

CAHIER DES CLAUSES

TECHNIQUES PARTICULIERES

(C.C.T.P)

Objet du marché :

STRASBOURG (67) – Quartier Turenne

Relogement du bureau d'études de Strasbourg sur la caserne Turenne

Lot : Contrôle d'accès – Détection intrusion – Vidéosurveillance (CADIVS)

COSI n° 466037

Table des matières

1. DISPOSITIONS GENERALES DES OUVRAGES DE SURETE	4
1.1. GENERALITES	4
1.2. LES ATTENDUS DU SYSTEME INDUSTRIEL DE SURETE	4
1.3. LES ACTEURS ET LEURS ROLES	4
1.3.1. <i>Le SID</i>	4
1.3.2. <i>L'intégrateur</i>	4
1.3.3. <i>Le bénéficiaire : Bureau d'étude (BE)</i>	4
1.4. DOCUMENTS	5
1.4.1. <i>Documents techniques applicables au marché</i>	5
1.4.2. <i>Plans joint au marché</i>	5
1.4.3. <i>Autres documents joints au marché</i>	5
1.4.4. <i>Pièces à fournir par le titulaire du marché</i>	5
1.4.5. <i>Documents de références</i>	6
1.4.6. <i>Acronymes</i>	6
1.5. ESSAI ET CONTROLES	6
1.6. PRESCRIPTION GENERALES D'EXECUTION	7
1.6.1. <i>Réservations – percements - scellements</i>	7
1.6.2. <i>Mise en oeuvre de source de chaleur</i>	7
1.6.3. <i>Préventions contre l'incendie</i>	7
1.6.4. <i>Produits et matériaux</i>	7
1.6.5. <i>Nettoyage et protections des ouvrages</i>	7
1.7. BORDEREAU DE SUIVI DES DECHETS	8
1.7.1. <i>Procédures et généralités</i>	8
1.7.2. <i>Déchets électroniques</i>	8
1.7.3. <i>Gestion des déchets dangereux</i>	8
2. CONTENU ET DEROULE DU PROJET	8
2.1. REUNION DE LANCEMENT	8
2.2. REALISATION	9
2.2.1. <i>Mise en œuvre d'un démonstrateur</i>	9
2.2.2. <i>Recette du démonstrateur (VdR)</i>	9
2.2.3. <i>Déploiement sur site</i>	10
2.2.4. <i>Mise en ordre de Marche (MOM)</i>	10
2.3. HOMOLOGATION	10
2.3.1. <i>Vérification d'Aptitude (VA)</i>	11
2.3.2. <i>Conditions de passage de la VA à la VSR</i>	11
2.3.3. <i>Vérification de Service Régulier (VSR)</i>	11
2.3.4. <i>Conditions de passage de la VSR à l'exploitation</i>	12
2.4. FORMATIONS	12
2.5. GARANTIES	13
2.6. MCO PREVENTIFS (TRANCHE OPTIONNELLE N°1)	13
2.6.1. <i>Durée</i>	13
2.6.2. <i>Prestations de MCO maintenance préventive</i>	13
3. DISPOSITIONS TECHNIQUES DES OUVRAGES DE SURETE	16
3.1. LIMITES DE PRESTATION	16
3.2. DESCRIPTION DES TRAVAUX DU PRESENT LOT	16
3.3. PRINCIPES DE BASE	17
3.3.1. <i>Principe du zonage</i>	17
3.3.2. <i>Principe de fermeture/ouverture</i>	17
3.3.3. <i>Principe d'accès aux locaux de la ZP</i>	17
3.3.4. <i>Principe des zones d'alarme</i>	17
3.3.5. <i>Principe de la vidéosurveillance</i>	18
3.3.6. <i>Report du CADIVS</i>	18
3.3.7. <i>La distribution du bâtiment</i>	18

3.3.8.	<i>Equipements centraux Existants</i>	18
3.4.	LES INFRASTRUCTURES PHYSIQUES DU SYSTEME DE SURETE	19
3.4.1.	<i>Alimentation électrique des baies</i>	19
3.4.2.	<i>Architecture physique demandée</i>	19
3.4.3.	<i>Infrastructure physique</i>	20
3.5.	LES INFRASTRUCTURES SI DU SYSTEME DE SURETE	20
3.5.1.	<i>Architecture logique retenue</i>	21
3.5.2.	<i>Sécurisation de l'infrastructure</i>	21
3.6.	CARNET DES MATERIELS ET SOLUTIONS TECHNIQUES	22
3.7.	PRECISIONS TECHNIQUES DU VIDEOPORTIER	23
3.8.	PRECISIONS TECHNIQUES DU CCGE	23
3.8.1.	<i>Matériel du système</i>	23
3.8.2.	<i>Puissance du matériel informatique</i>	23
3.8.3.	<i>Alimentation électrique 220V</i>	23
3.8.4.	<i>Câble « réseau »</i>	23
3.8.5.	<i>Les différents comptes</i>	23
3.8.6.	<i>Règles de Sauvegarde</i>	23
3.8.7.	<i>Implantation</i>	24
3.8.8.	<i>Spécifications particulières</i>	24
3.9.	PRECISIONS TECHNIQUES SUR LE SYSTEME DE CONTROLES D'ACCES	24
3.9.1.	<i>Note préliminaire</i>	24
3.9.2.	<i>Caractéristiques des matériels</i>	24
3.10.	LE SYSTEME DE DETECTION INTRUSION (DI)	26
3.10.1.	<i>Note préliminaire</i>	26
3.10.2.	<i>Equipement des locaux</i>	27
3.11.	LE SYSTEME DE VIDEOSURVEILLANCE	27
3.11.1.	<i>Note préliminaire</i>	27
3.11.2.	<i>Zone de surveillance</i>	28
3.11.3.	<i>Performances de surveillance</i>	28
3.12.	PRECISIONS TECHNIQUES SUR LA SUPERVISION TECHNIQUE	28
3.13.	PRECISIONS TECHNIQUES SUR LES COMPTES UTILISATEURS ET L'ADMINISTRATION DU S2I	29
3.13.1.	<i>Principes généraux des comptes utilisateurs</i>	29
3.13.2.	<i>Principes d'administration et procédures</i>	29
4.	ANNEXE 1 – DOCUMENTS DE REFERENCE	30
5.	ANNEXE 2 – ACRONYME	34
6.	ANNEXE 3 - TERMINOLOGIE	42
7.	ANNEXE 4 – SERVEUR PRINCIPAL DU LOCAL PRINCIPAL CADIVS	43
8.	ANNEXE 5 – SERVEUR DE SECOURS DU LOCAL DE SECOURS CADIVS	44
9.	ANNEXE 6 _ GAMMES DE MAINTENANCE	45
10.	INDEX SCHEMAS ET TABLEAUX	50

1. Dispositions générales des ouvrages de sûreté

1.1. Généralités

Le présent document a pour but de définir les prestations des travaux de Sûreté pour la mise en œuvre d'un système de contrôle d'accès, de détection intrusion et de vidéo surveillance (CADIVS) en vue du relogement du bureau d'études de Strasbourg (BE STG) au dernier étage du bâtiment 009 de la Caserne Turenne, 67000 Strasbourg. Le projet se situe dans une enceinte militaire clôturée avec un poste d'accueil et de filtrage (PAF).

1.2. Les attendus du système industriel de sûreté

Les ouvrages du présent lot CADIVS comprendront les études de conception et la réalisation des installations suivantes :

- ▶ Les Infrastructures Sûreté
- ▶ Le Contrôles d'Accès
- ▶ La Détection Intrusion
- ▶ La Vidéosurveillance
- ▶ Une surveillance technique
- ▶ Une vidéophonie/interphonie à l'entrée du BE reportée au secrétariat indépendante
- ▶ Un coffre à clé à gestion électronique (CCGE)

Enfin, il a aussi pour but de définir les exigences pour le maintien en condition opérationnelle (MCO) et de sécurité (MCS) sur 2 ans.

1.3. Les acteurs et leurs rôles

1.3.1. Le SID

Le SID est chargé de conduire, ou de faire conduire, les travaux relevant de sa responsabilité d'opérateur d'infrastructure. Il est notamment responsable de la validation des travaux relevant de ses compétences :

- ▶ travaux bâtimentaires : murs, clôtures, obstacles ;
- ▶ énergie : courants forts, groupe électrogène, onduleurs ;
- ▶ climatisation ;
- ▶ incendie.

1.3.2. L'intégrateur

L'intégrateur est chargé de :

- ▶ de réaliser les études de conception du système,
- ▶ de le mettre en œuvre,
- ▶ de contribuer au montage du dossier d'homologation pour l'autorité compétente (voir paragraphe 1.1.4) ;
- ▶ d'assurer le maintien en condition opérationnelle (MCO) et de mise en condition de sécurité (MCS) pendant deux ans du système

Il aura aussi l'administration du système pour l'installation/mise à jour, la configuration ainsi que le suivi du bon paramétrage de l'ensemble des composants matériels et logiciels du système d'information. Il devra notamment assurer ceux-ci pour les services principaux de sécurité, y compris pendant la durée de deux ans du MCO/MCS sur :

- ▶ segment d'interface,
- ▶ équipement de sécurité (pare-feu, proxy application, etc.),
- ▶ analyseur de contenu,
- ▶ solutions d'authentification,
- ▶ solution d'analyse des journaux d'évènements,
- ▶ solutions de sauvegarde et de restauration,
- ▶ solution de bascule.

1.3.3. Le bénéficiaire : Bureau d'étude (BE)

La menace opérationnelle est une donnée d'entrée pour définir la vulnérabilité d'un site et par conséquent pour définir le besoin opérationnel en termes d'effet à produire. Le bénéficiaire est à l'origine de l'expression de ce besoin.

A ce titre, lors de la phase d'exécution :

- ▶ il participe aux groupes de travail permettant de définir les interfaces Homme/Machine (IHM) et de prendre en compte les processus métier ;
- ▶ il est convié aux séances de formation permettant la prise en main du système ;

- il participe à la validation du système lors de la période de vérification d'aptitude et de service régulier (VSR).

1.3.3.1. L'AUTORITE D'HOMOLOGATION (DIRECTEUR DC BE)

L'autorité d'homologation (AH) du système d'information industriel (S2I) du contrôle d'accès, de détection-intrusion et de vidéo-surveillance (CADIVS) est le directeur de la direction centrale du bureau d'étude ou son représentant désigné.

1.3.3.2. LE RSSI-P (DC BE)

Le responsable de la sécurité du système d'information en phase projet (RSSI-P) est responsable du niveau de sécurité que doit atteindre le système d'information industriel (S2I) de protection. Il doit s'assurer que le système d'information industriel (S2I) mis en œuvre respecte les règles de la sécurité des systèmes d'information (SSI) imposées par le ministère augmenté par les règles en vigueur au sein du bureau d'étude qui sont retranscrites dans le contrat. Il est également chargé de s'assurer de la constitution du dossier d'homologation qui sera présenté à la commission d'homologation.

A ce titre, il participe à tous les groupes de travaux SSI du S2I du projet.

1.3.3.3. LE RSSI-A : BE LOCAL (CHEF OU SOP OU CZSIC)

Le responsable de la sécurité du système d'information aval (RSSI-A) définit la politique de sécurité du système d'information industriel (S2I). Il est responsable de faire appliquer le processus de maintien en condition de sécurité (MCS) sur le système. Il est notamment responsable du maintien du niveau de sécurité du système de protection homologué par l'autorité d'homologation, pendant toute la durée de son exploitation.

A ce titre, il participe, autant que de besoin, aux groupes de travaux SSI du projet.

Pour les systèmes SECPRO déployés, le RSSI-A est désigné par le représentant de l'autorité d'emploi, précisée dans la stratégie d'homologation.

1.4. Documents

1.4.1. Documents techniques applicables au marché

Les prescriptions techniques incluses dans le présent document prennent valeur contractuelle pour l'exécution des travaux exceptés dans le cas des dérogations explicitement mentionnées dans le présent DTP.

Les installations devront être établies suivant les règles de l'art (cahiers et avis techniques) et les prescriptions des lois, décrets, arrêtés ministériels en vigueur à la date de la signature du marché et tous documents publiés par le C.S.T.B.

1.4.2. Plans joint au marché

Les plans joints au marché sont au nombre de 4 définis ci-dessous :

Numéro	Intitulé	Etat
1	plan de masse	Futur
2	Vue en plan du niveau RDC	Futur
3	Vue en plan du niveau 002	Futur
4	Vue en plan du niveau 003	Futur

1.4.3. Autres documents joints au marché

- Diagnostic amiante, plomb avant travaux.,
- PGC.

1.4.4. Pièces à fournir par le titulaire du marché

Durant la période de préparation :

- Le plan d'hygiène et de sécurité mis à jour, en 3 exemplaires ; (2 au chargé de prévention du régiment et 1 au maître d'œuvre) ;
- Le calendrier d'exécution ;
- L'échéancier prévisionnel des acomptes, 3 exemplaires ;

- La liste mise à jour des véhicules du chantier avec les photocopies des cartes grises, en 2 exemplaires numériques ;
- La liste mise à jour des personnels appelés à intervenir sur le chantier, avec les photocopies des cartes d'identité, passeports ou titres de travail, en 2 exemplaires numériques, accompagnée également de 1 photo d'identité couleur ;
- Les plans d'exécution et les plans de détails, ;
- Les schémas et notes de calcul d'équilibrage ;
- Les notices techniques complémentaires d'entretien et de réglage des matériels ;
- Les avis techniques complémentaires sur les matériaux et procédés proposés ;
- Les documentations techniques ou technico-commerciales complémentaires des produits et matériels proposés ;
- Les attestations complémentaires de garantie.

Cette liste n'est en aucun cas exhaustive et pourra être complétée, au fur et à mesure de l'avancement du chantier par le maître d'œuvre.

Chaque envoi de documents sera accompagné d'un bordereau d'envoi daté donnant le détail précis (désignation de chaque document et nombre), section technique par section technique, des pièces adressées au maître d'œuvre.

Ne pourront recevoir un commencement d'exécution que les travaux définis sur les plans et documents ayant été visés par le maître d'œuvre.

Ne pourront être posés que les appareils et matériaux ayant reçu l'approbation du maître d'ouvrage.

Pendant les travaux

Un reportage photographique des différentes étapes des travaux sera réalisé sous format photos numériques.

Fourniture des plans, notes de calculs, schémas et notices techniques des produits employés à la demande du maître d'œuvre.

Après achèvement des travaux.

Il sera fourni au maître d'œuvre trois (3) exemplaires (1MOE, 1 Antenne USID SHC, 1 cellule environnement SID N-E), sous classeurs et une version numérique du dossier de récolement (DOE) comportant :

- Les fiches techniques par section technique de l'ensemble des matériaux et matériels mis en œuvre dans le cadre du chantier ;
- Les notices techniques de fonctionnement et d'entretien des matériels installés ;
- Les plans et autres documents conformes à l'exécution. Ces documents seront fournis sur support papier, plié au format A4, ainsi que sur support magnétique (zip ou CD) au format DGN (Micro station version 8) pour les plans des travaux effectués, sur Autocad dernière version (format DWG) et WORD pour les textes ;
- Les schéma d'implantation des matériels en 3 exemplaires
- 1 dossier de maintenance qui précise les gammes, les références des éléments à remplacer régulièrement.
- L'ensemble de ces documents, à l'exception des notices de fonctionnement et d'entretien qui seront remis à la réception des travaux, seront à fournir au plus tard dans les deux (2) mois après la réception.

Le titulaire du marché regroupera l'ensemble des documents demandés sous forme d'un dossier unique (en quatre (4) exemplaires identiques pour les besoins du maître d'œuvre et quatre (4) autres exemplaires pour la constitution du dossier d'intervention ultérieur sur les ouvrages- D.I.U.O.) en version numérique.

Il est demandé à ce que la présentation des documents fournis soit homogène, le MOE fournira les fonds de plans en DWG.

La non-fourniture d'un des documents précisés ci-avant fera l'objet d'une retenue dont le montant est défini à l'article 4.4 du CCAP.

1.4.5. Documents de références

Voir ANNEXE 1 – DOCUMENTS DE REFERENCE

1.4.6. Acronymes

Voir **Erreur ! Source du renvoi introuvable.**

1.5. Essai et contrôles

Tout ouvrage ou partie d'ouvrage, non conforme sera déposé et changé par l'entrepreneur, à ses frais, et dans les délais impartis par l'administration.

Le présent titulaire du marché doit la réalisation des essais et contrôles

1.6. Prescription générales d'exécution

1.6.1. Réservations – percements - scellements

Les réservations, percements et trous éventuels sont à la charge du titulaire ainsi que leur bouchage et la remise en état des maçonneries et ouvrages touchés. **Rétablissement obligatoire du degré CF1h lors de percements ou lors de dépose de matériels.**

1.6.2. Mise en oeuvre de source de chaleur

L'exécution des travaux nécessitant la mise en œuvre d'une source de chaleur mobile (chalumeau, lampe à souder, etc..) devra être précédée de la remise au maître d'œuvre, d'une fiche indiquant :

- La nature, le lieu, la date et la durée du travail à effectuer ;
- Les mesures de prévention prises contre les risques d'incendie ;
- Les moyens éventuels de lutte contre l'incendie prévus sur le chantier concerné.
- Un permis de feu devra être établi par le chargé de prévention du Quartier Turenne sur demande de l'entrepreneur.

1.6.3. Préventions contre l'incendie

Le titulaire du marché assurera, sous sa seule responsabilité et à ses frais, les mesures de protection contre l'incendie conformément aux réglementations en vigueur dans les établissements de la Défense et adaptées aux conditions spécifiques du chantier. En outre, l'entrepreneur titulaire désignera une personne du chantier assurant la responsabilité, à chaque arrêt de travail, de l'extinction des feux et du contrôle de l'exécution des mesures de sécurité.

De plus, il devra assurer la présence obligatoire sur le chantier :

- D'un extincteur adapté à chaque type de feux pouvant être provoqués par les matériels, engins, véhicules employés ;
- D'un extincteur sur chacun des véhicules ou engins à moteur thermique de son entreprise et/ou relevant de sa responsabilité.

1.6.4. Produits et matériaux

L'entrepreneur indiquera la provenance et la qualité des produits et matériaux qu'il va employer sur le chantier, les modalités de transport et de stockage de ces produits et matériaux.

