/Backup)
    - Fourniture et installation d'un disque dur externe pour double hébergement des sauvegardes
  - Fourniture et installation d'une baie serveurs, équipée de contacts de porte sur tous les ouvrants (câblage en série accepté).
    - La dimension de la baie sera adaptée aux équipements, comme par exemple :
      - Tiroir optique
      - Switchs
      - Serveur Exploitation
      - Serveur AD/AV/Backup
      - Serveur VMS
      - Serveur stockage vidéo
      - Onduleur de baie
      - Bandeau de prises
      - ...
      - Le disque dur externe sera connecté au réseau, mais installé dans un autre bâtiment.
  - Fourniture et installation d'un nouveau réseau de communication :
    - Tous les switchs existants (leur nombre est estimé à 4) sur l'ancien réseau sont à remplacer pour pouvoir supporter les niveaux 2 et 3 et le management du réseau (vlans MacAdress, gestion des ports, etc). Ces switchs sont dédiés exclusivement au CADIVS.
    - Une période de visite des équipements permettra de s'assurer du nombre, en début de marché, si nécessaire.

- Les switchs existants pourront être conservés dans le cas où d'autres connexions « exotiques » ont été raccordées, mais les nouveaux switchs dédiés au CADI devront être installés à proximité, dans les mêmes coffrets, si possible.
  - Les ports utilisés pour les alarmes existantes devront être reconnectés dans les bons Vlan (CA ou DI), sur les nouveaux switchs.
- Le contrôle d'accès doit être migré sur le nouveau serveur, mais puisqu'aucun lecteur de badge n'est à ajouté à l'existant, aucune rupture d'exploitation ni modification n'est à faire sur le système.

De manière synthétique, le Magasin à munitions construit sur l'emprise devra être équipé de la manière suivante (**les quantités seront précisées ultérieurement**) :

- Téléphonie :
  - Un téléphone d'alerte en circulation centrale ;
- Incendie :
  - Une alarme incendie positionnée en local technique avec report au poste de sécurité ;
  - 17 détecteurs de fumée ;
  - 2 déclencheurs manuels.
- Détection intrusion :
  - Une alarme positionnée en local technique avec report au poste de sécurité ;
  - 17 détecteurs volumétriques ;
  - 18 détecteurs d'ouverture de portes magnétiques ;
  - 18 voyants lumineux témoins d'état d'alarme ;
  - 18 claviers à code activation/désactivation alarme.
- Vidéosurveillance :
  - 2 caméras de vidéosurveillance ;
  - Ecran + enregistreur, déportés au poste de sécurité.
- Le cœur de système, la baies, les serveurs, etc devront être installés dans le **bâtiment 18 (OPC)**.
  - le positionnement de la baie et les arrivées de câbles seront à définir ultérieurement, après vérification des cheminements et de l'occupation du lieu choisi ; il faudra éviter les nuisances sonores.
- Les PC clients seront distribués comme suit :
  - Vidéosurveillance :
    - 1 PC/écran 42" au PAF (Poste de contrôle des accès) – entrée du site
    - 1 PC/écran 42" au service OPC – Bât 18
  - Contrôle d'accès – détection intrusion et supervision CADI :
    - 1 PC/écran au PAF (Poste de contrôle des accès) – entrée du site
    - 1 PC/écran au service OPC – Bât 18
    - 1 PC/écran au service SG – Bât 17

- Un pc portable, dédié à la maintenance (MCO/MCS) devra être fourni , paramétré et livré au maitre d'ouvrage. Il sera conservé sur site, dans l'armoire forte du C2 et sera mis à disposition du prestataire de maintenance. Aucune machine extérieure ne devra être connectée au réseau du site.

Au terme de l'installation, le système CADI sera hébergé sur un cœur de système autonome, secouru et sauvegardé. Son réseau IP dédié totalement intégré au présent marché, sera autonome (isolé du Net et autres systèmes), protégé de toute intrusion, contrôlé et managé. Ce système d'exploitation bénéficiera de ses propres servitudes : authentification, antivirus, sauvegarde locale et exportée (NAS) sur le réseau et secouru électriquement.

Les 2 nouvelles caméras devront être gérées par leur propre système autonome et indépendantes du VMS existant.

Il n'y aura aucun lien entre les systèmes et réseau IP existants sur site avec le système CADI demandé et son réseau.

Les liens filaires seront à installer au titre de ce marché, et totalement dédiés (fibres optiques et câbles Ethernet).

Les liens Wifi et/ou Internet sont à proscrire.

#### 1.4 POINT D'ATTENTION

Ces installations sont liées à la sécurisation du Magasin à Munitions et au périmètre technique affairant (locaux techniques et poste de contrôle). Elles sont totalement indépendantes des prestations décrites pour l'usage de l'informatique de la DIRISI.

**En cas de sujet évoqué doublement, dans le CCTP et dans le présent chapitre, c'est le présent chapitre qui devra être suivi. Les informations ne devraient jamais être contradictoires, toutefois, si cela était le cas, le candidat devra lever le doute en posant la question auprès du MOE/MOA. Les délais sont précisés dans le règlement de la consultation.**

#### 1.5 REMARQUES

**R1** : les locaux techniques décrits par la DIRISI sont à l'usage exclusif de la DIRISI. Les systèmes liés aux solutions techniques et de sureté (CADIVS) installées au titre de ce projet, devront être installés dans des locaux indépendants des LTI de ceux de la DIRISI.

**R2** : Aucune maintenance à distance ne devra être effectuée, aucun accès distant ne sera accepté sur tout ou partie du système, l'usage des réseaux hertziens est à proscrire.

**R3** : Le réseau informatique dédié à la communication des solutions techniques devra être totalement indépendant des réseaux installés pour la DIRISI, physiquement et logiquement.

## 2 PRESCRIPTIONS PRINCIPALES

---

### 2.1 DOSSIER D'OUVRAGE EXECUTE - DOE

Il sera fourni le dossier complet d'ouvrage exécuté pour les CADIVS installés. La fourniture au format BIM des plans et annexe au format BIM est à privilégier.

Les documents attendus sont :

**A fournir avant LA PERIODE DE PREPARATION, puis au terme du marché en version TQC<sup>2</sup>.**

- Tous les plans et schémas de raccordement des installations
- **Le document des spécifications techniques,**
- **Le document des spécifications fonctionnelles,**
- Le planning d'intervention,
- Le planning des tâches en y incorporant la constitution de la maquette (si nécessaire), les essais et la mise en service provisoire de réception des installations et de levée des réserves,
- Le plan de prévention,
- Le Dossier d'Assurance Qualité,
- Le plan de Management Qualité,
- Le « plan qualité » logiciel,
- La liste prévisionnelle des documents et plans.

Les documents réalisés par le titulaire respecteront le formalisme et les règles d'identification données en vigueur.

Ils seront rédigés exclusivement en français.

Ils seront aussi remis sous format informatique, compatible avec les logiciels utilisés

### 2.2 ECHANGES ET MESSAGERIE ELECTRONIQUE

Tous les plans et documents portant des informations de configurations ou autre plan de situation ou de câblage devront être envoyés sous conteneur crypté à l'aide des logiciels de chiffrement ACID de préférence, ou ZED! PRO (Version Free exclue), si la messagerie électronique est utilisée.

A défaut, ils seront livrés au format papier et sur support de masse (clé USB), en main propre ou envoyés par la Poste.

Aucun document, décrivant toute ou partie de la solution CADIVS et plus largement des systèmes installés au titre de ce marché, ne devra transiter en clair sur les messageries des prestataires. Seule la messagerie de la Maitrise d'ouvrage (Intredef) est libre de ses échanges.

---

<sup>2</sup> TQC : Tel Que Construit

### 3 EXIGENCES APPLICABLES EN MATIERE DE CYBERSECURITE : REGLES GENERIQUES

---

Les exigences s'appliquent, de manière générique, à tous les systèmes de gestion inclus au projet.

Toutes les configurations, fonctionnalités et précisions techniques décrites dans ce document doivent être impérativement fournies, paramétrées et mises en service.

Pour assurer une cohérence par rapport au besoin du MOA, une période de collecte des besoins, en termes de fonctionnalités et de droits d'usage, devra être prévue, effectuée, documentée et faire l'objet d'un livrable détaillé.

#### 3.1 INSTALLATION DES SYSTEMES

Il est impératif que tous les travaux d'installation et paramétrage des solutions de sureté soient effectués par du personnel habilité (CD pour le cœur du système : réseau IP et Serveurs). Chaque modification devra faire l'objet d'une description détaillée dans le livrable que devra fournir le titulaire : « **Spécifications techniques et fonctionnelles détaillées** ».

##### 3.1.1 Stabilisation de l'exploitation

Les consoles de programmation seront dédiées à l'installation, ainsi qu'à la maintenance future. Les consoles de programmation devront être soutenues et maintenues (MCO et MCS) par le titulaire du futur marché de maintenance. Aucun poste de travail, provenant d'intervenants extérieurs ne devra être connecté sur l'architecture objet du présent marché. Ceci inclut les commutateurs réseaux, routeur, passerelle de communication, les serveurs, les PC, les UTL, les automates, etc.

En cas d'intervention pendant toute la durée du marché et dans sa période de GPA (Garantie de parfait achèvement), des tests de non régression devront être effectués au préalable. Ils permettront de vérifier que des modifications n'altéreront pas le fonctionnement des applications, ainsi que de l'hypervision.

Ces tests pourront être effectués sur une plateforme de tests dans les locaux du prestataire (s'il en dispose), mais sans aucune donnée de la MOA. Une procédure devra être présentée au MOA en amont de toute action sur son site, précisant la marche à suivre, les risques et les délais pour recouvrer le point nominal de l'exploitation, y compris les phases de sauvegarde/restauration.

Le titulaire devra expliciter la mise en œuvre des processus afin de maintenir (maintenance préventive et corrective), de rétablir (maintenance curative) les systèmes et ce, pendant toute la durée du marché ainsi que dans sa période de GPA.

La solution complète, ainsi que chacun des systèmes qui la compose, devra être conservée dans un état opérationnel et sécurisé.

Ces prestations comprennent :

- Les interventions curatives (premier niveau) : remplacement des équipements en panne, redémarrage des applications, etc. ;
- Les interventions de maintenance corrective ;
- Les interventions pour des modifications mineures ;
- Les interventions au titre de la MCO (maintien en condition opérationnelle) et de la MCS (maintien en condition de sécurité) qui feront l'objet d'un autre marché.
- La gestion des obsolescences matériels et logiciels.

Chacun des systèmes installés ne devra pas avoir d'état stable de non fonctionnement.

### 3.1.2 Compétences des intervenants

Le marché fait appel à différents métiers, et donc des profils de compétences différents :

- Informaticien : Réseau et Serveur, système et base de données
- CADIVS : compétences en installation et paramétrage des équipement et de la solution d'hypervision.
- Electricien
- Climaticien
- Et tout autre nécessaire à la réalisation de cette opération.

**Les candidats devront fournir les « CV professionnels » des personnes destinées à intervenir. Ces documents devront faire apparaître les références et compétences acquises.**

**Les intervenants devront être habilités CD (Confidentiel Défense) lorsque le marché sera référencé Diffusion Restreinte et/ou lorsque qu'ils devront intervenir sur l'hyperviseur de sécurité (CADIVS<sup>3</sup>).**

**Le tableau « Matrice des Compétences » fourni en annexe devra être complété.**

L'objectif de cette matrice étant d'assurer la MOA que le salarié de l'entreprise intervenant sur le système dispose bien des compétences pour agir. Il s'agit ici de vérifier les aptitudes des personnes. En effet, l'entreprise peut posséder le savoir-faire en tant que « Personne Morale », mais l'intervenant devra être identifié personnellement comme porteur de la formation ou de la compétence.

Chaque rôle du prestataire sera identifié en tant que « Profil » et ses compétences, sa maîtrise seront désignées par une croix dans le tableau, sur la ligne correspondant à sa compétence. Ce tableau n'est pas exhaustif, il peut être amendé selon le besoin, selon les logiciels et les produits proposés par le Titulaire.

---

<sup>3</sup> CADIVS = Contrôle d'accès, détection intrusion et vidéosurveillance

### 3.1.3 Certification des Editeurs de logiciel (CADIVS)

Le candidat au présent marché devra être impérativement être partenaire certifié par l'entreprise éditeur du logiciel, et ce pour chaque solution proposée. Son niveau de compétence doit lui permettre de maîtriser l'ensemble de la solution physique (modules et composants) et logicielle (paramétrage et programmation) afin d'intervenir de manière sécurisée sur la plateforme en exploitation.

S'agissant de respecter des bonnes pratiques d'une architecture sécurisée, le niveau de certification délivrée par l'Editeur doit correspondre au niveau exigé.

S'agissant de Serveurs et de PC sous environnement Windows, une certification de type MCSE sera appréciée.

*La certification Microsoft Certified Solutions Expert (MCSE) atteste que le titulaire disposera de l'expertise nécessaire dans les domaines suivants : gestion des identités, gestion des systèmes, virtualisation, stockage et mise en réseau.*

## 3.2 ORGANISATION

Le prestataire doit fournir un descriptif de l'organisation de son activité d'intégration et de maintenance en termes de cybersécurité. Ce descriptif devra intégrer la communication au sein de l'entreprise, ainsi que le stockage des données numériques et papier.

