



MINISTÈRE DE L'INTÉRIEUR

SECRÉTARIAT GÉNÉRAL DE LA ZONE DE DÉFENSE ET DE SÉCURITÉ SUD-OUEST
SECRÉTARIAT GÉNÉRAL POUR L'ADMINISTRATION DU MINISTÈRE DE L'INTÉRIEUR SUD-
OUEST
DIRECTION DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION
CELLULE ZONALE SECURITE DES SYSTEMES D'INFORMATION

Site de la PRÉFECTURE DE TULLE (19)

Cahier des Clauses Techniques Particulières. Création d'un système de mise en sûreté.

Rénovation de la solution de Détection Intrusion

Référence du CCTP	SGAMI SO/ DSIC / CZSB / PREF_19 / 2025
Rédacteurs	DEWAELE MATHIEU
Responsables techniques	Bertrand SOUBIE
Adresse	89 cours Dupré de Saint Maur 33000 Bordeaux
Téléphone	05 57 19 42 30 / 06 80 75 93 98
Email	bertrand.soubie@interieur.gouv.fr
Date d'émission du cahier des charges	05/06/2025
Version	1
Pièces jointes	CRT,DPGF, Annexes

Référence : CCTP réalisé à partir de celui du SZSIC 59 du 3/10/2013.

Table des Matières

Table des matières

1. DESCRIPTION GÉNÉRALE DU PROJET.....	5
1.1. OBJET DE LA CONSULTATION.....	5
1.2. DESCRIPTION BATIMENTAIRE.....	5
1.3. DESCRIPTION SYNTHÉTIQUE DES PRESTATIONS.....	6
1.3.1. PROGRAMMATION DES COMMUTATEURS.....	7
1.3.2. EN CAS DE PRÉSENCE DE PARE-FEUX.....	8
1.3.3. DIAGRAMMES DE FLUX.....	8
1.3.4. PRINCIPE RETENU.....	12
1.3.5. PRESTATION ATTENDUE.....	12
1.3.6. PROPOSITION DE PLAN D'UNE ANALYSE FONCTIONNELLE D'UNE SOLUTION DE SÛRETÉ BÂTIMENTAIRE.....	18
1.3.7. EXEMPLES DE SCÉNARIOS D'ASSERVISSEMENTS :.....	20
2. DESCRIPTION DE L'EXISTANT.....	21
2.1. ARCHITECTURE EXISTANTE ET SYSTÈME INSTALLÉ.....	21
2.2. ÉNERGIE.....	22
3. DESCRIPTION DES PRESTATIONS À RÉALISER.....	22
3.1. INFRASTRUCTURE RÉSEAU.....	22
3.1.1. LES RÉPARTITEURS.....	22
3.1.2. LES SERVEURS DE LA PRÉFECTURE.....	22
3.1.2.1. SERVEUR PRINCIPAL.....	22
3.1.2.2. SERVEUR DE REDONDANCE.....	23
3.1.3. LA DORSALE OPTIQUE.....	23
3.1.4. LE CAPILLAIRE CUIVRE.....	23
3.1.5. LES ÉLÉMENTS ACTIFS.....	23
3.1.6. LES BAIES DE SÛRETÉ.....	24
3.1.6.1. IMPLANTATION TYPE BAIE DU RÉPARTITEUR ET/OU SOUS-REPARTITEUR.....	24
3.2. CONTRÔLE D'ACCÈS.....	26
3.2.1. LES BADGES.....	26
3.3. DÉTECTION D'INTRUSION.....	26
3.3.1. GÉNÉRALITÉ LE SYSTÈME D'ALARME ATTENDU.....	26
3.3.2. LES UNITÉS DE TRAITEMENT LOCAL (UTL).....	27
3.3.3. MODULES COMPLÉMENTAIRES.....	28
3.3.4. MAQUETTE.....	28
3.4. LES ORDINATEURS DE GESTION.....	28
3.4.1. LES SERVEURS.....	28
3.4.1.1. LE SERVEUR D'APPLICATION.....	28
3.4.1.2. LE SERVEUR DE TEMPS (NTP).....	29
3.4.1.3. LE SERVEUR DE REDONDANCE.....	29
3.4.2. LES STATIONS.....	29

3.4.2.1. LE POSTE DE GESTION ET DE VISUALISATION ÉVÉNEMENT INTRUSION.....	30
3.4.3. SERVEURS ET POSTES INFORMATIQUES A FOURNIR.....	30
3.5. COURANT FAIBLE, COURANT FORT, ÉTIQUETAGE.....	31
3.5.1. COURANT FAIBLE.....	31
3.5.2. COURANT FORT ET ONDULEURS.....	31
3.5.3. ÉTIQUETAGE.....	32
3.5.4. ACTEUR.....	32
3.6. PRESTATIONS SUPPLÉMENTAIRES ÉVENTUELLES.....	32
4. INTERFONCTIONNEMENT DES SYSTÈMES.....	32
5. EXPLOITATION DE LA SOLUTION.....	32
5.1. GESTION DU SYSTÈME.....	32
5.1.1. PRÉSENTATION DES PROFILS UTILISATEURS.....	32
5.2. EXPLOITATION PAR L'ADMINISTRATEUR DU SYSTÈME.....	33
5.2.1. CONFIGURATION DES DROITS OPÉRATEURS.....	33
5.2.2. GESTION DES JOURNAUX.....	34
5.3. EXPLOITATION PAR LE GESTIONNAIRE DES BADGES.....	35
5.3.1. GESTION DES BADGES.....	35
5.3.1.1. PERSONNALISATION DES BADGES UTILISATEURS.....	35
5.3.1.2. GESTION DES PROFILS.....	36
5.3.1.3. INVALIDATION DES BADGES.....	36
5.3.1.4. ÉTAT D'UN BADGE.....	37
5.3.2. GESTION DES RAPPORTS.....	37
5.4. EXPLOITATION PAR LES OPÉRATEURS.....	37
5.4.1. GESTION TYPE.....	37
5.4.1.1. AMÉNAGEMENT DU POSTE DE GESTION.....	37
5.4.1.2. GESTION DES ENQUÊTES.....	38
5.4.1.3. GESTION DE LA CARTOGRAPHIE.....	38
5.4.1.4. GESTION DES ALARMES.....	39
5.4.1.5. GESTION DU SYSTÈME VIDÉO ET SCENARIOS.....	39
5.4.2. PRINCIPE DE GESTION DES RÉACTIONS À ÉVÉNEMENT.....	40
6. EXIGENCES SÉCURITAIRES.....	41
7. DÉMONTAGE.....	45
7.1. DÉPOSE.....	45
7.2. STOCKAGE.....	45
7.3. RECYCLAGE.....	45
8. DOCUMENTATION.....	46
8.1. DOCUMENTATION TECHNIQUE.....	46
8.2. DOCUMENTATION D'ADMINISTRATION ET D'EXPLOITATION.....	46
8.3. SAUVEGARDE - RESTAURATION.....	46
9. FORMATIONS.....	47

9.1. FORMATION DES ADMINISTRATEURS.....	47
9.2. FORMATION DES GESTIONNAIRES DE BADGES.....	47
9.3. FORMATION DES OPÉRATEURS.....	47
10. RECETTE.....	48
10.1. RECETTE DE L'INFRASTRUCTURE RÉSEAU.....	48
10.1.1. LE CONTRÔLE VISUEL.....	48
10.1.2. LE CONTRÔLE FONCTIONNEL.....	48
10.1.2.1. TESTS DES LIAISONS CUIVRE.....	49
10.1.2.2. TESTS DES LIAISONS OPTIQUES.....	49
10.2. RECETTE DU COURANT FORT.....	50
10.2.1. LE CONTRÔLE VISUEL.....	50
10.2.2. LE CONTRÔLE FONCTIONNEL.....	50
10.3. RECETTE DES DIFFÉRENTS SYSTÈMES.....	50
10.3.1. LE CONTRÔLE QUANTITATIF ET QUALITATIF.....	50
10.3.2. LE CONTRÔLE FONCTIONNEL.....	51
10.4. PROCÈS VERBAL DE RECETTE.....	51
10.5. LES FICHES DE RECETTE.....	51
10.6. VABF.....	51
10.7. VSR.....	52
10.8. RÉCEPTION DÉFINITIVE.....	52
11. GARANTIE.....	53
11.1. MODALITÉS.....	53
11.2. INTERVENTIONS PENDANT LA PÉRIODE DE GARANTIE.....	53
11.2.1. DÉFINITION DE LA GRAVITÉ DE L'INCIDENT.....	53
11.2.2. GARANTIES DE TEMPS DE RÉTABLISSEMENT (GTR).....	53
11.3. MISES À JOUR.....	54
11.4. INTERVENTIONS APRÈS LA PÉRIODE DE GARANTIE.....	54
12. ANNEXES.....	54
13. ANNEXE 1 : PRINCIPES CÂBLAGE ÉQUIPEMENTS RACCORDEMENT.....	54
14. ANNEXE 2 : CONTRÔLE D'ACCÈS.....	54
15. ANNEXE 3 : NORMES ET RÉGLEMENTATIONS.....	55
16. ANNEXE 4 : DÉTECTION INTRUSION.....	55
17. ANNEXE 5 : PRINCIPE D'EXPLOITATION.....	55
18. PLANS.....	55
19. SYNOPTIQUES DU PROJET.....	55
20. CADRE DE RÉPONSE TECHNIQUE.....	55
21. DÉCOMPOSITION DU PRIX GLOBAL ET FORFAITAIRE.....	56

1. DESCRIPTION GÉNÉRALE DU PROJET

1.1. OBJET DE LA CONSULTATION

Le présent document décrit les prestations à exécuter, fixe les règles d'ingénierie et les spécifications techniques à respecter ainsi que les composants à mettre en œuvre, pour la mise en sûreté de :

La PRÉFECTURE de TULLE

ATTENTION !

Les annexes ci-après et celles fournies en pièces jointes font partie intégrante de ce CCTP.

À ce titre, leurs prescriptions sont à appliquer, en fonction du périmètre de la prestation demandée, aussi bien **pour l'établissement de la proposition financière et technique,**
que lors de la réalisation des travaux.

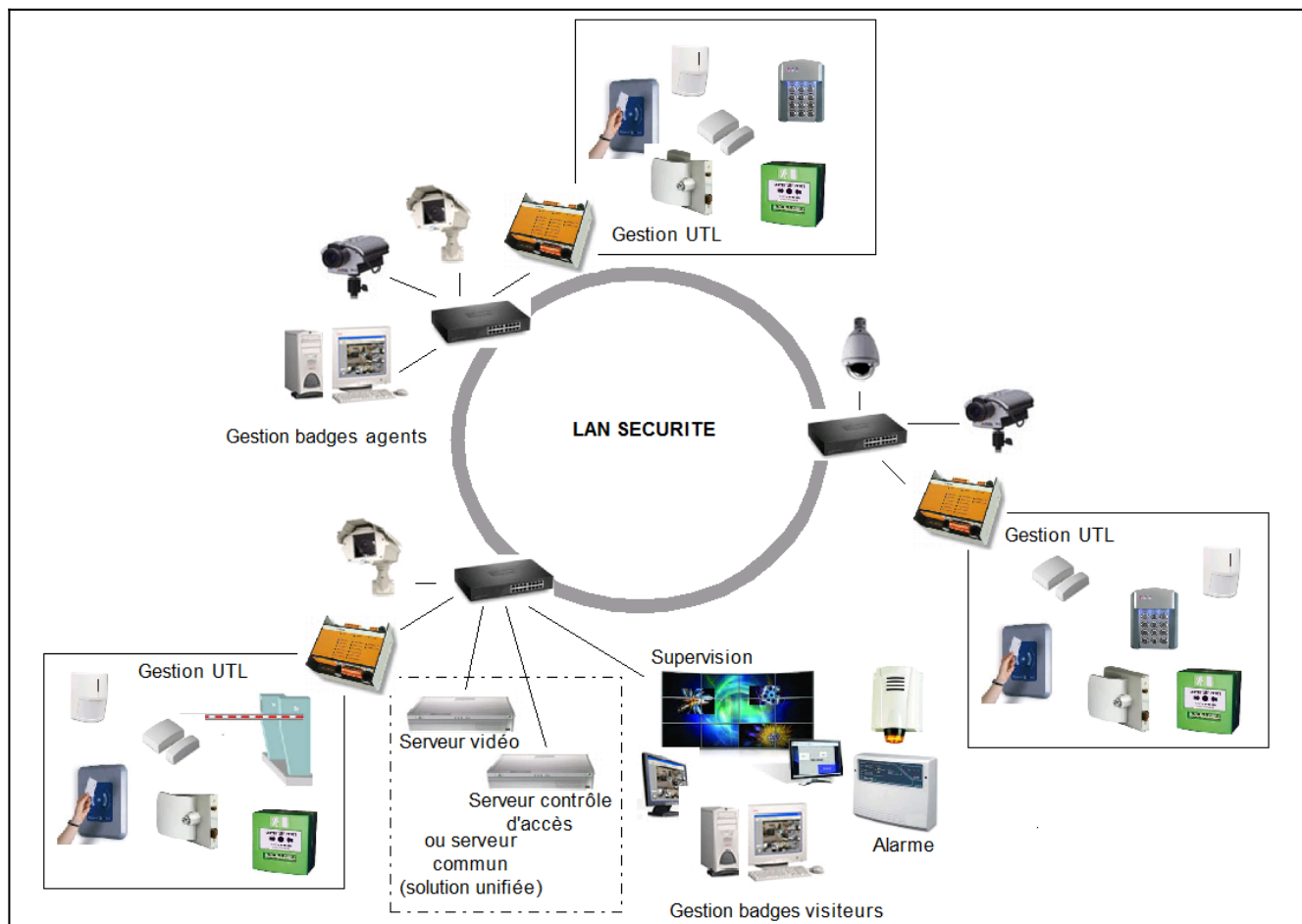
1.2. DESCRIPTION BATIMENTAIRE

La préfecture de Tulle est la Préfecture de Corrèze est implantée dans un secteur géographique délimité par :

- au **Nord**, une partie de la rue Marcelle Tinayre et la rue Pièce Verdier ;
- à l'**Est**, la rue Souham ;
- au **Sud** la place Roosevelt ainsi que des habitations (pavillons) desservies par la rue du Fouret ;
- à l'**Ouest**, la rue du Fouret et une partie de la rue Marcelle Tinayre.