Les produits et matériaux manufacturés seront livrés dans leurs emballages d'origine sur lesquels on pourra distinctement lire les marquages du fabricant :

- Nom commercial, type ;
- Certificat ;
- Avis technique ;
- Destination du produit ;
- Indications relatives à l'emploi ;
- Date de fabrication ;
- Principales caractéristiques dimensionnelles et performantielles.

1.6.5. Nettoyage et protections des ouvrages

Le titulaire du marché a la responsabilité du nettoyage et de la protection des ouvrages réalisés par ses soins ou par des entreprises sous-traitantes jusqu'à la réception de l'ensemble :

En cours de chantier :

Le titulaire doit assurer régulièrement l'enlèvement et l'évacuation des déchets divers du chantier. Des bennes seront mises en place pour assurer le tri des déchets et leur évacuation rapide. A l'extérieur des locaux touchés par les travaux, les emplacements de stockage seront délimités et balisés.

Pour ce qui concerne le nettoyage final avant réception :

Le titulaire doit l'enlèvement et l'évacuation des protections mises en place et le nettoyage des ouvrages ou équipements qui étaient protégés.

Le titulaire du marché doit le nettoyage des ouvrages salis et des abords.

1.7. Bordereau de suivi des déchets

1.7.1. Procédures et généralités

Les entreprises candidates au stade de la période de soumission devront produire un mémoire technique décrivant le plan détaillé de gestion et de valorisation des déchets. Ce document sera apprécié par le maître d'œuvre au moment de l'étude des différentes offres. La gestion des déchets sera réalisée dans le respect des dispositions réglementaires en vigueur. Le titulaire fournira un schéma d'organisation et de gestion des déchets (SOGED) ainsi qu'un schéma d'organisation et de suivi de l'élimination des déchets (SOSED).

1.7.2. Déchets électroniques

La collecte des déchets d'équipements électriques et électroniques (DEEE) doit s'accompagner du tri, du traitement sélectif et de la valorisation des déchets. Elle est mise en œuvre par l'entreprise, ou confiée à des éco-organismes agréés (les sociétés Ecosystèmes et Ecologic ou équivalent). Sont concernés tous les équipements qui fonctionnent grâce à des courants électriques ou à des champs électromagnétiques, mais également les équipements de production, de transfert et de mesure de ces courants et champs. Les DEEE sont transmis à l'organisme agréé et le transfert de responsabilité est matérialisé par le bordereau d'enlèvement, une copie sera transmise au maître d'œuvre.

1.7.3. Gestion des déchets dangereux

Les bordereaux de suivi de déchets dangereux sont suivis par l'administration au travers du logiciel « TRACKDECHETS ».

Leurs dématérialisations étant obligatoire depuis le 01 juillet 2022, l'entrepreneur titulaire de la présente section technique devra assurer la traçabilité des déchets dangereux au travers de cette plateforme.

Informations minimales nécessaires à l'établissement d'un BSD sont :

- Description du déchet : nature, code de nomenclature, dangerosité, volume : quantité, conditionnement (type, nombre), lieu de stockage temporaire/chantier ;
- Identifications des acteurs : transporteur (avec son habilitation pour les déchets dangereux) exutoire (numéro de certificat préalable d'acceptation si déchets dangereux)

Il est rappelé que l'enlèvement des déchets dangereux par le collecteur ne pourra être réalisé qu'une fois cette validation effectuée.

Le titulaire veillera à faire créer le bordereau de suivi de déchets (BSD) par le collecteur/transporteur sur le compte TRACKDECHETS du SID N-E en utilisant les informations suivantes :

- Producteur/émetteur : SID N-E
- N° SIRET : 13000190200373
- Coordonnées du producteur/émetteur : Caserne NEY – 1 rue Maréchal LYAUTEY - 57000 - METZ.
- Le champ « description du déchet » devra impérativement commencer par le numéro du département du chantier / lieu d'enlèvement suivi du signe « / », ceci afin de faciliter l'identification du BSD une fois celui-ci intégré dans le compte du SID NE. (Exemple 57/dalles = colle amiantées pour un chantier réalisé en Moselle).

2. Contenu et déroulé du projet

Dans le cadre de cette étape, le Titulaire réalise l'ensemble des travaux décrits dans son offre conformément au planning de mise en œuvre validé par l'Administration.

2.1. Réunion de lancement

L'objectif est de partager, avec l'ensemble des parties prenantes du projet, les éléments structurants permettant de piloter le projet et de planifier les différentes interactions entre les parties.

Cette réunion a pour objet principal :

- ▶ la présentation de l'organisation et des interlocuteurs du projet ;
- ▶ la présentation des structures de pilotage et de travail du projet ;
- ▶ l'initialisation de la planification générale des instances de pilotage et de travail ;
- ▶ le rappel des prestations et fournitures dues au titre de la commande (les « livrables ») ;
- ▶ l'identification précise des différentes tâches du projet (à partir d'une première identification déjà réalisée par le Titulaire dans sa proposition de réalisation) ;

- ▶ la déclinaison opérationnelle du planning de réalisation (à partir du planning proposé initialement et accepté par l'Administration) et prenant en compte les contraintes opérationnelles ;
- ▶ les aspects logistiques (droits d'accès, déclarations préalables) ;
- ▶ les rappels et échanges autour des enjeux, contraintes et risques du projet de réalisation.

La réunion de lancement fait l'objet d'un compte-rendu synthétique, rédigé par le Titulaire et adressé à l'Administration, dans les 5 jours ouvrés suivants la réunion, pour validation.

L'Administration dispose d'un délai de 10 jours ouvrés pour valider le compte-rendu. Passer ce délai, le compte-rendu est réputé validé.

2.2. Réalisation

Les étapes de réalisation des travaux CADIVS se décomposent de la manière suivante :

- ▶ mise en œuvre d'un démonstrateur appelé « plate-forme de référence » sur le site du Titulaire ;
- ▶ recette du démonstrateur (VdR) ;
- ▶ intégration sur la plate-forme de référence ;
- ▶ déploiement sur site du système de protection ;
- ▶ formation ;
- ▶ mise en ordre de marche (MOM).

2.2.1. Mise en œuvre d'un démonstrateur

Le but de ce démonstrateur est de prouver à l'Administration le bon fonctionnement des équipements, des choix de raccordement et des configurations des différents équipements du système CADIVS. Il devra notamment permettre de confirmer les choix de configuration de l'hyperviseur au regard de la matrice des exigences.

Ce démonstrateur permet à l'Administration de valider l'installation proposée avant tout déploiement sur site. Pour cela, une recette doit être réalisée avec un cahier de tests formels fourni par le Titulaire validé par l'Administration.

Avant tout déploiement sur le site du bénéficiaire, le Titulaire doit implémenter un démonstrateur permettant à l'Administration de réaliser la VdR.

Ce démonstrateur est représentatif de l'installation de protection prévue sur le site. Les équipements le constituant sont démontés pour être déployés sur le site à l'issue de la VdR.

Le Titulaire rédige un document décrivant la plate-forme de démonstration (architecture, système d'information, éléments constitutifs, éléments de sécurité, paramètres de configuration, ...).

Le Titulaire rédige un cahier de tests de validation présentant pour chaque test : la description du test, les étapes d'exécution du test, les résultats attendus, si en relation, le point réglementaire couvert.

Durant cette phase, le Titulaire rédige la stratégie de tests visant à optimiser l'effort de tests tout au long du projet.

2.2.2. Recette du démonstrateur (VdR)

A l'issue de la mise en œuvre du démonstrateur, le Titulaire informe l'Administration de sa mise à disposition pour présentation et réalisation de la vérification de réalisation (VdR).

Le Titulaire informe l'Administration, 20 jours ouvrés avant la date de VdR, de la mise à disposition de la plate-forme de démonstration pour effectuer la recette et confirme 10 jours ouvrés avant la date de la disponibilité réelle de la plateforme pour la VdR.

Remarque : la durée de la VdR est proportionnelle à la complexité du projet et peut le cas échéant durer plusieurs jours.

La VdR est un jalon obligatoire auquel doit participer :

- ▶ le responsable de projet pour les aspects techniques ;
- ▶ le bénéficiaire pour les aspects fonctionnels (si la prestation est commandée) ;
- ▶ le RSSI-P pour les aspects SSI ;
- ▶ le contributeur au dossier d'homologation.

10 jours avant la date de présentation, le Titulaire fournit le document de description de la plate-forme de référence à jour et un exemplaire du cahier de test qui sera inclus dans le futur cahier de recette

Le jour de la présentation, le Titulaire fournit le document de description de la plate-forme de référence à jour et un dossier présentant les résultats des tests pouvant être réalisés sur la plateforme et déjà effectués décrits dans le cahier de recette.

L'Administration a 5 jours ouvrés suivants la date de VdR pour prononcer cette dernière ou effectuer des remarques [CSFVdR].

Si certaines réserves sont jugées bloquantes pour la suite de la prestation, alors le Titulaire doit proposer un plan d'actions pour effectuer les corrections sur sa plate-forme de référence et convoquer de nouveau une VdR.

Remarque : la mise en œuvre de ce plan d'actions n'a aucune incidence sur la date de livraison finale, aussi, il convient de l'anticiper lors de la fourniture de la date de VdR par le Titulaire et reste l'unique responsabilité du Titulaire.

2.2.3. Déploiement sur site

A la suite de la VdR et de la pré qualification dans l'environnement de tests, le Titulaire du marché « CADIVS » réalise les travaux de mise en œuvre sur le site de l'Administration conformément au planning de réalisation et en prenant en compte les contraintes du site tant sur les accès et droit d'accès au site que sur le respect de la sécurité du site et des travaux pouvant nécessiter des délais de mise en œuvre.

Les intervenants doivent tous avoir eu un contrôle primaire de sécurité (CPR) et fournir à l'Administration ainsi qu'au BE local les biodatas des personnels.

Le Titulaire du marché met à jour la matrice de couverture d'exigences avec les tests s'y afférant et doit :

- ▶ respecter la comitologie et le pilotage ;
- ▶ mettre en œuvre et coordonner l'ensemble des prestations quelle que soit la nature des travaux SIC ;
- ▶ rédiger et/ou mettre à jour l'ensemble de la documentation liée à la phase de réalisation et déploiement sur site ;
- ▶ remonter les difficultés au comité de suivi et escalader au comité de pilotage si nécessaire.

En parallèle du déploiement et au fur et à mesure de l'avancement des travaux, la documentation est mise à jour et les éléments permettant de constituer le dossier d'homologation sont fournis par le Titulaire à l'Administration et au RSSI-P en titre.

2.2.4. Mise en ordre de Marche (MOM)

La Mise en Ordre de Marche (MOM) est le point de départ des opérations de vérification, elle est prononcée par le Titulaire qui indique à l'Administration la livraison de l'ensemble de l'installation commandée. La MOM ne constitue pas une opération de réception complète du système, seuls les livrables de formation et la documentation sont réceptionnés. L'Administration évalue également, au regard de la couverture des tests effectués, les résultats obtenus et les anomalies résiduelles, si le système est prêt à être recetté.

Le Titulaire fournit :

- ▶ l'ensemble de la documentation à jour nécessaire à la VA, y compris les supports de formation (si commandés) ;
- ▶ le système de protection du site opérationnel ;
- ▶ un bilan des tests effectués

A la réception des documents constitutifs de la MOM, l'Administration dispose de 10 jours ouvrés pour en prendre connaissance et faire ses remarques.

Si la documentation fournie ne permet pas à l'Administration de démarrer les activités de réception, alors le Titulaire doit compléter ses livrables et procéder de nouveau à une étape de MOM.

2.3. Homologation

La phase de qualification vise à permettre à l'Administration de valider les prestations réalisées par le Titulaire.

La phase de réception des travaux du S2I démarre à l'issue de l'acceptation de la MOM par l'Administration.

Les étapes de la qualification du S2I se décomposent en 2 volets :

- ▶ Un volet Fonctionnel ;
- ▶ Un volet Technique.

Chacun des volets peut émettre un avis sur sa partie sur les qualifications suivantes :

- ▶ la Vérification d'Aptitude (VA) : la Vérification d'Aptitude a pour but de constater que les matériels, les logiciels et les prestations associées, livrées et exécutées présentent les caractéristiques techniques qui les rendent aptes à remplir les fonctions précisées dans le dans le marché subséquent. Elle est effectuée sur le système déployé sur un site par l'Administration ;

- ▶ la Vérification de Service Régulier (VSR) : la Vérification de Service Régulier a pour but de constater que, dans la durée, l'ensemble de l'infrastructures livrée est capable de remplir les fonctions précisées dans le marché subséquent. Elle est effectuée sur le système opérationnel par l'Administration.

La démarche d'homologation est choisie en fonction de la classe du système d'information. Cette démarche sera de type « simplifiée », le système CADIVS de l'Administration étant évalué en **classe 2**.

2.3.1. Vérification d'Aptitude (VA)

L'Administration déroule les tests prévus dans le cahier de recette.

L'objectif pour l'Administration est de valider que le système fourni est conforme au CCTP. Pour cela, l'Administration effectue tous les tests de mise en situation qu'elle estime nécessaire.

La VA n'a pas vocation à réaliser les tests unitaires et/ou d'intégration (ces derniers sont de la responsabilité du Titulaire) mais l'Administration peut effectuer tous les tests qu'elle juge utiles.

Préalablement aux opérations de VA, réalisées par l'Administration, le Titulaire doit mettre à disposition l'environnement nécessaire à la bonne exécution des tests de la solution déployée.

Durant la phase de VA, le Titulaire doit impérativement assister les équipes de l'Administration notamment dans l'enregistrement des défauts constatés et dans la qualification de ces derniers.

Le Titulaire doit corriger l'ensemble des défauts détectés par l'Administration dans des délais compatibles avec la durée de la prestation.

La vérification d'aptitude doit être réalisée dans un délai 3 mois hors période de suspension ou d'ajournement.

Durant la VA, l'Administration s'autorise à provoquer des « incidents de sécurité volontaires » afin de tester la réactivité du système CADIVS.

Toutefois, ces incidents doivent être autorisés par le chef de projet.

De plus, un audit interne ou externe de sécurité (par des personnels habilités) peut-être demandé par l'Administration afin de diagnostiquer et de renforcer la robustesse de la sécurité du système d'information du S2I CADIVS. Les remarques de cet audit devront être impérativement pris en compte et remédié pour l'homologation du S2I en commission.

2.3.2. Conditions de passage de la VA à la VSR

Il suffit qu'une seule des conditions suivantes ne soit pas remplie pour que la VA soit refusée. Les conditions d'acceptation de la VA sont :

- ▶ 100% des formations terminées ;
- ▶ 100% des tests présents dans le cahier de test sont effectués et plus de 80% des tests sont OK ;
- ▶ aucune anomalie critique ;
- ▶ au moins 80% des anomalies majeures fonctionnelles, techniques et SSI sont résolues et les anomalies majeures résiduelles ont un plan de remédiation approuvé par l'Administration ;
- ▶ au moins 50% des anomalies mineures sont résolues ;
- ▶ au moins 80% des livrables sont disponibles et validés.

En cas de dysfonctionnement constaté, par suite de l'intégration du nouvel environnement CADIVS (période de VSR), un retour à l'environnement initial à isofonctionnalité et isopérimètre doit être possible.

A l'issue de la période de VA, l'Administration prononce l'acceptation ou non de la VA (CSFVA).

En cas d'acceptation avec réserve ou de refus, le Titulaire doit rédiger un plan d'actions visant à corriger les défauts constatés dans un délai fixé par l'Administration conforme aux échéances du projet.

2.3.3. Vérification de Service Régulier (VSR)

La VSR s'exécute sur l'environnement de production, avec les équipes en charge de l'exploitation du système de protection et a pour objectif de constater le bon fonctionnement du système en usage nominal.

Durant cette phase l'Administration s'assure, qu'après un certain temps de fonctionnement, les performances et caractéristiques demandées sont bien respectées tant du point de vue fonctionnel que technique.

Le Titulaire doit avoir la capacité d'assister les équipes fonctionnelles et techniques en charge de la VSR.

La durée de cette vérification de service régulier doit être réalisée dans un délai d'2 mois continu, hors période de suspension ou d'ajournement.

2.3.4. Conditions de passage de la VSR à l'exploitation

Il suffit qu'une seule des conditions suivantes ne soit pas remplie pour que la VSR soit refusée. Les conditions d'acceptation minimales de la VSR doivent être :

- ▶ aucune anomalie critique fonctionnelle, technique ou SSI ;
- ▶ aucune anomalie majeure fonctionnelle, technique ou SSI ;
- ▶ au moins 80% des anomalies mineures résolues et les anomalies résiduelles avec ont un plan de remédiation approuvé par l'Administration ;
- ▶ tous les livrables fonctionnelles, techniques et SSI sont disponibles et réceptionnés par l'Administration.

A l'issue de la période de VSR, l'Administration prononce l'acceptation ou non de la VSR (CSFVSR).

2.4. Formations

Les formations se tiendront exclusivement sur site, et seront basées sur des stages ou séminaires de durée variable. Chaque formation ne sera dispensée que pour un groupe de 4 personnes maximum.

Des supports de cours couvrant le domaine étudié (fonctionnel ou technique, ou les deux) seront constitués sous forme de synthèse sur la base des notices techniques de maintenance et des matériels, des manuels de maintenance, des manuels d'utilisation et de l'expérience terrain du Titulaire.

Les durées de formation devront être adaptées par l'Entreprise du présent lot dans le cadre du planning général d'exécution, et en fonction du volume nécessaire à la prise en main efficace de ses systèmes et de ses matériels par du personnel qui en ignore le fonctionnement. La durée des formations sera adaptée au nombre et à la complexité des stages exigés, et devra tenir compte des contraintes d'exploitation du Maître d'Ouvrage.

Les formations seront assurées par un formateur compétent et qualifié possédant les qualités pédagogiques nécessaires au public visé et au niveau de compétence final désiré.

Le Titulaire devra communiquer au Maître d'œuvre, par écrit, les dates proposées pour ces formations et le programme correspondant.

Les formations ne pourront effectivement commencer qu'après approbation du programme par la Maîtrise d'œuvre et de la maîtrise d'ouvrage.