Il doit mettre en place une chaîne de responsabilité de la cybersécurité pour les besoins de ses prestations. En particulier, il doit définir un point de contact pour la cybersécurité lors de la prestation, qui sera en charge de la liaison avec la chaîne de responsabilité du MOA/MOE, de la garantie du respect de la politique de cybersécurité,

Il devra accepter les audits demandés par le MOE/MOA, au sein de son entreprise et ou que soit son activité de développement. L'objectif étant de vérifier que toutes les mesures de cybersécurité demandées contractuellement sont bien appliquées.

Il doit fournir au commanditaire un Plan d'Assurance Sécurité (PAS) pour les prestations qu'il effectue, détaillant la prise en compte des aspects liés à la cybersécurité lors des différentes actions d'intégration et d'intervention qu'il effectue tout au long du marché.

## 3.3 PROPRIETE INTELLECTUELLE

La propriété intellectuelle, et en particulier, celle des codes sources développés ou intégrés par le prestataire pour les systèmes mis en place (CADIVS) resteront la propriété entière du MOA.

Le Titulaire s'engagera à supprimer de ses machines et de son entreprise de manière globale toutes traces informatiques ou édition de ses développements, paramétrage, mots de passe et autres outils, qui pourraient permettre d'avoir accès au système installé, au terme du marché.

L'ensemble de ces éléments devra être fourni sous double enveloppe cachetée à la direction du Maître d'Ouvrage, ou à son représentant, sur support informatique (USB) et dossier papier.

De manière générale, l'ensemble des documents relatifs à la conception, à la configuration ou au fonctionnement du système doivent être considérés de niveau « Diffusion Restreinte ». C'est l'ESID qui apposera la mention de protection sur les documents. Ils porteront au préalable la mention « Document de Travail ».

### 3.4 DEVELOPPEMENT /INTEGRATION

Les caractéristiques de cybersécurité des équipements ainsi que leurs certifications doivent rester un critère de choix dans le processus d'achat du titulaire. Il pourra s'appuyer sur les profils de protection publiés sur le site de l'ANSSI (<http://www.ssi.gouv.fr>).

Le titulaire doit soumettre à la validation du MOE la liste et les caractéristiques de l'ensemble des équipements qui seront intégrés sur le site.

**Une « fiche produit » type (une page A4) sera fournie pour description des matériels. Elles devront être validées AVANT APPROVISIONNEMENT. Ces « fiches produits », accompagnées de la fiche technique du fabricant, feront l'objet d'une liste et intégrées au DOE.**

Dans tous les cas, le titulaire devra effectuer des tests de robustesse, pour les développements et paramétrage qu'il réalise. L'objectif est de vérifier la qualité des développements et l'absence de bugs « élémentaires » régulièrement utilisés lors d'attaques informatique (débordement de pile « buffer overflow », par exemple).

Le titulaire devra prévoir la création de comptes personnels, associés à des droits spécifiques (Entreprise, Administrateur, Utilisateur) pour permettre la traçabilité des actions sur les logiciels qu'il installe (GTC, CADIVS, SSI etc). Il devra également prévoir de mettre en place une gestion des comptes utilisateur, ainsi que le verrouillage après 3 tentatives infructueuses. Les mots de passe devront être complexes (14 caractères : majuscules, minuscules, chiffres, caractères spéciaux) et changés tous les 90 jours, au plus tard.

Ces paramètres seront modifiés et précisés par la Maitrise d'Ouvrage au moment de l'installation.

Si l'usage des comptes de service avec des droits à privilèges est imposé par l'application « métier », ils ne devront être accessibles qu'au travers d'une application de rebond avec un login nominatif permettant de maintenir l'exigence d'imputabilité. Aucun compte de service ne devra avoir de droit administrateur de domaine.

Tous les mots de passe d'origine, de tous les outils de gestion, des systèmes et des équipements industriels, doivent être changés au profit de nouveaux. **Ceux-ci seront fournis au MOA sous enveloppe cachetée à la réception du marché, au terme de la « Cérémonie des Clés », moment privilégié du changement de tous les mots de passe, à la livraison de la solution CADIVS installée et de ses servitudes.**

### 3.5 TRAÇABILITE ET LIVRAISON

Le titulaire doit garantir, dans son processus de livraison, l'intégrité et l'authenticité de l'ensemble des logiciels, programmes, éléments de configuration et documentation. Les éléments concernés sont en particulier : les micrologiciels, les systèmes d'exploitation, les progiciels SCADA et autres logiciels



utilisés pour le CADIVS, les programmes d'automates et de SCADA, les fichiers de configuration des équipements réseau, les mises à jour, etc.

Le titulaire doit être en mesure de garantir la confidentialité des éléments précédents si le MOE/MOA en fait la demande. La confidentialité des éléments de configuration sera systématiquement assurée

### 3.6 VEILLE

Le titulaire doit mettre en œuvre un processus de veille sur l'évolution des moyens techniques pour renforcer le niveau de cybersécurité des systèmes industriels, tout au long du marché.

En cas de d'alerte Cybersécurité ANSSI concernant les équipements installés, des mesures de protection seront immédiatement mises en œuvre. Le MOA/MOE sera informé en amont et tout au long du processus, des risques et actions correctives choisies.

### 3.7 EXIGENCES RELATIVES AUX OUTILS ET A L'ENVIRONNEMENT DE DEVELOPPEMENT

Si le titulaire doit développer au sein de son entreprise, ou ailleurs que sur le site, il doit utiliser un environnement de développement sécurisé, afin que celui-ci ne soit pas le point d'entrée pour atteindre les systèmes (par l'insertion de codes malveillants par exemple). Il devra dédier des locaux physiques pour le développement. Le mécanisme de contrôle d'accès doit permettre de tracer l'identité des personnes y pénétrant et l'heure d'accès.

Le titulaire doit également veiller à la protection des documents au format papier utilisés dans le cadre de sa prestation. Les éditions ne devront pas pouvoir être lancées puis oubliées sur une imprimante réseau partagée. Les éditions seront donc contrôlées par le prestataire, en interne.

L'environnement de développement devra être dédié et séparé des autres environnements informatiques du titulaire. En particulier, cet environnement ne doit pas être connecté à internet ni directement (sans filtrage et mesures de sécurité) au réseau bureautique de son entreprise.

Le niveau de sécurité de l'environnement de développement pourra être vérifié par des audits (organisationnels et techniques) réguliers, effectués par le MOA/MOE, au sein de l'entreprise du Titulaire.

Ces mesures intègrent les plateformes de tests et d'intégration

### 3.8 MAQUETTES

Si le titulaire le souhaite, il pourra réaliser une maquette pour valider la migration des systèmes, par exemple et pour valider le bon fonctionnement des installations et réaliser. Dans ce cas, une pré-réception technique basée sur un cahier de tests qui sera rédigé et proposé par le titulaire est à prévoir. Le lieu (protégé) de cette maquette sera déterminée au lancement du marché.

Les tests proposés pourraient ainsi permettre de vérifier le maximum des capacités techniques prévues (réseau, serveurs etc), ainsi que les fonctionnalités principales du CADIVS.

Seule la validation de la maquette par la MOA et le MOE permettra alors d'obtenir l'aval pour son installation sur le site. La majorité des équipements seront donc à paramétrer comme in fine.

### 3.9 INTERVENTION ET MISE EN OEUVRE

Les prestations sur le périmètre du 1<sup>er</sup> RTP devront être organisées et planifiées et ceci pour tous les intervenants réalisant des activités de mise en service (Titulaire, sous-traitants, etc) au titre de ce marché.

- Ils doivent être individuellement clairement identifiés et leurs rôles précisés.
- L'accès aux installations doit être validé par le MOE/MOA.
- Les intervenants doivent respecter les règles de cybersécurité exigées par le MOE/MOA et s'être assurés qu'un protocole d'intervention, identifié dans un permis ou bon de travail par exemple, a bien été validé par les deux parties.
- Aucune intervention non planifiée, non validée par le MOE/MOA en amont de l'intervention ne sera acceptée.

#### 3.9.1 Moyens utilisés lors de la mise en œuvre

Les interventions sur l'installation du 1<sup>er</sup> RTP doivent être réalisées avec des outils validés.

L'ensemble des équipements matériels et logiciels utilisés pour les interventions sur les systèmes objet du présent marché (comme les consoles de programmation) doit être recensé afin d'être bien identifié pour faciliter leur maintien en condition de sécurité.

Les équipements utilisés doivent être exclusivement dédiés aux systèmes industriels (pas de bureautique).

En cas de besoin particulier, suite à un incident (de cybersécurité ou autres) par exemple nécessitant l'utilisation d'outils spécifiques non identifiés parmi les outils habituels, l'intervenant doit être en mesure d'analyser, avec le MOE/MOA, les risques liés à leur utilisation et de mettre en œuvre les mesures pour traiter ces risques.

Ces interventions feront l'objet d'un rapport d'intervention immédiat.

Les coordonnées du point de contact du SID seront transmises au titulaire, en début de marché.

## 4 PERIMETRE TECHNIQUE CADIVS

Chacun des items est applicable aux 2 systèmes, dans son domaine professionnel bien entendu.

### 4.1 PRESTATIONS ATTENDUES

#### 4.1.1 Pour le système de CADIVS

Mise à jour de la version du système de contrôle des accès, de détection intrusion et migration de l'ensemble sur la plateforme des serveurs d'exploitation et de servitudes (ordre des actions à définir par le titulaire), mise en place du management réseau : réseau, administration système, filtrage et contrôle. Aucune migration de la partie vidéo existante.

Le Titulaire prévoira dans son offre tous les matériels, licence des logiciels, serveurs et PC Client permettant de fournir une solution complète, contrôlée, protégée et pérenne :

- |   |                 |
|---|-----------------|
| ➤ Mise à jour du Logiciel d'hypervision, de CA-DI | → serveur « A » |
| ➤ Antivirus Sauvegarde AD                         | → serveur « B » |
| ➤ Serveur dédié à l'application VMS               | → serveur « C » |
| ➤ Stockage vidéo (30 jours- 2 caméras – FIFO°     | → serveur « D » |

#### 4.1.2 Le système de protection Contrôle d'accès et Détection Intrusion (Synchronic)

Il n'y a pas d'adjonction au contrôle d'accès PcPass Evolution (SYNCHRONIC) prévu au titre de ce marché, aucun lecteur de badge n'est à ajouter. Seule une mise à jour de la licence serveur et clients, ainsi qu'une migration depuis la machine actuelle, vers le nouveau serveur dédié à fournir.

Les prérequis techniques du logiciel PC Pass ne sont donc pas détaillés dans ce document, puisque l'intervenant aura la maîtrise complète du logiciel.

En revanche, s'agissant d'un système en exploitation permanente, toute rupture d'exploitation pendant l'intervention du Titulaire du marché, devra faire l'objet d'une demande préalable d'intervention, elle devra être quantifiée et planifiées avec le Maître d'ouvrage (C2 du site), au moins 15 jours avant.

Toutes les dispositions devront être prises en amont de cette intervention (sauvegarde doublée), aucune perte de données ou de logs ne sera acceptée.

Au terme de la migration, des **tests de non régression** devront être effectués, ils permettront de vérifier que les interventions n'auront pas altéré le fonctionnement des applications, ainsi que de l'hypervision.

#### 4.1.3 Supervision des alarmes et Gestion des catégories de variables

**Les fonctionnalités décrites ci-dessous doivent être respectée et mises en œuvre :**

Le paramétrage de l'IHM du système de sûreté devra être précédé d'une « collecte des données » à organiser auprès du MOA et/ou du Chef de Poste afin que le paramétrage de l'IHM reflète exactement le fonctionnement du Poste de Sécurité pour la gestion du magasin munition. Le titulaire du marché devra poser lui-même les bonnes questions et être force de proposition pour adapter la solution au plus près des besoins.

La mise à jour du système de sûreté intégré et centralisé devra **obligatoirement continuer** gérer les applications contrôle d'accès – intrusion – supervision sur la même base de données et depuis le même IHM pour limiter les impacts et les risques de failles informatiques.

Les solutions basées sur des piles de logiciels et des bases de données différentes seront à proscrire.

##### 4.1.3.1 Précautions :

S'agissant d'un système en exploitation, toutes les précautions devront être prises pour assurer le 1<sup>er</sup> RTP contre toute dégradation de services.

Les précautions avals devront être de l'ordre de

- Procédure détaillée de l'intervention prévue et de son périmètre, intégrant les sauvegardes préalables aux actions
- La définition des installations et programmations proposées
- La procédure de tests transverses à mettre en œuvre pour contrôler la non-régression du système en place. L'ensemble devra être décrit dans une procédure dite de « non-régression »
- La correction si nécessaire
- La validation finale.

**Aucune rupture d'exploitation ne devra être provoquée sans avoir été planifiée avec le RSSI-A et le MOE, afin que les mesures compensatoires soit prévues et organisées.**

#### 4.1.4 Le contrat de service

Le titulaire proposera un contrat de service de l'éditeur du système (SMA) dans le cadre d'un forfait annuel de mise à disposition des évolutions logicielles & patches avec le client final.

Ce contrat aura pour objectif d'assurer les services suivants sur le logiciel central du système :

- Maintenance curative : Mise à disposition des correctifs/patches (corrections de bug)
- Maintenance évolutive : Mise à disposition des nouvelles versions
- Fournir les informations synthétiques des évolutions de chaque version

#### 4.1.5 La cérémonie des clés : CADIVS – système et réseau

Préalable à la livraison, et postérieur à la Formation, la « cérémonie des clés » doit être organisée par le Titulaire. Elle réunira le Titulaire, le MOE, le MOA et ses représentants.