1.3. DESCRIPTION SYNTHÉTIQUE DES PRESTATIONS



Le système est prévu pour apporter une solution de sécurité unifiée et ouverte en assurant la préservation des biens et des personnes, un renforcement de la protection des biens contre tout acte de vandalisme, contre les dégradations et contre toute agression.

Toutes les liaisons entre les éléments du réseau sûreté (commutateurs, serveurs, stations, caméras) seront filaires.

Aucun lien sans-fil ne sera admis, sauf spécification explicite contraire présente dans ce CCTP.

Le réseau Ethernet Sûreté sera destiné à accueillir les applications suivantes :

- Vidéosurveillance,
- Contrôle d'accès,
- Détection d'intrusion.

Le LAN sûreté physique sera constitué d'un commutateur Ethernet qui sera le cœur de concentration. Le commutateur est de type distribution (équipé de ports SFP-1000Base-X), et « POE ».

Ce commutateur possède plusieurs ports 1000baseT pour le raccordement des périphériques critiques (serveur, station d'affichage ou autre).

Le commutateur servira de référence pour tous les raccordements de périphériques « Ethernet-IP ». Il disposera d'un nombre suffisant d'interfaces gigabits pour supporter les équipements qui y seront raccordés.

Une réserve de 10 % d'interfaces de chaque type sera prévue pour une éventuelle extension.

Les règles de sécurité définies par le Haut Fonctionnaire de Défense (HFD/RCSSI) imposent une étanchéité stricte entre les flux vidéo extérieurs et le reste du Système d'Information de Sûreté (SIS). Afin d'assurer l'homogénéité du réseau et la compatibilité avec les composants actifs en service sur le site, les commutateurs Ethernet et pare-feu utilisés dans la solution figureront au catalogue des solutions informatique du Ministère de l'Intérieur.

Cette contrainte s'explique par l'obligation de respecter sur tous les sites du Ministère de l'Intérieur des préconisations d'architectures réseau précises et strictes, et basées sur des matériels validés pour leur aptitude à répondre à ces besoins.

Le respect de ces préconisations, tant du point de vue des éléments actifs est le prérequis incontournable à l'intégration du réseau de protection au réseau local du site objet du présent marché.

Les commutateurs des séries HP 5140, HP 5520 (utilisation en niveau 2-accès) sont conformes et déployés actuellement par le Ministère de l'Intérieur.

Les commutateurs seront fournis par l'administration, configurés et installés en collaboration avec les techniciens du ministère de l'Intérieur.

1.3.1. PROGRAMMATION DES COMMUTATEURS

Le soumissionnaire devra fournir à l'issue de l'installation :

- Le plan d'adressage IP
- Les protocoles mis en œuvre
- Les ports (origine et destination)
- Les fichiers TXT de chaque commutateur sous format électronique (*.Txt)
- Les remarques éventuelles

Le LAN sûreté sera constitué d'autant de réseaux virtuels (VLANs) qu'il y aura de types de matériels installés. Les commutateurs Ethernet seront configurés par les techniciens du ministère en fonction de ces éléments.

Dans ce CCTP seul le contrôle d'accès est abordé mais dans les prochains exercices budgétaires l'anti-intrusion, vidéosurveillance seront renouvelés. En conséquence les VLANs de ses métiers sont demandés dès la création de la bulle sûreté.

Pour le contrôle d'accès et l'intrusion, les VLANs suivants seront créés :

- pour l'administration de contrôle d'accès,
- pour le serveur de contrôle d'accès,
- pour les UTL,
- pour les autres équipements éventuels.
- pour les alarmes

Pour la vidéosurveillance les VLANs suivants seront créés :

- pour l'administration et la supervision vidéo,
- pour la gestion et l'enregistrement des images,
- pour les caméras intérieures,
- pour les caméras extérieures,
- pour la visiophonie.

Le commutateur n'assurera en aucun cas le routage inter Vlan.

1.3.2. EN CAS DE PRÉSENCE DE PARE-FEUX

La fonction de routage inter Vlan sera exclusivement assurée par un pare-feu de niveau 3 qui aura la double fonction de filtrage et de routage des Vlan.

Les pare-feux du réseau Ethernet Sûreté devront être conformes aux préconisations du Ministère de l'Intérieur.

Les pare-feux des séries FORTINET Fortigate 60D/100D/200D/300D sont conformes et déployés actuellement par le Ministère de l'Intérieur.

Le pare-feu sera fourni par l'administration, configuré et installé en collaboration entre les techniciens du ministère de l'Intérieur et ceux du soumissionnaire.

Le soumissionnaire fournira les informations nécessaires à l'établissement d'une matrice de flux. Cette base servira à l'administration qui se chargera de la configuration des pare-feux.

Ces informations comprendront notamment :

- Les adresses IP source et destination,
- Les flux source et destination,
- Les ports origine et destination,
- Les protocoles,
- Les débits,
- Les fréquences (flux permanent ou ponctuel),
- Les remarques éventuelles,
- Tout paramétrage autorisé pour assurer le fonctionnement sécurisé de la solution.

Le soumissionnaire présentera ces renseignements dans le tableau joint en annexe dont l'administration lui communiquera une version électronique.

Compte tenu du délai de deux mois nécessaire à l'administration au traitement de ces informations pour leur mise en forme et à l'intégration dans une base de données nationale, la mise en réseau de la solution de sûreté bâtiminaire, objet du présent CCTP, ne pourra pas intervenir avant l'issue de ces deux mois. Le soumissionnaire tiendra compte de ce délai et l'intégrera dans le calendrier de déploiement de la solution qu'il proposera.

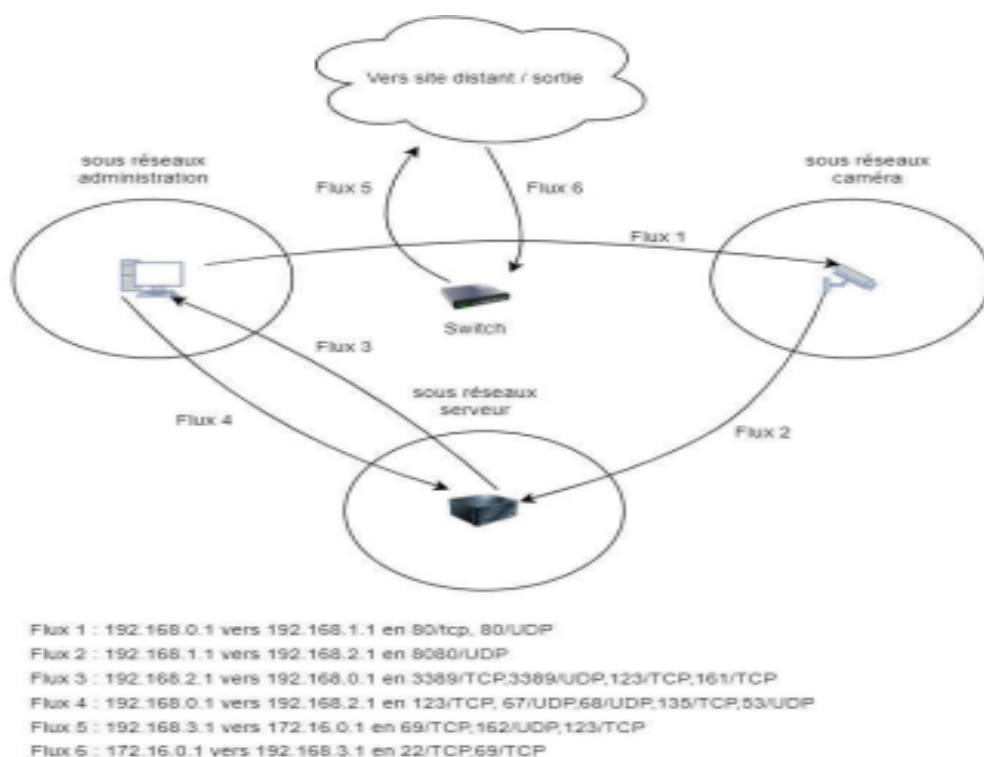
Le réseau de sûreté devra être indépendant du réseau existant du site.

1.3.3. DIAGRAMMES DE FLUX

Un Diagramme de Flux réseaux représente schématiquement l'ensemble des flux entre chaque équipement du réseau qui le compose. Il a pour but d'indiquer de façon claire et précise les protocoles, numéros de port ainsi que son mode de fonctionnement (connecté et/ou non connecté).

Le sens des flèches définit la direction du flux. Il doit également représenter le sens du trafic. Il convient également de modéliser les sous-réseaux qui le compose.

Tout ce qui n'est pas déclaré dans le diagramme ne sera pris en compte. Exemple pour une solution de vidéosurveillance:



Afin de réaliser un diagramme de flux réseaux, il faut prendre en compte tous les tenants et aboutissants de la solution. En effet, vous devez lister un par un les équipements qui devront communiquer sur le réseau après les avoir répartis par type en amont.

Vous devez vous référer aux documentations techniques des constructeurs et en extraire seulement les protocoles et ports utiles à la solution.

Vous relierez ceux-ci les équipements entre eux selon les flux nécessaires.

Exemple :

sous réseau administration

PC 192.16
8.0.1

sous réseau
caméra

caméra 192.16
8.1.1

sous réseau
serveur

serveur
switch 192.16
8.2.1

Switch-1
192.168.3.1

Protocoles numéro mode :

NTP 123 TCP

HTTP 80 TCP

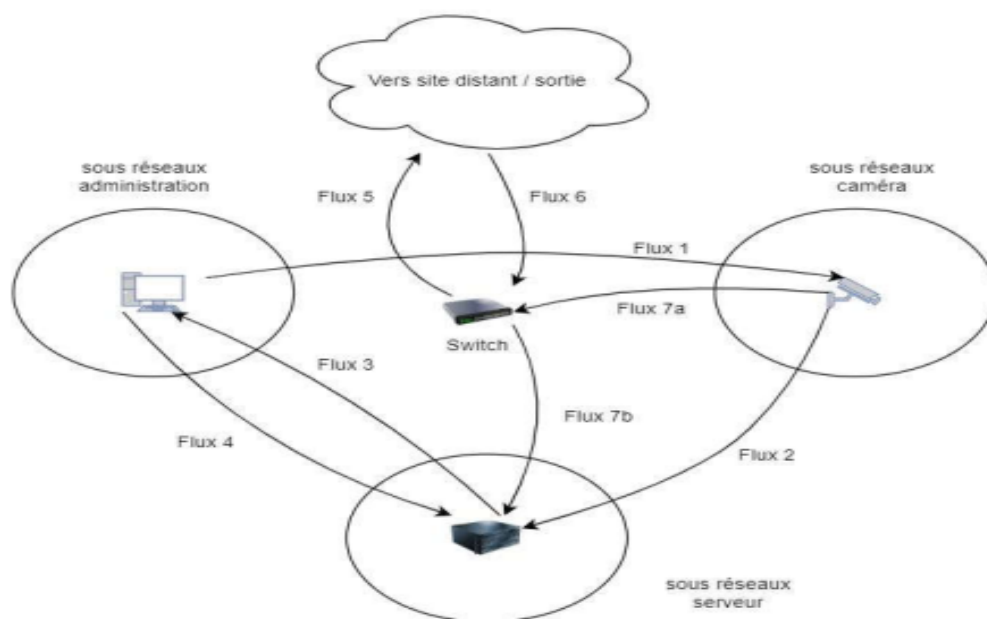
SNMP 161 UDP

RDP 3389 TCP/UDP

... ..

Les équipements de même type par constructeur pourront être représentés que par une seule icône. Un flux allant d'un équipement à un autre via un équipement de commutation sera désigné par Xa Xb.

Exemple :



Pour la formalisation littérale de ces flux, pour chacun d'eux appliquer la formule suivante :

- Flux [numéro] : [de l'adresse IP source] vers [l'adresse IP destination] en [numéro port] / [mode de connexion].

Exemple :

Flux 1 : 192.168.0.1 vers 192.168.1.1 en 80/TCP, 80/UDP

Ce qui donne une fois tous les flux référencés :

Flux 1 : 192.168.0.1 vers 192.168.1.1 en 80/tcp, 80/UDP

Flux 2 : 192.168.1.1 vers 192.168.2.1 en 8080/UDP

Flux 3 : 192.168.2.1 vers 192.168.0.1 en 3389/TCP,3389/UDP,123/TCP,161/TCP

Flux 4 : 192.168.0.1 vers 192.168.2.1 en 123/TCP, 67/UDP,68/UDP,135/TCP,53/UDP

Flux 5 : 192.168.3.1 vers 172.16.0.1 en 69/TCP,162/UDP,123/TCP

Flux 6 : 172.16.0.1 vers 192.168.3.1 en 22/TCP,69/TCP

Flux 7a,7b : 192.168.1.1 vers 192.168.2.1 en 1812/TCP,1813/TCP

Le soumissionnaire effectuera le même traitement pour les métiers du contrôle d'accès et de l'anti-intrusion. Il transmettra l'étude globale au chef de projet du SGAMI.

1.3.4. PRINCIPE RETENU

L 'objet de ce CCTP porte sur :

- La fourniture, installation, raccordement et mise en service d'un nouveau système de détection d'intrusion (câblage courants forts et faibles, éléments matériels actifs, passifs et logiciels).
- La dépose, stockage et/ou enlèvement du matériel obsolète.
- La fourniture de la documentation détaillée.
- La formation des personnels chargés de la gestion et l'exploitation du système mis en œuvre.
- La garantie sur le matériel et les logiciels comprenant la maintenance préventive, corrective, évolutive et adaptative (architecture technique, logiciels) livrés.

La prestation devra respecter les mesures de sécurité (cf.§6 p42) et la réglementation en vigueur.

Les plans et documents nécessaires à l'élaboration du projet seront remis par l'administration ou son représentant lors de la visite de site.

Les fonds de plans au format « dwg ou pdf » seront remis au titulaire du marché pour mise à jour et confection du DOE à fournir dans le cadre de la recette (cf. §10 p49). La version logicielle sera à définir pour une lecture aisée des documents.

Le soumissionnaire devra fournir, dans le dossier technique présenté dans son offre, toute certification ou agrément délivré par les constructeurs des matériels ou logiciels constituant son offre technique.

Qualifications requises ou équivalentes (à préciser):

- APSAD R81, R82, D83, ou équivalent;
- Preuve de partenariat avec éditeur / constructeur sûreté disposant certification / qualification suivant dernier référentiel ANSSI à jour;
- ISO 27001 ou équivalent;

Autres:

- Justification des références sur des projets de mise en sûretés similaires pour opérateurs étatiques (3 dernières années) avec certificats de capacité;
- Justification d'une preuve d'une représentation locale;
- Justification d'un centre d'intégration qui lui est propre pour un maquettage à l'échelle 1;
- Justification de l'existence d'un centre de veille des vulnérabilités (CERT : Computer Emergency Response Team).