Les formations s'effectueront une fois les systèmes opérationnels et validés par la maîtrise d'œuvre et préalablement à la réception pour que le personnel formé soit en capacité d'utiliser le S2I CADIVS dès la réception.

Les formations comprendront obligatoirement des simulations de mise en situation, avec des actions effectives sur les équipements ou les logiciels. Le volet pratique est important et doit être équilibré avec la théorie qui ne devra pas excéder 40% du temps de formation total.

En fin de formation, les stagiaires devront savoir agir sans hésitation ni ambiguïté sur les matériels et logiciels en place sachant exactement les actions produites et les bonnes pratiques à mettre en œuvre.

Les formations à assurer pour les utilisateurs et/ou bénéficiaires seront à minima les suivantes, l'entrepreneur ayant en charge de définir et d'adapter les durées des sessions en fonction de la durée nécessaire à un enseignement complet (à minima 4h par formation) :

- ▶ sur le CCGE, sur l'enrôlement et l'encodage des badges des personnels du SOP et du chef de BE
- ▶ sur le fonctionnement du CADIVS
- ▶ sur le report du CADIVS à l'entrée du site pour les gardiens
- ▶ sur la supervision technique du correspondant zonal SIC, des personnels du SOP du chef du BE, du RSSI-P CADIVS.

Des supports de formation adaptés au projet et à chaque thématique devront être remis à chaque participant. Une version numérique devra à minima être parallèlement fourni pour archivage au sein de l'Administration.

L'analyse fonctionnelle Sécurité sera jointe à ce support ainsi que les bonne pratique SSI à avoir envers le système CADIVS.

Toutes les formations seront validées par un acquit de stage à faire signer aux stagiaires, à remettre au maître d'œuvre.

2.5. Garanties

Pendant le délai de garantie de l'installation, soit au minimum un an, l'Entreprise du présent lot devra procéder à ses frais (main d'œuvre comprise) à la fourniture et à la remise en état de fonctionnement de toutes les parties défectueuses.

Elle devra, à ses frais, effectuer les déplacements et procéder au remplacement, ou à la modification, du matériel ou de certains organes, en vue de remédier à des défauts systématiques ou à des défauts de conception caractérisés.

S'il est constaté au cours de cette période une panne, dans le cadre d'une utilisation normale du matériel, l'Entrepreneur est tenu de faire gratuitement toutes réparations, remplacements et modifications nécessités par vice de matière, de construction, de fonctionnement ou de conception entraînant une altération des caractéristiques fonctionnelles ou techniques initiales.

Si au cours de la période de garantie, une anomalie, qui aurait échappé aux essais successifs, est découverte, l'Entrepreneur est tenu d'y remédier dans les mêmes conditions que pour celles des essais généraux.

Par contre, si un vice profond est découvert, le Maître d'œuvre se réserve le droit de neutraliser le déroulement de la période de garantie. Il est entendu que, pendant la période de neutralisation, l'Entrepreneur garde ses obligations de garantie.

En cas de neutralisation, le délai de garantie sera alors augmenté d'un temps égal à la période de neutralisation et toutes les obligations qui y sont liées seront prolongées d'autant.

Cependant, la garantie ne s'applique pas dans les cas suivants :

- ▶ Si la panne résulte d'une négligence ou d'une exploitation et/ou d'une utilisation non conforme aux recommandations de l'Entreprise du présent lot ;
- ▶ Pour toute pièce consommable ayant subi une usure normale de fonctionnement ;
- ▶ Si des modifications ou des substitutions de pièces ont été effectuées sans l'accord de l'Entreprise du présent lot sur des matériels fournis par elle. Les pièces ou parties ainsi altérées passent de faite hors garantie sans pour autant affecter la garantie des équipements et systèmes d'origine.

En cas d'apparition d'une panne, une déclaration sera envoyée à l'Entreprise du présent lot qui aura un délai de 24 heures pour intervenir et procéder aux réparations.

2.6. MCO PREVENTIFS (Tranche optionnelle n°1)

2.6.1. Durée

2.6.1.1. PRESENTATION DE LA PRESTATION

Les prestations forfaitaires comprennent :

- Les visites périodes de maintenance préventive avec remplacement des consommables, des pièces d'usures et de fonctionnement (pièces à remplacement programmé) ;
- La maintenance corrective curative (réparation) avec remplacement de pièces jusqu'à 600 € HT inclus ;
- La production des rapports et documents liés à l'exécution du contrat ;

2.6.1.2. PHASAGE

Un contrat de maintien en condition opérationnelle et de sécurité sera inclus au présent marché pour couvrir les périodes de garantie de parfait achèvement (GPA) et de bon fonctionnement (GBF).

Tranche optionnelle 1 :

Un MCO/MCS préventif d'une durée de deux ans (2) sera affirmé pour la durée de la garantie de parfait achèvement.

2.6.2. Prestations de MCO maintenance préventive

Ce contrat prévoira :

- ▶ une maintenance préventive ;

Le MCO définit l'ensemble des moyens techniques, humains et organisationnels mis en place, par le Titulaire, pour réaliser les prestations de maintenance sur le périmètre des installations CADIVS définie au § II.7 Les prestations de MCO attendues comprennent :

- ▶ la maintenance préventive comprenant notamment des prestations de mise à jour logicielle et matérielle régulière ajustable selon les règles SSI appliqués définis par l'Administration ;

2.6.2.1. DOCUMENTS REGLEMENTAIRES ET NORMATIFS

Les opérations de maintenance devront être effectuées dans le respect des normes en vigueur, des documents techniques et des prescriptions du constructeur, notamment :

- ☐ le code du travail-hygiène, sécurité et condition de travail,
- ☐ spécifications formelles du constructeur,
- ☐ FD X 60 000 portant sur la maintenance industrielle;
- ☐ NF EN 13 306 portant sur la terminologie de la maintenance;
- ☐ NF X 60 012 portant sur les termes et définitions des éléments constitutifs et de leur approvisionnement ;
- ☐ FD X 60 100 portant sur les inventaires et expertises des biens préalables aux contrats de maintenance;
- ☐ EN 50131-1 à 50131-6 portant sur les alarmes
- ☐ NF A2P type 2 ou 3 Matériels de détection intrusion
- ☐ décret n°88-1056 du 14 novembre 1988, relatif à la protection des travailleurs contre les courants électriques,
- ☐ la norme européenne NF EN 62676-1-1 de mai 2014 relative aux systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité.

Cette liste de normes ou de décrets n'est pas exhaustive.

Le titulaire est tenu d'informer le bénéficiaire des évolutions de la réglementation sur l'installation et les matériels existants.

2.6.2.2. CONDITIONS D'EXECUTION DES PRESTATIONS

2.6.2.2.1 Modalités d'exécution

Le titulaire s'engage à mettre en œuvre tous les moyens nécessaires afin de réaliser les prestations, objets du présent marché. Il reconnaît avoir pris connaissance des contraintes liées à leur réalisation.

Les opérations de maintenance préventives s'effectueront annuellement en respectant les horaires suivants : jours ouvrés : du lundi au jeudi entre 8h et 17h et le vendredi entre 8h et 11h30.

Cependant, afin de ne pas gêner le fonctionnement des sites en fonction de leur plan de charge, les travaux d'entretien pourront avoir lieu à d'autres plages horaires (les créneaux retenus seront alors validés par ordre de service).

Au plus tard un mois après la notification de la phase/tranche optionnelle, le titulaire soumettra pour approbation au bénéficiaire, un planning prévisionnel des visites.

L'équipe intervenante sera composée obligatoirement d'un technicien spécialisé et habilité en fonction du type d'intervention. Ce personnel devra se présenter au responsable d'exploitation ou à son représentant avant toute intervention sur les installations afin de prendre connaissance des dernières directives.

L'équipe intervenant sur le site, devra se munir de moyens techniques et mécaniques adaptés aux opérations de maintenance des installations.

2.6.2.2.2 Compte rendu d'exécution des prestations

A l'issue de chaque opération de maintenance préventive un rapport de maintenance sera établi en un (1) exemplaire au format informatique par le titulaire qui les transmettra au bénéficiaire, sous deux (2) semaines à compter de l'achèvement de la visite sur site.

Toutefois, le titulaire étant responsable du fonctionnement des installations, il devra lorsqu'il découvre une usure de matériels pouvant provoquer une défaillance, en avertir le bénéficiaire et l'antenne USID concernée par écrit sous 24 h 00 ouvrées.

De manière non exhaustive il devra comporter les éléments suivants :

- ☐ l'identification du lieu d'intervention ;
- ☐ l'identité du (des) technicien(s) du titulaire ;
- ☐ les dates et heures de début et fin d'intervention ;
- ☐ la nature de l'intervention ;
- ☐ les opérations, vérifications et mesures effectuées ;
- ☐ les pièces remplacées ;
- ☐ les éléments mis en cause et les dispositions prises pour remédier aux défauts ;
- ☐ la liste des travaux à envisager afin de maintenir le bon fonctionnement et la pérennité des installations avec proposition de devis de remplacement ou d'amélioration et planification prévisionnelle limite des interventions curatives.

Ce compte-rendu devra être transmis par courrier électronique au format word/excel.

La non remise de ces comptes rendus dans les délais entraînera l'application d'une pénalité, conformément à l'article 4.5 du C.C.A.P.

2.6.2.3. MAINTENANCE PREVENTIVE (MCO PREVENTIVE)

La maintenance préventive a pour but d'effectuer un entretien régulier des équipements et logiciels dans l'objectif de maintenir dans un état de bon fonctionnement le(s) système(s) CADIVS confié(s).

La maintenance préventive comprend une visite semestrielle d'une durée suffisante pour la maintenance du CADIVS dont :

- ▶ le contrôle de l'ensemble des sous-systèmes informatiques ;
- ▶ La maintenance préventive de l'intégralité des points CADIVS du service (UTL, caméras, détecteurs d'ouverture, détecteurs volumétriques, lecteurs de badges...) le nécessitant ;
- ▶ des opérations de restauration des sauvegardes au moins une fois par an .

Cette prestation comprend, a minima, les activités suivantes :

- ▶ la rédaction d'un dossier de maintenance préventive (gammes de maintenance) décrivant la liste détaillée des actions à mener et leurs programmations ;
- ▶ une assistance aux administrateurs techniques et à l'exploitation : dans le cadre des actions d'administration techniques et d'exploitation, le Titulaire doit mettre en place un outil/service permettant de poser des questions et d'obtenir un accompagnement ponctuel de manière à ne pas faire d'erreur ;
- ▶ les opérations de maintenance préventive incluant a minima :
 - le nettoyage et le contrôle (entre autres leur fixation) des équipements,
 - le réglage et la mise à jour des équipements et logiciels (dont la base de temps/horodatage),
 - la mise à jour des dossiers techniques de maintenance et du dossier site,
 - la vérification des points de sauvegardes et restaurations,
 - le remplissage des journaux des applications et systèmes,
 - l'espace disponible sur les serveurs et le stockage vidéo,
 - un compte rendu vers l'Administration des actions menées ;
- ▶ l'établissement et la mise à jour d'un dossier de suivi des visites.

Les prestations de maintenance préventive de l'installation dans sa configuration initiale seront réalisées sur la base d'un forfait annuel.

2.6.2.3.1 Modalités d'intervention en maintenance préventive :

Les opérations de maintenance préventive devront être effectuées avec confirmation de la date et de l'heure de l'arrivée sur site par écrit (télécopie, courriel, etc.) au minimum deux (2) semaines à l'avance à l'antenne USID concernée.

Ces visites se dérouleront pendant les heures ouvrées suivantes :

▫ 8 h 00 – 17 h 00 du lundi au jeudi ;

▫ 8 h 00 – 11 h 30 le vendredi.

Le personnel devra se présenter au responsable de l'antenne USID concernée avant toute intervention sur les installations pour prendre connaissance des dernières directives.

Tout décalage d'intervention imputable au titulaire entraînera l'application d'une pénalité, conformément à l'article 4.3.1 du C.C.A.P.

2.6.2.3.2 Gestion des fournitures et des consommables

1) Outillages et matériels

Le titulaire du présent marché devra mettre en place l'ensemble des moyens nécessaires à la bonne exécution de ses prestations notamment au niveau de l'outillage, des équipements de manutention, des moyens d'accès (nacelle, échafaudage, échelle) et des protections. Tous matériels et moyens d'accès seront conformes à la réglementation.

2) Consommables et pièces de rechanges

Le titulaire du présent marché disposera en permanence d'un stock de petites fournitures de rechange correspondant aux différents modèles de matériels utilisés.

Tous les consommables nécessaires à la réalisation des prestations objet du présent marché seront à la charge du titulaire et ce quel que soit le montant unitaire de ces consommables.

3) Compte-rendu annuel – contrôle qualité

Dans le dernier mois de la période en cours, le titulaire fera parvenir un compte-rendu annuel d'activité.

Ce compte-rendu annuel d'activité se devra d'être une synthèse de la période écoulée et une image du parc matériels à la fin de la période considérée. Il devra contenir à minima les éléments suivants :

- ☐ les différences de dates entre le planning initial de prestations de maintenance défini en début de période et le planning réel des prestations réalisées ;
- ☐ la liste des prestations de maintenance préventive réalisées au cours de la période ;
- ☐ la liste des prestations de maintenance corrective réalisées au cours de la période ;
- ☐ la mise à jour annuelle de la classification de l'état des équipements ;
- ☐ les problèmes rencontrés ainsi que les améliorations éventuelles à apporter afin d'obtenir un meilleur rendement des installations et garantir leur fonctionnement opérationnel ;
- ☐ des propositions d'amélioration des équipements pour la période suivante.

La non remise du compte-rendu annuel dans les délais entraînera l'application d'une pénalité, conformément à l'article 4.5 du C.C.A.P.

2.6.2.3.3 Garantie des pièces et des équipements remplacés

Les équipements et ensembles techniques homogènes remplacés au titre du présent marché seront garantis deux (2) ans à compter de la mise en place. Les pièces seront strictement identiques à la configuration initiale afin de garantir un parfait fonctionnement. Toute pièce remplacée sera inscrite dans le carnet d'entretien avec la date de prise d'effet de la garantie.

Pour toute intervention concernant une pièce sous garantie, le déplacement et la main d'œuvre sont à la charge du titulaire.

3. Dispositions techniques des ouvrages de sûreté

3.1. Limites de prestation

Les installations suivantes sont à la charge du titulaire :

- ▶ La filerie nécessaire au fonctionnement de son installation ;
- ▶ Les baies CADIVS ;
- ▶ Les onduleurs locaux sur courant secteurs ;

Le reste du document décrit les autres éléments CADIVS à la charge du titulaire.

Les installations suivantes sont à la charge du SID et de ses corps d'état :

- ▶ Les coffrets électriques comprenant les protections électriques normale (2 bandeaux de 8 PC) et ondulée (2 bandeaux de 8 PC) des baies CADIVS ;

3.2. Description des travaux du présent lot

De façon générale, les prestations dues au titre du présent lot comprendront :

- ▶ Si besoin, la dépose soigneuse des plafonds et de l'isolation des plafonds suspendus. Ils devront être stockés à proximité et protégés de la poussière.
- ▶ Les goulottes et les moulures polychlorure de vinyle (PVC) sur l'ensemble des ouvrants du projet ;
- ▶ Les chemins de câbles et fourreaux dédiés à ces installations ;
- ▶ Les percements et fourreaux pour les traversées de plancher et de cloisons ;
- ▶ Le rebouchage de l'ensemble des percements et fourreaux mis en œuvre ; Les études et la production des plans d'exécution nécessaires à la réalisation des ouvrages,
- ▶ Les alimentations électriques normale (2 bandeaux de 8 PC et ondulée (2 bandeaux de 8 PC des baies CADIVS ;
- ▶ Les Dossiers des Ouvrages Exécutés (DOE) complété par la liste des matériels installés avec les documentations techniques, références constructeurs et fournisseurs,
- ▶ Le montage et la fourniture du dossier d'homologation du S2I CADIVS contenant toute les pièces, dossier et documents nécessaire adapté selon la charte graphique et les usages du BE,
- ▶ La participation aux réunions d'études, de chantier et de synthèse,
- ▶ Le transport, la fourniture et la mise en place de l'ensemble du matériel et des canalisations décrits dans le présent CCTP,
- ▶ Les frais liés aux installations de chantier de l'Entreprise du présent lot,
- ▶ Les frais liés à la coordination des travaux sur site,
- ▶ La mise en équipotentialité de toutes les masses métalliques de l'installation à raccorder sur le conducteur de protection,
- ▶ Le raccordement et le réglage de tous les appareils et organes nécessaires au bon fonctionnement des installations,
- ▶ Le rebouchages des percements demandés ;
- ▶ Les essais préalables sur site ainsi que la participation aux essais et réception effectués à la demande du Maître d'œuvre ou du Maître d'Ouvrage,
- ▶ Les percements, scellements, saignées, rebouchages et raccords, le rebouchage coupe-feu des gaines à chaque niveau de plancher,
- ▶ Les frais de transport, d'emballage, d'entrepose provisoire, ainsi que tous les frais auxiliaires de main d'œuvre s'y rattachant,
- ▶ L'enlèvement des gravats,
- ▶ L'entretien gratuit de l'installation pendant la période correspondant au délai de Garantie et de Parfait Achèvement (GPA) soit au minimum pendant un an,
- ▶ La main d'œuvre et le matériel nécessaires à l'exécution des travaux,
- ▶ La protection contre la corrosion de tous les éléments métalliques,

- ▶ La mise à la terre des ouvrages du présent lot, conformément à la réglementation,
- ▶ Le démontage et l'évacuation des équipements et matériels non réutilisés (mesure de Dépollution du site),
- ▶ Les essais et réglages des installations et des appareillages,
- ▶ La mise en service et assistance à l'exploitation du système jusqu'à réception,
- ▶ La formation des personnels d'exploitation et de maintenance,
- ▶ Les pièces de rechanges requises,
- ▶ Enfin, d'une manière générale, tous les travaux, fournitures et prestations divers nécessaires à la parfaite et complète exécution des installations, conformément à la réglementation en vigueur et aux pièces du marché.