Le Titulaire organisera le changement des mots de passe du système de CADIVS, saisie que devra effectuer le MOA seul, sans la présence de l'entreprise. Ces mots de passe sont secrets, conservés par le MOA.

La Cérémonie des clés pourra être effectuée en 2 temps :

1<sup>er</sup> temps : CADIVS

2<sup>ème</sup> temps : Système principal

- a. Windows serveur +++
- b. logiciels de servitude : serveur Anti-virus + sauvegarde + authentification (AD)
- c. Mot de passe management réseau.

#### 4.1.6 Serveur de Temps

Un service NTP sécurisé doit être mis en place pour chacun des systèmes : CADIVS, afin d'assurer la synchronisation horaire de l'ensemble des équipements raccordés sur le réseau.

#### 4.1.7 Normes et règlements applicables

Les propositions de l'Entreprise devront être conformes aux clauses de l'ensemble des lois, décrets, arrêtés, règlements, circulaires, normes et tous les textes nationaux ou locaux applicables aux ouvrages de la présente opération.

Les documents, ci-après, sont applicables dans leur dernière édition, cette liste n'est pas exhaustive.

- **norme NF C15.100** : installations électriques à basse tension,
- **norme C18.510** : installations courants faibles et forts,
- **norme NF C63.410** : ensembles d'appareillages basse tension montés en usine,
- **norme NF C91.101** : perturbations radioélectriques et systèmes d'antiparasitage, textes officiels concernant le matériel alimenté en réseau de première catégorie et dont le rayonnement direct est faible,
- **norme NF C91.104.** : perturbations radioélectriques et systèmes d'antiparasitage et textes officiels concernant les appareils servant aux réceptions individuelles ou collectives des émissions et radiodiffusion sonore ou visuelle,
- **norme NF C92.130** : appareils électroniques et appareils associés à usage domestique ou à usage général analogue, reliés à un réseau de règles de sécurité.

- **norme NF P25.362** : fermetures pour baies libres et portails, Spécifications techniques, Règles de sécurité,
- **norme C32.321** : conformité des câbles de distribution basse tension,
- **norme C32.201** : conformité du conducteur de protection,
- **norme C32.310** : conformité des câbles basse tension résistant au feu,
- **Directive SEVESO** : comptage des personnes en zone à risque
- **Déclaration CNIL**: obligatoire pour le contrôle d'accès et la biométrie
- **Titres de transport anonymes (CNIL AU-015)** : Etanchéité des identifiants entre les applications/les services quand le titre de transport est utilisé pour le contrôle d'accès
- **RoHS** : Respect des directives européennes qui interdisent certaines matières dans les cartes, composant électroniques
- **Guide ANSSI** : « Référentiel Général de Sécurité » (RGS) du 26 janvier 2010 : conformité avec un cryptage AES128 bits minimum
- **Guide ANSSI** : « SECURITE DES TECHNOLOGIES SANS-CONTACT POUR LE CONTROLE DES ACCES PHYSIQUES » du 19/11/2012 : conformité avec ce document
- **Guide ANSSI** : « Profil de protection d'un commutateur industriel » Version 1.0 court-terme du 13 juillet 2015 : conformité sur la compatibilité des automates industrielles avec 802.1x
- **Guide ANSSI** : « Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection » du ANSSI-PA-72 du 10/10/2023.

## 5 SPECIFICATIONS TECHNIQUES CADIVS

---

### 5.1 VIDEO SURVEILLANCE

#### 5.1.1 Mode de fonctionnement attendu

Le système de vidéosurveillance aura pour mission de gérer et d'administrer les 2 caméras installées dans un premier temps. D'autres caméras pourront être installées à l'avenir, le système proposé sera donc en capacité d'absorber les adjonctions sans complication au niveau du système.

##### *5.1.1.1 Proposition des fonctions potentielles :*

Deux les caméras situées à l'extérieur :

- La visualisation de l'ensemble de la périphérie du Magasin de munitions,
- La réalisation d'une recherche sur alarme provenant du système de détection
- L'enregistrement permanent des images issues des caméras ;
- La visualisation des accès véhicules ;
- L'identification des personnes se présentant au magasin à munitions;
- L'identification d'une personne utilisant une platine / une clé;

#### 5.1.2 Centralisation du système

Le système de vidéosurveillance sera centralisé dans une baie à installer dans le Local Technique Sûreté du bâtiment 18 ou 24. Le choix du bâtiment sera établi en fonction des facilités de câblage et de l'architecture du réseau. L'ensemble des informations en provenance des caméras sera centralisé et transitera de manière numérique de la caméra au cœur de système du VMS.

2 postes de travail visualiseront les flux vidéo provenant du serveur vidéo :

- Responsable Sûreté du PAF (poste de contrôle des accès)
- Accueil du Bat 18 (SG)
- Les écrans de visualisation des flux vidéo seront adaptés

#### 5.1.3 Fonctionnalités du système

Le système de vidéosurveillance disposera au minimum :

- D'interfaces logiques ou physiques avec les centrales intrusions et d'interphonie ;
- D'une interface de gestion graphique ;
- D'une matrice virtuelle permettant de distribuer les flux vidéo sur différents écrans ;
- De disposition permettant le pilotage des caméras par joysticks et clavier de type PC ;

- D'un nombre de connexions utilisateur simultanées vers des postes clients supérieur à 5 ;
- D'un nombre de connexions de caméras extensible à 250 ;
- D'un dispositif de gestion des droits utilisateurs à la carte ;
- D'une supervision tant du réseau physique que logicielle ;
- D'une configuration pour que la déconnection d'une caméra provoque une remontée d'alarme immédiate ;

D'un paramétrage pour que le branchement d'un matériel non autorisé sur le réseau vidéo génère une alarme immédiate et visible sans gêner l'exploitation par l'opérateur : management réseau.

#### 5.1.4 Licences des logiciels utilisés

Il sera fourni l'ensemble des licences logicielles et modules divers permettant la gestion des éléments suivants :

- Caméras et postes clients
- Interface logique ou physique avec les centrales intrusions et l'interphonie permettant :
  - De réaliser l'affichage de chaque caméra fixe sur alarme intrusion bâtiment, périphérique ou appel platine interphone,
  - De réaliser les prépositions par dôme sur alarme intrusion bâtiment, périphérique ou appel platine interphone
- Affichage des caméras fixes et mobiles sur écran d'alarme piloté par l'intrusion ou l'interphonie
- Connexion de clavier de pilotage
- Gestion graphique
- Supervision des systèmes incluant la gestion des alarmes selon un processus guidé dédié et adapté

#### 5.1.5 Stockeurs numériques

Les stockeurs numériques utilisés seront au format « rackables » standard 19". Chaque système en IP disposera par voie et en simultané des capacités suivantes :

- Résolution 1080 p ;
- Compression : H264 ou H265 ;
- Images par seconde : 25 ;
- Interface Ethernet : 10/100/1000 base-T.

Ainsi que :

- D'un nombre d'entrées contacts secs adapté aux besoins ;
- Des protocoles adaptés



### 5.1.6 Capacité d'enregistrement

Le système d'enregistrement permettra le stockage des images issues de l'ensemble des caméras en simultanée pour l'ensemble des voies utilisées dans les conditions suivantes :

- Enregistrement permanent de l'ensemble des caméras ;
- Enregistrement des images pour permettre la visualisation ou l'identification a posteriori ;
- Enregistrement des images à 25 images par seconde ;
- Enregistrement sur une durée de 30 jours. Cette durée devra être confirmée par des tests ;
- Ecrasement des données automatiques une fois la durée d'enregistrement maximale atteinte (FIFO);

### 5.1.7 Scénario de pré-alarme

Afin d'optimiser le processus de reconnaissance, l'affichage des caméras fixes sera effectué avec une pré-alarme réglable de 0 à 30 secondes permettant de visualiser une scène avant le déclenchement de l'alarme issue du système de détection d'intrusion

### 5.1.8 Exploitation

#### 5.1.8.1 *Dimensionnement serveur vidéosurveillance*

Le serveur de vidéosurveillance sera dimensionné de manière à pouvoir au minimum :

- Gérer l'ensemble des caméras,
- Gérer l'ensemble des postes clients
- Gérer l'accès aux enregistrements
- Gérer 30% d'équipements en plus (caméras en visualisation et enregistrement, postes client)

#### 5.1.8.2 *Dimensionnement postes clients*

Les postes clients correctement dimensionnés et permettant l'exploitation du logiciel de supervision de vidéosurveillance seront fournis.

Les deux postes clients seront répartis de la manière suivante :

- 1 PC/écran au PAF (Poste de contrôle des accès) – entrée du site
- 1 PC/écran au service OPC – Bât 18

#### 5.1.8.3 *Gestion de l'affichage*

Concernant la station du poste de sécurité :

- Mise à disposition de deux écrans sur le poste de travail permettant :
- Gestion graphique ;

- Bandeaux d'alarmes ;
- Traitement d'un événement ;
- Relecture (selon droits d'utilisateurs).

Mise à disposition d'un mur d'images permettant l'affichage :

- Gestion par scénario du mur d'images ;
- Écran d'alarmes.

#### **5.1.8.4 Ecrans de visualisation 42"**

Les écrans de visualisation au poste de sécurité disposeront :

- D'une possibilité d'accroche par support situé à l'arrière de chaque écran ;
- De connecteurs DVI – HDMI ;
- D'une technologie prévue pour un fonctionnement 24 heures sur 24 ;
- D'un angle de visualisation horizontal minimum de 40° ;
- D'un angle de visualisation vertical minimum de 30°.

#### **5.1.8.5 Supports d'écrans**

Les écrans 42" seront livrés avec des supports muraux permettant

- Le réglage de l'inclinaison des écrans,
- Le réglage de l'orientation des écrans,
- Le blocage des réglages en position définitive
- L'accès aux connecteurs sans qu'il soit besoin de sortir l'écran de son support,

#### **5.1.8.6 Mosaïques préprogrammées**

Le logiciel sera paramétré pour permettre la visualisation des différents scénarios d'affichage. Ces scénarios seront commandés depuis les touches programmables présentes sur les joysticks et depuis les ensembles claviers souris.

#### **5.1.8.7 Joystick**

Chaque poste client sera équipé d'un joystick permettant :

- Le pilotage des caméras mobiles ;
- La commande de prépositions des caméras mobiles ;
- La sélection de la caméra à afficher ;
- La sélection de scénarios d'affichages sur des boutons programmables.

#### **5.1.8.8 Recherche synchronisée**

La fonction de relecture devra présenter la fonctionnalité de recherche synchronisée permettant d'afficher et de relire plusieurs séquences vidéo de manière synchronisée.

### **5.1.9 Gestion graphique**

#### **5.1.9.1 Niveaux de plans**

L'interface de la gestion graphique gèrera 3 niveaux de plans :

- Niveau 1 : Site ;
- Niveau 2 : Entrée Magasin à Munitions ;
- Niveau 3 : Zones et partie de la périphérie

#### **5.1.9.2 Etats des symboles dynamiques**

L'interface de gestion graphique gèrera différents états des symboles caméras :

- Caméra fonctionnelle,
- Caméra défectueuse,

#### **5.1.9.3 Bandeau d'alarmes**

L'interface de gestion graphique sera équipée d'un bandeau d'alarme qui affichera :

- Les défauts sur l'installation ;
- Les caméras en alarmes ;

Le bandeau d'alarme permettra d'accéder directement à l'enregistrement de la caméra issue de l'alarme par une action simplifiée (double clic ou équivalent). La séquence vidéo s'affichera sur l'écran d'alarme.

### **5.1.10 Droits utilisateurs**

#### **5.1.10.1 Matrice de droits utilisateurs**

Sans que la liste ne soit exhaustive, les profils utilisateurs pourront s'inspirer de la matrice suivante.

PROFILS	Mainteneur	Administrateur	Chef de poste	Opérateur
Configuration du système	Oui	Oui	Non	Non
Attribution des droits	Non	Oui	Non	Non
Accès aux enregistrements	Non	Oui	Non	Pré-alarme
Extraction vidéo	Non	Oui	Non	Non
Edition de rapports et historique	Non	Oui	Oui	Non
Accès à la télémetrie	Oui	Oui	Oui	Oui
Modification affichage	Oui	Oui	Oui	Préprogrammé
Accès au fils de l'eau	Non	Oui	Oui	Oui
Accès au bandeau d'alarmes	Non	Oui	Oui	Oui
Accès à la gestion graphique	Oui	Oui	Oui	Oui

### 5.1.11 Implantation des caméras

#### 5.1.11.1 *Emplacement des caméras*

Les caméras seront implantées de manière à surveiller les accès au Magasin à Munitions,

- Le portail d'accès
- L'entrée du dépôt, sur un mât déporté, de manière à obtenir une vision globale.

Les supports de caméras devront être disposés pour ne pas constituer d'aide au franchissement depuis l'extérieur (système de détection périphérique et/ou clôtures et/ou portails portillons, etc.).

#### 5.1.11.2 *Pose sur mâts*

La hauteur de pose préconisée est de 4m et les mâts seront adaptés aux conditions climatiques locales afin de ne pas générer de perturbation dans l'exploitation par l'utilisateur.

De plus, les mâts devront présenter les caractéristiques suivantes :

- Être réalisés en acier galvanisé ;
- Être conique ou conique avec une section octogonale ;
- Présenter un déport par rapport au bâtiment équivalent aux obstacles et excroissances
- Une mise à la terre conforme à la réglementation en vigueur ;
- Être équipés des supports de caméras adaptés ;
- Disposer d'un cheminement intérieur pour le câblage des caméras et de leur support.