1.3.5. PRESTATION ATTENDUE

Le système de détection intrusion existant de la préfecture étant obsolète. Il se doit d'être remplacé par une solution fiable et évolutive. Cette solution s'inscrivant dans une refonte du système globale de sûreté – à savoir la vidéosurveillance, le Contrôle d'Accès et la détection intrusion – du site. Dans cette thématique une solution unifiée, commune entre le contrôle d'accès et la détection d'intrusion trouve sa pertinence des points de vue budgétaire et technique. C'est une des directions technologiques d'évolution des solutions de contrôle d'accès qui embarquent le métier de la détection intrusion.

Cette solution est l'objet de ce présent Cahier des Clauses Techniques Particulières.

Cette prestation consiste à la mise en place d'un serveur, des licences nécessaires, d'Unités de Traitement Local autant que de besoin, afin d'assurer le remplacement du système de détection intrusion existant.

L'introduction de cette solution permettra d'optimiser les dépenses budgétaires et de poursuivre l'architecture IT de sûreté cible grâce au déploiement de ce serveur.

Cette machine sera :

- d'une part, le serveur principal mutualisé des 3 métiers de la sûreté du site
- Et d'autre part, le serveur de gestion centralisée départementale, du futur contrôle d'accès et de la détection intrusion. Il prendra en charge la gestion des sites l'Administration Territoriale de l'État distants tels que les sous-préfectures.

L'ensemble de cette refonte du système de détection intrusion a pour but d'apporter une nouvelle protection des ouvrants, les lieux de travail, et certains locaux sensibles.

Les prestations attendues dans le cadre de ce projet sont :

- Se raccorder au réseau local indépendant du réseau bureautique dénommé « réseau sûreté (en DMZ) » ou encore « bulle sûreté »
- Mettre en place à la préfecture un serveur ondulé hébergeant en machine virtuelle le logiciel Gestion d'Accès Contrôlés (commun à l'intrusion et au C.A. PCPass Evolution ou équivalent). Sur cette machine sera implémenté à l'avenir en machines virtuelles un VMS pour la vidéosurveillance, l'enregistrement, et les rôles serveurs associés à la cybersécurité tel que le Radius (AD,LDAP,NPS).
- Mettre en place à la préfecture une station d'exploitation.
- Déposer les centraux et claviers du système de détection intrusion existants pour les remplacer par de nouveaux équipements.
- Remplacer, voir de compléter, les détecteurs intrusion de présence, contacts magnétiques/chocs existants (intérieur).
- Prévoir la reprise, l'ajout, et le remplacement des alimentations secourues.
- Proposer une offre de contrat de maintenance associé à ce projet afin d'assurer les Maintiens en Condition Opérationnelle et de Sécurité (MCO, MCS) de la solution de sûreté objet du présent CCTP à la préfecture .

L'objet du présent CCTP concerne :

a) pour l'intrusion :

Le soumissionnaire prévoira la fourniture d'une ou plusieurs UTL qu'il installera dans le local technique désigné par l'administration. Il abondera aussi les modules UTR.

L'ensemble est nécessaire au bon fonctionnement du système de détection intrusion.

Les alarmes seront à renvoyer vers un poste de supervision à fournir dans le cadre de la prestation. Il prévoira également un renvoi d'alarmes par contacts secs via le boîtier RAMSES, (fourni par l'administration).

Le soumissionnaire renverra toutes les alarmes générées par les détecteurs anti-intrusion :

- détecteurs d'ouverture
- détecteurs de chocs
- détecteurs volumétriques
- autoprotection
- agression

Pour résumer :

☐ Le titulaire prévoira la fourniture et l'installation, autant que de besoin, soit en nombre suffisant à définir par le titulaire des modules et des unités de traitement local. Les modules de détections (UTR) pourront être déportés.

☐ Le titulaire prévoira la fourniture et l'installation, le remplacement, autant que de besoin tel que défini par la maîtrise d'ouvrage, de détecteurs intrusions afin de détecter une intrusion des lieux indiqués par l'administration.

☐ Le titulaire prévoira la fourniture et l'installation, le remplacement, des claviers de commande.

Le système doit-être évolutif et éprouvé.

A noter:

- Que le système existant est totalement obsolète et à remplacer.
- Le soumissionnaire fournira obligatoirement un synoptique de fonctionnement détaillé de l'installation qu'il propose. Il développera un descriptif expliquant le fonctionnement de la solution.
- Le soumissionnaire expliquera la méthodologie d'intégration de la solution qu'il propose, avec une description particulière de l'analyse fonctionnelle qu'il mettra en œuvre, accompagnée d'un calendrier prévisionnel de déploiement. La fourniture de ce document est obligatoire et son absence dans l'offre du soumissionnaire est éliminatoire.

b) pour le contrôle d'accès :

Le renouvellement du C.A. n'est pas l'objet du présent CCTP, celui-ci sera traité dans un exercice budgétaire différent. Le C.A. prenant en charge la gestion de la détection intrusion, il devra

répondre aux préconisations suivantes.

La base de données du système de contrôle d'accès est de type SGDBR (Système de Gestion de Base de Données Relationnelle). Les bases de données dites « propriétaires » seront proscrites. Le soumissionnaire indiquera dans son offre son choix de base de données (éditeur, type de licence, etc.)

La solution de contrôle d'accès déployée doit permettre la mise en place de bus terrain sécurisé homologué ANSSI.

☐ La fourniture et l'installation des UTLs qui seront installées, autant que possible, à l'intérieur de la baie informatique de la solution de sûreté.

La solution devra pouvoir gérer la technologie DESFIRE EV1/EV2 et EV3 compatible carte agent architecturée autour de la puce JCOP 4.5 de la nouvelle carte agent et compatible avec l'ancienne puce OBHERTUR de l'ancienne carte.

Le système doit-être évolutif et éprouvé.

c) pour la vidéo protection :

☐ Prévoir la possibilité d'hébergement d'une future VM de Vidéosurveillance sur le serveur à fournir.

e) pour le réseau, baie et câblage:

☐ Le soumissionnaire prévoira dans son offre la fourniture, l'installation et le câblage d'une baie à la **préfecture** de format **42U en 800x1000**. Elle sera sécurisée à minima en fermant à clé et totalement close (les joues latérales et la paroi arrière de la baie seront présentes). Elle sera fournie avec l'ensemble des accessoires nécessaires (passe câbles, plateaux, rails ...) et son câblage est à la charge du soumissionnaire.

Le commutateur et le serveur seront installés dans la baie de sûreté à fournir, suffisamment dimensionnée afin d'accueillir la totalité des équipements de la solution.

☐ Elle sera secourue individuellement par un onduleur à fournir et à installer (secours du switch de sûreté et du serveur pour une durée de 30 minutes). Cette prestation est à prendre en compte par le soumissionnaire.

☐ Cet onduleur doit être muni d'une carte réseau SNMP afin de communiquer avec le serveur pour lui ordonner son extinction propre.

☐ Quant au câblage de la solution de détection intrusion existant, il sera intégralement à remplacer.

Si de nouveaux détecteurs sont demandés, la fourniture et le câblage de ceux-ci sera également à prévoir dans votre réponse financière et technique.

Tous les câblages, fibre optique ou Ethernet, en extérieur (façade) comme en intérieur dans les passages accessibles au public, seront protégés par des goulottes métalliques type oméga.

Pour information dans un exercice budgétaire différent, un serveur de redondance assurera la résilience de la solution. Une rocade fibre dédiée, sera à mettre en place en liaison directe entre les 2 serveurs afin de pouvoir assurer la haute-disponibilité de la redondance.

f) pour les serveurs et les postes d'exploitations :

Le titulaire fournira l'ensemble des serveurs et licences nécessaires au fonctionnement de la solution.

- ☐ Un serveur est à prévoir dans le cadre du présent CCTP avec les licences nécessaires en Machines Virtuelles (VM) comme PCPass Evolution ou équivalent.
- ☐ Ce serveur devra être équipé d'une carte réseau compatible pour permettre de réaliser, à l'avenir, la redondance en haute disponibilité (Carte avec 1 port SFP et son module Gbic).
- ☐ Un poste d'exploitation sera à mettre en œuvre dans le bureau du futur PCS. R+3 du Bâtiment 2. À noter : le client final prévoira la condamnation des portes latérales de ce bureau.

Chaque élément de la solution doivent pouvoir évoluer indépendamment des autres sur le seul critère du respect des prérequis techniques qui doivent, pour les matériels, exclure toute spécification de constructeur, explicite ou implicite.

Le titulaire fournira l'ensemble serveur et licences nécessaires au fonctionnement de la solution. Chaque élément de la solution doivent pouvoir évoluer indépendamment des autres sur le seul critère du respect des prérequis techniques qui doivent, pour les matériels, exclure toute spécification de constructeur, explicite ou implicite.

Le titulaire fournira :

- les prérequis des équipements constitutifs de la solution garantissant le bon fonctionnement de la solution.
- une documentation d'installation détaillée de la solution ainsi que tous les paramètres de configuration et mots de passe.

Tout accès via internet et autres réseaux externes est formellement interdit, de même que les alertes par SMS.

Pour rappel, les commutateurs seront fournis, configurés et installés par le Ministère de l'Intérieur.

g) Cybersécurité (obligatoire selon ANSSI et CCN) :

Prévoir la possibilité d'hébergement d'une future VM RADIUS sur le serveur à fournir. L'architecture de protection en cybersécurité sera constituée de 4 briques :

Brique de sécurité N°1 :

Les flux vidéo entre les caméras et les serveurs seront chiffrés par activation du protocole SRTP (Secure Real Time Protocol) conformément à la recommandation RFC 3711.

Les équipements déployés dans la solution devront être compatibles avec ce protocole.

Brique de sécurité N°2 :

Les flux d'administration entre les serveurs et les autres équipements raccordés sur le réseau de sûreté bâtiminaire (serveurs et périphériques tels que caméras..) seront chiffrés par activation du protocole HTTPS (HyperText Transfer Protocol Secure) conformément à la recommandation RFC 2818. HTTPS sera déployé sans certificat auto-signés. Les certificats auto-signés, sans autorité tierce, sont proscrits.

Brique de sécurité N°3 :

Contrôle d'Accès : Chaîne de sécurité sans faille du badge jusqu'au serveur de gestion de la solution de CA.

L'ensemble des matériels (UTL, modules d'extension, lecteurs,..) et logiciels proposés devront être conformes aux recommandations du guide de l'ANSSI : « SECURITE DES TECHNOLOGIES SANS CONTACT POUR LE CONTROLE DES ACCES PHYSIQUES » (Version du 19/11/2012) selon l'architecture 1 de façon native sans convertisseur.

La solution devra être sécurisée de bout en bout, du badge jusqu'au serveur.

Les principes et fonctionnalités suivants devront être disponibles et réalisés par les équipements et logiciels fournis : Conforme ANSSI architecture 1,

La solution devra être compatible avec le réseau VLAN, VPN du site,

La solution devra être compatible avec l'annuaire LDAP du site pour la gestion des opérateurs et de leurs droits, Communications réseau IP cryptées TLS AES 256 bits et signées (intégrité et authentification) entre le serveur et les UTL d'une part et les postes clients d'autre part,

Communications bus RS485 cryptées AES 128 bits et signées,

Toutes les clés de communications sur IP et RS485 devront être changées périodiquement de manière automatique par le système sans action humaine pour durcir le cryptage contre toute malveillance,

Le client final aura obligatoirement la maîtrise de sa clé de communication initiale, qui créera automatiquement les clés suivantes périodiquement, par la saisie, sur un poste client lourd, de cette clé (cérémonie des clés),

Protection des attaques par déni de service (DoS) par le Firewall des automates UTL,

Paramétrage de la configuration IP des UTL à travers un Web serveur embarqué sécurisé HTTPS, SSH, UTL compatible avec serveur radius 802.1X.

Le module de porte communiquera en bus RS485 crypté AES128 bits avec les lecteurs et protocole SSCP V2 sera activé pour le chiffrement des flux de données entre les lecteurs de badge contrôlant les portes, et les unités de traitement de porte de la solution de contrôle d'accès.

Brique de sécurité N°4 :

Un serveur d'authentification RADIUS, local ou zonal selon les directives de l'administration, sera pré-installé par activation du protocole 802.1 X (avec certification EAP-TLS) sur le réseau de sûreté bâtiminaire afin garantir la sécurité des ports des commutateurs réseaux et autres équipements raccordés sur ce réseau.

Les ports non utilisés des commutateurs réseaux et autres équipements raccordés seront neutralisés logiquement par programmation et physiquement par des bouchons, même dans les baies de sûreté bâtiminaire. Cette préparation permettra d'intégrer le service Radius sans avoir à reconfigurer l'ensemble du système lors de l'accueil de la vidéosurveillance.

Le serveur d'authentification Radius sera dans un autre exercice, implémenté en machine virtuelle sur le serveur physique principal de la solution de sûreté, et en cas de présence d'un

serveur physique de secours, il sera aussi implémenté en machine virtuelle sur ce serveur redondant.

Il ne sera en aucun cas installé sur un serveur physique indépendante et isolé sur le réseau.

Le protocole FTP (File Transfert Protocol) sera désactivé et les guides de durcissement des constructeurs des équipements déployés seront appliqués.

Les certificats auto-signés, sans autorité tierce, sont proscrits. Ils seront générés par un service d'authentification tierce géré par un Active Directory à proposer à la solution de sûreté. Cet AD sera à déployer, dans la VM du Radius, par le soumissionnaire lors du renouvellement de la solution de vidéosurveillance dans une phase ultérieure.

Si l'activation de la cybersécurité n'est pas retenue pour la solution de sûreté traitée, les briques de cybersécurité seront préinstallées sur les serveurs. Ceci afin de pouvoir les activer ultérieurement, en évitant toute réinstallation complète des serveurs.

Le réseau déployé sera conforme au Cahier des Clauses Techniques Simplifiées de Cybersécurité pour les marchés publics (arrêté du 18/09/2018), au Règlement Général de Sécurité de l'ANSSI.

- Le soumissionnaire fournira obligatoirement un synoptique de fonctionnement détaillé de l'installation qu'il propose. Il développera un descriptif expliquant le fonctionnement de la solution.
- Le soumissionnaire expliquera la méthodologie d'intégration de la solution qu'il propose, avec une description particulière de l'analyse fonctionnelle qu'il mettra en œuvre, accompagnée d'un calendrier prévisionnel de déploiement. La fourniture de ce document est obligatoire et son absence dans l'offre du soumissionnaire est éliminatoire.