3.3. Principes de base

3.3.1. Principe du zonage :

- ▶ Zone 1 : la caserne Turenne
- ▶ Zone 2 : le bâtiment 0009
- ▶ Zone 3 : la Zone protégée du BE (étage) hors locaux spécifique en zone 4
- ▶ Zone 4 : les trois zones sensibles (chiffre, LT SIC BE et LT CADIVS) et le local de stockage dans les combles (local 003).
- ▶ Zone 5 : tous les autres combles n'appartenant pas au BE (hors local 003).

3.3.2. Principe de fermeture/ouverture

- ▶ Accès principal contrôlé de la ZP BE (Zone 3)
 - Fermeture 3 points
 - Si fermeture motorisée (penne motorisé), alors clé de déverrouillage ;
 - Si fermeture électromagnétique (bandeau ventouse), alors clé de verrouillage.
- ▶ Accès secondaire mécanique de la ZP BE (Zone 3)
 - Fermeture 3 points
 - Sera utilisé essentiellement en issue de secours.
- ▶ Locaux de la ZP BE (Zone 3) – fermeture mécanique un point
- ▶ Locaux sensibles (Zone 4) – fermeture mécanique trois points
- ▶ Stockage des clés :
 - Coffre à clé mécanique pour l'accès principal et secondaire de la ZP (Zone 3) couvert par la VS du Service au niveau de l'entrée principale en extérieur du BE. Le coffre doit être équipé d'un détecteur d'ouverture raccordé à la détection intrusion (DI) du CADIVS du BE ;
 - Coffre à clé à gestion électronique (CCGE) pour les locaux de la zone 3 et 4 couvert par la VS du Service installé en zone 3. Le coffre doit être raccordé à la détection intrusion (DI) du CADIVS du BE .

3.3.3. Principe d'accès aux locaux de la ZP

- ▶ Accès zone 1 ou sur site : hors projet
- ▶ Accès zone 2 ou bâtiment : hors projet
- ▶ Accès zone 3 ou ZP du BE : accès contrôlé
 - Par badge spécifique au Service (MIFARE Desfire EV3 8k ou supérieur) ;
 - Par badgeage en entrée ;
 - Par badgeage en sortie.
- ▶ Accès aux locaux de la zone 3 : via CCGE avec badgeage + codier
- ▶ Accès zone 4 :
 - Via CCGE avec badgeage + code ;
 - Et badgeage sur lecteur de présence – LdB (p) en entrée et en sortie (sauf local 003).
- ▶ Accès zone 5 : accès contrôlé
 - Par clé mécanique disponible sur le CCGE installé en zone 3.

3.3.4. Principe des zones d'alarme

- ▶ Une zone d'alarme unique pour l'ensemble des locaux ZP de la zone 3 avec :
 - activation / désactivation par lecteur de badge + codier – LdB (a) ;
 - contact d'ouverture sur chaque ouvrant (porte et fenêtre) ;
 - détecteur bi-volumétrique dans chaque local ;
 - indicateur d'action aux deux entrées de la ZP BE (Zone 3).
- ▶ Quatre zones d'alarme indépendante (physiquement ou programmable) zone 4 :
 - avec activation / désactivation par lecteur de badge + codier – LdB (a) ;
 - contact d'ouverture sur chaque ouvrant (porte et fenêtre) ;

- détecteur bi-volumétrique dans chaque local ;
- indicateur d'action à l'entrée de chaque local.
- ▶ Une zone d'alarme des locaux de la zone 5 avec :
 - activation / désactivation par lecteur de badge + codier – LdB (a) installé en zone 3;
 - contact d'ouverture sur chaque porte ;
 - détecteur bi-volumétrique dans chaque local ;
 - indicateur d'action dans chaque cage d'escalier avec panneauage précisant « COMBLES ».

3.3.5. Principe de la vidéosurveillance

- ▶ Surveillance périmétrique en observation
- ▶ Surveillance des deux accès de la zone protégée (Zone 3) en identification ou en reconnaissance
- ▶ Surveillance des accès des trois locaux sensibles : zone 4 en identification
- ▶ Surveillance des couloirs du BE en reconnaissance (à ne pas redonder avec la surveillance des accès aux LT si l'angle permet de couvrir l'entrée d'un LT et le couloir avec la même caméra)

3.3.6. Report du CADIVS

Le Poste d'entrée (ou de Sécurité) du site :

- ▶ Surveillance de toutes les alarmes (périmétrique et volumétrique, zone 3, 4 et 5) sans dénomination précise de la pièce concernée ;
- ▶ Surveillance de la vidéo surveillance périmétrique

Le secrétariat ou SoutOps du BE :

- ▶ 1 poste d'exploitation avec moniteur 24" pour le contrôle d'accès, ainsi que d'un lecteur / encodeur et d'une imprimante thermique pour la création de badge
- ▶ 1 poste de supervision technique ;
- ▶ 1 poste d'exploitation pour le CADI pour la surveillance de l'ensemble des alarmes
- ▶ 1 poste d'exploitation avec double écran pour la surveillance de la totalité de la vidéosurveillance

Téléphone d'astreinte du cadre de permanence du BE :

- ▶ Surveillance de toutes les alarmes (zones 3, 4 et 5) avec distinction des zones.

3.3.7. La distribution du bâtiment

L'entreprise devra la fourniture et pose des équipements suivants selon sont implantations pour répondre à la prestation du marché :

- ▶ Les moulures PVSC de 2cm par 1 cm d'épaisseur.
- ▶ Dans le plénum des dégagements : Chemin de câble de type dalle perforées, Matière : Z275 galvanisé, Couleur : gris, Dimensions : Hauteur 50 largeur 150 minimum avec 10% de réservation, Couvertures pour dalles en fonction du chemin de câble, Coudes directionnelles, Accessoires de fixation, Console murale pour mur ou gaine technique.
- ▶ De la goulotte de 190mmX50mm en PVC et constituée de trois compartiments au format MOSAIC 45x45mm)
- ▶ Prise RJ 45 de type MOSAIC se montant sur un plastron de 45*45, blindées à 360° de catégories 6 certifiée SFTP, muni d'un volet anti-poussières et de 8 plots plus terre, compatible avec des câbles 100 Ohms,
- ▶ Les prises 10/16 A, 2 P + T sont conformes à la norme NFC 61.303 et pourront recevoir des broches de diamètre 4 et 4,8 mm. Adaptable au goulotte d'installation
- ▶ Les prises informatiques sont du type MOSAIC 45 avec plastron adapté au modèle de la goulotte d'installation : type 45 x 45 au format MOSAIC ou compatible de couleur rouge, intégrée dans un plastron de dimensions adaptées à la goulotte dans le compartiment réservé au courants forts.
- ▶ La fourniture et pose des protections indépendantes de chaque circuit. Le titulaire devra remettre à jour les plans du TGBT se trouvant dans la porte du tableau,
- ▶ L'ensemble des câbles BT et TBT nécessaire à la réalisation de son marché selon les normes en vigueur.

3.3.8. Equipements centraux Existants

Les équipements centraux de sûreté existants du site (contrôle d'accès, détection intrusion et vidéosurveillance) étant vétuste, aucune connexion ne sera acceptée entre les deux installations.

3.4. Les infrastructures physiques du système de sûreté

3.4.1. Alimentation électrique des baies

Les baies CADIVS « principal » et « secours » seront alimentées par 2 chaînes :

- ▶ Une chaîne ondulée (voie A)
- ▶ Une chaîne normale (voie B).

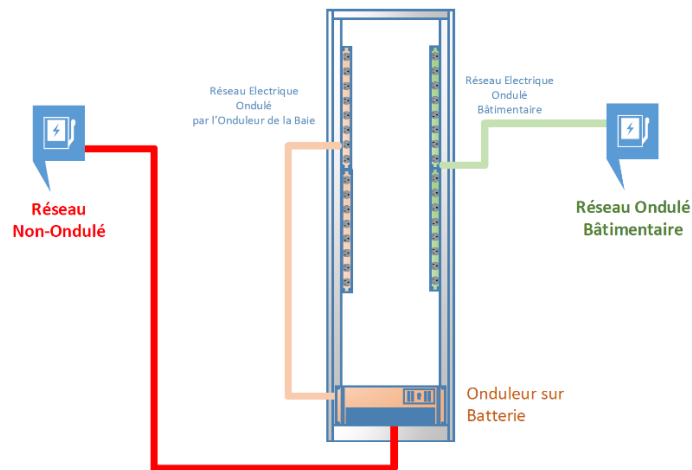


Figure 1 : Principe d'alimentation électrique des Baies Informatiques du SII CADIVS

Il est prévu :

- ▶ une baie principale dans le local CADIVS ;
- ▶ une baie secours dans le local SIC BE.

3.4.2. Architecture physique demandée

Présentation :

- ▶ Une architecture physique séparée pour le vidéo portier ;
- ▶ Une architecture physique commune pour le CADIVS et le CCGE avec séparation logique CA-DI-VS-CCGE

Synoptique

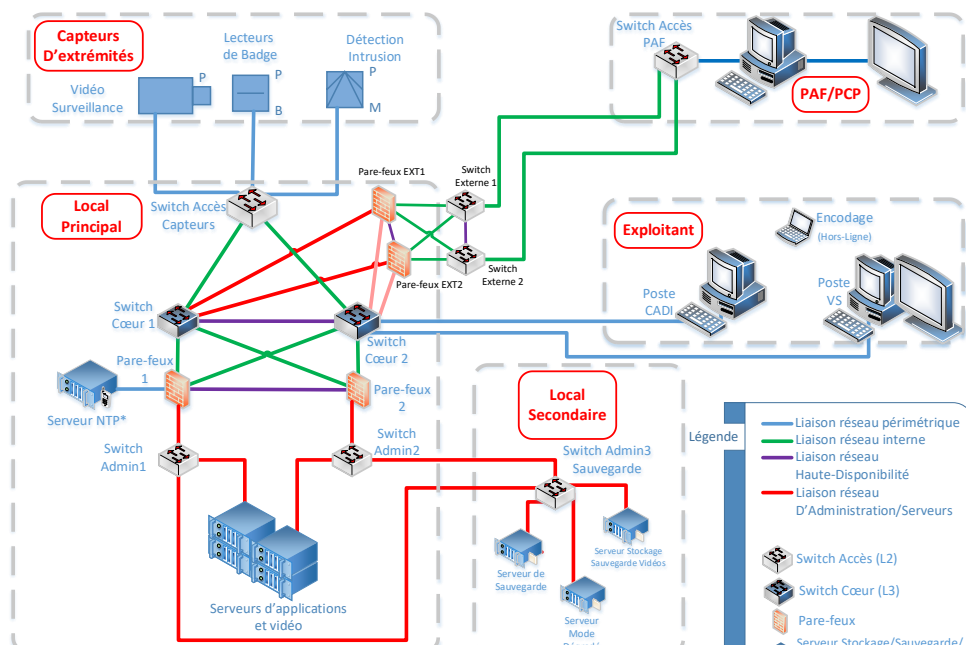


Figure 2 : Schéma Synoptique CADIVS du BE

3.4.3. Infrastructure physique

Une infrastructure informatique de type Ethernet-IP est mise en œuvre par le présent lot dans la ZP BE STG du bâtiment afin d'accueillir les applications sûreté. Ce réseau en double étoile est constitué de 2 cœurs de réseaux, de liens fibre optique OM4 et de commutateurs administrables dans des coffrets Sûreté installés en local technique dédié et rattachés à chacun des cœurs.

Cette infrastructure, de type en étoile sera constituée :

- ▶ de switches de desserte pour les équipements d'extrémités distinct (CADI et VS) ou à minima avec VLAN ;
- ▶ 1 cœur de réseau unique au local CADIVS constitué de 2 switches en redondance parfaite ;
- ▶ des switches de desserte des serveurs en redondance principe de double attachement de chaque serveur physique (réseau interne serveur – ADMIN / STOCKAGE) ;
- ▶ 1 serveur principal de virtualisation installé dans la baie du local CADIVS principal (détaillé en ANNEXE 4 – Serveur Principal du Local Principal CADIVS) :
 - 2 contrôleurs de domaine (principal et secondaire),
 - 1 serveur Radius pour les équipements réseaux,
 - 1 serveur de logs principal,
 - 1 serveur PKI si nécessaire uniquement pour mise en place 802.1X sur les équipements terminaux,
 - 3 serveurs de mise à jour :
 - 1 serveur pour MAJ Windows,
 - 1 serveur pour MAJ Linux,
 - 1 serveur pour MAJ Anti-Virus,
 - 2 serveurs d'administration technique :
 - 1 serveur de supervision,
 - 1 serveur d'administration centralisé,
 - 1 serveur de vidéosurveillance (CASD) principal,
 - 1 serveur de contrôle d'accès (TIL) principal,
 - 1 serveur de gestion des boîtes à clé (CCGE),
 - 1 serveur d'hypervision si nécessaire,
 - 1 ou plusieurs Serveur de bases de donnée virtualisé ;
- ▶ 1 Serveur de secours de virtualisation dans la baie CADIVS de secours du local SIC BE hébergeant les services minimum suivant (détaillé en ANNEXE 5 – Serveur de Secours du Local de Secours CADIVS) :
 - 1 serveur de temps NTP secondaire,
 - 1 Contrôleur de domaine de secours,
 - 1 ou plusieurs Serveur de bases de donnée virtualisé,
 - 1 Serveur de vidéosurveillance (CASD) de secours,
 - 1 Serveur de contrôle d'accès (TIL) de secours,
 - 1 serveur de logs de secours ;
- ▶ Des solutions de reroutage depuis le local CADIVS vers la baie secours CADIVS du LT SIC BE pour pallier une éventuelle défaillance du serveur principal,
- ▶ Depuis le local CADIVS, une distribution fibre optique alimentera des commutateurs administrables,
- ▶ Des commutateurs administrables optique/cuivre (POE ou Non POE) alimentés par le réseau ondulé et secouru répartis à chaque étage dans des locaux sûreté dédiés suivant les besoins des applications précitées (Contrôle d'accès/intrusion et vidéosurveillance). Ces locaux seront sous lecteur de badge en base, ou accessible sur clef disponible dans une armoire en clef en option.

À partir de ces commutateurs, seront raccordés les différents matériels (postes d'exploitation, UTL de contrôle d'accès, caméras, prises RJ 45...) par des liaisons cuivre catégorie 6A (liaisons capillaires). Ces matériels supporteront la norme IEEE 802.1X.

Les liaisons capillaires aboutiront côté équipements sur des boîtiers 1 RJ45 ou directement sur des prises RJ45 mâles (cas des vidéophones, UTL et caméras).

Tous les Coffrets Sûreté seront munis de dispositifs d'autoprotection. Il n'est pas prévu de contrôle d'accès ou de clés prisonnière sur les centrales. Celles-ci sont positionnées dans des locaux sécurisés à accès restreint par lecteur de badge en base, ou accessible sur clef disponible dans une armoire en clef en option.

Le repérage des locaux de sûreté est représenté sur le carnet de zoning Sûreté.

3.5. Les infrastructures SI du système de sûreté

3.5.1. Architecture logique retenue

Présentation :

- ▶ Un domaine fonctionnel « administration » (ADMIN) ;
- ▶ Un domaine fonctionnel « CADI » ;
- ▶ Un domaine fonctionnel « VS » ;
- ▶ Un domaine « supervision technique » (SVT) ;
- ▶ Pas d'hypervision.

Synoptique générale d'un CADIVS

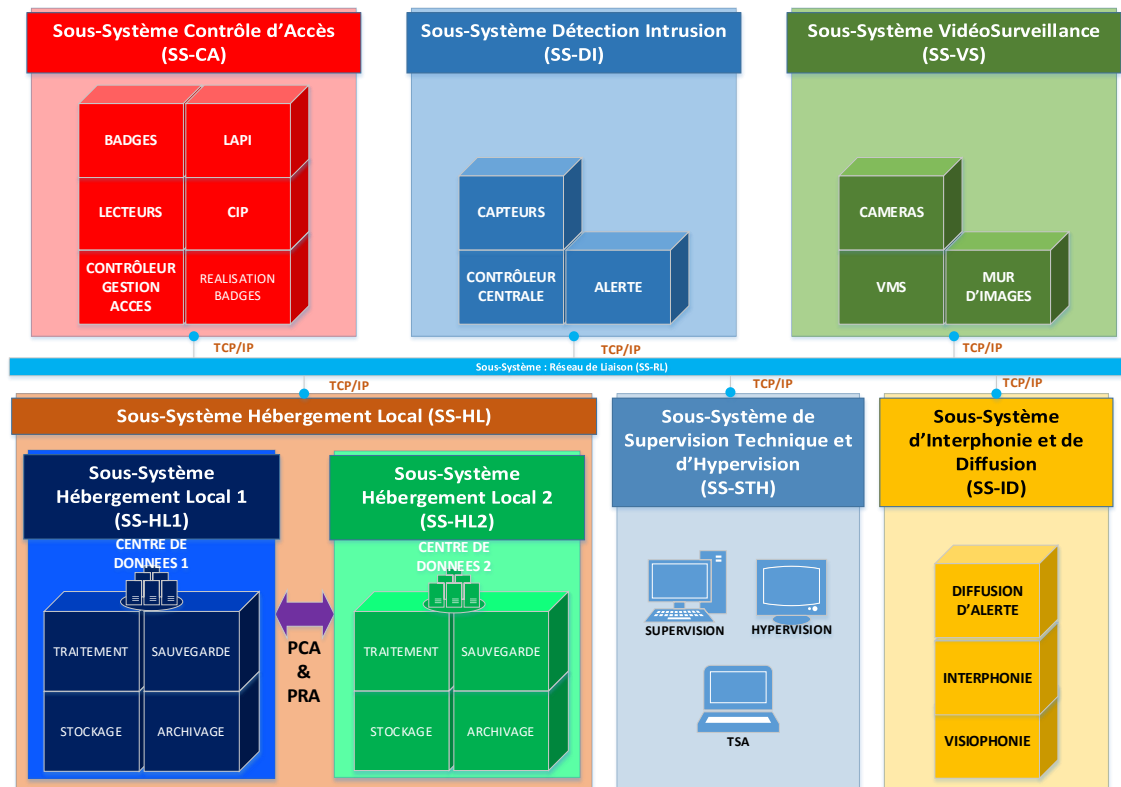


Figure 3 : Principes et Architecture logique global d'un S2I CADIVS

Dans notre cas et s'il est présent uniquement, le sous-système d'Interphonie et de Diffusion (SS-ID en jaune) sera isolé physiquement du reste du CADIVS.