Chaque mât disposera en partie basse d'une boîte de raccordement de classe II.

Cette boîte de raccordement sera accessible depuis l'extérieur, par une trappe de visite intégrée dans le mât. La boîte de raccordement devra être dimensionnée pour recevoir les câbles d'alimentation des caméras. Chaque boîte de raccordement disposera également d'un organe de coupure de l'alimentation intégré.

### 5.1.11.3 VRD

Les VRD existantes sont exploitables, les fourreaux sont en état et permettent le passage des câbles de raccordement.

Il est toutefois possible que quelques mètres soient à créer pour l'accès final au magasin.

Sans que la liste ne soit exhaustive, l'ensemble des prestations nécessaire à la mise en œuvre du système vidéo comprend :

- La réalisation et la pose des massifs ;
- L'établissement du cheminement des câbles :
  - Par la création de passages de câbles ;
  - La pose de chambres de tirages dans les règles de l'art ;
  - Une implantation des cheminements à l'intérieur du site.

## 5.1.12 Politique de sécurisation des connexions IP

### 5.1.12.1 Contraintes

En application des directives de l'IGI-1300 en vigueur et des directives de l'ANSSI, la politique sécurité suivante sera appliquée pour ce qui concerne la pose des caméras IP :

Caméras	Hauteur de pose	Disposition 1	Disposition 2
Caméras accessibles depuis l'extérieur du site	H<5.50 m H>5.50 m	Caissons IK10 fermés avec boulons à empreintes spécifiques Ou Caméra cryptée Ou Caméra avec sortie FO directe	Câble ou fibre optique cheminant directement de la caméra à l'intérieur du site sans liaison visible depuis l'extérieur.
			Protocole d'authentification 802.1X + Security ports
Caméras non accessibles depuis l'extérieur du site	H<4.50 m	Caissons IK10 fermés avec boulons à empreintes spécifiques Et Angle de vue de la caméra non modifiable sans outil	Câble ou fibre optique cheminant directement de la caméra à l'intérieur du site sans liaison visible depuis l'extérieur.
	H>4.50 m	Caissons IK10 fermés avec boulons à empreintes spécifiques	Protocole d'authentification 802.1X + Security ports

### 5.1.12.2 Cérémonie des clés

L'administration reste propriétaire des éléments de sécurisation racine de cryptographie (certificats/mots de passe) du réseau , du système et des logiciels d'exploitation. Ces éléments seront injectés par l'administration dans le système lors d'une cérémonie des clés.

## 5.2 DETECTION INTRUSION

### 5.2.1 Centralisation et supervision

#### 5.2.1.1 *Centralisation*

##### 5.2.1.1.1 Centrale de détection intrusion

Chaque équipement de détection intrusion sera raccordé sur une centrale de détection intrusion dédiée et autonome. Celles-ci seront implantées dans le Local Technique du magasin à munitions ou dans l'endroit le plus adapté. Les informations provenant de chaque système seront transmises au superviseur en vue de leur transcription sur le synoptique de l'interface graphique.

Les centrales disposeront des caractéristiques suivantes :

- IP en fonction des contraintes mentionnées ci-avant
- Interopérable avec la supervision ;
- Fonctionnement en réseau natif
- Filaire (bus entre les modules entrées/sorties, boucles équilibrées avec les détecteurs) ;
- 16 à 256 zones d'alarmes ;
- Gestion de 16 groupes ;
- NFA2P Type 2 ;
- Module IP natif;
- 128 sorties relais ;
- Sortie avec buzzer extérieur ;
- Sortie sirène avec + de blocage ;
- Transmetteur téléphonique paramétrable ;
- Paramétrable depuis le clavier de commande ou par un PC local ;
- Transmetteur vocal.

##### 5.2.1.1.2 Claviers de commande

Chaque centrale sera associée à des claviers de commande. Ils seront installés :

- Dans les alvéoles pour permettre l'armement/désarmement de la détection
- Ils activeront le voyant VERT/ROUGE (vide/occupé), positionné à l'extérieur de CHAQUE alvéole
- Ils permettront la gestion de la centrale associée suivant les droits paramétrés et notamment :

- Mise en/hors service de groupe d'alarmes
- Gestion des alarmes provenant de la centrale
- Gestion des défauts alimentation, défauts techniques
- Buzzer intégré
- Programmation système
- Rétro-éclairage

#### 5.2.1.1.3 Alimentations complémentaires

Le système de détection d'intrusions doit être équipé d'alimentations complémentaires permettant d'assurer une autonomie de 24 heures pour l'intégralité de l'installation. Ces alimentations sont surveillées par le système pour transmettre les différents défauts au poste de sécurité. Sans que la liste soit exhaustive, les défauts à transmettre sont :

- Défaut alimentation secteur ;
- Défaut de charge des batteries ;
- Défaut batteries ;
- Ouverture du capot ;
- Arrachement ;
- Défaut fusibles internes.

#### 5.2.1.1.4 Fonctionnalités

Via son interface de supervision, le système de détection intrusion disposera des fonctionnalités décrites au paragraphe **4.1.2 Le système de protection Contrôle d'accès et Détection Intrusion (Synchronic)**

Et notamment :

- Les fonctionnalités
- Fonctionnement sur plage horaire
- La supervision intégrée avec synoptiques dynamiques → mise à jour du synoptique existant
- Différents types d'alarmes, dont :
  - Détection intrusion,
  - Auto surveillance et sabotage,
  - Disqualification (pour l'utilisation de barrières infrarouge par exemple),
  - Défauts d'alimentation
  - Alarmes techniques,
  - Alarmes 24/24h,
  - Défauts divers.
- Processus guidés en cas d'alarmes
  - Consignes

- Asservissement des caméras pour consultation des vidéos sur alarmes
- Bandeau d'alarme
- Compteur d'évènements

### 5.2.1.2 Supervision

#### 5.2.1.2.1 Interfaces homme/machine

La supervision existante intègre une interface graphique. Celle-ci sera mise à jour pour refléter l'ensemble des plans du Magasin à munitions sur le synoptique animé du site permettant en temps réel, à minima :

- De visualiser les différents secteurs et zones de détection sur le plan général du site
- De piloter la mise en, mise hors des secteurs de détection depuis l'interface graphique
- De connaître l'état des zones et secteurs de détection :
  - Activé/désactivé ;
  - En alarme ;
  - En défaut.
- De différencier les événements par la couleur du changement d'état aux niveaux suivants :
  - Plans ;
  - Bandeau d'alarmes.
- Les couleurs et icônes utilisées devront être du même type que ceux en exploitation sur le site, auxquels les utilisateurs sont habitués.

De plus, un « fil de l'eau » sur un écran dédié affichera un descriptif de changement d'état des points ou groupes d'alarmes ainsi que la date et l'heure de la modification (mise en/hors service par opérateur X, alarme, défaut, ...).

#### 5.2.1.2.2 Matrice des droits

Les sessions opérateurs et administrateurs seront distinctes. Les profils pourront respecter les règles en vigueur sur le site, mais en cas de besoin d'évolution, ils pourront s'inspirer de la matrice suivante :

Profil	Mainteneur	Administrateur	Chef de poste	Opérateur
Configuration du système	Oui	Oui	Non	Non
Attribution des droits	Non	Oui	Non	Non
Mise en et hors service	Non	Oui	Oui	Oui
Acquittement d'évènements	Non	Oui	Oui	Oui
Réarmement d'évènement	Non	Oui	Oui	Oui
Edition de rapports/historiques	Non	Oui	Oui	Non
Modification affichage	Oui	Oui	Oui	Oui
Accès à l'historique (fils de l'eau)	Non	Oui	Oui	Non
Accès au bandeau d'alarmes	Non	Oui	Oui	Oui



Accès à la gestion graphique	Oui	Oui	Oui	Oui
------------------------------	-----	-----	-----	-----

Les opérateurs du poste de sécurité pourront acquitter l'ensemble des alarmes.

Dans tous les cas, au déclenchement d'une alarme intrusion ou d'un défaut critique, une notification sonore d'au moins 80dB retentira sur le poste jusqu'à la prise en compte de l'alarme.

#### 5.2.1.2.3 Serveur d'exploitation (logiciel CADIVS principal)

Le serveur sera dimensionné de manière à pouvoir gérer l'ensemble de l'installation incluse la capacité d'augmentation du système de 30%. Il devra être dimensionné pour rester fonctionnel et opérationnel même dans le cas où une erreur d'exploitation consistant à armer l'ensemble des groupes et secteurs en période de présence des personnels.

Le temps de traitement d'une information du capteur au superviseur devra être inférieur à 1 seconde dans la limite de 20 événements en simultané.

Il sera placé dans la baie sûreté située dédié.

#### 5.2.1.2.4 Serveur de servitudes

Il sera positionné dans la baie sûreté (celle du serveur d'exploitation décrit au dessus), il hébergera :

- Active Directory - paramétré selon les règles en vigueur (décrit plus bas)
- Antivirus Serveur et ses Clients (à valider avec l'éditeur du CADI avant choix)
- Sauvegardes (nocturnes + mensuelles) pour backup / restore

#### 5.2.1.2.5 Postes clients

Trois postes seront fournis. Ces derniers doivent permettre l'exploitation du logiciel de supervision intrusion au travers d'un écran de 24" et seront répartis de la manière suivante :

- 1 PC/écran au PAF (Poste de contrôle des accès) – entrée du site
- 1 PC/écran au service OPC – Bât 18
- 1 PC/écran au service SG – Bât 17

#### 5.2.1.2.6 Disque dur externe

Positionné dans un endroit protégé et éloigné des serveurs (autre bâtiment), il sera connecté sur le réseau et stockera les sauvegardes en FIFO.

#### 5.2.1.3 Interface avec le système de vidéosurveillance

Pour asservir les caméras de surveillance au système de détection intrusion, des interfaces contact sec entre les deux systèmes seront nécessaires. Le système de vidéosurveillance pourra ainsi être automatiquement orienté vers une zone de détection afin de permettre aux opérateurs de réaliser une levée de doute. Dans ce cas, des contacts secs devront être mis en place, aucun lien IP ne devra relier la VS au CADI.

## 5.2.2 Détection bâtimementaire

### 5.2.2.1 *Avant-propos*

La détection bâtiment assurera la détection de toute intrusion dans le magasin à munition et de manière indépendante de tout autre détection.

Les alarmes du système de détection bâtiment seront principalement exploitées depuis le service OPC, Bat 18.

### 5.2.2.2 *Implantation des équipements*

#### 5.2.2.3 *Politique générique d'implantation des détecteurs*

Les contacts d'ouvertures seront mis en place selon le principe suivant :

- 1 détecteur par ouvrant (porte, fenêtre, issue de secours, exutoire, ...) donnant sur l'extérieur ;
- 1 détecteur par ouvrant donnant sur un local sensible ;
- 1 détecteur par ouvrant donnant sur un local technique.

Les radars volumétriques seront mis en place selon le principe suivant :

- 1 radar volumétrique (ou plus selon configuration) par volume donnant sur l'extérieur ;
- 1 radar volumétrique (ou plus selon configuration) par circulation ;
- 1 radar volumétrique (ou plus selon configuration) par local sensible ;
- 1 radar volumétrique (ou plus selon configuration) par local technique ;

Ces radars volumétriques seront positionnés selon les règles de l'art.

**Cette disposition sera à valider avec la MOA ou son représentant avant mise en œuvre.**

### 5.2.2.4 *Implantation des équipements de centralisation*

Les équipements de centralisation seront implantés dans les Locaux Techniques Sûreté et/ou dans les coffrets dédiés.

### 5.2.2.5 *Détecteurs bi-technologie circulaire*

Ces détecteurs seront de technologie hyperfréquence bande X et infrarouge à miroirs, pour l'ensemble des faisceaux permettant une couverture de 360°. Ils devront avoir une portée de 7,5m de rayon minimum, avec une hauteur de pose maximale de 3,5m.

Les détecteurs auront les caractéristiques suivantes :

- - Tension : 6 Vcc à 15 Vcc,
- - Alimentation : 18 mA en veille, 75 mA sous alarme,
- - Contact d'autosurveillance normalement fermé (couvercle en place),
- - Relais à contacts scellés de forme C conçus pour une valeur nominale de 3,0 W, 125 mA à 28 Vcc pour les charges résistives,

- - Contacts NO/NF calibrés à 28 Vcc, 125mA maximum,
- - Boîtier en plastique ABS à résistance élevée aux chocs,
- - Kit de montage.

#### 5.2.2.6 Détecteurs infrarouge linéaire

Ces détecteurs seront positionnés exclusivement dans les circulations, si le besoin est exprimé, . Ils seront de type mono-technologie, avec focalisation des rayonnements infrarouge par miroirs, agréés NFA2P type 3 N°280280-01

Les détecteurs auront les caractéristiques suivantes :

- - Une signalisation automatique des tentatives de masquage par système anti-masquage (AM) à infrarouge actif (AIR),
- - Une réinitialisation AM sélectionnable,
- - Des voyants LED de test « Marche »,
- - Mémoire d'alarme intégrée,
- - Sorties autotest AM et IRP (distinctes du signal de masquage),
- - Distance de détection minimum 20m,
- - Kit de montage.

#### 5.2.2.7 Détecteurs bi-technologie linéaire

Ces détecteurs seront positionnés exclusivement dans les locaux techniques. Ils seront de technologie hyperfréquence bande X et infrarouge à miroirs, fonction anti-masquage et répondant aux normes NFA2P.