1.3.6. PROPOSITION DE PLAN D'UNE ANALYSE FONCTIONNELLE D'UNE SOLUTION DE SÛRETÉ BÂTIMENTAIRE

I CADRE RÉGLEMENTAIRE ET RECOMMANDATIONS

Livrables de la configuration atelier intégrateur

II SYNTHÈSE DU PÉRIMÈTRE PROJET

III SYSTÈME D'INFORMATION

A INFRASTRUCTURE INFORMATIQUE

- A1 SERVEURS PHYSIQUES**
- A2 RÔLE MICROSOFT WINDOWS SERVEUR**
- A3 FONCTIONNALITÉ MICROSOFT WINDOWS**
- A4 BASE DE DONNÉES – SQL EXPRESS**
- A5 SYNCHRONISATION HORAIRE**
- A6 AGRÉGATION DES LOGS – GRAYLOG**
- A7 POSTE CLIENT**

B INFRASTRUCTURE RÉSEAU

- B1 ARCHITECTURE LOGIQUE**
- B2 ROUTAGE**
- B3 CONFIGURATION PORT D'ACCÈS**

- B4** **CONTRÔLE D'ACCÈS RÉSEAU**
- B5** **GESTION DES BOUCLES RÉSEAU - SPANNING TREE**
- B6** **LIEN VERS L'EXTÉRIEUR**
- C** **HAUTE DISPONIBILITÉ / TOLÉRANCE AUX PANNES**
 - C1** **ENREGISTREMENT DES FLUX VIDÉO**
 - C2** **RÉPLICATION SYNCHRONE DE MACHINES HYPER-V / BASCULEMENT**
 - C3** **HAUTE DISPONIBILITÉ DES SERVICES ACTIVE DIRECTORY DU DOMAINE SURETE.LOCAL**
 - C5** **INTERRUPTION DE SERVICE**
 - C6** **FONCTIONS SPLIT BRAIN ET VM CHECKER DU LOGICIEL DE BASCULEMENT**

D **LOGICIEL VIDÉO**

- D1** **PRÉAMBULE**
- D2** **LOCALISATION ET DISTRIBUTION DES SERVICES DU VMS**
- D3** **FONCTIONNALITÉS DÉPLOYÉES / CONFIGURÉES**
 - D3.1** **COMMUNICATION SÉCURISÉE CLIENT / SERVEUR**
 - D3.2** **CHIFFREMENTS ET SIGNATURE DES ENREGISTREMENTS**
 - D3.3** **COMMUNICATIONS SÉCURISÉES CAMÉRA / SERVEUR**
- D4** **ORGANISATION DES GROUPE DANS LE VMS**
 - D4.1** **GROUPE DE CAMÉRA**
 - D4.2** **GROUPE DE MICROPHONE**
 - D4.3** **GROUPE DE HAUT-PARLEURS**
 - D4.4** **GROUPE DE MÉTADONNÉES**
 - D4.5** **GROUPE DES ENTRÉES**
 - D4.6** **GROUPE DES SORTIES**
- D5** **GROUPE DE VUES**
- D6** **LES VUES**
 - D6.1** **VIDÉO**
 - D6.2** **MATRICE (ÉCRAN D'ALARME)**
- D7** **LES ALARMES DE DÉTECTION D'INTRUSION (PÉRIMÉTRIE)**
 - D7.1** **NOTIFICATION**
 - D7.2** **SECTEURS ET CAMÉRAS ASSOCIÉS**
 - D7.3** **ACQUITTEMENTS DE L'ALARME**
- D8** **LES RÔLES ET UTILISATEURS**
- D9** **LES RÈGLES**
- D10** **MONITORING DU SYSTÈME VIDÉO**
 - D10.1** **SERVEUR**
 - D10.2** **CAMÉRAS**
 - D10.3** **DISQUES**
 - D10.4** **STOCKAGES**
- D11** **PRÉPOSITION DES DÔMES PTZ**

E LOGICIEL D'ANALYSE D'IMAGE –

E1 ANALYSE TYPE INTRUSION

E1.1 SCÉNARII D'INTRUSION

E1.2 ZONES D'INTRUSION

F CENTRALE INTRUSION

F1 SECTEURS

F1.1 BÂTIMENT A...

F1.2 JUSQU'À BÂTIMENT N..

F1.3 PÉRIMÉTRIES

F2 ZONES

F3 UTILISATEURS ET DROITS

F3.1 GROUPES

F3.2 UTILISATEURS

F4 MISE EN ET HORS SERVICE

F4.1 MES / MHS :

F4.2 DÉROGATIONS

F4.3 POINT D'ENTRÉE / POINT DE SORTIE

F5 CONNEXION ETHERNET

F6 TÉLÉSURVEILLANCE

F7 LIEN AVEC LE VMS

A l'issue de l'analyse fonctionnelle, le soumissionnaire écrira et programmera les scénarios d'asservissement des caméras aux ouvrants contrôlés par le contrôle d'accès dans la limite de deux scénarios en moyenne par ouvrants.

1.3.7. EXEMPLES DE SCÉNARIOS D'ASSERVISSEMENTS :

1er exemple :

Création de drapeaux, ou pointeurs, ou icônes dans la time line digitale de la solution globale au niveau de l'hyperviseur (affichage écran.)

Ces drapeaux signalent un événement avec un code couleur pour savoir si celui – ci a été acquitté par l'opérateur.

Exemple de time line classique : le curseur d'enregistrement avec multiflèches d'un magnétoscope

Dans cet exemple : un drapeau = un événement

2ème exemple :

Association de séquence vidéos courte de levée de doute sur pré-alarme ou poste-alarme sur événement en temps réel.

Une séquence vidéo d'une trentaine de secondes (max mais possibilité moins) est associée via une icône dans le fil de l'eau des alarmes au niveau de l'hyperviseur.

L'opérateur quitte son poste pour une raison quelconque. Pendant son absence, un événement se produit générant une alarme qui s'affiche dans le fil de l'eau.

A son retour, il appuie sur l'icône apparaissant sur la ligne de l'alarme, ce qui a pour effet de lancer un pop-up affichant la séquence vidéo, pendant 30 s, de la caméra associée afin de lever le doute.

La séquence affichée peut-être pré ou poste alarme.

Ne peut-être utilisée que sur un poste de gestion ou un agent est présent 24 h/24 ou 7 j/7 ou bien encore hors heures ouvrables (cad avec présence durable de l'opérateur).

3ème exemple :

Scénarios de réposition de dôme PTZ de levée de doute, en cas de présence de ce type d'équipement dans la solution (scénarios génériques).

Ces scénarios trouvent leurs origines dans l'expression de besoins des opérateurs ou des utilisateurs de la solution. Il faut donc qu'ils se la soient appropriés au travers de la présentation qui leur en sera faite grâce à l'analyse fonctionnelle.

En résumé, l'intégrateur doit expliciter dans l'analyse fonctionnelle clairement en langage simple les différentes actions programmées dans chaque scénario (qui peuvent être génériques) souhaitées par les utilisateurs de la solution.

2. DESCRIPTION DE L'EXISTANT

2.1. ARCHITECTURE EXISTANTE ET SYSTÈME INSTALLE

Le système de détection Intrusion

La solution de détection intrusion obsolète de la préfecture est du constructeur ELKRON, version CENTRALE MC05 PN/5.

Une soixantaine de détecteurs y sont raccordés et répartis :

- sur 13 boîtiers (ou centrales) extension raccordé à 1 centrale.
- 22 détecteurs volumétriques
- 27 détecteurs d'ouvertures (17 simples, 5 doubles)
- 5 détecteurs de chocs
- 2 boutons agressions (standard + accueil)
- 1 pédale d'alarme
- 17 claviers de commande mise en/mise hors. (16 claviers de zone, 1 clavier opérateur)
- 10 boîtiers à clé.

La nouvelle solution technologique unifiée devra être évolutive et homologuée ANSSI.

LOCAUX TECHNIQUES				
Site	Bâtiment	Étage	Répartiteur	Descriptif
Préfecture	Bat 2	R+3	RG	Local Autocom / Serveur / Centrale Intrusion

EMPLACEMENTS DES ALIMENTATIONS				
Site	Bâtiment	Étage	Emplacement	Commentaire

Préfecture	-		Standard	
	Bat 2	R+3	Salle opé Bat 2 R+3	
	Bat 2	R+2	Salle 202 Bat 2 R+2	Contrôler la Hauteur
	Bat 2	RDC	WC Bat 2 RDC	
	-		Entrée Cabinet	Contrôler la Hauteur
	Bat 1	R+1	Placard Bat 1 R+1	
	Bat 1	R+1	Placard Bat 1 R+1	
	Bat 3	RDC	WC Bat 3 RDC	Contrôler la Hauteur
	Bat 3	RDC	Bat 3 RDC vers Bat 2 RDC	Contrôler la Hauteur

Câblage capillaire

Nombre de prises non conformes indéfini

Catégorie de câblage 6 ou +

Année de mise à niveau indéfinie

RÉSEAUX SÛRETÉ

Toutes les données liées à la sûreté, de chaque entité, sont véhiculées par un réseau local dénommé « réseau sûreté », inter-sites si besoin et physiquement séparé des réseaux bureautiques existants.

2.2. ÉNERGIE

Le local technique est alimenté par le réseau ondulé 230 V lui-même raccordé sur le groupe électrogène du site de la préfecture.

3. DESCRIPTION DES PRESTATIONS À RÉALISER

3.1. INFRASTRUCTURE RÉSEAU

Il sera réalisé conformément aux caractéristiques et aux principes décrits dans l'annexe du présent CCTP dénommée :

ANNEXE 1 : CCTP SÛRETÉ SGAMI DSIC_PRINCIPES CÂBLAGE ÉQUIPEMENTS RACCORDEMENT

Toutes les liaisons entre les éléments du réseau sûreté (lecteurs de badges, UTL, commutateurs, serveurs, stations, caméras) seront filaires. Aucun lien sans-fil ne sera admis, sauf spécification explicite contraire présente dans ce CCTP.

3.1.1. LES RÉPARTITEURS

LOCAUX TECHNIQUES				
Site	Bâtiment	Étage	Répartiteur	Descriptif

Préfecture	Bat 2	R+3	RG	Local Autocom / Serveur / Centrale Intrusion
------------	-------	-----	----	--

Le local technique est alimenté par le réseau ondulé 230V lui-même raccordé sur le groupe électrogène du site.

3.1.2. LES SERVEURS DE LA PRÉFECTURE

3.1.2.1. SERVEUR PRINCIPAL

Un serveur hôte hébergera en machines virtuelles les rôles de la solution de sûreté suivants :

- Gestion du contrôle d'accès et de Gestion Intrusion. Il sera capable de supporter dans un avenir proche :
 - Gestion de la vidéo et Enregistrement des flux vidéos
 - Cybersécurité
 - Supervision gérant l'ensemble des métiers précédents
 - Les serveurs associés aux rôles de la cybersécurité dont le Radius

Il est équipé d'une source d'énergie secteur secourue par groupe électrogène mais un onduleur est à prévoir.

3.1.2.2. SERVEUR DE REDONDANCE

Sans Objet.

3.1.3. LA DORSALE OPTIQUE

Sans Objet.

3.1.4. LE CAPILLAIRE CUIVRE

Il fait partie des prestations répondant aux prescriptions de l'annexe du présent CCTP dénommée :

ANNEXE 1 – CCTP SÛRETÉ SGAMI DSIC_PRINCIPES CÂBLAGE ÉQUIPEMENTS RACCORDEMENT

Tous les périphériques de type « Ethernet/IP » (serveurs, stations, caméras, etc.) proposés dans la solution seront raccordés sur le répartiteur désigné par l'administration (dans la plupart des cas, le plus proche) par un lien « Ethernet » catégorie 6^A / classe E^A ou catégorie 7 respectant les règles de l'art.

L'établissement de ces liens fait partie des prestations répondant aux prescriptions de l'annexe.

3.1.5. LES ÉLÉMENTS ACTIFS

Leur fourniture est exclue de la présente prestation.

Le Ministère de l'Intérieur a réalisé une estimation du nombre de commutateurs réseau à mettre en œuvre et les fournira, ainsi que le pare-feu nécessaire à l'établissement des liens sécurisés inter-sites.

Il fournira tous les éléments permettant la segmentation du réseau (Numéros de VLAN, adresses IP des LAN, masques de sous-réseaux, etc.) via son Bureau des Réseaux Fixes de la DSIC du SGAMI.

Pour information :

Le soumissionnaire dimensionnera précisément l'architecture du réseau de sûreté à mettre en place en se conformant au besoin décrit dans le CCTP et aux principes décrits dans l'annexe 1. Il précisera le nombre exact de commutateurs nécessaires au déploiement de cette architecture en tenant compte du nombre et de l'emplacement des locaux techniques auxquels les périphériques (des trois métiers) de la solution de sûreté sont rattachés (contrainte du câblage sur les distances de raccordement)

Les commutateurs et pare-feux sont listés ci-après :

Répart. : Répartiteur où l'équipement sera installé

P : Pare-feu

C : Commutateur

Haut. : Hauteur en nombre de U

SUR LE SITE DE LA PRÉFECTURE							
Bâtiment	Etage	Répart.	Fonction	P	C SFP	C PoE	Haut. (U)
Bat 2	R+3	RG AUTOCOM	Répartiteur Serveur Connexion des éléments sûreté (pare-feu, serveurs, commutateur, UTL)	1 Exist ant	1	1	42 à prévoir par soumis sionnai re
Bat 2	R+3	Bureau 307	Poste d'exploitation Client				
Éléments actifs à fournir par l'administration, quantités totales :					1	1	1

*1 pare-feu fortinet type 60 ou 200D

*SFP : switchs SFP HP 5520

*PoE : switchs POE HP 5140

3.1.6. LES BAIES DE SÛRETÉ

La fourniture et l'installation est à prévoir dans la présente prestation :

- 1 baie 800 × 1000 42U à installer dans le local technique pour le serveur de gestion.

La baie sûreté devra être complète avec présence des joues latérales, fond, toit, sol, et serrures. Elle devra également être équipée de ventilation, tiroir optique, bandeau RJ45 avec noyau, passage de câble, plateau, bandeau de prises...