Les autres sous-systèmes sont soit isolés physiquement, si cela est possible, soit à minima séparés par des VLAN pour chaque sous-système.

3.5.2. Sécurisation de l'infrastructure

Pour toutes les installations de câblage, des règles de sécurité des cloisonnements seront appliquées.

- ▶ Cloisonnement physique entre les zones publiques (Z1) et les zones réservées (Z2) commutateur public / commutateur réservé.
- ▶ Cloisonnement logique entre réseaux par VLAN.
- ▶ La modification de paramètres ou d'éléments de maintenance opérationnelle sans arrêt du système (Mise à jour de fonds de plans, ...).
- ▶ Les modifications qui peuvent être apportées sont obligatoirement liées à l'identification d'un profil autorisé.

La configuration de l'interface homme-machine doit permettre à l'agent en poste de se concentrer sur ses objectifs et missions en s'affranchissant complètement des aspects techniques.

Les principales fonctionnalités attendues sont (étude du besoin et réponse appropriée au cas par cas):

- ▶ Gestion de la cartographie : fond de plan sous forme d'image – cartographie statique et/ou issue d'un système d'information géographique – SIG.

- ▶ Pilotage des caméras : clavier et souris seront mis à disposition (joystick proscrit).
- ▶ Gestion de l’affichage : affectation des caméras à visualiser depuis la carte et/ou mise à disposition d’une liste hiérarchisée des caméras vers le système d’affichage.
- ▶ Gestion d’une arborescence : regroupement des caméras par zone géographique sous forme arborescente de manière à ce que l’opérateur puisse accéder rapidement à l’ensemble des caméras correspondant à la zone géographique choisie.
- ▶ Gestion des cycles et prépositions : lorsqu’une caméra n’est pas pilotée par l’agent en poste, elle décrit, en cycle, un ensemble de cadrage prédéfinis ou prépositions.
- ▶ Caméra postée : possibilité, pour l’agent en poste, de désactiver le cycle d’une caméra et de la figer volontairement sur un cadrage.
- ▶ Relecture d’images enregistrées : la fonction relecture des images doit être disponible sur une application dédiée.

3.6. Carnet des matériels et solutions techniques

L’intégrateur devra installer les solutions suivantes ou similaires :

Equipements	Matériels CADIVS
Contrôle d'accès	TIL TECHNOLOGIES - MICROSESAME CUBE - Dernière version au moment du déploiement (société française)
	TIL est la seule solution CA certifiée par l'ANSSI. Elle peut intégrer : <ul style="list-style-type: none"> ▶ AXIS ▶ CASD VISIMAX VM500 ▶ Hyperviseur bâtiment : PRYSM, ▶ Centrale intrusion GALAXY NFA2P GALAXY via leur protocole natif IP Galaxy ▶ Centrales intrusion Honeywell GALAXY
	TIL TECHNOLOGIES - TILLYS CUBE
	TIL TECHNOLOGIES
	lecteur "activation/désactivation" d'alarme : lecteur TIL TECHNOLOGIE - évolution KB
	lecteur d'identification : lecteur TIL TECHNOLOGIES évolution ST
	Lecteur de présence : lecteur TIL TECHNOLOGIES évolution ST
	Badge MIFARE Desfire Evolution 3 8K à minima
	<ul style="list-style-type: none"> ▶ Armoire à clés DEISTER ELECTRONIC (version 2,8,1 à minima) avec lecteur de badge + clavier (ProxSafe) ▶ Synchronisation des identifiés avec le logiciel COMMANDER 4 avec les options/modules supplémentaires de gestion des horaires nécessaires pour un contrôle horaire des Keytags
Intrusion	Centrale intrusion Honeywell GALAXY NFA2P GALAXY
	▶ AXIS I8016-LVE à confirmer / COMMEND autre solution
	clavier compatible avec Honeywell GALAXY NFA2P GALAXY
	AXIS D4100-E
	détecteur infrarouge compatible avec Honeywell GALAXY NFA2P GALAXY
Vidéosurveillance	extension avec Honeywell GALAXY NFA2P GALAXY
	CASD VISIMAX dernière version en cours
	CASD est une solution française
	Exclusion : GENETECH (solution canadienne), Milestone (solution canadienne) CASD = Petite structure pouvant apporter une meilleure réactivité d'intervention et de conseil que ses deux concurrents
Cœur de réseau et desserte réseau	Axis Q6315-LE + AXIS P3719PLE + AXIS P1465-LE + AXIS P3265-LVE
	Axis P4707 + Axis P4705 + Axis M4216-LV
	CISCO - C9300-24S-E + module C9300-NM-8X
Cybersécurité	CISCO - C9200L-24P-4X-E ou C9200L-24P-4G-E
	CISCO - C9200L-24T-4X-E ou C9200L-24T-4G-E
	STORMSHIELD - dernière version (à minima SN3xx)
	TAPICS - dernière version
	TAPICS - dernière version

Tableau 1 : Matériel et équipements demandés

3.7. Précisions techniques du vidéoportier

Moniteur intérieur : (à poser dans les locaux 016/007 2° étage)

- ▶ Alimentation électrique : 100-240 V / 50-60 Hz 0,6A 24Vdc 1 A - Bloc secteur pour prise de courant
- ▶ Fixation : En saillie avec support mural fourni
- ▶ Température de fonctionnement : -10°C +55°C
- ▶ Dimensions : 130 x 185 x 22 mm
- ▶ Portée Radio : 200 m (en champ libre)
- ▶ Fréquence radio : RTS - 433,42 MHz
- ▶ Deux boutons de commande différent permettrons d'ouvrir les portes palières CR4 équipés de gâche électrique.

Platine de rue : (à poser dans sur les paliers 014/001 2° étage)

Sorties :

- ▶ 1 sortie contact sec pour portail
- ▶ 1 sortie pour serrure électrique 12V 800 mA (temps d'ouverture paramétrable : 2, 5 ou 10s)

Fixation : En saillie via visière pare-pluie

- ▶ Température de fonctionnement : -20°C +55°C
- ▶ Y compris câblage et essai

+ (prise en compte du câblage/programmation de l'interphone pour l'ouverture des portes)

3.8. Précisions techniques du CCGE

Le coffre à clés à gestion électronique DEISTER Electronic V8 devra intégrer les spécifications suivantes :

3.8.1. Matériel du système

Il sera nécessaire de mettre en place un ou plusieurs des éléments ci-dessous :

- ▶ Un PC serveur CCGE rackable + clavier, écran, souris ;
- ▶ Un PC portable ;
- ▶ Une UC (tini) + clavier, écran, souris.

3.8.2. Puissance du matériel informatique

- ▶ Intel Core I5 Génération 12 ;
- ▶ 16 Go de ram (8 Go minimum) ;
- ▶ DD système 500 Go 1 Partition ;
- ▶ Ecran 24 pouce dans l'idéal et 15 pouce minimum pour un portable ;
- ▶ Windows 10 LTS ;
- ▶ 2 HDD Externes 2To USB 3.0 ;
- ▶ 1 câble réseau SRV↔CCGE ;
- ▶ 1 Câble Alarme 4 paires relié à la DI.

3.8.3. Alimentation électrique 220V

- ▶ 1 câble pour le CCGE ;
- ▶ 1 câble pour le PC (+1 pour l'écran si besoin).

3.8.4. Câble « réseau »

- ▶ 1 câble « réseau » 4 paires pour le CCGE ;
- ▶ 1 câble « réseau » 4 paires pour le PC
- ▶ 1 câble « alarme » 2 paires pour le CCGE ;

3.8.5. Les différents comptes

- ▶ 1 Admin Mainteneur SIC/CADIVS
- ▶ 1 Admin Technique SIC BE ;
- ▶ 1 Admin (COSSI-COSIC),
- ▶ 1 Admin (CZSIC/CCGE) ;
- ▶ 1 Générateur de sauvegarde ;
- ▶ 1 Administrateur fonctionnel (Commander 4 + Utilisateur Local).

3.8.6. Règles de Sauvegarde

- ▶ 1 par semaine sur HDD Externe ;

- ▶ Changement HDD externe / 6 mois ;
- ▶ 2^{ème} HDD au coffre.

3.8.7. Implantation

- ▶ PC au secrétariat ou local CADIVS ;
- ▶ CCGE à proximité de l'accès principal.

3.8.8. Spécifications particulières

Le CCGE est équipé d'un lecteur de badge + codier permettant à chaque utilisateur de s'identifier et de libérer certains trousseaux (keytags) en fonction des droits d'accès qui lui sont affectés.

Les armoires sont connectées au réseau sûreté CADI (sur un VLAN particulier au minimum) et une interface permet de visualiser et rechercher les historiques.

Les badges utilisés sont les mêmes que les badges du système de contrôle d'accès (CADI).

Une interface logiciel est prévue afin de faciliter la programmation des armoires DEISTER depuis le système TIL.

La capacité de l'armoire sera de 48 clés minimum (les 32 portes et des clés de véhicules de service

3.9. Précisions techniques sur le système de contrôles d'accès

3.9.1. Note préliminaire

Le système de contrôle d'accès (CA) respectant les recommandations ANSSI du « Guide des technologies sans-contact pour le contrôle des accès physiques » et mettant en œuvre l'architecture N°1 avec tête de lecture transparente, authentification de bout en bout, est constitué :

- ▶ D'un ou plusieurs serveur(s) physique(s)/virtuel(s) implanté(s) dans la Baie Sûreté du LT CADIVS Principal redondé sur un serveur secondaire dans le LT CADIVS de sauvegarde
- ▶ De son propre logiciel/système de supervision
- ▶ D'une station portable d'encodage avec son lecteur/encodeur stocké au coffre
- ▶ D'un poste d'exploitation-enrôlement au secrétariat
- ▶ De lecteurs de badges de type 13,56Mhz de technologie Mifare Desfire EV3 et conforme à la norme ISO 14443 permettant une authentification du badge par des clefs de codage, et la lecture des puces EAL4+.
- ▶ Un stock de badges Mifare Desfire EV3 – 8K : 150 badges
- ▶ De systèmes de verrouillage et environnement
- ▶ De boîtiers de demande d'ouverture d'urgence (BBG vert avec alarme local dans le boîtier et lumineux)
- ▶ D'Unités de Traitement Locales (UTL) sur lesquelles seront raccordés les environnements de portes (lecteurs de badges, systèmes de verrouillage, détecteurs d'ouverture et boîtiers de demande d'ouverture) et capables de fonctionner de manière autonome en gérant l'attribution des droits d'accès et en mémorisant les derniers événements.

3.9.2. Caractéristiques des matériels

3.9.2.1. POSTE OPERATEUR / STATION PORTABLE ENCODAGE

Un poste opérateur portable est dédié à l'encodage des badges. Il comprend :

- ▶ Un poste opérateur type PC portable fonctionnant sous windows
- ▶ Un lecteur/encodeur de badge de type MIFARE DESFIRE EV3
- ▶ Un logiciel d'encodage de badge compatible TIL Technologie

3.9.2.2. POSTE OPERATEUR / STATION ENROLEMENT

Un poste opérateur est dédié à la création et l'administration des porteurs de badge. Il comprend :

- ▶ Un poste opérateur type PC fonctionnant sous windows
- ▶ Un lecteur de badge enrôleur pour badge de type MIFARE DESFIRE EV3
- ▶ Un logiciel d'enrôlement de badge sur le système de Contrôle d'Accès (CA)
- ▶ Un dispositif de prise de vue couleur (appareil photo ou caméra de 4k minimum)
- ▶ Un logiciel de personnalisation des badges
- ▶ Une imprimante à badge

La personnalisation des badges proposées devra être intégrée au logiciel de contrôle d'accès. Le module de personnalisation devra posséder les fonctionnalités suivantes :

- ▶ Un éditeur graphique pour la personnalisation de la carte recto et verso
- ▶ L'importation de la photo, du nom, du prénom, du numéro de matricule, de la date de validité, de la zone autorisée ou d'un autre champ venant de la base de données des porteurs de badge.

- ▶ L'acquisition de photos à partir d'une source vidéo extérieure : Webcam, appareil numérique, , etc...

Le dispositif de prise de photo est laissé libre au Titulaire du présent lot. Mais celui-ci devra être compatible avec le logiciel de création de badge. Il sera alors possible de prendre le contrôle du dispositif afin de réaliser une prise de vue offrant une qualité satisfaisante en termes de rendu des couleurs et lumière (approbation de la maîtrise d'œuvre). Cette phase de prises de vues pourra se faire des 2 façons suivantes :

- ▶ Soit lors de la création des badges, directement depuis le logiciel de personnalisation, sans avoir à réaliser une importation,
- ▶ Soit en réalisant une importation depuis une base de données de photographies extérieure.

L'imprimante à badge aura les caractéristiques suivantes :

- ▶ Impression simple face couleur à sublimation
- ▶ Impression bord à bord
- ▶ 300Dpi
- ▶ Chargeur et rejet de cartes d'une capacité de 100 unités
- ▶ Vitesse d'impression couleur de 100 cartes simple face pour motif complexe (=vitesse minimale)
- ▶ Garantie impression 100 000 cartes

Il sera fourni avec cette imprimante tous les consommables pour l'impression de 100 badges.

Type Zebra P330i ou équivalent techniquement

3.9.2.3. UNITE DE TRAITEMENT LOCAL (UTL)

Les UTL seront raccordées directement sur le réseau Ethernet (sans convertisseur intermédiaire) dans le réseau CADI (à minimum VLAN CADI spécifique). Elles assureront une mémorisation locale des droits d'accès, des plages horaires, des historiques et une gestion autonome des accès même en cas de déconnexion au réseau Ethernet. Lors de la reconnexion du réseau, les informations seront restituées automatiquement au serveur.

Les UTL auront une capacité de gestion de 1000 badges et une mémorisation de 10 000 événements.

Les UTL gérant des accès disposeront des entrées/sorties nécessaires à la bonne gestion d'un accès sécurisé. Cela comprend :

- ▶ Entrée de gestion des données du lecteur de badge
- ▶ Entrée pour la position de la porte ou de l'obstacle (ouvert / fermé)
- ▶ Entrée auxiliaire de commande (Bouton poussoir ou action sur la béquille libre)
- ▶ Sortie de commande de la serrure, du verrou, de la barrière, ...

L'entreprise doit le câblage et raccordement de l'ensemble des équipements ci-dessus y compris l'alimentation des serrures et verrous.

Tous les accès contrôlés seront équipés de détecteurs d'ouverture sur chacun de leurs vantaux. Les obstacles unicitaires, et la barrière parking disposeront d'une information de déverrouillage.

Les UTL auront la capacité de dialoguer avec les lecteurs de badge sous différents protocoles : Wiegand, mag stripe, clock/data et RS (pour les échanges de données avec le contrôle d'accès).

1 bus d'extension type RS-485 permettant d'ajouter des UTL sur réseau de terrain (Ce bus ne sera pas utilisé lors de la mise en œuvre mais servira de capacité d'extension au système).

Une alimentation basse tension secourue par batterie (8 heures d'autonomie en marche normale demandée).

La base de données du serveur devra pouvoir gérer 5000 badges, l'UTL effectuant une requête auprès de cette base de données si le badge en lecture n'est pas référencé dans la mémoire de l'UTL.

Les UTL seront mise en œuvre dans le local LS dédiés et protégés en ouverture (fermeture à clé et alarme à l'ouverture). Elles disposeront d'une source d'énergie autonome permettant un fonctionnement de 8 heures en heure de pointe.

L'état des UTL sera reporté individuellement sur les plans graphiques du superviseur. Les états suivants seront au minimum reportés :

- ▶ Etat normal
- ▶ Défaut alimentation (marche sur batterie)
- ▶ Défaut batterie

3.9.2.4. LECTEURS DE BADGE (ENTREE, SORTIE, PRESENCE)

Les lecteurs de badge seront :

- ▶ Posés en sailli à proximité des accès
- ▶ En entrée ET en sortie (pas de bouton poussoir)
- ▶ Montés sur potelet en amont des barrières ou portails pour les accès véhicules et piétons au bâtiment.
- ▶ Les unités de lecture de badges seront naturellement compatibles avec les badges décrits et prévus dans ce CCTP.
- ▶ Les lecteurs auront les caractéristiques minimales suivantes :

- Liaison avec l'UTL de type RS-485 pour le MIFARE Desfire
- Liaison, avec le badge de type Mifare 13,56 Mhz
- Dimensions maximales du lecteur 102x76x20mm
- Durée du cycle d'identification avec l'UTL inférieure à 1/10 sec
- LED de signalisation
- IP65 pour les lecteurs extérieurs

Les unités de lecture de badges seront placées à proximité immédiate de l'accès à contrôler. Ils assureront une lecture globale des données du badge suivant le protocole de haut-niveau ISO 14443-4, en respectant le format de trames ISO 14443-3.

Une LED rouge signalera un accès refusé et une LED verte un accès autorisé. Une LED de couleur bleu signalera le mode attente du lecteur.

Chaque accès sera équipé d'un détecteur d'ouverture sur chaque vantail permettant de signaler l'état ouvert ou fermé de l'accès. Le verrouillage de l'accès s'effectuant lorsque celui-ci est refermé, ou s'il n'a pas été ouvert après une temporisation de quelques secondes (réglable depuis le logiciel individuellement par accès).

Un lecteur/encodeur sera fourni sur le poste isolé d'encodage

Un lecteur enrôleur sera fourni et installé avec le poste opérateur.

3.9.2.5. LES BADGES

Les badges auront les caractéristiques suivantes

- ▶ Technologie MIFARE DesFire EV3 ;
- ▶ Capacité de stockage : 8 Kilo Octets (8K)
- ▶ Dimension selon norme ISO 7810 ID1 « carte de crédit ». Epaisseur inférieure à 0.79mm
- ▶ Sans élément actif

3.9.2.6. LOGICIEL DE CONTROLE D'ACCES (CA)

Cette application de contrôle d'accès permettra :

- ▶ La gestion des droits d'accès par groupe en créant des autorisations par lecteurs et fuseaux horaires.
- ▶ L'attribution d'un ou de plusieurs badges à une personne.
- ▶ La gestion des événements en temps réels tels que les autorisations ou refus d'accès, les alarmes systèmes ou portes forcées,
- ▶ La gestion des rapports d'événements tels que la liste des accès demandés sur un lecteur ou groupe de lecteurs, ou sur un porteur de badge
- ▶ La remontée d'information en cas d'utilisation d'un badge précis
- ▶ L'impression des listes des droits d'accès par utilisateur, par lecteur ou globalement.
- ▶ La gestion de fiche d'accès /utilisateur permettant pour chaque personne une édition au format A4
- ▶ La gestion synthétique des droits d'accès permettant une édition résumée (1 ligne par porteur de badge)
- ▶ La visualisation sur plans graphiques des équipements techniques installés (lecteurs de badges, ouverture porte, ...) et leur animation en fonction de leur état.
- ▶ La personnalisation et la création des designs de badges.