Les détecteurs auront les caractéristiques suivantes :

- Alimentation 9-15 Vcc ; ondulation crête à crête max. 2 V à 12 Vcc,
- Consommation très faible de 15mA en fonctionnement normal,
- Angle utile 86°,
- Contact inverseur NO/NF,
- Couverture de 16m,
- Consommation très faible de 15mA en fonctionnement normal,
- Commutation par micro-interrupteur des portées infrarouge et hyperfréquence,
- Optique à miroir de précision multi-rideaux,
- Réglage de sensibilité de la fonction anti masque,
- Kit de montage.

#### 5.2.2.8 Détecteurs d'ouverture

Les contacts magnétiques d'ouverture sous agrément NF-A2P seront constitués de 2 éléments (le détecteur et l'aimant). Les contacts à bille sont à proscrire.

Le boîtier détecteur est moulé et muni d'un câble 4 conducteurs (boucle d'alarme et boucle d'autoprotection), sous gaine métallique, d'une longueur de 80cm. La masse polaire de l'aimant est constituée de deux éléments reliés entre eux par une contre plaque métallique, ceci permettant une installation sur support ferreux magnétique.

Les détecteurs seront conçus pour s'affranchir des vibrations des portes. L'ouverture de la boucle est effective si les deux parties du détecteur d'ouverture sont distantes de plus de 35 mm.

Par ailleurs une équerre de fixation est fournie avec chaque ensemble, pour permettre d'ajuster la position de l'aimant.

Le raccordement des contacts magnétiques de chaque porte s'opérera par l'intermédiaire d'une boîte auto-protégée, incorporant les résistances d'équilibrage.

#### 5.2.2.9 *Marquage des câbles et codes couleurs*

Tous les câbles d'alarme seront parfaitement repérés, identifiés à chaque extrémité et constitueront le point d'accès visuel des chemins de câbles. L'étiquetage devra comporter de manière indélébile le numéro de la pièce, étiquette imprimée fixée par deux colliers nylon.

Les fils constituant les câbles 6 conducteurs seront de couleur blanche, jaune, rouge, vert, gris et orange.

Les paires seront :

- Vert/Jaune pour l'autoprotection et alarme,
- Blanche et rouge pour l'alimentation,
- Orange et grise pour la réserve.

#### 5.2.2.10 *Chemins de câbles*

Tous les câbles sûreté emprunteront les chemins de câbles unique « SURETE-SECURITE ». En dehors des chemins de câbles, les câbles seront installés sous tube « IRO » ou techniquement équivalent, positionnés dans le faux plafond et au plus loin des équipements perturbateurs.

### 5.3 LE CONTROLE D'ACCES

Comme précisé plus haut, le contrôle d'accès n'est pas à mettre en œuvre sur le Magasin à munitions.

Cependant, puisque le système de sûreté Synchronic gère le CA et la DI en exploitation, toutes les précautions devront être mises en œuvre pour que le CA existant ne subisse aucune perturbation.

#### 5.3.1 Les accès au réseau : paramétrage des switches

Il sera mis en œuvre sur les équipements actifs de réseau un processus d'identification / authentification des matériels connectés. Il doit s'appuyer sur le filtrage MAC par port et la désactivation des ports inutilisés.

Chaque face avant d'actif réseau (switch) doit être documentée afin de connaître par port :

- - Le VLAN de rattachement ;
- - L'adresse IP ;
- - L'adresse MAC ;
- - Les protocoles utilisés.

### 5.3.2 Procédures et responsabilités liées à l'exploitation

Un processus de gestion documentaire permettant le suivi des indices sera utilisé. Cela concerne aussi bien la documentation technique que la mise à jour des systèmes.

## 5.4 RESEAU SURETE

### 5.4.1 Architecture technique

#### 5.4.1.1.1 Architecture attendue

L'architecture réseau sera dissociée physiquement en 2 réseaux physiques distincts :

- Le réseau contrôle d'accès /détection intrusion: celui-ci disposera de ses propres câbles optiques/Ethernet et de ses propres équipements actifs , **mais** isolé par les fonctionnalités du management du réseau (Vlans/port, MacAdress, etc)

**NB : les fibres optiques seront dimensionnées en conséquence, même si le contrôle d'accès n'est pas à développer, le CA existant doit être reconnecté sur les nouveau switchs .**

- Le réseau intrusion : celui-ci disposera de ses propres fibres (brins) et sera discriminé du CA par les ports des switchs, lesquels pourront être communs.
- Le réseau vidéo : celui-ci disposera de ses propres fibres et de ses propres équipements actifs qui seront différentes et isolés des 2 réseaux précédents (CA et DI). Les switchs ne seront pas communs avec ceux du CADI.

#### 5.4.1.1.2 Liens entre les locaux

Quatre liens optiques devront être installés lorsque nécessaire, pour permettre d'établir les liaisons 1Gbits/s inter-bâtiments. Ces liens seront dédiés aux systèmes de sûreté CADIVS.

Chaque liaison aura les caractéristiques suivantes :

- Multimode 50/125 µm ;
- OM3 ;
- 12 brins.

## 5.5 ALIMENTATION

### 5.5.1 Alimentation régulée – Source d'alimentation

L'ensemble des équipements seront alimentés sur la source régulée. Le cœur applicatif (serveur, switch, etc.) sera pourvu de blocs double alimentation pour une meilleure continuité de service.

## 6 SECURISATION DU CŒUR DE SYSTEME

### 6.1 ANNUAIRE CENTRALISE : AD+ GPO

#### 6.1.1 Protection centralisée du système CADIVS - comptes et accès

Une GPO doit être mise en œuvre : Le Group Policy Object ( GPO ) est un ensemble de paramètres de configuration pouvant être appliqués à un utilisateur ou un groupe. Dans le cas du projet, il s'agit de la protection du système CA-DI-VS.

Aucun mot de passe ne devra être installé en local, hormis celui de l' « administrateur local » de la machine (celui du PC client), connu seulement de l'administrateur du système.

Un annuaire LDAP (Active directory) doit être activé et correctement paramétré. Tous les mots de passe doivent être créés, nominativement sur cet annuaire centralisé (Active Directory).

##### 6.1.1.1 *Rappel de mise en œuvre*

**CF RT4** : Les comptes fonctionnels sont interdits, mais, s'ils sont indispensables, il sera nécessaire de définir ces comptes **en compagnie de la maîtrise d'ouvrage** afin que ces droits soient limités au strict nécessaire, sans privilège particulier et être désactivés en dehors des périodes autorisées d'utilisation.

**RT 5** : Les comptes doivent être identifiés avec les logiques de séparation des rôles et du moindre privilège. Cette gestion des comptes doit se faire depuis leur création jusqu'à leur suppression. Une désactivation des comptes inutiles doit être réalisée au moins une fois par an.

**RT 6** : Chaque intervenant sur le système doit bénéficier d'une liste de pouvoirs proportionnée aux objectifs de sécurité définis pour son rôle sur le système. Les comptes nominatifs sont également obligatoires, il ne sera pas possible de créer des comptes fonctionnels et anonymes du type « gardien ». Toutefois, si cette contrainte est trop bloquante, des mesures organisationnelles devront être prises par la MOA, qui permettront d'identifier l'auteur des actions associées (comme un cahier de consigne nominatif, par exemple).

La politique de mots de passe à mettre en place devra respecter les prérequis de la PSSIA.

L'authentification par mot de passe doit suivre les règles de gestion (complexité, durée de vie, stockage, blocage session ...) de la [PSSI-M-T].

- Il est composé au minimum de 9 caractères (14 pour les administrateurs) dont au moins trois des catégories suivantes : lettre majuscule, lettre minuscule, chiffre arabe (0 à 9), caractère spécial ( ; ! ? . / \$ \* % » ' ( - , etc.);
- Il ne doit pas contenir tout ou partie de l'identifiant, du nom de l'utilisateur, de son rôle ou de son grade ;
- Il a une durée de validité fixée à 45 jours pour les administrateurs et trois mois dans les autres cas ; mais cette durée peut être abaissée, jamais augmentée.
- Il a une durée de vie minimale de 7 jours ;

- Il ne peut être identique aux 6 derniers mots de passe utilisés.
- Par ailleurs, le seuil d'avertissement de l'obligation de changer de mot de passe est fixé à 14 jours.

Pour limiter le nombre de mot de passe à retenir et pour sécuriser la gestion des mots de passe, il serait bon de lier l'accès de la solution proposée à celui du système.

### 6.1.2 Les sauvegardes

La mise en œuvre d'une solution de sauvegarde complète, de type ACRONIS est attendue. Si une licence ad'hoc est installée elle devra être mise à jour et migrée également, sur le serveur de Servitudes.

Les sauvegardes devront être automatiques. Une sauvegarde périodique devra être programmée et une supplémentaire devra être lancée à chaque modification du système (évolution, paramétrage, etc).

Un plan de sauvegarde devra être proposé. Le système complet, paramétrages et données seront sauvegardés. Cette sauvegarde permettra une restauration rapide et totale des systèmes (CA-DI).

Le dispositif de sauvegarde et de rechargement de la configuration et des paramètres du système seront effectués

- sur un disque externe (type NAS ou USB accepté), dédié et positionné dans un autre local (éloignée de la baie des serveurs), protégé contre l'intrusion.
- Une surveillance du bon déroulement des sauvegardes sera à mettre en place.

La mise en œuvre d'une procédure organisée et automatique pourra être, par exemple :

- |                             |                                 |
|-----------------------------|---------------------------------|
| ➤ Nocturne et journalière : | Pourront être conservées 1 mois |
| ➤ Hebdomadaire :            | Pourront être conservées 2 mois |
| ➤ Mensuelle :               | Pourront être conservées 1 an   |
| ➤ Annuelle :                | Pourront être conservées 5 ans  |

Une fois par mois, la copie d'une sauvegarde sera effectuée sur un support externe (disque USB par exemple) et emmenée par le RSSI-A (ou toute autre personne le représentant) dans un local habilité (Commandement), et protégé (coffre fort).

### 6.1.3 Les restaurations

Les sauvegardes ne valent que parce qu'elles peuvent être utilisées pour récupérer les données. Il est donc indispensable de tester les « restaurations ». De cette manière, on s'assure de pouvoir remonter le système en cas de crash.

Tester la restauration de manière régulière (une fois par mois, par exemple), attention à bien créer une procédure de non-régression.



## 6.2 LA PLATEFORME D'HEBERGEMENT

La solution complète sera exploitable sur une plateforme de serveurs physiques et/ou virtuels et 5 PC Client.

L'objectif de la structure d'hébergement est de consolider l'architecture serveur nécessaire au déploiement du système CADIVS.

### 6.2.1 Les serveurs d'application et d'administration

Le(s) serveur(s), quelque soit le nombre dont l'entreprise aura besoin pour héberger les solutions de CADIVS, devront respecter les prérequis suivants, à minima :

- Serveur rackable en baie, type PowerEdge R830
- Processeur
  - Gamme de processeurs Intel® Xeon® E5-4600 v4
- Disponibilité
  - Disques durs enfichables à chaud, blocs d'alimentation redondants enfichables à chaud, ventilateurs redondants enfichables à chaud, mémoire ECC, double module SD interne
- Communications
  - Cartes Select Network (cartes filles réseau) A calculer selon le besoin
- Mémoire
  - 32 minimum ou 64 Go
- Stockage
  - 5 disques durs SSD/SAS de 2,5" (10 000, 15 000 tr/min)
- RAID :
  - Raid 0 pour le système : 2 DD
  - Raid 5 pour les bases de données : 3 DD

Pour mémoire, les solutions logicielles attendues sont :

#### **pour le CADIVS**

- L'hyperviseur, le contrôle des accès et la détection intrusion
- La solution de sauvegarde
- La solution Anti-Virus Serveur
- Le service NTP
- Les contrôleurs de domaine (DC1 – DC2) physiques
- Et toutes les ressources liées à l'administration des utilisateurs et ordinateurs (AD+GPO).

## 6.3 L'ARCHITECTURE RESEAU

L'architecture réseau du CADIVS est exclusivement dédiée au contrôle d'accès et la détection intrusion.

Le réseau local est totalement hermétique et n'offre pas d'accès depuis l'extérieur, d'aucune sorte, même pas pour la MCO/MCS (pas d'accès internet, ni extranet, ni wifi, ...)

Toutes les adresses IP, des équipements, adressage réseau, des switches, des automates industriels, des UTL de sureté, des PC, des centrales intrusion, etc, devront être clairement identifiés et détaillés dans le document des spécifications techniques détaillées.

### 6.3.1 Internet

Aucune maintenance à distance ne devra être effectuée, aucun accès distant ne sera accepté sur tout ou partie du système, tel que précisé dans l'introduction.

### 6.3.2 Interfaçage autres systèmes

Aucune interface n'est prévue au titre de ce marché, mais si le besoin était exprimé, le principe de report des alarmes en **contacts secs exclusivement** devra être utilisé, en particulier pour permettre l'interfaçage des systèmes suivants :

- Détection incendie (les alarmes devront être intégrées au système de sureté CADIVS par des contacts secs exclusivement, et en aucun cas par une liaison Ethernet (IP).
- Alarme NFA2P
- Alarmes techniques (état des serveurs, switchs etc)

Toutes ces informations, leur méthode et schéma de câblage devront être précisées dans le document des Spécifications Techniques et Fonctionnelles, AVANT INSTALLATION POUR VALIDATION PREALABLE A LA MISE EN ŒUVRE .