3.1.6.1. IMPLANTATION TYPE BAIE DU RÉPARTITEUR ET/OU SOUS-REPARTITEUR

HAUT		
	U	ÉLÉMENT
2U	42	Panneau télécom (opérateur)
	41	Passe cordons télécom
	40	Panneau sûreté 24 noyaux RJ45
	39	Passe cordons
	38	Commutateur sûreté 24 ports POE
	37	Passe cordons
2U	36	Pare-feu sûreté
	35	
		Vide
		Vide
		Vide
		Vide
		Vide
2U	18	KVM
	17	
	15	Vide
	14	Vide
	13	Vide
	12	Vide
	11	Vide
	10	Vide
	9	Vide
	8	Serveur solution vidéo et contrôle d'accès
	7	
	6	Vide
	5	
	4	Onduleur sûreté
	3	
	2	Bandeau arrière 6 PC 220v+T sur onduleur
	1	Bandeau arrière 6 PC 220v+T
BAS		

3.2. CONTRÔLE D'ACCÈS

ATTENTION !

Il sera réalisé conformément aux principes décrits dans l'annexe à ce CCTP dénommé :

ANNEXE 2 – CCTP SÛRETÉ SGAMI DSIC_PRINCIPES CONTRÔLE ACCÈS

3.2.1. LES BADGES

Type de badge (CAM)

LA SOLUTION DE CONTRÔLE D'ACCÈS ET ANTI-INTRUSION DOIT ÊTRE COMPATIBLE AVEC LA CARTE AGENT DU MINISTÈRE DE L'INTÉRIEUR

La solution doit permettre la gestion de différents types de badge portés par des modèles de badge différents. On différenciera naturellement le type de badge, des droits ou profils liés à chaque badge.

Pour simplifier les choses et pour ne pas dévoiler d'informations vitales, il existe au niveau de la personnalisation des badges à minima les catégories suivantes pour les personnes :

- Badge **P** : badge nominatif pour les **permanents** toutes directions confondues ; La personnalisation graphique varie pour les badges de la classe P,
- Badge **V** : badge non nominatif, journalier, pour des **visiteurs** occasionnels externes. Les droits d'accès associés aux badges V sont définis par le bureau des badges. Ce sont des droits minimums.

La carte sans contact, de format ISO 7816 avec capacité sans contact ISO 14 443, utilisée pour l'identification aux contrôles d'accès est fondée sur la puce Mifare DesFire EV1/EV2/EV3.

Le titulaire devra la livraison de 0 badges, PVC blanc, format ISO 7816 avec capacité sans contact ISO 14 443, badge vierge, libre de droit, tel que sorti d'usine, sans modification de clés (clé maître notamment) ni de droits.

3.3. DÉTECTION D'INTRUSION

Cette solution s'inscrit dans une refonte du système globale de sûreté – à savoir la vidéosurveillance, le Contrôle d'Accès et la Détection Intrusion – du site.

La technologie de détection intrusion retenue sera une solution unifiée, commune entre le contrôle d'accès et la détection d'intrusion.

Le GAC gèrera la détection intrusion.

ATTENTION !

L'installation du système de détection intrusion sera réalisée conformément aux principes décrits dans l'annexe à ce CCTP dénommé :

ANNEXE 4 – CCTP SÛRETÉ SGAMI DSIC_PRINCIPES DÉTECTION INTRUSION

3.3.1. GÉNÉRALITÉ LE SYSTÈME D'ALARME ATTENDU

Le système devra être évolutif et permettra, à l'avenir, le raccordement de nombreux points d'alarmes complémentaires.

Le système d'alarme aura une autonomie minimum de **72 heures** en cas de coupure de l'alimentation électrique.

Par ailleurs, la centrale d'alarme devra permettre d'activer un **code alarme « sous contrainte »** et une **alarme technique** devra prévenir de la **rupture d'alimentation** électrique principale.

Les claviers à remplacer sont listés ci-après :

Cette centrale sera pourvue de claviers d'activation/désactivation et permettra de paramétrer au moins seize zones d'alarmes.

Désignation	Référence	Quantité	Répart. organe de contrôle
Claviers d'activation/désactivation		17	
Total de clavier		17	

Les détecteurs à remplacer sont listés ci-après :

Désignation	Référence	Quantité	Répart. organe de contrôle
Détecteurs de présence (volumétriques)		22	
Détecteurs d'ouvertures (17 simples, 5 doubles)		27	
Détecteurs de chocs		5	
Boutons agressions		2	
Pédale d'alarme		1	
Total de détecteurs		57	

Les boîtiers à clés à remplacer sont listés ci-après :

Désignation	Référence	Quantité	Répart. organe de contrôle
Boîtiers à clé		10	
Total de boîtiers à clé		10	

3.3.2. LES UNITÉS DE TRAITEMENT LOCAL (UTL)

Le nombre d'unités de traitement local sera déterminé proportionnellement au nombre de modules d'alarmes en respectant les règles de l'art émises par le constructeur.

Elles seront installées dans le local autocom désignés par l'administration pour bénéficier entre-autres de l'énergie secourue.

Afin de pouvoir en déterminer leur nombre, le soumissionnaire se reportera aux plans du bâtiment et sur les propositions de rattachement listées ci-dessous. À défaut, le soumissionnaire proposera une solution alternative qui devra être validée.

Un point d'accès « Ethernet » catégorie 6_A / classe E_A ou supérieur sera créé entre la ou les UTL présente-s dans le local et la baie hébergeant le commutateur « sûreté ».

Le déploiement d'UTL rackable sera privilégiée lorsque la configuration d'infrastructure réseau le permet. Cette possibilité sera à traiter lors de la visite de site.

L'autonomie attendue des alimentations en cas de perte d'énergie, sera de 30 minutes minimum (pour les coffrets UTL).

La durée réduite de maintien des batteries est conséquente à la présence d'un groupe électrogène sur le site.

L'autonomie estimée de chacun coffret secourue devra être justifiée par la production d'un bilan de puissance par le soumissionnaire dans son offre.

3.3.3. MODULES COMPLÉMENTAIRES

Le soumissionnaire proposera en nombre suffisant les modules de détections (type UTR) pour permettre le raccordement de la totalité des détecteurs et sorites nécessaires.

3.3.4. MAQUETTE

Dans le cadre de ce projet, une maquette usine à l'échelle 1 ou partielle, de la solution sera à construire par le soumissionnaire. Elle sera présentée à l'équipe de gouvernance collégiale du projet.

3.4. LES ORDINATEURS DE GESTION

Les caractéristiques techniques concernant les ordinateurs liés au contrôle d'accès sont définies dans l'annexe 2 pour les serveurs, enregistreur, stations, écrans simples ou de grande diagonale.

3.4.1. LES SERVEURS

L'ensemble des rôles de la solution de sûreté y compris l'archivage des images, seront hébergés en machines virtuelles sur une seule machine hôte physique.

3.4.1.1. LE SERVEUR D'APPLICATION

Le titulaire devra fournir, installer et mettre en service le serveur principal. Il hébergera la VM pour la solution de gestion de la détection intrusion commune au contrôle d'accès. Ce serveur devra pouvoir accueillir dans un futur proche la VM pour la gestion de la vidéo-surveillance, le stockage des images, la sécurisation des périphériques (RADIUS authentification 802.1x EAP-TLS), la gestion des utilisateurs et de l'exploitation (contrôleur de domaine & management système).

Chaque élément de la solution doivent pouvoir évoluer indépendamment des autres sur le seul critère du respect des prérequis techniques qui doivent, pour les matériels, exclure toute spécification de constructeur, explicite ou implicite.

Il sera installé et intégré dans la baie à fournir, et respecteront les critères suivants :

- technologie « x86 64 bits »,
- sans modification logicielle (e.g. BIOS) ou matérielle qui ne serait pas transposable sur tout autre serveur de même technologie,
- rackables,
- alimentation redondante,
- produit par un des 5 premiers constructeurs mondiaux de serveurs généralistes en volume qui doit avoir noué des partenariats avec les principaux intégrateurs couvrant le territoire français (à justifier dans la réponse),
- garantie 5 ans pièce et main d'œuvre

Les systèmes d'exploitation devront être la dernière version stable de Windows Server ou Debian.

Une infrastructure virtualisée est à privilégier ; l'hyperviseur sera Proxmox ou Microsoft Hyper-V.

Configuration technique minimale des serveurs :

- 2xCPU 16 cœurs (AMD ou Intel)
- RAM: 128Go minimum
- RAID1 SYSTEME de 256 Go mini en SSD
- 4 Ports Ethernet
- 1 Port minimum SFP Gb/s et son module Gbic
- Licence Windows server STD 2022 (permet de couvrir 2xCPU 8 cœurs + 2VMs)
- RAID5 n disques montés en Raid 5, (n sera précisé par l'intégrateur qui le justifiera en produisant la note de calcul permettant de dimensionner le serveur d'archivage vidéo)
- Standard, License & Media, VMs: 2 Licensed Cores: 16
- Kit rail de montage

3.4.1.2. LE SERVEUR DE TEMPS (NTP)

Le serveur de temps (NTP) sera la référence d'horodatage de l'ensemble de la solution, fourni par l'administration.

3.4.1.3. LE SERVEUR DE REDONDANCE

Dans un exercice différent, un serveur redondant, équipé des licences nécessaires et systèmes d'exploitation associés sera à fournir et devra pouvoir exécuter les services proposés.

Une redondance haut débit, du serveur principale vers le serveur redondant, sera gérée par le logiciel SafeKit d'Evidian.

3.4.2. LES STATIONS

Le poste de gestion devra avoir les caractéristiques minimums suivantes :

- processeur Intel® Core Processor i7- 13 700, 4,9 Ghz, 5,4 GHz Turbo, 30MB, 8C,
- 16GB de RAM,
- disque dur de Solid State PCIe NVMe M.2, 256GB (Class 40)
- une carte graphique NVIDIA Quadro P2200 5GB,
- OS Windows 11 Professional License Desktop, ou équivalent.

3.4.2.1. LE POSTE DE GESTION ET DE VISUALISATION ÉVÉNEMENT INTRUSION

Le poste de gestion est à fournir, installer et mettre en service.

En plus des caractéristiques citées ci-dessus, ce poste sera équipé d'écran LED de 27 pouces avec son support de bureau.

Il permettra :

- Le pilotage de l'ensemble du système de détection intrusion et l'affichage des événements.
- La gestion des droits utilisateurs
- La gestion du fil de l'eau des événements. Affichage sur écran dont les caractéristiques techniques sont définies dans l'annexe 6.

3.4.3. SERVEURS ET POSTES INFORMATIQUES A FOURNIR

Les serveurs et postes informatiques à fournir sont listés ci-après :

Fonction du matériel informatique	Serveur	Poste lourd	Poste client léger	Écrans		Lieu installation
				27 pouces	42 pouces	
Système de gestion en machines virtuelles le contrôle d'accès, la vidéosurveillance, le Radius, et intégrera la détection intrusion)	1 serveur hôte					Local Autocom
Système de gestion redondant en machines virtuelles le contrôle d'accès, la vidéosurveillance, le Radius, et intégrera la détection intrusion)	0					
Commutateurs clavier-écran-souris (Keyboard-Vidéo-Mouse = KVM).	A fournir, quantité 1, quelle que soit la configuration					
Claviers + souris compatibles KVM	A fournir, quantité 1, quelle que soit la configuration					
Poste de visualisation du système de Détection Intrusion (Cartographie, Fil de l'eau événements, Gestion)		1				

Serveurs	1					
Postes lourds		1				Salle SIDSIC / Futur PC Sécurité
Postes client léger						
Ecrans 27 pouces		1				
Ecrans 42 pouces						
Ensemble KVM						1 ensemble

3.5. COURANT FAIBLE, COURANT FORT, ÉTIQUETAGE

3.5.1. COURANT FAIBLE

L'ensemble du câblage de détection intrusion est à remplacer.

Pour information :

Tous les périphériques de type « Ethernet/IP » (serveurs, stations, caméras, UTL, etc.) proposés dans la solution seront raccordés sur le répartiteur désigné par l'administration (et dans la plupart des cas, le plus proche) par un lien « Ethernet » catégorie 6^A / classe E^A en respectant les règles de l'art.

3.5.2. COURANT FORT ET ONDULEURS

Tous les organes de sûreté seront raccordés sur le réseau ondulé existant et ou sur le groupe électrogène.

Alimentation en énergie électrique ondulée et secourue

Un onduleur pour le serveur est à fournir dans le cadre de la première phase.
Il doit être équipé d'une carte SNMP permettant de communiquer en IP avec le serveur et d'assurer sa coupure proprement dès que sa charge tombe sous les 20 %.
Ci après, la répartition et les caractéristiques :

Bâtiment	Etag e	Répartiteur	Fonction	Onduleur	Carte SNMP
Bat B	R+3	RG	Répartiteur du serveur Alimentation serveurs et commutateurs	1	1
Onduleur à fournir, quantité totale :				1	
Carte SNMP à fournir, et programmation à réaliser, quantité totale :					1

Caractéristiques du ou des onduleurs :

- format 19 pouces rackable
- raccordé à l'installation par un circuit 230 V-16 A 2P+T protégé par un disjoncteur différentiel 30mA hautement immunisé (type HI)
- branchement effectué sur la distribution électrique secourue désignée par l'administration

- bandeau électrique 6 prises 2P+T, au format 19 pouces, à fournir, intégrer dans la baie et raccorder sur sa sortie.
- l'onduleur devra maintenir l'alimentation électrique pour une durée minimale de 30 mn.
- autonomie de secours à prévoir de 30 minutes pour chacun des onduleurs.
- **une carte SNMP** afin de communiquer en IP avec le serveur et d'assurer sa coupure proprement dès que sa charge tombe sous les 20 %.

La puissance de l'onduleur devra être justifiée par la production d'un calcul de budget énergétique par le soumissionnaire dans son offre.

3.5.3. ÉTIQUETAGE

Tous les matériels installés au titre du présent marché devront être identifiables au moyen d'une étiquette accessible et visible.

3.5.4. ACTEUR

Toutes ces prestations sont à la charge du titulaire.

3.6. PRESTATIONS SUPPLÉMENTAIRES ÉVENTUELLES

Le cas échéant.

4. INTERFONCTIONNEMENT DES SYSTÈMES

Au terme des futurs exercices budgétaires, l'objectif de la solution sera de superviser le système en proposant sur une interface unifiée la gestion de la vidéosurveillance, du contrôle d'accès et de l'anti intrusion.

Cette solution sera constituée d'un superviseur qui permettra la gestion conjointe du contrôle d'accès, de la vidéosurveillance et de l'anti intrusion.