Les événements consignés sont horodatés et affichent simultanément l'indication du numéro d'ordre du porteur de badge ou de la porte concernée. Le paramétrage des programmes de gestion du contrôle d'accès sont dus par le présent lot.

Le système sera fourni avec les capacités suivantes :

- ▶ Base de données de badge 1500
- ▶ Mémoire des enregistrements d'événements limitée à la capacité du disque,
- ▶ Gestion jusqu'à 16 lecteurs de badges
- ▶ Base de données SQL ou SQL express (sur un serveur séparé du serveur d'application fonctionnel CA)
- ▶ Une sauvegarde du logiciel fonctionnel CA, de son paramétrage ainsi que de la base de donnée sera prévue et configurée selon les règles indiquées par le BE (fonctionnel et technique).

3.10. Le système de détection intrusion (DI)

3.10.1. Note préliminaire

L'ensemble des équipements actifs de l'installation disposera d'une autonomie de 30 min et les UTL disposeront d'une autonomie de fonctionnement de 8 heures en cas de coupure secteur.

Le système de détection intrusion est composé :

- ▶ De centrales intrusion NF&A2P, 3 boucliers ;

- ▶ De modules d'entrée / sortie déportés sur lesquelles seront raccordés les terminaux ;
- ▶ Contact d'ouverture à double contact pour remonter les informations au contrôle d'accès et à la détection d'intrusion ;
- ▶ Détecteurs bivolumétriques : IR et HF ;
- ▶ De lecteur de badge + codier pour la commande d'activation/désactivation intrusion ;

La centrale sera raccordée au réseau Ethernet de Sûreté (à minimum avec un VLAN dédié) décrit au chapitre 3.4.

Chaque ouvrant ou accès, équipé d'un détecteur de chocs et d'un détecteur d'ouverture câblés en série, fournira une information de synthèse d'alarme.

Une information d'alarme sera remontée à la supervision technique par contact sec de l'état du réseau ondulé du bâtiment.

3.10.2. Equipement des locaux

Les locaux seront équipés de :

- ▶ Contact d'ouverture sur l'ensemble des ouvrants
 - de la ZP BE,
 - du local de stockage sous comble
 - du comble inoccupé (portes uniquement)
- ▶ Détecteur volumétrique pour chaque local
 - de la ZP,
 - du local de stockage
 - du comble
- ▶ Un lecteur d'alarme à badge + codier
 - pour chaque local sensible,
 - pour le local de stockage et
 - pour les combles (le lecteur de badge sera installé dans la Zone 3 avec indicateur d'action en zone 3 avec un report dans chaque cage d'escalier entre le 2^e étage et les combles avec panneautage indiquant les combles).

3.11. Le système de vidéosurveillance

3.11.1. Note préliminaire

Pour le Bâtiment, l'architecture du système de vidéosurveillance de type IP mis en œuvre, communique et utilise les baies et câblage de l'infrastructure « Sûreté » décrit au § 3.4.

Ce système respectant les recommandations ANSSI (N°524/ANSSI/SDE), APSAD R82 et NF EN 62676-4 est constitué :

- ▶ D'un ou plusieurs serveur(s) physique(s)/virtuel(s) implanté(s) dans la Baie Sûreté du LT CADIVS Principal redondé sur un serveur secondaire dans le LT CADIVS de sauvegarde comme décrit précédemment ;
- ▶ De son propre logiciel/système de supervision
- ▶ D'un poste d'exploitation double écran au secrétariat ;
- ▶ D'un poste d'exploitation des images de vidéo extérieure au poste d'accueil et de filtrage de l'emprise ;
- ▶ De caméras IP dômes fixes couleurs (intérieures) ;
- ▶ De caméras IP fixes couleurs sous caisson (extérieures) ;
- ▶ D'Enregistreurs Vidéo Numériques Réseau (Network Video Recorder - NVR) dont un de secours positionné dans le second local CADIVS permettant d'enregistrer en local, les images en provenance des diverses caméras (intérieurs et extérieurs)

La durée d'enregistrement est de 30 jours en continu à 25 images/s en format 4K (Full HD minimum respectant les fonctions et normes de pixel DORI).

Il est prévu un ensemble de 6 enregistreurs Raid 5 double alimentation (dont 1 dédié aux caméras des salles CD) + 1 enregistreur de secours utilisé en cas de défaillance d'un des 6 enregistreurs. La capacité totale d'enregistrement est >350 To.

Lorsqu'un serveur d'enregistrement principal tombe en panne, le serveur de gestion initie le serveur d'enregistrement de basculement disponible dès qu'il détecte la panne. La commande ainsi que la configuration du serveur d'enregistrement défaillant seront envoyées au serveur d'enregistrement de basculement, qui démarrera le moteur d'enregistrement et commencera à extraire les flux de tous les appareils associés.

Les caméras de type IP (full HD) jour/nuit H264 25ips, conforme ONVIF et supportant la norme IEEE 802.1X, sont alimentées depuis les commutateurs des baies dédiées à la sûreté, alimentées depuis des onduleurs.

Des protections foudre sont également prévues pour la protection IP entre les caméras extérieures et les coffrets vidéo. Les alimentations sont quant à elles déjà protégées en amont.

3.11.2. Zone de surveillance

L'installation de vidéosurveillance mise en place permet la surveillance :

- ▶ Des façades et abords bâtiment 0009 (ext) en observation
- ▶ De tous les accès et issues de secours de l a ZP BR (int) en identification
- ▶ Des zones sensibles (locaux classés en zone 3) en identification
- ▶ Des couloirs du BE en reconnaissance

3.11.3. Performances de surveillance

L'installation et les réglages des caméras sont adaptés pour répondre à 4 objectifs (norme DORI) :

- ▶ Objectif 1 – Détection : Visu permettant de détecter une approche ou un mouvement d'individus. Résolution horizontale minimale de 25 pixels/mètre (8 pixels/pouces)
- ▶ Objectif 2 – Observation/Surveillance/levée de doute : Visu permettant de confirmer la présence et le mouvement d'individus. Résolution horizontale minimale de 63 pixels/mètre (19 à 20 pixels/pouces).
- ▶ Objectif 3 – Reconnaissance : Visu permettant la reconnaissance en temps réel d'un individu. Résolution horizontale minimale de 125 pixels/mètre (38 à 40 pixels/pouces).
- ▶ Objectif 4 – Identification : Visu permettant l'identification à posteriori d'un individu. Résolution horizontale minimale de 250 pixels/mètre (76 à 80 pixels/pouces).

3.12. Précisions techniques sur la supervision technique

La supervision technique doit être une fonctionnalité d'un système à part entière qui communique avec l'intégralité des sous-ensemble tel que le ou les hyperviseur (s), les machines virtuelles, les switches les UTL et les caméras.

Ce sous-ensemble propose, a minima, une IHM unifiée intégrant un outil de cartographie dynamique et personnalisable permettant d'ajuster la finesse du scope par sous-ensemble souhaité.

Ce sous-ensemble aura en charge la supervision de l'état de fonctionnement des matériels présents sur les sous-réseaux/VLAN dont :

- ▶ Les communications informatiques sur les couches physiques :
 - Poste client,
 - Caméra,
 - UTL,
 - CCGE, ...soit tout équipement relié au réseau informatique)
- ▶ Les switches ou tout équipement réseau
- ▶ Les parefeux et systèmes de sécurité implémenté
- ▶ Les serveurs physiques :
 - Etat de fonctionnement,
 - Occupation disque
 - Occupation mémoire,
 - Etat réseau
 - Débit réseau,
 - Services importants...soit tout indicateur pertinent pour le type de serveur monitoré
- ▶ Les serveurs virtuels
 - Etat de fonctionnement,
 - Occupation disque virtuel
 - Occupation mémoire virtuel,
 - Etat réseau
 - Débit réseau,
 - Services importants...soit tout indicateur pertinent pour le type de serveur monitoré
- ▶ Les postes d'exploitation des différents réseaux

- Etat de fonctionnement,
- Occupation disque,
- Occupation mémoire,
- Etat réseau
- Débit réseau,
- Services importants (superviseur CADI, superviseur VS...)

soit tout indicateur pertinent pour le type de serveur monitoré

- ▶ Les éléments industriels (UTL, lecteurs, caméras, contacteurs ...)
 - Etat de fonctionnement,
 - Occupation mémoire si disponible,
 - Etat réseau,
 - Débit réseau,
 - Services importants si disponible (service Web, flux de données, ...)

soit tout indicateur pertinent pour le type de serveur monitoré

- ▶ Surveillance des sauvegardes et de leur état de consistance

De façon générale, la supervision technique gère les fonctionnalités suivantes :

- ▶ gestion des événements sur les composants CADIVS et les serveurs/incidents réseaux ;
- ▶ gestion de la performance de l'infrastructure ;
 - gestion des capacités de stockage ;
 - engorgement/état du réseau ;
 - traduction des traps SNMP ;
- ▶ sauvegarde de la configuration et des événements ;
- ▶ génération de rapports avec mise en exergue des problèmes (incidents récurrents) dans l'IHM et sur papier ou support informatique.
- ▶ Synchronisation avec un système secondaire si besoin ou présent

3.13. Précisions techniques sur les comptes utilisateurs et l'administration du S2I

3.13.1. Principes généraux des comptes utilisateurs

Par principe, chaque compte devra être nominatif et pris en compte par le personnel utilisant le S2I.

Chaque compte sera cantonné à un niveau défini. Un compte administrateur ne sera pas utilisé pour une utilisation normale et quotidienne du système. Ceci a pour but de permettre de limiter une atteinte et ou altération potentiel volontaire ou non du S2I.

3.13.2. Principes d'administration et procédures

L'administration doit autant que possible se faire par des GPO pour les paramètres pouvant être administrés ainsi

Les configurations doivent être sauvegardé régulièrement et permettre un retour en arrière en cas de problème.

La traçabilité et l'imputabilité de chaque action effectuée sur le système est une composante permanente et essentielle.

La documentation et sa qualité concernant les procédures d'administration et de gestion doit être :

- ▶ Claire,
- ▶ Précise,
- ▶ Et irréprochable dans son contenu.

Des procédures d'urgence pour les arrêts/redémarrages et la récupération du système en cas d'incident doivent exister et être testé. Leurs précisions et leurs fiabilités contribuent à la sécurité du système et des opérations qui seront menées par la suite.

4. ANNEXE 1 – DOCUMENTS DE REFERENCE

Le Titulaire doit appliquer les normes existantes. La liste fournie ci-dessous est donnée à titre indicatif et reste non exhaustive. Si des nouvelles normes, annexes ou fiches d'interprétation sont amenées à remplacer une partie ou le tout, ces dernières doivent être impérativement prises en compte.

Référence	Objet	Date
PIA Cyber	Politique interarmées de la cyber sécurité des systèmes d'information des armées	24/10/2016
	Profil de protection d'un automate programmable industriel	
INS 4450/DSAE/DIRCAM	Instruction relative à l'infrastructure, aux équipements, aux procédures d'exploitation et de maintenance, aux conditions d'homologation et de surveillance des aérodromes de la défense	01/03/2017
Directive DIRISI n°9	Directive d'assignation des fréquences et de gestion des sites et des servitudes radioélectriques au sein du Ministère de la Défense	30/11/2009
Directive DIRISI n°67	Gestion des Trigrammes	16/06/2015
Directive DIRISI n°73	Directive d'installation et de nommage OGIT	04/04/2016
Directive DIRISI n°78	Nommage des serveurs	26/11/2012
Directive DIRISI n°80	Nommage des VLAN	11/06/2013
Directive DIRISI n°129	Directive d'exploitation du plan IPV4 du Ministère de la Défense	07/05/2014
Directive DIRISI n°199	Directive d'exploitation et de soutien du système de surveillance et de sécurité pour la protection défense	15/02/2017
Guide de la DIRISI	Guide traitant de la CIMS et le contrôle d'accès en version simplifiée	05/09/2017
Guide technique de la DIRISI	Guide technique traitant du contrôle d'accès v1.0	01/08/2017
Norme Défense NORMDEF 0301-1	Norme relative à l'Evaluation et emploi des systèmes d'armes et munitions équipés de dispositifs électro-pyrotechniques soumis aux effets des rayonnements électromagnétiques non-ionisants	Avril 2017

Référence	Objet	Date
Directive Technique n°270/ARM/EMA/COMCYBER/CALIDDR	Directive technique relatives aux formats des journaux d'évènement attendus par le CALID	13/07/2020
Règlement d'exécution 2019/947	Relatif aux règles et procédures applicables à l'exploitation d'aéronefs sans équipage à bord	24/05/2019
Directive ATEX 1999/92/CE	Prescriptions minimales visant à améliorer la protection en matière de sécurité et de santé des travailleurs susceptibles d'être exposés aux risques d'atmosphères explosives (ATEX)	23/03/1994
Directive 2014/34/UE	Relative aux appareils et systèmes de protection destinés à être utilisés en atmosphère explosible	20/04/2016
Directive nationale de sécurité	Directive nationale de sécurité « activités militaires de l'État »	02/07/2018
Instruction ministérielle n°7326/DEF/CAB	PSSI du Ministère de la Défense	07/08/2014
Instruction ministérielle (IM) n°900/DEF/CAB/DR	Relative à la protection du secret de la défense nationale au sein du MINDEF	26/01/2012
Instruction ministérielle (IM) n°1544/DEF/CAB/DR	Relative à la défense-sécurité des activités, moyens et installations relevant du Ministère de la Défense	17/01/2017
Instruction générale interministérielle (IGI) n°1300	Relative à la protection du secret de la défense nationale approuvée par arrêté du 30 novembre 2011	30/11/2011
Instruction générale interministérielle (IGI) n°6600	Relative à la sécurité des activités d'importance vitale approuvée par arrêté du 07 janvier 2014	07/01/2014
Instruction ministérielle (IM) 2004 n° 04/DEF/DGSIC	IM, relative à la fonction d'administrateur de systèmes d'information et de communication au sein du Ministère de la Défense.	14/12/2009
Directive DGSIC n°18	Relative à l'organisation du domaine des fréquences	31/07/2011
Directive DGSIC n°23	Relative à l'utilisation du WIFI au sein du MINARM	06/02/2012
Directive DGSIC n°27	Homologation des systèmes d'information du Ministère de la Défense	24/01/2013
Directive DGSIC n°36	Marquage des flux IP sur les réseaux du Ministère de la Défense	03/07/2015

Référence	Objet	Date
Directive DGSIC n°39	Sécurité des systèmes industriels	05/07/2016
Directive 485/DEF/DGSIC/OGF/DR	Note relative à l'établissement et gestion des plans de servitudes radioélectriques du Ministère de la Défense.	30/08/2016
CCT V2.0 DGSIC	Cadre de cohérence technique des systèmes d'information et de communication du Ministère de la Défense	28/07/2016
Directive n°1000/EMZD Metz/DIVADF/BSECPRO/DR	Directive de sécurité de la zone terre nord-est	23/06/2017
Politique ministérielle de la DPID	Relative à l'utilisation de la carte d'identité multi-services pour le contrôle d'accès v2.0	01/05/2019
Note n°258/ARM/DPID	Relative à la mise à la clé des systèmes de contrôle d'accès utilisant la CIMS de la DPID	10/10/2018
Guide DPID version 1	Relatif à la gestion des éléments secrets de la puce sans contact de la CIMS	01/12/2016
Directive n°73 OGIT	Directive qui fixe les règles de numérotation et les couleurs normalisées	03/04/2017
Directive 485/SGDN/TTS/SSI	Installation des sites et systèmes d'information sur la protection contre les signaux compromettants	20/11/2013
Directive 495/SGDN/DCSSI	Zonage TEMPEST : protection contre les SPC	20/11/2013
Instruction interministériel (II) n°300	Relative à la protection contre les signaux parasites compromettants	23/06/2014
Note n° 524/ANSSI/SDE	Recommandations de sécurité relatives aux mots de passe pour la mise en œuvre de dispositif de vidéo protection préconisées	14/02/2013
22/ANSSI/SDE/NP	Recommandations relatives à l'administration sécurisée des systèmes d'information	20/04/2018
20/ANSSI/SDE/NP	Recommandations pour le déploiement sécurisé du navigateur Mozilla Firefox sous Windows	04/02/2015
24/ANSSI/SDE/NP	Recommandations de configuration matérielle de postes clients et serveurs x86	23/03/2015
25/ANSSI/SDE/NP	Recommandations pour la sécurisation d'un commutateur de desserte	24/06/2016
17/ANSSI/SDE/NP	Recommandations de sécurité relatives à Active Directory	10/09/2014

Référence	Objet	Date
012/ANSSI/SDE/NP	Recommandations de sécurité pour la mise en œuvre d'un système de journalisation	02/12/2013
008/ANSSI/SDE/NP	Recommandations de sécurité relatives aux environnements d'exécution Java sur les postes de travail Microsoft Windows	19/04/2013
011/ANSSI/SDE/NP	Problématiques de sécurité associées à la virtualisation des systèmes d'information	26/09/2013
19/ANSSI/SDE/NP	Recommandations de sécurité concernant l'analyse des flux HTTPS	09/10/2014
007/ANSSI/SDE/NP	Recommandations pour un usage sécurisé d'(Open)SSH	21/01/2014
006/ANSSI/SDE/NP	Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu	30/03/2013
003/ANSSI/SDE/NP	Recommandations de sécurité relatives à Ipv6 1 pour la protection des flux réseau	31/08/2012
3248/ANSSI/ACE	Guide de définition d'une architecture de passerelle d'interconnexion sécurisée	08/12/2011
Guide ANSSI	Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection version 2.0	04/03/2020
Guide ANSSI	Guide pour la sécurité des technologies sans contact pour le contrôle des accès physiques	19/11/2012
GTCSI	Profil de protection d'une passerelle VPN industrielle Profil de protection d'une borne sans-fil industrielle Profil de protection d'un pare-feu industriel Profil de protection d'un commutateur industriel GTCSI	06/02/2015