### 6.3.3 Les switchs ou commutateurs réseau

Le réseau informatique de sécurité doit convenir aux exigences des règles de Cybersécurité. Des commutateurs évolués doivent être fournis et paramétrés dans les règles de l'art.

- Ils seront manageables et des « Vlans sécurité » seront configurés.
- Ils seront intégrés en baie et coffrets, autoprotégés. D'une manière générale, tous les coffrets et baies, y compris les centrales, devront être équipés de contact de porte de type ILS, sur tous les ouvrants. L'information d'ouverture devra être reportée sur des modules de report d'alarmes (contacts secs) du même fabricant, dans le local technique, prêts à être intégrés sur l'hyperviseur.
- Tous les ports des switchs doivent être intégrés aux Vlans, tous les ports USB ou CLI devront être bloqués logiquement et physiquement (obturateur de port et/ou adhésif de sécurité avec transfert).

La disponibilité du service de transport entre tous les points d'entrée sur un commutateur d'accès du LAN (réseau local) et tout point de sortie est à garantir. Aucun arrêt global n'est toléré. Le niveau de redondance de l'infrastructure des équipements actifs, de leurs alimentations, des liaisons entre les équipements, devra aboutir à une architecture disponible.

Seuls les équipements autorisés pourront se connecter sur le réseau, ce qui impose de poursuivre la gestion des Mac-address (Medium Access Control) par port, sur les commutateurs, et donc la fourniture de switchs capables d'offrir cette qualité de service.

**La liste des MacAdress, des Vlans et @IP est attendue dans le document des spécification techniques et fonctionnelles**

#### **6.3.3.1 La liste des équipements (Carte d'identité)**

Cette liste comportera tous les équipements raccordés sur le réseau (les serveurs, commutateurs, les routeurs, les passerelles protocolaires, etc.). Pour chaque équipement, le titulaire précisera :

- La marque ;
- Le modèle et la référence ;
- La version des logiciels et des firmwares embarqués.
- L'emplacement physique (bâtiment, pièce, armoire, baie).
- La liste des protocoles utilisés

Le titulaire précisera les numéros de VLAN pour chaque port des commutateurs.

#### **6.3.3.2 Les Vlans**

Un cloisonnement logique par la mise en place de Vlans doit être configuré.

Leur configuration assure le cloisonnement des systèmes afin que l'intervenant d'un métier pour une solution spécifique ne puisse pénétrer sur l'autre.

En principe, les Vlans paramétrés seront les suivants. Si l'existant ne correspond pas tout à fait à la liste ci-dessous, l'avis de l'AMO sera requis par le Titulaire, avant toute implémentation.

- Vlan par métier
- VLAN d'administration pour les composants réseau,
- VLAN Serveurs
- VLAN des postes client;
- 1 VLAN par procédé contenant les automates et autres équipements associés (entrées/sorties déportées, etc.).
- 1 VLAN « Quarantaine » pour tous les ports libres, en état « Shut Down »

La liste des Vlans n'est pas limitative. L'architecture globale intégrera l'ensemble des VLANS nécessaires au cloisonnement des domaines d'activité.

Les échanges inter-vlans seront établis par machine et type de protocole.

Les fonctions de routage devront être mises en œuvre sur la base de la matrice des flux préalablement validée par la MOA.

Lors de la réception des travaux, une cartographie de la configuration matérielle et logicielle installée ainsi que des flux actifs devra être établie par le Titulaire.

### 6.3.3.3 Les fonctionnalités <sup>4</sup>

#### 6.3.3.3.1 Fonctionnalités de sécurité nécessaires

- **SSH** « Secure Shell » et **SNMPv3** « Simple Network Management Protocol Version 3 » ;
- **SPAN** « Switched Port Analyzer » ;
- **MAC address notification** permettant aux administrateurs d'être notifiés lorsqu'un utilisateur est connecté ou déconnecté du réseau ;
- **Compatible 802.1x** avec fonction RADIUS de **CoA** « change of authorization » ;
- Authentification **TACACS+** et **RADIUS** ;
- **ACLs** « Access Control Lists » compatible IPv6 et IPv4 ;
- **BPDUGuard** « Bridge Protocol Data Unit » permettant de désactiver des ports paramétrés en port-fast en cas de boucle réseau ;
- **STRG** « Spanning-tree Root Guard » protection du ROOT spanning tree sur un réseau ;
- IGMP filtering ;
- Sécurisation des ports, type « Port-Security » de chez Cisco

#### 6.3.3.3.2 Fonctionnalités de redondance

- **RSTP** « IEEE 802.1s/w Rapid Spanning Tree Protocol » et **MSTP** « Multiple Spanning Tree Protocol » ;
- **PVRST+** « Per-VLAN Rapid Spanning Tree » ;

#### 6.3.3.3.3 QoS « Quality of Service »

- Minimum **4 queues** avec support du contrôle de la bande passante,
- Classification **CoS** « 802.1p class of service », avec un marquage et une classification par paquet, par source et destination d'adresse IP, MAC adresse, ou niv 4 TCP/UDP.

#### 6.3.3.3.4 Fonctionnalités supplémentaires

- **UDLD** « Unidirectional Link Detection Protocol » pour la détection d'erreur sur les Fibre optique ;
- **Proxy ARP local** « Address Resolution Protocol » pour la limitation des broadcast sur le réseau ;
- **IGMP** « Internet Group Management Protocol » **snooping** ;
- Broadcast, Unicast et multicast, storm control ;

---

<sup>1</sup> Le fabricant du produit proposé par le Candidat peut libeller ses fonctionnalités différemment, mais leur action doit être équivalente.

- **NTP** « Network Timing Protocol ».

#### 6.3.3.3.5 Fonctionnalités de management de la consommation

- IEEE 802.3az Energy Efficient Ethernet (EEE).
- POE (nativement adapté à la puissance des caméras, sans injecteur additionnel)

#### 6.3.3.4 *Qualification de l'infrastructure de câblage*

La qualification de l'infrastructure de câblage permettra de contrôler sa conformité aux normes en vigueur pour les réseaux hauts débits.

Elle permettra de valider l'ensemble des chaînes de liaison entre les points d'accès terminaux et les locaux de répartition y compris les cordons de brassage.

Toutes les liaisons feront l'objet d'un rapport de tests.

Au préalable, le cahier de définition des procédures et le document de recette « vierge » seront remis par le Titulaire pour validation de la forme.

La qualification sera réalisée par une entreprise spécialisée indépendante du ou des installateurs.

#### 6.3.3.5 *Surveillance des switches*

Même en cas de redondance activée, la supervision devra afficher les alarmes en cas de problème sur un switch, afin qu'une intervention soit déclenchée. Il sera donc nécessaire de remonter les Trap SNMP émis par les switches.

Le blocage des ports Ethernet et USB non utilisés doit être mis en place, ôté et réactivé à chaque mis à jour, à chaque intervention.

Les journaux de configuration doivent être analysés et conservés, la programmation sauvegardée régulièrement.

#### 6.3.3.6 *Les MacAdress*

L'adresse physique (MacAdress) de tous les équipements connectés sur le réseau (UTL, PC, serveur, tous les périphériques, etc) doivent faire l'objet d'un filtrage.

Pour mémoire, la procédure de filtrage consiste à allouer l'accès à toutes les adresses MAC connues du réseau technique de sécurité et empêcher toutes les autres de s'y connecter.

### 6.4 **LA LIAISON FIBRES OPTIQUES**

Les liaisons optiques sont dédiées à la communication du réseau technique CADIVS.

Ces liaisons sont indépendantes des rocares optiques demandées au titre de l'usage du MOA, par la DIRISI par exemple.

#### 6.4.1.1 *Les Têtes optiques : soudées*

Le raccordement est une étape importante dans la construction d'un réseau car il correspond à la mise à disposition et à l'exploitation d'un câble optique.

Étape nécessaire au déploiement, le raccordement de la fibre optique a un impact direct sur les performances du réseau et sur la facilité d'intervention lors de la maintenance. Le raccordement devra être effectué impérativement dans les règles de l'art, soit :

- le respect des rayons de courbure des fibres et des câbles
- un passage des fibres limitant tout risque de cassures, de macros ou micro-courbures postérieures à l'installation
- une identification des différentes connexions et des différentes fibres afin de faciliter l'utilisation et l'évolution du réseau (étiquettes à câbles : tenant et aboutissement ainsi qu' à chaque passage de mur, de chambre de tirage, à défaut tous les 2mètres)
- des valeurs de soudures et de composants (pigtaills, raccords) respectant le budget optique

##### 6.4.1.1.1 La soudure fibre optique ou épissurage par fusion

Le raccordement devra être effectué par soudure optique, selon le principe de l'alignement cœur à cœur.

Cette prestation exige la méthodologie et la compétence nécessaires afin de les pertes associées.

#### 6.4.2 Caractérisation des liaisons Fibres optiques

Les liaisons fibres optiques de type extérieur permettront le raccordement des commutateurs sur lesquels les équipements de sécurité devront être connectés.

La liaison fibres optiques sera constituée d'un câble multifibres monomode 9/125.

Ce câble sera armé, à structure tubée serrée, étanches, remplis, sans halogène, diélectriques avec une protection de classe C2 conforme à la norme NFC 32-070.

Les fibres optiques élémentaires seront conditionnées par tubes.

Les fibres optiques devront satisfaire les caractéristiques conformément à la norme ISO/IEC 11801 qui définit de façon complète l'ensemble des caractéristiques techniques des différents types de fibre multimode et monomode. Le titulaire présentera dans son offre la justification des différents choix et son adéquation avec la norme ISO/IEC 11801 en vigueur.

**Une attention particulière sera portée sur les bandes passantes et dispersion maximum.**

L'ordre de raccordement des fibres suivra le principe du code FOTAG IEEE 802.8 :

	Fibre 1	Bleu
	Fibre 2	Orange
	Fibre 3	Vert
	Fibre 4	Marron
	Fibre 5	Gris
	Fibre 6	Blanc
	Fibre 7	Rouge
	Fibre 8	Noir
	Fibre 9	Jaune
	Fibre 10	Violet
	Fibre 11	Rose
	Fibre 12	Turquoise

### 6.4.3 Spécifications des têtes de câbles optiques

Les tiroirs optiques seront rackables au format 19 pouces modulo 12 ou 24

Les encombrements **imposés** seront de 2U :

Caractéristiques des tiroirs de connexion :

Tiroir constitué de cassette 12 ou 24 connecteurs auto-verrouillables et pivotables

#### **Cassette équipée:**

- D'un logement de lovage et système d'arrimage des tubes.
- Dispositif de protection des points d'épissures.
- Dispositif de guidages des Pig-tails.
- Support des raccords de connectique en face avant pour permettre le brassage.
- Dispositif d'arrivée latérale des câbles, des jarretières et des Pig-tails.
- Dispositif de lovage des surlongueurs de jarretière.

Les tiroirs seront pré-équipés afin de garantir le respect des rayons de courbure des fibres et des cordons.

Les Interfaces d'épissurage auront des caractéristiques similaires aux tiroirs optiques mais sans façade de connecteur.

Ces racks seront équipés d'un platine de verrouillage en face avant sur lesquelles devront être apposées des étiquettes de repérage précisant le tenant / aboutissant et type de rocade fibres optiques.

#### 6.4.3.1 Spécifications des connecteurs optiques et épissures

Tous les connecteurs optiques devront être équipés de bouchon.

Les fibres optiques seront raccordées par épissurage de « pig-tail ».

Les connexions devront satisfaire les caractéristiques présentées ci-après.

#### **Spécifications imposées pour les connecteurs MT RJ**

Connecteur	Modularité	Multimode	Monomode	Pertes d'insertion par connexion
MT RJ	duplex	OUI	OUI	0.2 Db max

**Remarque :** Une connexion est constituée de deux fiches et d'un raccord.

Epissures	Multimode		Monomode	
	Nominal	Maximal	Nominal	Maximal
	0.1 dBb	0.15 dB	0.15 dB	0.3 bB

#### 6.4.3.2 Spécifications des jarretières optiques

Les jarretières optiques permettent le brassage dans les répartiteurs optiques et le raccordement sur les équipements actifs.

Ces cordons seront constitués de fibres ayant des caractéristiques identiques à celles des câbles d'infrastructure.

**Les jarretières doubles seront équipées de gaine « simplex » juxtaposées et collées.**

#### **Spécifications minimales à respecter :**

Diam. Ext tube (mm)	Protection	Temp. De service	Tension pose (daN)	Ecrasement (daN/cm)	Rayon de courbure (mm)	Perte insertion
0.9	Gaine colorée diam. 2.5 mm	-10/+70 °C	>=15	>=20	=<60	Norme CEI 874-1



#### 6.4.4 Qualification de l'infrastructure de câblage

La qualification de l'infrastructure de câblage permettra de contrôler sa conformité aux normes en vigueur pour les réseaux hauts débits.

Elle permettra de valider l'ensemble des chaînes de liaison entre les points d'accès terminaux et les locaux de répartition y compris les cordons de brassage.

**Toutes les liaisons feront l'objet d'un rapport de test.**

Au préalable, le cahier de définition des procédures et le document de recette « vierge » seront remis pour validation.

La qualification sera réalisée par une entreprise spécialisée indépendante du ou des installateurs.

##### 6.4.4.1 *Validation du réseau fibres optiques*

###### **Avant la pose**

Les câbles seront livrés avec un procès verbal de contrôle de sortie usine qui décrira leurs caractéristiques.