Tous les événements (identifiant, alarmes, sorties, entrées, états) liés à un point d'accès ou un point d'intrusion sont horodatés et enregistrés. Ces événements indexent les flux vidéo des caméras associés au point d'accès ou d'intrusion.

Tous les événements associés aux points d'accès supervisés par le système vidéo sont liés aux images correspondantes et accessibles par simple clic dans l'interface de supervision.

Les alarmes sont couplées au système vidéo pour l'enregistrement, la levée de doute avec pré-positionnement sur les zones en alarme et naturellement l'interface de traitement et d'acquiescement.

Les alarmes sont affichées avec toutes les possibilités vidéo associées de la visualisation des points de fuite.

5. EXPLOITATION DE LA SOLUTION

5.1. GESTION DU SYSTÈME

5.1.1. PRÉSENTATION DES PROFILS UTILISATEURS

L'administration précise les profils utilisateurs en vigueur dans le cadre de la gestion des dispositifs plus généralement de sûreté :

- L'accès « **Administrateur système** » permet à un opérateur clairement désigné et habilité, de vérifier le bon état de fonctionnement du dispositif et d'en administrer l'ensemble (paramétrage, configuration, supervision, sauvegardes, lectures, cartographie...) ainsi que la visibilité des informations qu'il contient,
- L'accès « **Gestionnaire de badges** » permet à un opérateur, sous-réserve de ses droits, d'administrer et gérer les profils, de produire des badges, etc. En aucun cas le profil « Gestionnaire de badges » ne pourra porter atteinte à l'intégrité des données vidéo enregistrées par le système,
- L'accès « **Opérateur** » permet à un exploitant, sous-réserve de ses droits, de consulter la cartographie, gérer des alarmes, produire des badges, gérer des portes, ainsi que de consulter les fiches réflexes, etc. En aucun cas le profil « Opérateur » ne pourra porter atteinte à l'intégrité des données vidéo enregistrées par le système.
- L'accès « **Opérateur d'extraction** » permet à un exploitant, sous-réserve de ses droits, de consulter les images, faire des recherches de séquences, extraire des images, etc. (pour le format) En aucun cas le profil « Opérateur d'extraction » ne pourra porter atteinte à l'intégrité des données vidéo enregistrées par le système.

L'implantation des différents terminaux se fera en fonction du choix retenu par le maître d'ouvrage.

5.2. EXPLOITATION PAR L'ADMINISTRATEUR DU SYSTÈME

Le système doit permettre de définir des profils utilisateurs permettant de gérer des « droits » ou privilèges sur les objets Équipement/Événement/Alarmes/Actions/Espace de Travail dans tous les applicatifs utilisés. Cette gestion doit, par exemple, quand l'objet est une action, permettre de définir des droits de Création/ Suppression / Exécution/ Modification.

Toutes les actions sur le système sont réservées et protégées par des droits liés au compte applicatif de l'opérateur. Il y a à minima trois types de droits :

- Le droit de lecture confère à un opérateur le pouvoir de visibilité,
- Le droit d'écriture confère à un opérateur un pouvoir d'action,
- Le droit de modification confère à un opérateur les droits de modification.

5.2.1. CONFIGURATION DES DROITS OPÉRATEURS

Les éléments suivants sont configurés en droits (profil par opérateur), pour permettre à minima les fonctions suivantes :

- Des droits sont gérés pour la création/visualisation/configuration des entités du système (utilisateur, badge, alarme, actions, fiche de porteur, rapport, équipement),
- Des droits sont gérés par équipement pour permettre la création, la visualisation, la configuration, le changement d'état (actif/inhibé),
 - Un équipement (porte, lecteur de badge, détecteur) peut être invisible à un utilisateur,
 - Un équipement (porte, lecteur de badge, détecteur) peut être en accès lecture seule,
 - Une porte en lecture seule doit permettre la visualisation de son état mais inhibe les droits d'actions Ouverture/Fermeture.
- Des droits sont gérés pour les éléments partagés,
 - Infériorisation des commandes joystick,
 - Priorisation sur l'accès à des écrans et vignettes des murs d'images,
 - Accès en lecture seule sur la définition des écrans et vignettes des murs d'image,
 - Accès en modification seule sur la définition des écrans et vignettes des murs d'image,
- Des droits sont gérés pour la création, la visualisation, le déclenchement des actions programmées ou natives,
- Des droits sont gérés pour la création, la visualisation, la modification de l'espace de travail,
- Des droits sont gérés pour l'accès aux applications de la solution.

Un opérateur « poste de contrôle et de sécurité » doit pouvoir :

- Disposer d'un retour type fil de l'eau événement/alarme sur les équipements dont il aura la visibilité,
- Disposer de droit en écriture sur un accès pour l'ouvrir/le fermer,
- Visualiser certaines caméras.

Un opérateur « gestionnaire des badges » doit pouvoir :

- Configurer son espace de travail ;
- Créer/modifier des profils, des groupes de porteurs, des porteurs de badge,
- Disposer d'un droit en écriture sur des accès pour l'ouvrir / le fermer,
- Disposer d'un retour type fil de l'eau événement/alarme sur les équipements dont il aura la visibilité,
- Disposer des droits de lecture/écriture/modification des équipements d'accès,
- Éditer un badge.

Un opérateur « extraction d'images » doit pouvoir :

- Configurer son espace de travail ;
- Recherche des séquences d'images enregistrées sur le stockeur,
- Faire des extractions d'images (lecture seule)
- Disposer d'un droit en écriture sur les ports USB de son espace de travail,
- Disposer d'un retour type fil de l'eau événement/alarme sur les équipements dont il aura la visibilité,

Seuls les opérateurs déclarés avec un profil « administrateur » disposent d'un accès en écriture sur tous les équipements.

Le système de gestion des droits est paramétrable. Le système doit permettre une gestion sécurisée des mots de passe des utilisateurs.

Le système de gestion des droits doit permettre de définir des droits relatifs à la

définition/modification de l'espace de travail.

Le système doit avoir une gestion des droits permettant de gérer des équipements partagés ou des informations partageables, que ce soit dans le cadre de « raccordements » (fédération, déport, supervision multi-site) ou dans le cadre d'utilisation locale (partage de la motorisation des caméras, des murs d'images).

La documentation doit fournir une description détaillée des possibilités natives offertes par le système de gestion des droits.

5.2.2. GESTION DES JOURNAUX

La solution doit permettre la consultation de l'ensemble des actions effectuées sur le système que ce soit au niveau des postes clients ou au niveau des postes serveurs mais selon les droits octroyés à l'utilisateur.

Les actions tracées sont à minima :

- Système
 - Arrêt / Lancement des services applicatifs (journalisation incluse),
 - Arrêt critique sur incident,
 - Arrêt système par exploitant (identifiant, date/heure),
 - Démarrage système par exploitant (identifiant, date/heure), Évènement de ressources systèmes ;
- Administration applicative
 - Ajout/suppression d'équipements,
 - Gestion des comptes (création/suppression/modification des droits).
- Exploitation courante
 - Heure de connexion, déconnexion,
 - Action sur un équipement,
 - Action sur un badge.

La solution doit protéger cette traçabilité par son système de droits (profil).

5.3. EXPLOITATION PAR LE GESTIONNAIRE DES BADGES

5.3.1. GESTION DES BADGES

5.3.1.1. PERSONNALISATION DES BADGES UTILISATEURS

La solution doit permettre la gestion de porteurs de badges et de groupes de porteurs de badge. Les groupes de porteurs sont des listes de porteurs créés par direction/service ou site.

La solution doit permettre de paramétrer les propriétés suivantes d'un porteur de carte :

Nom
Prénom
Matricule
Grade
Fonction
Observation
Dates

Les champs nominatifs acceptent toutes les lettres donc les caractères accentués et ponctuations utilisés dans la langue française.

La solution doit permettre la gestion de :

- Champs personnalisés (au moins 15),
- Date d'activation/ Date d'expiration,
- Gestion d'une photo capturée à partir d'un périphérique numérique (web cam ou caméra de vidéo surveillance) ou importé par fichier,
- Statut (profil activé ou désactivé, perdu, volé, bloqué, etc.).

Les champs personnalisables sont des entités type :

- Booléen,
- Date,
- Entier,
- Images ou fichiers graphiques,
- Nombres décimaux,
- Texte.

La solution doit permettre l'association d'un porteur de carte et d'un groupe de porteurs avec plusieurs badges.

La solution détecte les doublons à partir du nom, prénom, date de naissance et/ou service, société.

Tous les champs ne sont pas obligatoirement renseignés. Les champs de la fiche de porteurs de badge doivent pouvoir être obligatoires ou non.

La solution doit pouvoir permettre la création de fiches similaires. L'objectif est de pouvoir attribuer plusieurs badges à une même personne.

La solution doit permettre d'activer ou d'inhiber un badge ou un groupe de badges manuellement sous réserve des droits utilisateur.

La photo imprimée sur le badge doit être sans déformation et conforme au cadrage réalisé. La déformation d'image est interdite, le facteur d'échelle doit être conservé.

La solution doit permettre le réglage d'un cadre de base au taille réglementaire passeport et paramétrable. Le cadre doit pouvoir faire 2,4 x 3,2 cm. Ce paramétrage doit être conservé.

L'historique de la fiche de porteurs de badge doit comprendre les événements d'impression de carte.

La solution doit permettre la gestion des erreurs à l'importation.

Le serveur de contrôle d'accès doit permettre la gestion simultanée de 200 porteurs de badges au maximum.

5.3.1.2. GESTION DES PROFILS

La solution doit permettre la création de profils à partir de règles d'accès associées à des groupes de points d'accès.

La solution doit permettre l'association de porteurs ou des groupes de porteurs à des règles d'accès et des profils.

La solution doit permettre de paramétrer les droits d'accès en fonction des points d'accès et de plages horaires et calendaires :

- 32 plages horaires comprenant chacune 3 intervalles par jour, pour chaque jour de la semaine. Une notion de "jours spéciaux" permettant de programmer des droits d'accès contextuels et non hebdomadaires sera prévue,
- 32 jours fériés :
 - ponctuels,
 - annuels reconductibles, jours fériés calendrier français recalculé automatiquement d'une année sur l'autre.

La solution doit permettre la gestion d'un grand nombre de profils (supérieur à 50).

5.3.1.3. INVALIDATION DES BADGES

La solution doit permettre de rendre automatiquement invalide un badge à la fin de sa période de validité. Cette fonction est particulièrement mise en service pour les badges journaliers V.

La solution doit permettre de bloquer un badge lorsqu'il n'est pas utilisé pendant une durée supérieure à un temps paramétré (de l'ordre de 2 mois). Cette fonctionnalité peut être activée sur certains profils ou badges.

La solution doit permettre d'invalider n'importe quel badge de la solution sous réserve d'avoir les droits utilisateurs.

5.3.1.4. ÉTAT D'UN BADGE

L'opérateur disposant des droits peut, en recherchant un badge (recherche multicritères à partir d'un nom/numéro d'identifiant) décider de positionner le badge comme :

Actif	Toutes les fonctions prévues
Inactif	Le badge n'ouvre aucun accès. Sa présentation sur un lecteur déclenche une alarme précisant : « Badge inactivé le jj/mm/aa à hh:mn par nom_personne ».
Perdu	Le badge n'ouvre aucun accès. Sa présentation sur un lecteur déclenche une alarme précisant : « Badge déclaré perdu le jj/mm/aa à hh:mn par nom_personne »
Volé	Le badge n'ouvre aucun accès. Sa présentation sur un lecteur déclenche une alarme précisant : « Badge déclaré volé le jj/mm/aa à hh:mn par nom_personne ».
Expiré	Le badge n'ouvre aucun accès. Sa présentation sur un lecteur déclenche une alarme précisant : « Badge bloqué le jj/mm/aa à hh:mn par nom_personne ».

5.3.2. GESTION DES RAPPORTS

Les rapports standards d'activité courante seront :

- Liste des alarmes,
- Historique des mouvements d'un utilisateur,
- Historique des mouvements de badges,
- Liste des badges non présentés dans telle zone depuis N jours (N paramétrable),
- Historique des événements par type d'objet,
- Taux d'utilisation des lecteurs.

Les rapports d'activité opérateurs seront :

- Historique des login,
- Journal des acquittements trié par date, filtré pour tout ou partie des opérateurs.

Les rapports liés aux utilisateurs seront :

- Liste des badges,
- État des badges,
- Liste des badges ayant accès à un ou plusieurs lecteurs,
- Liste des badges venant à expiration à une date donnée,
- Liste des badges appartenant à une série de groupe d'utilisateurs,
- Liste des utilisateurs avec leur fiche d'identification,
- Liste simplifiée des utilisateurs.

5.4. EXPLOITATION PAR LES OPÉRATEURS

5.4.1. GESTION TYPE

5.4.1.1. AMÉNAGEMENT DU POSTE DE GESTION

Un poste de gestion est à fournir pour gérer la sécurité du site.

Ce poste disposera d'un écran:

- l'écran affichera le plan graphique renseigné du site, en 2D avec noms des lieux, numéro de l'étage, nom ou numéro de la pièce, type et qualité des moyens, ainsi que la disposition des moyens mis en place tels que caméra, détecteur/contrôleur d'ouverture de porte, détecteur de mouvement, le lancement de commandes directes (mise en/hors service de point d'entrée, activation de sortie, déverrouillage d'accès, etc.).

Sur le même écran, **une fenêtre** présentera une fiche « main courante » précisant les événements du jour (prévus, arrivés, en cours, etc.), les incidents types, la conduite à tenir, les mesures prises qui permettent de prévoir, organiser et gérer la sécurité au quotidien en cas d'événement, qu'il soit anodin ou grave. Il sera aussi celui qui permettra l'acquiescement et la visualisation des alarmes, la gestion manuelle et automatique des caméras, le pilotage de l'éclairage, l'utilisation des prépositions des caméras sur le plan graphique, l'enregistrement numérique sur disque dur des événements du site).

5.4.1.2. GESTION DES ENQUÊTES

La solution doit permettre la recherche d'événements-alarmes, mémo, signet, métadonnées et de visualiser la vidéo éventuellement associée à l'événement.

5.4.1.3. GESTION DE LA CARTOGRAPHIE

Le système dispose d'un outil de cartographie dynamique permettant de localiser tous les équipements de sécurité (caméra, portillon, porte surveillée, contrôle d'accès, lecteur RFID, haut parleur, sirène, détecteur de présence, etc.) sur un plan. Le plan et ces équipements peuvent s'afficher à l'échelle (proportion respectées), par zone, par bâtiment et par étage.