5. ANNEXE 2 – ACRONYME

Acronyme	Description
ACN	Contrôle d'accès avec chiffre (Access Control Number)
ACT	Plan d'actions
AD	Service d'annuaire (Active Directory)
AMO	Assistance à la maîtrise d'ouvrage
AN	Alerte nomade
ANSSI	Agence nationale de la sécurité des systèmes d'information
ARP	Analyse de risques projet
ATEX	Atmosphère explosive
ATT	Attente de l'Administration
AVP	Dossier d'avant-projet
BdC	Bon de commande
BdS	Bulletin de sécurité
BE	Bureau d'Etude : nom désignant le bénéficiaire à inclure dans les documents
b	bit (Binary digIT) : unité de base des mesures informatique
B	octet (Byte) : unité de base des mesures informatique (1B = 1o = 8b)
BL	Bordereau de livraison
BPU	Bordereau de prix unitaire
BPU – OS	Bordereau de prix unitaire – opérations simples
BT	Bluetooth
CA	Contrôle d'accès
CADIVS	Contrôle d'accès, détection d'intrusion et vidéosurveillance
CALID	Centre d'appui à la lutte informatique défensive
CAT	Cahier de tests
CCAP	Cahier des clauses administratives particulières
CCTP	Cahier des clauses techniques particulières
CD	Confidentiel défense
CdF	Catalogue de formation
CdS	Convention de service
CEC	Centre d'élaboration des clés
CEI	Commission électrotechnique internationale

Acronyme	Description
CETID	Centre d'expertise des techniques de l'infrastructure de la Défense
CCGE	Coffre à Clé à Gestion Electronique
CFA	Courant faible
CFO	Courant fort
CGA	Coffre de gestion des accès
CIMS	Carte d'identité multi-services
CIP	Contrôleur d'identité portable
CIRISI	Centre interarmées des réseaux d'infrastructure et des systèmes d'information
CLR	Conception du lot de rechange
CMO – RD	Centre de mise en œuvre des réseaux de desserte
CNGF	Centre national de gestion des fréquences
CNI	Carte nationale d'identité
CNIL	Commission nationale de l'informatique et des libertés
CNMO-R	Centre national de mise en œuvre des réseaux
CONST	Documentation constructeur/éditeur
COP	Centre opérationnel de protection
COPIL	Comité de pilotage
COSUIV	Comité de suivi
COTS	Vendu sur étagères (Commercial Off The Shelf)
CSF	Constatation de service fait
CSPN	Certification de sécurité de premier niveau
CVE	Vulnérabilités et expositions communes (Common Vulnerabilities and Exposures)
CVPO	Contrôle et vérification périodique obligatoire
CVSS	Système d'évaluation standardisé de la criticité des vulnérabilités (Common Vulnerability Scoring System)
DAA	Demande d'autorisation d'accès
DAT	Dossier d'architecture technique
DBCT	Dossier de bilan de campagne de tests
DC DIRISI	Direction centrale de la DIRISI
DC SID	Direction centrale du service infrastructure de la Défense
DCS	Dossier des contraintes site
DDEM	Dossier de description de la plateforme de démonstration
DECT	Téléphone sans-fil numérique amélioré (Digital Enhanced Cordless Telecommunications)
DEEE	Déchets d'équipements électriques et électroniques

Acronyme	Description
DELIV	Dossier de livraison
DEV	Devis
DGNUM	Direction générale du numérique (nouvelle appellation de DGSIC)
DGSIC	Direction générale des systèmes d'information et communication
DHCP	Protocole de configuration dynamique d'hôte (Dynamic Host Configuration Protocol)
DI	Détection d'intrusion
DIR	Directive
DIRISI	Direction interarmées des réseaux d'infrastructure et des systèmes d'information
DL	DIRISI locale
DLIV	Dossier de livraison
DL DIRISI	Direction locale de la DIRISI
DNS	Nom de domaine du serveur (Domain Name Server)
DOE	Dossier des ouvrages exécutés
DOP	Détecteur d'ouverture de porte
DORI	Détection Observation Reconnaissance Identification
DR	Diffusion restreinte
DST	Dossier de stratégie de tests
EAL	Evaluation du niveau d'assurance (Evaluation Assurance Level)
EAR	Elément actif réseau
EBIOS	Expression des besoins et identification des objectifs de sécurité
ECO	Architecture économique
ECPI	Equipe de conduite de programme intégrée
EI	Ethernet industriel
EIB	Expression Initial du Besoin
ELI	Equipe locale intégrée
EQP	Recensement des équipements
EXI	Exigence
FdP	Feuille de présence
FE	Fiche d'événement
FEB	Fiche d'expression de besoin
FEROS	Fiche d'expression rationnelle des objectifs de sécurité
FFTP	Fiche de fait technique
FICE	Fiche individuelle de contrôle élémentaire
FIT	Fiche de test

Acronyme	Description
FOB	Fiche d'objectifs
FOD	Fiche d'orientation et de Définition
FRE	Fiche réflexe
Gb	Gigabits
Gb/s	Gigabits par seconde (Gigabit per second) : vitesse de communication informatique
Go	Giga-Octets (unité de mesure de stockage informatique)
GT	Groupe de travail
GTI	Garantie du temps d'intervention
GTR	Garantie du temps de rétablissement
GTRN	Garantie de temps de réparation nominale
GTRP	Garantie de temps de réparation palliative
HF	Hyper fréquences (High Frequency)
HL	Hébergement local
HTTP	Protocole de transfert hypertext (HyperText Transfert Protocol)
HTTPS	Protocole de transfert hypertext sécurisé (HyperText Transfert Protocol Secure)
HSM	Boîte noire transactionnelle (Hardware Security Module)
ID	Interphonie diffusion
IDS	Système de détection d'intrusion (Intrusion Detection System)
IPS	Système de prévention d'intrusion (Intrusion Prevention System)
IHM	Interface homme-machine
IK	Indice de protection contre les chocs
ILS	Système d'atterrissage aux instruments (Instrument Landing System)
Infra	Infrastructure
IP	Protocole internet (Internet Protocol)
IP	Indice de protection contre les corps solides et liquides
IRP	Infrarouge passif
IPSEC	Communications privées et protégées sur des réseaux IP (Internet Protocol SECurity)
JCOP	Nom d'un type de carte à puce (Java Card Open Platform)
KC	Container
KEYTAG	Porte-clé dans un coffre à clé (CCGE)
LAPI	Lecteur automatique de plaques d'immatriculation
LOG	Recensement des logiciels
LT	Local technique
LTE	Evolution en long terme (Long Term Evolution)

Acronyme	Description
MAC	Adresse physique d'un matériel informatique/électronique (Media Access Control)
Mb	Méga-bit
Mb/s	Méga-bit par seconde (Mega-bit per second)
MCEX	Matrice de couverture des exigences
MCO	Maintien en condition opérationnelle
MCS	Maintien en condition de sécurité
MEXi	Matrice des exigences
MEXp	Manuel d'exploitation
MINARM	Ministère des Armées
Mo	Méga-octet (unité de mesure de stockage informatique)
MOA	Maîtrise d'ouvrage
MOM	Mise en ordre de marche
MORPHO	Nom d'un type de carte à puce
MT	Mémoire technique
MU	Manuel utilisateur
NAS	Unité de stockage en réseau (Network Attached Storage)
NFC	Communication en champ proche (Near Field Communication)
NTI	Niveaux techniques d'intervention (1,2 ou 3)
NTP	Protocol de temps réseau (Network Time Protocol)
OARDHS	Outil d'aide à la rédaction des dossiers d'homologation simplifiée
OC	Opération complexe
OGIT	Outil informatique de gestion des infrastructures de télécommunications
OS	Opération simple
OS serveur	Système d'exploitation du serveur (Operating System server)
OSI	Norme de communication des SI (Open Systems Interconnection)
PAF	Poste d'accueil et de filtrage
PP	Point à préciser
PARA	Recensement des paramétrages
PC PRO	Poste de coordination de la protection
PCP	Poste central de protection (de contrôle, de surveillance, de permanence)
PCA	Plan de continuité des activités
PCI	Plan de continuité informatique
PdF	Plan de formation
PdS	Plan de sécurité

Acronyme	Description
PES	Procédure d'exploitation de la sécurité
PIC	Plans d'implantation des capteurs
PKI	Infrastructure à clés publiques (Public Key Infrastructure)
PL	Poids lourd
PLA	Planning prévisionnel détaillé
PMAS	Plan de maquettage des salles
PMP	Plan de management de projet
POE	Power over Ethernet
PPR	Plan de prévention
PRA	Plan de reprise d'activité
PRI	Plan de reprise informatique
PSSI	Politique de sécurité du ou des systèmes d'information
PT1	Perturbation électromagnétique de niveau 1
PT2	Perturbation électromagnétique de niveau 2
PTZ	Pan tilt zoom (contrôle panoramique / inclinaison /zoom)
PV	Procès-verbal
PVLAN	Réseau local virtuel privé (Private Virtual Local Area Network)
PVSF	Procès-verbal de service fait
QCM	Questionnaire à choix multiples
QEF	Questionnaire d'évaluation de la formation
QR CODE	Code-barres en deux dimensions (Quick Response CODE)
RADIUS	Protocole client-serveur pour centraliser des données d'authentification (Remote Authentication Dial-In User Service)
RGPD	Règlement général sur la protection des données
RIDA	Relevé d'information décision action
RL	Réseau local
RLI	Réseau local d'infrastructure
RNI	Rayonnements électromagnétiques non ionisants
RPA	Représentant du pouvoir adjudicateur
RSSI-A	Responsable de la sécurité du système d'information – aval
RSSI-P	Responsable de la sécurité du système d'information – projet
SAM	Modules d'application sécurisés
SAN	Réseau de stockage (Storage Area Network)
SCOE	Service conduite opération exploitation

Acronyme	Description
SD	Secret défense
SdF	Support de formation
SDK	Ensemble de logiciel de développement (Software Development Kit)
SECPRO	Sécurité protection
SFP	Module émetteur-récepteur compact (Small Form-factor Pluggable)
SI	Système d'Information
SIC	Systèmes d'Information et de Communication
SIG	Spécifications d'interface graphique
S2I ou SII	Système d'Information Industriel
SIND	Support de présentation des indicateurs de performance
SIPS	Système intégré de protection sécurité
SNMP	Protocole simple de gestion de réseau (Simple Network Management Protocol)
SPANINGTREE	Protocole réseau de niveau 2
SPS	Sécurité protection de la santé
SREU	Support de préparation de la réunion de lancement
SS	Sous-système
SS-CA	Sous-système de contrôle d'accès
SS-DI	Sous-système de détection intrusion
SS-HL	Sous-système d'hébergement local
SS-ID	Sous-système d'interphonie et de diffusion
SS-STH	Sous-système de supervision technique et d'hypervision
SS-VS	Sous-système de Vidéosurveillance
SSI	Sécurité des systèmes d'information
STG	Désigne la ville de Strasbourg
STH	Supervision technique et d'hypervision
TCP	Protocole de contrôle de transmissions (Transmission Control Protocol)
TdBS	Tableau de bord MCS
TLS	Sécurité de la couche transport (Transport Layer Security)
Tb	Tera-bit
To	Tera-Octet (unité de mesure de stockage informatique)
TSA	Espace aérien réservé (Temporary Segregated Area)
TTC	Toutes taxes comprises
UTL	Unité de traitement local
V2A	Acier inoxydable (2 austénites)

Acronyme	Description
VA	Vérification d'aptitude
VdR	Vérification de réalisation
VL	Véhicule léger
VLAN	Réseau local virtuel (Virtual Local Area Network)
VMS	Système de supervision vidéo (Video Management System)
VPN	Réseau privé virtuel (Virtual Private Network)
VRRP	Protocole de redondance de routeur virtuel (Virtual Router Redundancy Protocol)
VS	Vidéosurveillance
VSR	Vérification de service régulier
WIFI	Réseau sans fil (WIREless Fidelity)
WIMESH	Technologie de réseau maillé
ZDHS	Zone de défense de haute sécurité

6. ANNEXE 3 - Terminologie

Thème	Désignation
Généralités	<ul style="list-style-type: none"> ▶ CA : contrôle d'accès ▶ DI : détection intrusion ▶ VS : vidéo surveillance ▶ CCGE : coffre à clés à gestion électronique ▶ CCM : coffre à clé mécanique ▶ ADMIN : administration ▶ SVT : supervision technique ▶ SVF : supervision fonctionnel
Contrôle d'accès	<ul style="list-style-type: none"> ▶ LdB (e) = lecteur de badge – entrée ▶ LdB (s) = lecteur de badge – sortie ▶ LdB (p) = lecteur de badge – contrôle de présence
Détection Intrusion	<ul style="list-style-type: none"> ▶ LdB (a) = lecteur de badge à codier (alarme) ▶ CO (p) = contact d'ouverture (porte) ▶ CO (f) = contact d'ouverture (fenêtre) ▶ DVDT = détecteur volumétrique double technologie ▶ IA= Indicateur d'Action
Vidéosurveillance	<ul style="list-style-type: none"> ▶ VSe = vidéo surveillance extérieure ▶ VSi = vidéo surveillance intérieure
Système de fermeture	<ul style="list-style-type: none"> ▶ BV = bandeau ventouse (serrure trois point et clé de verrouillage) ▶ PM = Penne motorisée (serrure trois points et clé de déverrouillage)
Autres	<ul style="list-style-type: none"> ▶ VP = vidéo portier avec interphonie