###### **Après la pose**

Les fiches de caractérisation permettront le contrôle des mesures par réflectométrie et échométrie :

- Les critères de performance (voir ci-avant)
- de la conformité des longueurs de liaisons normalisées
- de l'atténuation des liaisons

Le titulaire du marché devra compléter ces réseaux de pré câblage et d'équipements actifs afin de permettre le déploiement des différents équipements nécessaires à la mise en œuvre de la solution de détection intrusion et de contrôle des accès.

#### 6.5 LA BAIE D'HEBERGEMENT SERVEURS ET RESEAU

Fourniture et pose d'une baie de brassage 42 U (selon l'occupation proposée)

- 800 mm x 800 mm, avec portes saloon, équipée de montants à l'arrière pour les équipements réseau
- 800 mm x 1000 mm, pour les serveurs.

La baie de brassage sera équipée :

- de tiroirs optiques équipés de traversées optiques SC/SC pour le raccordement des fibres optique;
- d'un bandeau électrique 8 PC avec interrupteur raccordé sur un disjoncteur 16A dédié ;
- de bandeaux 24 RJ45, équipés de noyaux catégorie 6A câblés selon la norme TIA 568B ;
- les noyaux des bandeaux RJ45 et des prises RJ45 des équipements et PC seront du même fabricant ;

- de bandeaux guide cordons ;
- la baie sera raccordée à la terre du bâtiment via une barrette à coupure positionnée à l'extérieur de la baie.

**Un contact sec de type ILS sera installé sur tous les ouvrants des baies et coffrets. L'alarme d'ouverture de poste devra être intégrée à la supervision du système de sécurité.**

Chaque baie technique doit être équipée comme suit :

- Elle est accessible en faces avant et arrière. Elle comporte tous les équipements nécessaires pour recevoir le matériel actif et passif (y compris les chemins de câbles, les accessoires de fixation des équipements actifs et passifs, ... ) ;
- d'un ensemble de portes équipées d'une serrure à trois clés (le canon de serrure sera au standard européen) ;
- de portes avec un oculus transparent en plexiglas ou en verre ;
- d'un ensemble d'équipements complémentaires améliorant l'installation et l'organisation de la connectique (support de passage de câble latéral ou central, ... ) ;
- de passages de câbles et peignes fonctionnels et structurés ;
- de guide ou passe cordons assurant une organisation fonctionnelle des câbles en face avant comme en face arrière de l'armoire ;
- de points de mise à la terre de l'armoire.
- L'implantation au sol des armoires et l'aménagement interne des équipements installés devront apparaître dans les dossiers techniques fournis au titre du DOE
- Chaque baie sera construite de manière à pouvoir supporter une charge de 350 Kg.

### 6.5.1 Équipement électrique des baies et coffrets

Les équipements électriques destinés à la basse tension (230V) seront conformes à la norme française NF C 15 100 sur les installations électriques.

Chaque baie sera équipée :

- d'une ou plusieurs rampes de huit prises secteur 16 A protégées par un disjoncteur plus le raccordement à la terre ; leur nombre devra être suffisant pour alimenter l'ensemble des matériels installés plus 30% de réserve ;
- d'un cordon de raccordement de cinq mètres à minima équipé d'une prise de courant normalisée ;
- d'une mise à la terre conforme aux règles en vigueur dont une borne de prise de terre et un cordon normalisé de raccordement de couleur vert et jaune d'un diamètre de 6 mm.
- L'installation doit être conforme au guide pratique pour la réalisation des masses « GAM T22 ». Toutes les terres dans l'enceinte du bâtiment doivent être interconnectées avec une barrette de coupure. Les terres pour courants faibles sont dites « terres informatiques » et seront installées selon la norme actuelle EN 50 174 dans le respect de l'état de l'art.

Afin d'améliorer la protection des matériels actifs hébergés et selon les exigences particulières définies pour le besoin du site, des onduleurs devront être proposés.

Les armoires doivent, par conséquent, pouvoir supporter l'installation d'onduleurs montés en rack.

Chaque coffret sera équipé d'une batterie, permettant l'alimentation des équipements pendant au mois 48h

### 6.5.2 Sécurisation des liaisons

L'ensemble des câbles de liaisons devra bénéficier d'un système d'autoprotection qui pourra se faire à plusieurs niveaux SSI :

- pour les capteurs, coffrets de gestion, baies, etc., et câbles de liaison associés, de manière classique par des capteurs d'autoprotection et une paire réservée sur le câble ;
- pour les matériels raccordés sur le réseau informatique dédié, par une mesure de la continuité de l'écran de la baie de raccordement jusqu'à la prise d'extrémité.
- Etc.

Dans tous les cas, dès qu'un défaut sera identifié, il sera ramené sur l'hyperviseur centralisé. Le graphisme des capteurs, matériels informatiques et câbles de liaison susceptible de détecter cet incident apparaîtront surfacé avec une couleur distincte, avec une consigne associée fournissant des éléments d'informations sur le câble et les matériels des deux extrémités (baie, poste informatique, capteur, .....).

## 6.6 **REPORTS DES ALARMES ET GESTION DE CONFIGURATION**

### 6.6.1 Borniers d'interconnexion et de prise d'informations alarmes

Toutes les alarmes techniques qui pourront être demandées en cours de réalisation devront être raccordées en « contact sec » sur les modules prévus à cet effet chez le même constructeur.

Ces modules seront dédiés aux alarmes techniques (des synthèses) ainsi que quelques contacts secs. Ils seront installés dans des coffrets auto-protégés (contacts d'ouverture), dans le local technique. Toutes les arrivées IP seront prévues entre les coffrets et la baie de manière à ce que le raccordement de ces informations soit prêt pour l'intégration dans l'hyperviseur.

Les alarmes d'état et de synthèse des centrales incendie seront remontées sur l'hypervision du CADIVS, **en contacts sec** (aucun lien informatique)

### 6.6.2 Pré Requis au déroulement des reports d'alarmes

Avant toute opération de report des alarmes, il sera procédé à une réception partielle permettant de valider les modifications et compléments matériels et logiciels effectués.

Les actions intermédiaires à valider sont les suivantes :

- la création et la gestion du carnet de brassage,

- la préparation, l'organisation et le suivi des essais de report,
- la réalisation des essais unitaires et transverses.

Deux types d'essais sont demandés :

- les essais unitaires permettant de valider les modifications et le câblage réalisés,
- les essais transverses (ou d'intégration) permettant de valider chaque alarme depuis le capteur jusqu'au poste d'exploitation de l'hyperviseur **CADIVS**.

### 6.6.3 Tests unitaires

Une première série de tests unitaires a pour fonction la vérification de la conformité du câblage par rapport aux carnets de câbles et aux schémas de câblage : type de bornes, numéros de bornes, type de câbles, couleur des conducteurs, repérage des câbles.

Ils permettent aussi de valider le respect des règles de l'art (fils non utilisés raccordés à la masse, ...).

Dans tous les cas suivants et pour chaque ligne d'alarme raccordée, ces essais contrôleront l'impédance de ligne :

- Contact au repos,
- Contact en alarme,
- Court-circuit,
- Ouverture de ligne.

Compte tenu des résultats attendus, ils nécessiteront donc la mise en œuvre réelle de l'instrumentation ou d'une simulation par shunt au plus près du capteur .

Une deuxième série de tests unitaires permettra de vérifier le bon fonctionnement et l'atteinte du résultat attendu des évolutions des systèmes modifiés tels que les sorties TOR des centrales incendie et les nouvelles informations traitées suites à la reprise de configuration des installations.

### 6.6.4 Essais transverses

Ils ont pour objectif la validation du câblage, de la transmission et de la programmation des alarmes.

Après les contrôles internes et les tests unitaires, les essais transverses permettront de valider exhaustivement la totalité de la base de données des alarmes.

Au même titre que les tests unitaires, ces tests d'intégration s'appuieront sur le changement d'état des capteurs autant que faire se peut.

Tous les essais seront produits à partir de dossiers d'essais tels que plans d'essais, fiches de tests unitaires et transverses ; ils donneront lieu à l'édition de rapports d'essais finaux.

L'organisation des essais est basée sur le rôle et la mission de chacune des parties définies de la façon suivante :

- Le titulaire chargé de la maintenance (Service Technique en charge du maintien en configuration de l'installation) aura en charge le changement d'état du capteur à l'origine de l'alarme à tester,
- Le titulaire aura pour mission de vérifier et de contrôler le changement d'état au niveau de la supervision,
- Le titulaire consignera le résultat du test pendant la phase opérationnelle de ces essais ; préalablement, le titulaire de ce marché aura préparé et organisé tous ces tests, pour la part technique proprement dite mais aussi en terme organisationnel : constitution du planning prévisionnel, organisation des séquences au travers de réunion avec les autres intervenants notamment, préparation des demandes d'intervention, gestion des clés des locaux, ...

Il est à prévoir une campagne d'essais par zone géographique et par système. Elle se déroulera en présence du maître d'œuvre (ou ses représentants).

Les moyens humains et matériels sont de la responsabilité du titulaire.

Les dossiers d'essais préparés par le titulaire du marché seront fournis 10 jours ouvrés minimum avant le déroulement des OPR.

Le titulaire doit prévoir la mise en configuration d'essais de l'installation et avoir obtenu toutes les autorisations préalables pour réaliser les essais.

Le titulaire prendra à sa charge les dépannages et essais correctifs nécessaires et suffisants pour atteindre les attendus.

Le titulaire réalisera un nouvel essai à sa charge si l'essai n'est pas concluant.

Au terme des travaux réalisés, le maître d'œuvre se réserve le droit de demander à ce que les essais soient repris par tranche, si une contrainte liée à l'exploitation du site l'exige.

#### 6.6.5 Livrables attendus

- le carnet de brassage rigoureusement tenu à jour et validé à T0 + 1 mois,
  - les rapports d'essais unitaires du câblage et des modifications de configuration à T0 + 1 mois,
  - les rapports d'essais transverses à T0 + 1 mois.

### 6.7 CABLES MULTIPAIRES DE LIAISON

Les câbles d'interconnexion à intégrer dans le système seront donc **de type C2**.

Les câbles mis en œuvre respecteront les exigences CEM du site ;

Ils présenteront un blindage général et seront écrantés par paires.

Le blindage général présentera une continuité avec les éléments de mise à la terre et notamment, ils seront mis en contact avec les carcasses métalliques des coffrets d'interconnexion.

Une mesure de continuité sera effectuée pour chaque câble et sur chaque pénétration de coffret.

Les câbles à utiliser seront de la gamme Câble SYT+ DIGITAL 8 SYT+ DIGITAL - LSOH - NPI marron.

## 6.8 COMPATIBILITE ELECTROMAGNETIQUE « CEM »

Le titulaire met en œuvre les moyens de protection adaptés à ces environnements pour protéger les composants de niveau standard « Industriel » conformes aux normes NF EN 61000-4-2 et NF EN 61000-4-6. Le titulaire respecte les procédures de tests et niveaux mentionnés dans ces deux normes et celles qui y sont mentionnées.

Ils présenteront un blindage général et seront écrantés par paires.

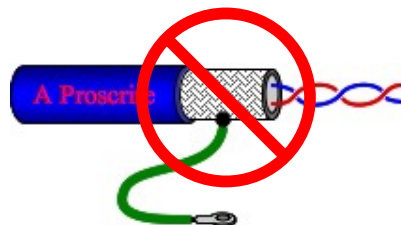
Le blindage général présentera une continuité avec les éléments de mise à la terre notamment seront mis en contact avec les carcasses métalliques des coffrets d'interconnexion.

Une mesure de continuité sera effectuée pour chaque câble et sur chaque pénétration de coffret.

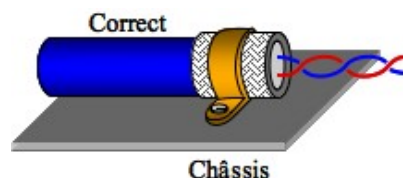
La protection contre les perturbations (radio, rayonnement d'étincelles, rayonnement de la foudre,...) est faite par l'écran du câble. Il doit impérativement être relié aux masses des équipements à chaque extrémité, en général à la tôle de fond d'armoire ou au maillage de la salle technique.

Cette interconnexion ne pose aucun problème de circulation de courant résiduel de foudre sur l'écran. Les calculs montrent que le courant circule préférentiellement dans les conducteurs de cuivre accompagnant la liaison.

A chaque extrémité, la liaison à la masse doit être faite par un cavalier métallique. Toute liaison par fil (queue de cochon), même court, est à proscrire.



Montage par queue de cochon à éviter absolument.



Toujours relier les écrans des câbles à la tôle ou grille de fond de coffret avec des cavaliers métalliques ou tout accessoire équivalent.

Les câbles signaux et alimentation doivent être éloignés au minimum de 30 cm pour éviter toute diaphonie.

## 6.9 LA FORMATION

Le titulaire établit un plan de formation afin de permettre le transfert de compétences au terme de la prestation de l'installation, suivi de la formation des utilisateurs lors de la mise en exploitation du système de GTC et de CADIVS.

Les formations porteront essentiellement sur le CADIVS, la GTC et le Système de sécurité incendie (SSI).

**Formation « utilisateur »** : 1 session de huit personnes – 1 journée maximum (2 demi-journées)

**Formation « utilisateur avec pouvoirs »** : 1 session de trois personnes – 1 journée maximum (2 demi-journées)

**Formation Administrateur** : 1 session de deux personnes - 2 x 2 jours

Pour chaque formation le titulaire prévoit la documentation et tout support nécessaire à la bonne administration et utilisation du système.