La cartographie accepte les fonctions de zooms avant/arrière à partir de la molette de la souris (par exemple).

Le système doit permettre de zoomer dans le plan, de se diriger à 360.

Le système dispose d'une cartographie multi sites et multi niveau.

La cartographie doit permettre d'exécuter des actions de type glisser/déposer de la cartographie vers toute vignette d'affichage pour permettre :

- De visualiser une caméra par action de déposer d'une caméra vers une vignette d'affichage,
- De visualiser les événements liés à une porte par action de déposer d'une porte vers une fenêtre,
- De visualiser les photos des titulaires identifiés sur une porte par action de glisser déposer d'une porte vers une vignette d'affichage.

La cartographie doit permettre de proposer une aide contextuelle par équipement. Il devra apparaître un encadré dans lequel devra figurer leur appellation, leur position (étage, zone de sûreté...) et le moyen de détection (détecteur, détecteur/contrôleur, caméra fixe, mobile, etc.).

Ce plan graphique, disponible sur les postes d'exploitation, servira en particulier à la visualisation

des événements.

Par ailleurs, ces événements entraîneront une animation des éléments graphiques représentant les équipements (barrières infrarouges, détecteurs d'intrusion, caméras, etc.) de la zone concernée.

Lorsqu'un événement se produit dans une zone qui est constituée d'une (ou plusieurs) caméra(s) et/ou d'une barrière infrarouge ou autre détecteur de mouvement, chaque équipement de la zone de détection, qui aura déclenché l'alarme, sera automatiquement signalé par un changement de couleur et d'un clignotement sur la cartographie.

Exemple : la caméra de visualisation passe en rouge de même que le (ou les) faisceau(x) franchi(s) reliant deux barrières infrarouges, etc.).

Par contre, ce changement de couleur sera différent suivant l'état du système :

- En rouge lors du déclenchement d'une alarme, restera en rouge tant que l'alarme ne sera pas acquittée,
- En orange lors du déclenchement d'une panne.

5.4.1.4. GESTION DES ALARMES

La solution doit permettre la définition d'une alarme ou d'un événement/alarme à partir de la combinaison d'événements détectés par le système, contact sec, détection d'ouverture, détection d'événements d'identification, d'événements natifs et programmables.

La solution doit permettre de paramétrer la notion d'alarme et d'événement pour pouvoir, sous réserve de ses possibilités, définir une alarme et un événement et éventuellement convertir une alarme en événement (et réciproquement).

Le système doit permettre une hiérarchisation des alarmes par niveau et une hiérarchisation des événements. La solution doit permettre la gestion de 10 niveaux d'alarmes et d'événements. Les niveaux d'alarmes doivent pouvoir être filtrés sur la console opérateur et affichés par des signes distinctifs (couleur, etc.).

Le terme alarme prioritaire utilisé dans ce document est une alarme de niveau 1.

Chaque alarme doit pouvoir être déclarée dans un champ de 1 à 255 caractères.

Le système doit permettre d'afficher une procédure à suivre en « alarme ».

Le système doit permettre de gérer des alarmes notifiées par l'opérateur.

Le système doit permettre une gestion des alarmes en cascades.

5.4.1.5. GESTION DU SYSTÈME VIDÉO ET SCENARIOS

Le ministère souhaite la mise à disposition d'une interface simple pour créer des scénarii d'actions. Ces scénarios sont déclenchés soit par un ou une association d'événements (alarme/calendaire), soit manuellement par l'opérateur.

L'utilisateur peut pour un scénario nommé :

- Définir des actions sur des portes, passages, équipements,
- Définir des actions sur des caméras.

Le système de vidéo-détection fera l'objet d'un fonctionnement particulier intégrant les informations ci-après :

- D'une prise en compte de plages horaires,
- D'un déclenchement d'alarme selon la zone de détection,
- D'une localisation sur un plan graphique.

Le système d'acquisition et de visualisation numérique des images doit pouvoir s'activer automatiquement dès le déclenchement de la caméra couplée à la détection de la zone traversée ou de mouvement particulier ou d'objet identifié ou d'interprétation et d'analyse d'images.

Il faut pouvoir créer et gérer pour chaque caméra des scénarii préprogrammés (rondes dans le temps ou rotation dynamique cyclique et cycles d'images pour différents groupes de caméras). Les caméras peuvent être individuellement programmées sur un scénario qui s'appliquera par défaut, au bout d'un laps de temps sans action (rondes, repositionnements).

- **Portes et Points d'Accès :**
Les actions natives pour les équipements portes/points d'accès sont : Ouvrir, Fermer, Inhiber.
- **Visiophonie :**
Les actions natives pour les équipements de visiophonie sont : Ouvrir, Fermer, Inhiber, mettre en attente une communication.
- **Point Alarme :**
Les actions natives pour les équipements d'alarmes sont : Armer, Désarmer.
- **Mur image :**
Positionner le mur d'image dans une configuration spécifiée,

L'utilisateur peut pour un scénario nommé :

- Définir des actions sur des portes, passages, équipements de détection d'intrusion,
- Définir des actions sur des caméras.

Exemples de scénarii modifiables :

Scénario 1 : Exploitation « normale de jour »,

Scénario 2 : Exploitation « normale de nuit »,

Scénario 3 : Exploitation « normale de week-end et de jours fériés »,

Scénario 4 : Exploitation en situation normale exceptionnel prévisible (exemple élections, visites de personnalités, etc.),

Scénario 5 : Situation de crise.

Pour chaque scénario il sera possible de programmer les fonctions de chaque caméra, les enregistrements à effectuer, les consignes à appliquer en cas d'alarme, etc.

Le passage d'un scénario à l'autre pourra indifféremment se faire automatiquement selon un programme horaire ou une action manuelle par un opérateur autorisé.

5.4.2. PRINCIPE DE GESTION DES RÉACTIONS À ÉVÉNEMENT

Les actions natives sont :

- Acquitter une alarme,
- Afficher un objet du système (fiche carte, fiche utilisateur/voiture, photo d'un identifiant),
- Afficher le signal d'une caméra / les signaux d'un groupe paramétrable de caméras sur une vignette du mur d'image,
- Ajouter un signet et/ou une métadonnée jointe au système vidéo,
- Automatiser la production d'un rapport,
- Déclencher l'asservissement du lecteur vidéo pour rejouer une séquence,

- Déclencher un scénario identifié par un nom,
- Déclencher une ronde vidéo,
- Déclencher/Arrêter un enregistrement,
- Diffuser un message audio depuis un fichier ou un micro,
- Ouvrir ou fermer la sortie relais d'un contrôleur.

Le système doit permettre d'adresser des actions natives et de définir par configuration avec un outil et/ou par programmation des actions « dédiées ».

Le système doit permettre d'associer une action à partir d'une liste d'actions.

Le système doit permettre de déclencher une action calendaire.

Le système doit permettre de déclencher une action programmée c'est-à-dire que toutes les actions sont activables sous la forme de trigger.

Le système doit permettre de gérer manuellement et automatiquement (via les actions) le mur d'image. Il doit par exemple pouvoir afficher une caméra en alarme sur une vignette numérique d'un moniteur informatique local ou distant.

Le système doit permettre de déclencher une action à distance sur un autre sous système dans le cas de raccordement ou d'utilisation multi-sites.

La solution doit permettre à un utilisateur, par une action simple et sous réserve de ses droits, de n'importe quel poste client de :

- Activer / Désactiver un équipement,
- Consulter l'état d'un équipement,
- Créer/Supprimer un équipement,
- Inhiber les alarmes associées à un équipement,
- Ouvrir/Fermer un accès.

Ces actions peuvent être faites directement au niveau cartographique et simplement par l'intermédiaire de menu.

6. EXIGENCES SÉCURITAIRES

Les mesures de sécurité complémentaires suivantes sont à prendre en compte.

N°	Domaine	Description de la mesure	Bien(s) support(s) concerné (s)
1	Organisation de la sécurité des SI	Contrat de maintenance 5j/7 – HO avec intervention sous 24H	UTL, serveurs, lecteurs
2	Organisation de la sécurité des SI	Ajouter à l'ensemble des marchés publics les clauses de sécurité établies par la DSIC (cf site SSI DSIC)	Serveur, UTL, postes administrateur
3	Organisation de la sécurité des SI	Exiger une enquête de sécurité sur les prestataires. Conformément aux PES, les administrateurs encadrent les prestataires pour chaque intervention technique. Pour les travaux nécessitant un accès aux locaux techniques, la présence d'un administrateur MI est obligatoire	Serveur, UTL, postes administrateur
4	Organisation de la sécurité des SI	Interdire la télémaintenance depuis les locaux d'une entreprise privée. La maintenance du SI devra se faire in situ.	Serveur, commutateur, UTL, lecteurs

5	Évaluation de la sensibilité et protection des documents	Protection des clefs de lecture Idéalement : La clé de lecture est répartie sur plusieurs porteurs ; sécurité liée à la gestion (introduction dans la solution) sécurité et inviolabilité des équipements de stockage des clés (lecteurs, coffres pour les badges de configuration éventuels, base de données éventuelles, etc.) sécurité liée au renouvellement ;	Lan Commutateurs, Serveur, UTL, Poste admin, Badges admin, lecteurs, Équipes admin, Badges utilisateurs,
6	Évaluation de la sensibilité et protection des documents	Les clefs et en particulier la clef de lecture, ne doivent en aucun cas être communiquées aux installateurs	Lan Commutateurs, Serveur, UTL, Poste admin, Badges admin, lecteurs, Équipes admin, Badges utilisateurs,
7	Ressources humaines	Formation et sensibilisation des administrateurs SIC aux PES et mesures de sécurité « Contrôles d'accès » et des gestionnaires d'accès aux règles de gestion des accès.	
8	Sécurité physique des locaux	Les équipements seront installés dans des locaux sécurisés par contrôle d'accès	UTL, Poste admin, Badges admin
9	Sécurité physique des locaux	Alimentation électrique secourue – onduleur, groupe électrogène – Climatisation – Détection incendie. En cas de coupure électrique, les portes ou portiques devront rester, par défaut, en position fermée.	Lan Commutateurs, Serveur, UTL, Poste admin , lecteurs,
10	Sécurité physique des locaux	Sécuriser l'accès aux locaux sensibles (locaux techniques...), par la mise en œuvre d'un second mécanisme de contrôle (ex : digicode ou biométrie). Avec deux mesures à mettre en œuvre : – une mesure technique pour la gestion des droits administrateur applicatifs – une mesure pour le processus de validation des droits	Serveur, commutateurs
11	Architecture et exploitation des SI	Redondance des UTL et répartition des lecteurs d'une même zone sur plusieurs contrôleurs.	UTL, lecteurs
12	Architecture et exploitation des SI	Redondance lecteurs : Utilisation d'un autre accès en cas d'indisponibilité d'un lecteur	Lecteur
13	Architecture et exploitation des SI	Redondance des commutateurs, architecture sécurisée Une architecture 2 minimum serait souhaitable pour disposer des moyens de sécurisation nécessaires. L'objectif est d'assurer un niveau de disponibilité maximum sur les commutateurs avec une durée d'indisponibilité maximum de 24 heures.	Commutateur LAN
14	Architecture et exploitation des SI	Prévoir plusieurs badges administrateurs	Poste admin , Badges admin,
15	Architecture et exploitation des SI	– Sauvegarde quotidienne au minimum des données sensibles (clefs de lecture, profil, logs)	Équipe d'administration Serveur

	Gestion de la continuité des SI		
16	Architecture et exploitation des SI	Mettre en place et vérifier le bon fonctionnement des mises à jour automatiques de l'antivirus de façon régulière sur l'ensemble des équipements informatiques. Appliquer la politique de configuration ministérielle Procéder à une analyse antivirus quotidienne des serveurs	Serveurs, postes admin
17	Architecture et exploitation des SI	Mettre en place les correctifs de sécurité et upgrade applicatifs matériels	Serveurs, postes admin, UTL, Commutateurs, Lecteurs
18	Architecture et exploitation des SI	Autonomie des UTL par rapport aux serveurs : Les UTL doivent avoir une copie de la base des droits afin de continuer à fonctionner de manière autonome. Toutes les UTL pourront fonctionner sans perturbation en cas de perte de la liaison avec les équipements en amont.	UTL
19	Architecture et exploitation des SI	Mettre en œuvre un réseau physique dédié aux équipements contribuant à la mise en œuvre des systèmes de sécurisation. À défaut, une solution basée sur les technologies VPN IPSEC (dont la configuration devra être conforme aux recommandations de l'ANSSI) sera mise en œuvre. L'objectif étant d'isoler les enclaves du système de contrôle d'accès (sous forme de DMZ) et les interconnecter entre elles par VPN IPSEC. Aucune interconnexion ne devra être possible entre le RGT et les enclaves « Contrôle d'accès » entre les VLANs RGT (serveur, postes de travail...) d'un site et les enclaves « Contrôle d'accès »	Lan Commutateurs, serveur, UTL, postes administrateur
20	Architecture et exploitation des SI	La communication entre le badge, la tête de lecture et l'UTL sera chiffrée de bout en bout par des mécanismes conformes aux référentiels cryptographiques recommandés par l'ANSSI (Annexe B1 du RGS27)	Lan Commutateurs, Serveur, UTL, Poste admin,
21	Architecture et exploitation des SI	Les outils d'administration devront intégrer les protocoles SSL/TLS. Ces protocoles seront également appliqués pour les échanges entre les lecteurs et les UTL.	Administrateur, UTL, lecteurs
22	Architecture et exploitation des SI	Protection physique des lecteurs : Les têtes de lecture devront être équipées d'un système de détection d'intrusion et d'arrachage, leurs fixations devront être renforcées.	Lecteurs
23	Architecture et exploitation des SI	Sécuriser les BDD de type Oracle conformément aux PES	Serveur
24	Architecture et exploitation des SI	Procéder au cloisonnement des ressources serveurs dans une DMZ dédiée à cet effet	Serveur
25	Gestion des autorisations ou accès logique aux ressources	Restreindre l'accès aux interfaces d'administration aux seuls administrateurs explicitement identifiés et authentifiés (ex : filtrage réseau, FW....)	Serveur, UTL, postes administrateur, commutateurs
26	Gestion des autorisations ou accès logique aux ressources	Interdire l'accès aux fichiers de données aux prestataires Créer des comptes nominatifs pour les prestataires. Ces comptes devront être supprimés dès la fin de la prestation (cf procédure circuit arrivée/départ)	Serveur, postes administrateurs