7. ANNEXE 4 – Serveur Principal du Local Principal CADIVS

Contenu minimal du serveur de PRINCIPAL

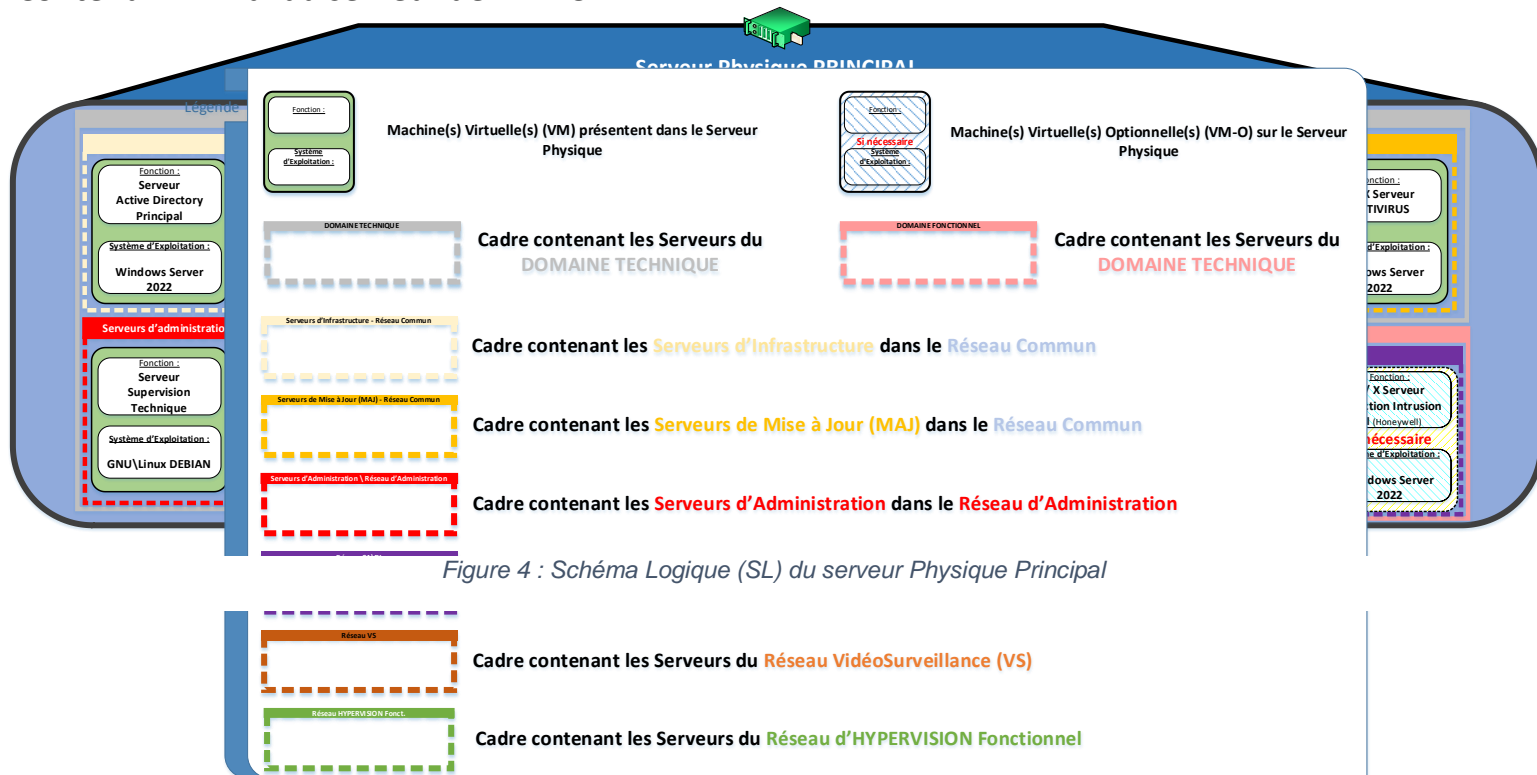


Figure 4 : Schéma Logique (SL) du serveur Physique Principal

8. ANNEXE 5 – Serveur de Secours du Local de Secours CADIVS

Contenu minimal du serveur de SECOURS/SAUVEGARDE

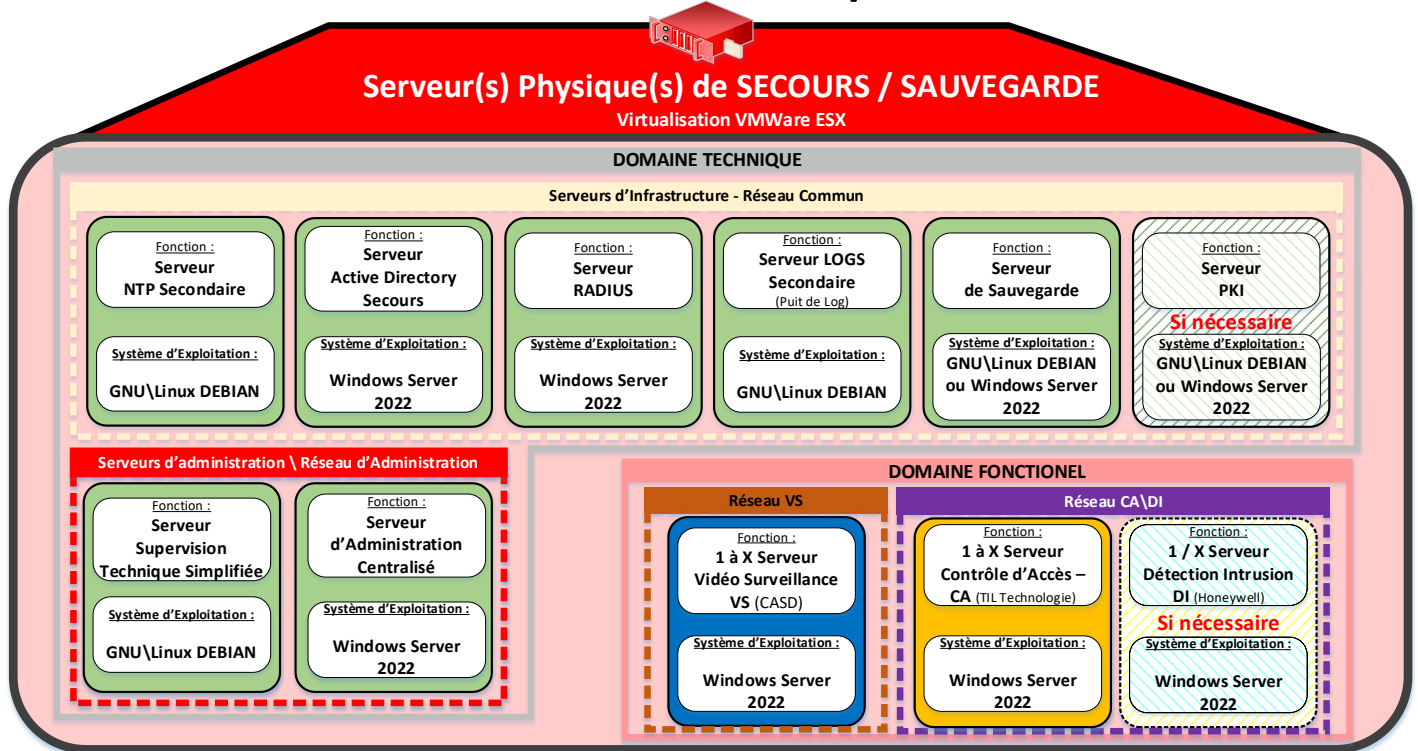
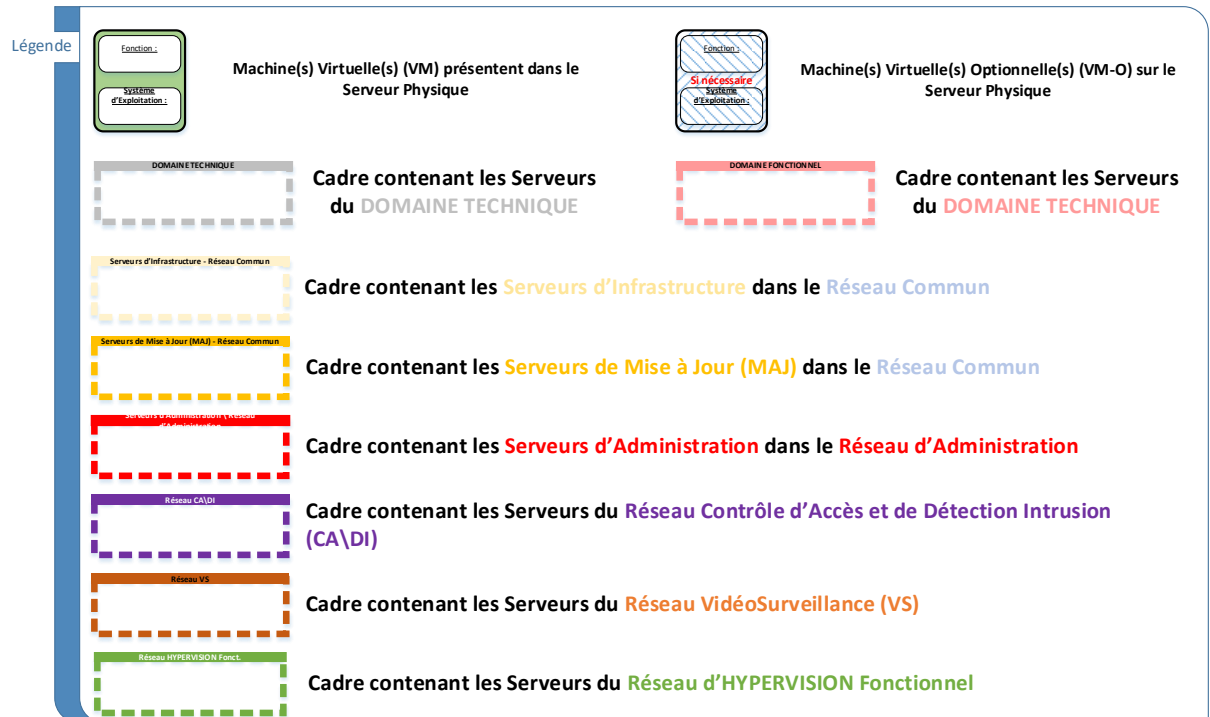


Figure 5 : Schéma Logique (SL) sur serveur Physique de Secours/Sauvegarde



9. ANNEXE 6 _ Gammes de maintenance

CONTRÔLE D'ACCES

- Examen des documents d'exploitation :
 - notice d'utilisation et d'exploitation,
 - carnet de contrôle du système de sûreté,
 - plan d'installation, dossier technique, schéma synoptique,
 - organisation des zones d'accès, des commandes et des créneaux horaires,
 - présence des notices constructeurs et des manuels d'exploitation.
- Contrôle de la conformité de l'installation, avec les documents d'exploitation et de son adéquation au risque.
- Contrôle visuel de l'état des matériels.
- Contrôle de la fixation des matériels de l'installation et resserrage suivant nécessité.
- Vérification des divers éléments de commande.
- Vérification des câblages.
- Dépoussiérage de tous les équipements.
- Nettoyage, vérification, resserrage et reprise éventuelle des connectiques.
- Contrôle des alimentations :
 - contrôle des tensions: piles, batteries, chargeurs,
 - contrôle des alimentations de secours,
 - vérification du fonctionnement sur les sources d'alimentations interne,
- Remplacement des piles.
- Remplacement des batteries d'accumulateurs (tous les 4 ans à compter de leur date de mise en service : à défaut d'indication sur la mise en place, le remplacement sera réalisé lors de la première période).
- Contrôle des mises à la terre.
- Contrôle des dispositifs de verrouillage.
- Mise à jour des logiciels.
- Sauvegarde des programmes et des données.
- Unité Traitement Locale :
 - essais mode dégradé,
 - essais de téléchargement.
- Unité de gestion :
 - état des écrans, qualité image, luminosité, contraste,
 - état des claviers, système de pointage,
 - nettoyage des filtres et vérification des ventilateurs,
 - vérification de la date et de l'heure,
 - vérification des communications avec les appareils existants,
 - vérification du paramétrage des lecteurs,
 - vérification, archivage des historiques,
 - réorganisation des fichiers.
- Contrôleur de portes et des lecteurs :
 - fixations, état du câblage,
 - contrôle des alimentations,
 - essais fonctionnels des lecteurs,
 - vérification des remontées d'événements,
 - vérification des ouvertures à distance,
 - vérification des remontées d'alarme,
 - vérification et réglages des ferme-portes,
 - vérifications des asservissements,
 - vérification des organes de verrouillage et de déverrouillage d'urgence, barrières, tourniquets, etc.
- Tripodes, tourniquets :
 - vérification et réglage des automates,
 - vérification et réglage des jeux fonctionnels des équipements,
 - nettoyage, réglage, graissage, lubrification des tringles, des crémaillères, des vis moteur, des chaînes, des charnières, etc.
- Serrures / gâches électro mécaniques :

- vérification et réglage des jeux fonctionnels des serrures et des supports sur lesquels ils sont fixés (portes, portails, etc.),
 - nettoyage, réglage, graissage, lubrification des tringles, des crémaillères, des vis moteur, des chaînes, des charnières, etc. des serrures et des supports sur lesquels ils sont fixés (portes, portails, etc.),
 - nettoyage et réglage des réflecteurs.
- Onduleurs :
- vérification état général (conditions d'installations, connexions, cartes électronique et connecteurs, ventilateurs, transformateurs, etc.),
 - vérification paramètres électriques sortie d'appareil (tension, courant, fréquence),
 - essais de l'appareil et commutation normal / secours (cycles de démarrage chargeur et onduleur, commutation circuits secours, vérification de l'autonomie des batteries en charge, etc.),
 - vérification des pièces dont les paramètres varient avec le vieillissement (capacités, self, etc.) et réglage des résistances variables ou autres composants permettant d'optimiser les performances de l'appareil,
 - vérification et échange des pièces à remplacement programmé : batterie, pièce de montage, jeu de câble, fusible, ventilateur, condensateur, carte d'alimentation (tous les 4 ans à compter de leur date de mise en service et tous les 10 ans pour les cartes d'alimentation, à défaut d'indication sur la mise en place le remplacement sera réalisé lors de la première période),
 - dépoussiérage général.
- Remplacement des pièces à remplacement programmé (pièces d'usures et de fonctionnement).
- Remplacement des pièces d'usures et de fonctionnement défectueuses.

ALARME INTRUSION

- Examen des documents d'exploitation :
- notice d'utilisation et d'exploitation,
 - carnet de contrôle du système de sûreté,
 - plan d'installation, dossier technique, schéma synoptique,
 - organisation des zones d'accès, des commandes et des créneaux horaires,
 - présence des notices constructeurs et des manuels d'exploitation.
- Contrôle de la conformité de l'installation, avec les documents d'exploitation et de son adéquation au risque.
- Contrôle visuel de l'état des matériels.
- Contrôle de la fixation des matériels de l'installation et resserrage suivant nécessité.
- Vérification de l'absence d'obstacle pouvant mettre en échec l'installation et vérification de masquage éventuel.
- Vérification des câblages.
- Dépoussiérage, nettoyage de tous les équipements.
- Nettoyage, vérification, resserrage et reprise éventuelle des connectiques.
- Contrôle des alimentations :
- contrôle des tensions: piles, batteries, chargeurs,
 - contrôle des alimentations de secours,
- vérification du fonctionnement sur les sources d'alimentations interne,
- Remplacement des piles.
- Remplacement des batteries d'accumulateurs (tous les 4 ans à compter de leur date de mise en service : à défaut d'indication sur la mise en place, le remplacement sera réalisé lors de la première période).
- Contrôle des mises à la terre.
 - Mise à jour des logiciels.
 - Sauvegarde des programmes et des données.
- Détecteurs :
- Vérification de la couverture de détection des détecteurs de mouvement,
 - Vérification des autres types de détecteurs (contact de portes, sismique, etc.),
 - Réglages éventuels.

- Vérifications des équipements de dissuasion (sirènes, flash lumineux, etc.).
- Vérification des divers éléments de commande.
- Unité Traitement Locale :
 - Vérification du paramétrage,
 - Vérification des temporisations d'entrée et de sortie,
 - Contrôle de l'auto surveillance.
- Unité de gestion :
 - État des écrans, qualité image, luminosité, contraste,
 - État des claviers, système de pointage,
 - Nettoyage des filtres et vérification des ventilateurs,
 - Vérification de la date et de l'heure,
 - Vérification des communications avec les appareils existants,
 - Vérification du paramétrage des lecteurs,
 - Vérification, archivage des historiques,
 - Réorganisation des fichiers.
- Essais des zones d'alarme quel que soit le dispositif de détection.
- Contrôle des organes de commande et asservissements.
- Vérification du bon fonctionnement des alarmes sonores et visuelles.
- Vérification des dispositifs de transmission des alarmes (transmetteurs téléphoniques).
- Vérification du fonctionnement de la transmission d'alarme.
- Essai des imprimantes ou enregistreurs.
- Nettoyage des capteurs et des organes de commande.
- Onduleurs :
 - vérification état général (conditions d'installations, connexions, cartes électronique et connecteurs, ventilateurs, transformateurs, etc.),
 - vérification paramètres électriques sortie d'appareil (tension, courant, fréquence),
 - essais de l'appareil et commutation normal / secours (cycles de démarrage chargeur et onduleur, commutation circuits secours, vérification de l'autonomie des batteries en charge, etc.),
 - vérification des pièces dont les paramètres varient avec le vieillissement (capacités, self, etc.) et réglage des résistances variables ou autres composants permettant d'optimiser les performances de l'appareil,
 - vérification et échange des pièces à remplacement programmé : batterie, pièce de montage, jeu de câble, fusible, ventilateur, condensateur, carte d'alimentation (tous les 4 ans à compter de leur date de mise en service et tous les 10 ans pour les cartes d'alimentation, à défaut d'indication sur la mise en place le remplacement sera réalisé lors de la première période),
 - dépoussiérage général.
- Remplacement des pièces à remplacement programmé (pièces d'usures et de fonctionnement).
- Remplacement des pièces d'usures et de fonctionnement défectueuses.

VIDEOPROTECTION

- Examen des documents d'exploitations :
 - notice d'utilisation et d'exploitation,
 - carnet de contrôle du système de sûreté,
 - plan d'installation, dossier technique, schéma synoptique,
 - organisation des zones d'accès, des commandes et des créneaux horaires,
 - présence des notices constructeurs et des manuels d'exploitation.
- Contrôle de la conformité de l'installation, avec les documents d'exploitation et de son adéquation au risque.
- Contrôle visuel de l'état des matériels.
- Contrôle de la fixation des matériels de l'installation et serrage suivant nécessité.

- Vérification de l'absence d'obstacle pouvant mettre en échec l'installation et vérification de masquage éventuel.
- Vérification des câblages.
- Dépoussiérage de tous les équipements.
- Nettoyage, vérification, resserrage et reprise éventuelle des connectiques.
- Contrôle des alimentations :
 - contrôle des tensions: piles, batteries, chargeurs,
 - contrôle des alimentations de secours,
 - vérification du fonctionnement sur les sources d'alimentations interne,
- Remplacement des piles.
- Remplacement des batteries d'accumulateurs (tous les 4 ans à compter de leur date de mise en service : à défaut d'indication sur la mise en place, le remplacement sera réalisé lors de la première période).
- Contrôle des mises à la terre.
- Mise à jour des logiciels.
- Sauvegarde des programmes et des données.
- Unité de gestion et de supervision :
 - état des écrans, qualité image, luminosité, contraste,
 - état des claviers, système de pointage,
 - nettoyage des filtres et vérification des ventilateurs,
 - vérification de la date et de l'heure,
 - vérification des communications avec les appareils existants,
 - vérification du paramétrage des lecteurs,
 - vérification, archivage des historiques,
 - réorganisation des fichiers.
- Caméras :
 - nettoyage et réglage de l'objectif,
 - nettoyage des ventilations,
 - contrôle de la qualité de l'image,
 - réglage de la netteté et de la mise au point,
 - réglage ligne – focus – target,
 - contrôle et réglage des tourelles, contrôle et réglage de la motricité des dômes,
 - vérification de masquage éventuel,
 - contrôle des zones de détection.
 - Caissons intérieurs et /ou extérieurs :
 - nettoyage, dépoussiérage,
 - vérification du bon fonctionnement des accessoires :
 - essuie-vitre,
 - thermostat,
 - télécommandes.
 - nettoyage des verres de protection.
- Système d'enregistrement :
 - contrôle du bon fonctionnement et de l'état des disques durs,
 - vérification du taux d'occupation des disques durs, des systèmes de sauvegarde,
 - vérification, archivage des historiques,
 - contrôle des programmes horaires.
- Moniteurs :
 - nettoyage, dépoussiérage,
 - contrôle des connexions.
- Projecteurs :
 - nettoyage, dépoussiérage,
 - contrôle des connexions.
- Onduleurs :
 - vérification état général (conditions d'installations, connexions, cartes électronique et connecteurs, ventilateurs, transformateurs, etc.),
 - vérification paramètres électriques sortie d'appareil (tension, courant, fréquence),
 - essais de l'appareil et commutation normal / secours (cycles de démarrage chargeur et onduleur, commutation circuits secours, vérification de l'autonomie des batteries en charge, etc.),

- vérification des pièces dont les paramètres varient avec le vieillissement (capacités, self, etc.) et réglage des résistances variables ou autres composants permettant d'optimiser les performances de l'appareil,

- vérification et échange des pièces à remplacement programmé : batterie, pièce de montage, jeu de câble, fusible, ventilateur, condensateur, carte d'alimentation (tous les 4 ans à compter de leur date de mise en service et tous les 10 ans pour les cartes d'alimentation, à défaut d'indication sur la mise en place le remplacement sera réalisé lors de la première période),

- dépoussiérage général.

- Remplacement des pièces à remplacement programmé (pièces d'usures et de fonctionnement).
- Remplacement des pièces d'usures et de fonctionnement défectueuses.

10. Index Schémas et Tableaux

INDEX DES SCHEMAS

Figure 1 : Principe d'alimentation électrique des Baies Informatiques du SII CADIVS.....	19
Figure 2 : Schéma Synoptique CADIVS du BE.....	19
Figure 3 : Principes et Architecture logique global d'un S2I CADIVS	21
Figure 4 : Schéma Logique (SL) du serveur Physique Principal.....	43
Figure 5 : Schéma Logique (SL) su serveur Physique de Secours/Sauvegarde	44

INDEX DES TABLEAUX

Tableau 1 : Relation entre la Note CVSS Environnementale et la Criticité... Erreur ! Signet non défini.	
Tableau 2 : Matériel et équipements demandés	22