- Plan de formation
- Manuel de formation
- Manuel de travaux pratiques
- Dossier système

**NB** : une Notice simplifiée doit être établie à l'attention des gardes du site, après validation du Maître d'œuvre.

## 7 DOCUMENTS A FOURNIR PAR LE TITULAIRE DU MARCHE

---

Toute modification sur l'installation en écart avec la documentation actuelle, nécessite une mise à jour de celle-ci à savoir, les plans d'implantation et les synoptiques, les carnets de détails, .....

Les documents réalisés par le titulaire respecteront le formalisme et les règles d'identification données en vigueur.

Ils seront rédigés exclusivement en français.

Ils seront aussi remis sous format informatique, compatible avec les logiciels utilisés.

Il sera fourni le dossier complet d'ouvrage exécuté pour les CADIVS installés. La fourniture au format BIM des plans et annexe au format BIM est à privilégier.

Les documents attendus sont :

**A fournir avant LA PERIODE DE PREPARATION, puis au terme du marché en version TQC<sup>5</sup>.**

- Tous les plans et schémas de raccordement des installations
- **Les documents des spécifications techniques,**
- **Le document des spécifications fonctionnelles,**
- Le planning d'intervention,
- Le planning des tâches en y incorporant la constitution de la maquette, les essais et la mise en service provisoire de réception des installations et de levée des réserves,
- Le plan de prévention,
- Le Dossier d'Assurance Qualité,
- Le plan de Management Qualité,
- Le plan « qualité logiciel »,
- La liste prévisionnelle des documents et plans,

Les documents réalisés par le titulaire respecteront le formalisme et les règles d'identification données en vigueur.

Ils seront rédigés exclusivement en français.

Ils seront aussi remis sous format informatique, compatible avec les logiciels utilisés

---

<sup>5</sup> TQC : Tel Que Construit



## 7.1 FOURNITURE DES FICHES TECHNIQUES

### Avant travaux :

- Dossier d'étude d'exécution
- les plans et schémas d'exécution.
- Dans un délai d'un mois après l'ordre de début de travaux, le titulaire du présent lot doit remettre, pour acceptation, les fiches techniques de l'ensemble des matériels à installer.

### Au fur et à mesure de la réalisation :

- le catalogue méthodique tenu à jour mensuellement, il permettra le suivi des publications par indice et du circuit de visa,
- les fiches-produit des nouveaux matériaux ou la référence aux fiches existantes, pour acceptation,
- les plans et schémas relatifs aux travaux, les plans modificatifs de l'existant,
- le certificat de classement des produits / matériaux (ex. porte coupe-feu, équipement de sécurité),
- les fiches d'écart ou de non-conformité, s'il y a lieu (en original).

### APRES ACHEVEMENT DES TRAVAUX

En fin de réalisation le titulaire du marché fournira le Dossier des Ouvrages Exécutés (DOE) comprenant :

- Les plans de recollement ;
- Procès-verbaux des essais réalisés ;
- Code constructeur.
- Le Dossier des Ouvrages Exécutés (DOE) suivant un reproductible, trois tirages et un CD informatique de l'ensemble du dossier composé de :
  - Plans mis à jour
  - Plans des constructeurs ;
  - Notices d'entretien des matériels ;
  - Recettes des matériels ;
  - Rapports des mesures.
- les fiches de contrôles et essais,

**Le titulaire doit aviser le maître d'œuvre, au moins 15 jours ouvrables avant la date de commencement des essais**

- les schémas mis à jour TQC sur la base des documents joints au présent DCE,
- le dossier de câblage mis au format EXCEL,
- toute la documentation existante impactée par les travaux.

Les DOE respecteront les instructions spécifiées « Instruction construction d'un DOE ».

Cette liste n'est pas exhaustive.

La non fourniture des documents précisés fera l'objet de pénalités.

Le titulaire est chargé de l'établissement des divers plans et schémas d'exécutions et notes de calculs relatifs à ses prestations. Les fiches Produits ainsi que tous les documents d'exécutions devront être soumis au visa préalable de représentant du maître d'Œuvre.

Le Titulaire devra produire et présenter au maitre d'œuvre pour acceptation les documents ci-après définis sous forme papier en nombre de trois exemplaires dans des boites « Cauchards » et sous forme de fichiers informatiques (clé USB).

## 8 RECEPTION DES PRESTATIONS

---

Un cahier de réception sera élaboré par le Titulaire et sera soumis à l'approbation de la Maîtrise d'Œuvre au plus tard 3 semaines avant les Opérations Préalables à la Réception (OPR).

Ces cahiers seront principalement constitués :

- Le document des spécifications techniques et détaillées
- Le document des spécifications fonctionnelles et détaillées,
- Les documents de Formation
  
- des fiches de tests unitaires et des fiches d'essais transverses,
- des fiches de réception des modifications matérielles et logicielles des équipements existants,
- des carnets de câbles validés,
- des schémas de câblage des armoires ou coffrets modifiés.

Ils feront état, rigoureusement et exhaustivement, de la configuration de l'installation réalisée.

## 9 ASSURANCE QUALITE

### 9.1 SYSTEME QUALITE

Pour la réalisation des prestations définies par le présent cahier des charges, le Titulaire doit mettre en œuvre et entretenir un système qualité conforme aux exigences de la norme ISO 9001 2000.

Ce système doit couvrir l'ensemble des missions de la prestation, l'ensemble des processus mis en œuvre pour réaliser ces missions et les activités de gestion de la qualité correspondant aux critères de la norme ISO 9001. Il doit traiter en particulier :

- la détection des amorces de dérive,
- la prévention des non-conformités, les actions correctives,
- la traçabilité des opérations,
- les enregistrements relatifs à la qualité.

Ce système qualité comprend :

- le manuel qualité (ou équivalent) du Titulaire,
- le plan d'assurance de la qualité – PAQ – spécifique à la prestation, les plans de contrôle de la qualité, le « plan qualité » logiciel,
- la liste des documents applicables,
- la liste des procédures (établies ou à établir),
- les procédures correspondant aux critères de la norme ISO 9001 et aux processus mis en œuvre pour préparer et réaliser les prestations,
- les modes opératoires, modèles (imprimés ou informatisés), etc.

**Nota :** Les procédures propres du Titulaire pourront être utilisées, après adaptation aux formes prescrites par le client.

Le Titulaire utilisera conformément aux règles de management les méthodologies et outils, en vigueur au sein du projet et applicables à son périmètre d'activité, en :

- exigences de management de programme,
- organigramme des tâches,
- organisation du programme,
- logique de déroulement et de suivi de programme,
- maîtrise des coûts et des délais (Périmètre coûts réservé au client),
- gestion de la Configuration,
- soutien Logistique Intégré,
- assurance de la Qualité,
- gestion de la documentation.

Cette organisation devra être décrite dans le PAQ du titulaire.

## 10 VERIFICATION DES INSTALLATIONS, ESSAIS ET MESURES

---

A l'issue des travaux, un organisme de contrôle agréé procèdera à la vérification initiale de toutes les installations et délivrera un procès-verbal de conformité (commande et règlement à charge du titulaire).

En préalable, le titulaire fournira pour acceptation du maître d'œuvre, les coordonnées de l'organisme de contrôle.

## 11 NETTOYAGE ET PROTECTION DES OUVRAGES

Le titulaire de la présente section technique a la responsabilité du nettoyage et de la protection des ouvrages réalisés par ses soins jusqu'à la réception de l'ensemble des travaux.

Le titulaire devra la gestion des bennes à gravats pendant toute la durée du chantier, le coût de ces bennes étant à sa charge.

Le nettoyage du chantier sera effectué chaque jour, à l'avancement des travaux. Le Maître d'œuvre se réservant le droit de faire exécuter aux frais du titulaire des nettoyages complémentaires si cela s'avérait nécessaire.

### 11.1 Tri et évacuation des déchets

En phase de travaux, le titulaire devra la gestion et l'évacuation de ses déchets. Les déchets inertes pourront être chargés directement dans les camions pour être évacués aux décharges prévues à cet effet. Les autres déchets seront stockés dans des bennes ou si besoin des conteneurs sélectifs appropriés suivant la famille de matériaux.

## 12 DOCUMENTS APPLICABLES ET DOCUMENTS DE REFERENCE

### 12.1 DOCUMENTS TECHNIQUES APPLICABLES AU MARCHÉ

- Le présent CCTP ;
- Les DTU et les normes en vigueur ;
- Le Code Civil ;
- Le Code du Travail ;
- Les documents cités dans cette section, en particulier ceux relatifs à la cybersécurité et aux exigences ANSSI.

### 12.2 LIVRABLES ATTENDUS

Le prestataire devra fournir

- le document détaillé des « Spécifications Techniques »
- et celui des « Spécifications Fonctionnelles » :

une première version en début de projet, suite à la collecte d'information, puis finalisé TQC pour les OPR. Ce document être synthétisé en un seul, mais il devra être bien organisé et détaillé.

Toutes les fonctionnalités et installations techniques fournies, paramétrées et mises en service doivent être décrites avec précision dans ce dossier (spécifications techniques et fonctionnelles).

Le prestataire devra fournir

- une procédure de tests pour les OPR
- et fournir le rapport contenant les risques résiduels.
- Tous les supports de formation devront être intégrés au DOE
- Le carnet de brassage rigoureusement tenu à jour et validé à T0 + 1 mois,
  - Les rapports d'essais unitaires du câblage et des modifications de configuration à T0 + 1 mois,
  - Les rapports d'essais transverses à T0 + 1 mois.

Le prestataire devra fournir

- une cartographie, un synoptique (physique, logique, applications (flux) et administration) en réponse au marché. Il devra mettre à jour ce document au moment des OPR.

Les synoptiques du réseau, des installations techniques et logicielles effectuées au titre de ce marché doivent faire l'objet de mise à jour de plan existants lorsqu'ils existent ou de création de nouveaux plans. Les formats requis sont papier et numérique.

## 13 ANNEXE 1 : MATRICE DE COMPETENCES

Le fichier Excel est fourni pour faciliter la saisie des informations

MATRICE DES COMPETENCES TECHNIQUES					
Compétences	Nb total intervenants	Profil 1 Expert	Profil 2 Ingénieur	Profil 3 Technicien	Profil 4 Débutant
<b>Gestion de projet</b>					
Suivi et gestion de projet					
Sécurité organisationnelle					
Gestion des risques					
Audit Organisationnel					
Audit LPM					
Conseil et gouvernance					
<b>Matériel réseaux :</b>					
Alcatel					
Hirschmann					
Scalance					
HP					
Cisco					
Moxa					
Dlink					
Checkpoint, Fortinet					
<b>Solutions CA-DI-VS</b>					
TIL-TECHNOLOGIE					
NEDAP					
SYNCHRONIC					
GUNNEBO					
CASTEL					
STENTOFON					
TRAKA					
autres					
ajoutez toutes marques présentées dans votre réponse					
<b>SOLUTION DE VIDEOSURVEILLANCE (Systèmes et marques)</b>					
GENETEC					
MILESTONE					
BOSCH					
AXIS					
GUNNEBO					



AXIS					
BOCH					
SAMSUNG					
autres					
<b>Administration Windows :</b>					
Windows 7					
Win US					
Windows Server 2003					
Windows Server 2008					
Windows Server 2012 R2					
Expertise Linux et systèmes UNIX					
<b>Réseau Informatique</b>					
Certification du constructeur proposé					
Fonctions avancées (802.1Q, 802.1X, VLAN Trunking Protocol,...)					
...					
<b>Informatique Industrielle : GTPC/GTB</b>					
VxWorks					
PC industriels, contrôle-commande					
Superviseur industriel PANORAMA E2 et P2, PC Vue,					
PC Vue					
Rétro ingénierie de protocole					
Fuzzing de protocole					
<b>Bureautique :</b>					
MS/office (Word, Excel, Powerpoint, Access, project)					
...					
<b>Développement :</b>					
Scripts système					
C, Python, C++, Go, Git					
<b>CFI-CFS :</b>					
Courants Faibles industriels et de sécurité					

Ces compétences et profils sont donnés ici à titre d'exemple seulement.

Le candidat pourra ajouter, modifier selon son besoin.

En revanche, chaque logiciel ou matériel proposé par le candidat devra être intégré dans cette matrice de compétences.

## 14 ANNEXE 2 : TAUX HORAIRES

### TAUX HORAIRES ET COEFFICIENT DE PEINES ET SOINS APPLICABLES AUX PRESTATIONS REMUNEREES EN DEPENSES CONTROLEES

Catégories de personnel	Taux Horaires	Taux horaires	Taux horaires
	heures ouvrées 6h00 / 21h00	heures non ouvrées 21h00/06h00	Jours fériés et Week-End
	Du Lundi au Vendredi (€ HT)	(€ HT)	(€ HT)
Chef de projet/Experts			
Ingénieur – administrateur système			
Automaticien – CFI CADIVS			
Projeteur			
Conducteur de travaux			
Chef de chantier			
Technicien de chantier			
Monteur			
Autre acteur projet (préciser)			

Coefficient de peines et soins	
--------------------------------	--

NB 1 : Les taux horaires "Ingénieur" doivent correspondre à des taux horaires moyens (quelque soit le profil d'ingénieur)

NB 2 : Les profils "Expert" et "Chef de projet" devront clairement être justifiés en termes de certifications

FIN DU DOCUMENT