27	Gestion des autorisations ou accès logique aux ressources	Journalisation des opérations réalisées par les administrateurs et installateurs Journalisation des actions sur le système de contrôle d'accès (création de badge, ouverture d'autorisation d'accès à des locaux, création d'utilisateurs dans la BDD, ...)	Serveur, postes admin
28	Gestion des autorisations ou accès logique aux ressources	Prévoir des badges temporaires ainsi qu'une procédure ad-hoc de délivrance et restitution de ces badges	Badges utilisateurs
29	Gestion des autorisations ou accès logique aux ressources	Utilisation de comptes nominatifs et de la carte agent pour l'authentification des administrateurs. Les comptes nominatifs des prestataires devront être activés/désactivés suivant les besoins d'intervention (cf procédure spécifique comptes nominatifs prestataires)	Administrateur
30	Gestion des autorisations ou accès logique aux ressources	Renouvellement des clefs et procédures de plusieurs porteurs Les clés sont classées par niveau de sensibilité. Idéalement les clés les plus sensibles (clé de lecture, etc.) sont réparties sur plusieurs porteurs Le système prévoit une gestion de renouvellement de clés minimisant les impacts fonctionnels	Badges utilisateur, badges administrateur
31	Gestion de la continuité des SI	En cas fonctionnement en mode dégradé (coupure électrique ou interruption des serveurs/UTL): garde statique, ouverture des accès stratégiques par clefs	Lecteurs, Lan Commutateurs, Serveur UTL, Système de verrouillage
32	Gestion de la continuité des SI	Assurer la continuité de la fonction administration du SI : gestion des congés, astreintes...	Équipes admin
33	Gestion de la continuité des SI	Rédiger des fiches réflexes à appliquer en cas d'activation du plan de reprise d'activité (PRA) – S'assurer que les logiciels listés dans les fiches réflexes soient disponibles	Serveur
34	Gestion de la continuité des SI	S'assurer de la disponibilité des matériels listés dans les fiches réflexes : (plate-forme de secours...),	Serveur
35	Gestion de la continuité des SI	Prévoir un stock de maintenance pour les commutateurs	Lan Commutateurs
36	Conformité et contrôle	Respect du « document de référence technique puce sans contact » rédigé par le SHFD	Lecteurs, Badges admin, Serveur , UTL, badges utilisateurs

7. DÉMONTAGE

7.1. DÉPOSE

Le démontage comprend la dépose des installations devenues inutiles (caméras, écrans, enregistreur, détecteurs, lecteurs de badges, fixations, réglettes de câblage, câbles, boîtes de distribution, prises, serrures, etc.), supports de câbles inclus (tubes, goulottes, plinthes, moulures, etc.). Ce démontage sera effectué soigneusement. Tous les câbles colliers, attaches, ferrures seront enlevés et les trous rebouchés. Les anciennes prises encastrées seront obturées par des caches appropriés. Si nécessaire des retouches de peinture devront être effectuées.

Le maintien de certains câbles dont le démontage entraînerait des dégradations trop importantes du point de vue esthétique (éclats de peinture, etc.) est soumis à l'accord du maître d'ouvrage. Ces câbles seraient alors laissés sur place et coupés à ras, de manière à rendre leur inutilité évidente et à faciliter leur retrait lors de travaux futurs.

L'administration se réserve le droit de conserver tout ou partie du matériel démonté.

Cette prestation sera définie avec le prestataire lors de la visite de site.

7.2. STOCKAGE

Un local fermant à clé sera mis à disposition du titulaire par l'administration. Son emplacement sera défini lors de la visite de site en accord avec le responsable du service immobilier du site. Ce local permettra d'entreposer le matériel en attente d'installation ainsi que tout élément démonté.

7.3. RECYCLAGE

Option 1 : Recyclage par l'administration

Tout le matériel démonté sera stocké dans un local indiqué par l'administration qui se chargera de le recycler.

Une exception sera faite pour tout élément contenant des données sensibles (disque dur, etc.). Les disques durs ne peuvent en aucun cas quitter le périmètre du site et seront remis à l'administration qui se chargera de les détruire. Aucune donnée ne peut être dupliquée sur tout support hors du site conformément aux recommandations SSI.

8. DOCUMENTATION

8.1. DOCUMENTATION TECHNIQUE

Le titulaire du marché devra mettre à disposition une documentation complète sur les systèmes mis en œuvre comprenant :

- Les documentations techniques en français des matériels installés (version électronique et papier),
- Le Dossier des Ouvrages Exécutés (D.O.E.) en trois exemplaires papier et version électronique comprenant :
 - L'emplacement de tous les équipements installés (caméras, détecteurs, UTL, postes clients),
 - Le cheminement des câbles posés (courant fort et faible),
 - Les plans mis à jour au format dwg et ou pdf.

Ce document devra revêtir le timbre « DIFFUSION RESTREINTE ».

Toutes les pièces constituant cette documentation seront fournies en français sous forme de fichier électronique lisibles à partir de logiciels libres et en format papier sous forme de classeur.

8.2. DOCUMENTATION D'ADMINISTRATION ET D'EXPLOITATION

Le titulaire du marché devra mettre à disposition une documentation d'exploitation des différents systèmes mis en œuvre comprenant :

- Un manuel d'administration système et des applications,
- Un manuel d'exploitation de chaque système,
- Une procédure de reprise des activités du système couvrant notamment l'arrêt forcé des équipements, leur redémarrage sur incident,
- Les consignes de sécurité pour le bon usage de la solution.

La documentation sera en version française.

8.3. SAUVEGARDE – RESTAURATION

Le titulaire du marché devra mettre à disposition une documentation sur les procédures de sauvegarde et restauration des données permettant :

- Une sauvegarde journalière, hebdomadaire,
- Une sauvegarde/restauration différentielle, incrémentielle et complète.

Les formations seront assurées par des animateurs de formation spécialisés et habitués à ces types de formation. Elles se dérouleront à temps plein sur le site du client.

L'objectif est, qu'à l'issue de la formation, les personnels soient pleinement opérationnels dans le domaine de travail qu'ils doivent assurer.

Les supports de cours seront fournis en langue française, au format papier et au format électronique lisible à partir de logiciels libres. Ils seront classifiés en « DIFFUSION RESTREINTE ».

Le titulaire proposera le contenu ainsi que la durée et le nombre de sessions qui seront adaptées au nombre de participants dans chaque domaine (administrateurs et exploitants).

9. FORMATIONS

Les formations seront assurées par des animateurs de formation spécialisés et habitués à ces types de formation. Elles se dérouleront à temps plein sur le site du client.

L'objectif est, qu'à l'issue de la formation, les personnels soient pleinement opérationnels dans le domaine de travail qu'ils doivent assurer.

Les supports de cours seront fournis en langue française, au format papier et au format électronique lisible à partir de logiciels libres. Ils seront classifiés en « DIFFUSION RESTREINTE ».

Le titulaire proposera le contenu ainsi que la durée et le nombre de sessions qui seront adaptées au nombre de participants dans chaque domaine (administrateurs et exploitants).

9.1. FORMATION DES ADMINISTRATEURS

Le module dédié à la formation des administrateurs leur permettra d'appréhender complètement les systèmes mis en œuvre pour ce qui concerne l'installation, la configuration et l'utilisation des différentes applications avec en particulier :

- La gestion des comptes exploitants,
- La gestion des clés de chiffrement,
- La gestion du temps,
- La gestion des calendriers,
- La gestion des scénarii,
- La gestion des sauvegardes,
- La gestion des images,
- Le stockage et exportation des données,
- Et tout autre item proposé par le titulaire.

La formation sera assurée pour 4 personnes minimum.

9.2. FORMATION DES GESTIONNAIRES DE BADGES

Le module dédié à la formation des gestionnaires de badges leur permettra d'appréhender complètement les systèmes mis en œuvre pour ce qui concerne l'enrôlement, la configuration et l'utilisation des badges avec en particulier :

- La gestion des profils,
- La gestion des badges,
- La gestion du temps,
- La gestion des calendriers,
- Et tout autre item proposé par le titulaire.

La formation sera assurée pour 4 personnes minimum.

9.3. FORMATION DES OPÉRATEURS

Le module dédié à la formation des opérateurs leur permettra d'utiliser de manière optimale les différentes applications mises à disposition avec en particulier :

- La présentation des équipements des postes PCS (stations, murs d'images, imprimantes),

- La présentation du poste de travail : les différentes fenêtres, agencement des écrans,
- Le démarrage et l'arrêt des stations de travail,
- La connexion et la déconnexion aux applications,
- L'exploitation du système vidéo, de l'alarme, du contrôle d'accès et de la visiophonie,
- La gestion de badges « visiteurs »,
- La gestion des événements et alarmes,
- Et tout autre item proposé par le titulaire.

La formation sera assurée pour 4 personnes minimum.

10. RECETTE

La réception de la prestation est conditionnée par la fourniture de la documentation détaillée des architectures et des systèmes installés (spécifications techniques, paramétrages, configuration et exploitation, plan de recollement, fiches réflexes, etc.).

La recette technique se compose d'un contrôle d'inventaire, d'un contrôle visuel et d'un contrôle fonctionnel.

La recette technique est l'opération qui doit permettre de garantir au maître d'ouvrage que l'installation est conforme :

- Au CCTP,
- Aux performances attendues,
- Aux normes et réglementations en vigueur,
- Au guide d'installation du constructeur pour l'obtention de la garantie,
- Aux règles de l'art.

10.1. RECETTE DE L'INFRASTRUCTURE RÉSEAU

10.1.1. LE CONTRÔLE VISUEL

Après un contrôle quantitatif et qualitatif des composants fournis, le contrôle visuel portera sur la qualité générale de la prestation. On vérifiera notamment :

- Le respect des contraintes d'environnement,
- La mise en œuvre des câbles,
- La fixation des éléments (baies, panneaux, prises, modules, supports, etc.),
- La mise à la terre des éléments,
- L'installation des éléments actifs,
- L'étiquetage et le repérage des différents éléments,
- L'aspect esthétique,
- Le rebouchage.

10.1.2. LE CONTRÔLE FONCTIONNEL

Le contrôle fonctionnel portera sur le comportement du système installé et plus particulièrement sur son aptitude à supporter les applications telles que définies dans le présent document. Pour ce qui concerne le câblage, ce contrôle comprendra notamment, pour chaque liaison permanente (permanent link), la mesure des paramètres définis dans la norme ISO/IEC 11801 2ème édition 1er amendement.

La recette fonctionnelle comprend les tests et mesures effectués sur l'installation de manière exhaustive.

Tous ces résultats seront consignés dans le dossier de recette du pré-câblage au format

électronique de type pdf.

10.1.2.1. TESTS DES LIAISONS CUIVRE

Les tests de mesures à effectuer auront pour objet de vérifier que chaque paire est conforme d'une part, au plan d'installation, et d'autre part, à la qualité de transmission exigée.

À ce titre, le contrôle devra s'assurer pour chaque paire :

- Du raccordement correct de chaque extrémité et de la continuité de chaque paire,
- Du respect des polarités et de l'absence de court-circuit entre les conducteurs,
- De l'isolement par rapport à la terre et aux autres conducteurs,
- De l'absence de désappairage,
- De la résistance en boucle,
- De l'exactitude de son identification par rapport aux plans d'installation.

Toutes les liaisons "cuivre" devront être testées en configuration "**Permanent Link**". Ces tests devront être conformes à la norme ISO/IEC 11801 Edition 2, le câblage conforme au standard EIA/TIA-568-B.

Chaque fiche de test devra au minimum indiquer :

- La date du test,
- L'identification du lien,
- L'affectation des paires (WIRE MAP),
- La longueur des paires,
- L'impédance,
- L'affectation des paires (WIRE MAP),
- La résistance de boucle (DC LOOP RESISTANCE),
- La perte par insertion (INSERTION LOSS),
- La paradiaphonie (NEXT et PS NEXT),
- La télédiaphonie (FEXT et PS FEXT),
- Le rapport Signal/Bruit (ACR et PS ACR / ELFEXT et PS ELFEXT),
- La perte par réflexion (RETURN LOSS),
- Le délai de propagation (PROPAGATION DELAY),
- L'écart de propagation (SKEW).

En outre, la copie du certificat d'étalonnage ou la preuve d'achat (pour un appareil de moins d'un an) du testeur devra accompagner le rapport de test final.

L'ensemble de ces tests est à la charge du titulaire.

10.1.2.2. TESTS DES LIAISONS OPTIQUES

Deux mesures, dans les deux sens et à des longueurs d'ondes différentes selon le tableau ci-dessous :

	Multimode		Monomode	
Longueur d'onde (Nm)	850	1300	1310	1550
Atténuation maximum (dB/Km)	3,5	1,5	1,0	1,0

Toutes les liaisons optiques devront être testées dans les deux sens à l'aide d'un réflectomètre FO (OTDR) suivant le standard ISO/IEC 14 763-3.

Ces mesures ont pour but de s'assurer qu'aucune anomalie n'est présente sur la liaison optique :

- Défaut de raccordement,
- Atténuation élevée,
- Début de cassure ou contrainte.
- Chaque fiche de test devra au minimum indiquer :
 - La date du test,
 - L'identification du lien,
 - La longueur de la fibre,
 - L'atténuation mesurée (ainsi que les valeurs de chaque connecteur),
 - La longueur d'onde pour le test,
 - La direction dans laquelle le test a été réalisé.

L'ensemble de ces tests est à la charge du titulaire.

10.2. RECETTE DU COURANT FORT

10.2.1. LE CONTRÔLE VISUEL

On vérifiera notamment :

- Le respect des contraintes d'environnement,
- Le cheminement des câbles,
- La mise en œuvre des câbles, fixation, connexion,
- La mise à la terre des éléments,
- L'étiquetage et le repérage,
- Le rebouchage.

10.2.2. LE CONTRÔLE FONCTIONNEL

Le contrôle fonctionnel portera sur :

- Le comportement en fonctionnement normal,
- Le comportement de l'installation en mode dégradé : coupure de l'énergie et vérification de la continuité de service correspondant aux dimensionnements des onduleurs.

10.3. RECETTE DES DIFFÉRENTS SYSTÈMES

Chaque système : contrôle d'accès, intrusion, système vidéo, visiophonie, postes de travail, sera contrôlé et réceptionné indépendamment.

Toutes les exigences décrites dans le chapitre correspondant sont testées à partir d'un cahier de recette qui sera défini durant les travaux préparatoires. Le titulaire propose à l'administration le cahier de recette que l'administration fait compléter et valider.

Les contrôles sont réalisés en présence du représentant de l'administration notamment pour ce qui a trait aux performances des équipements (détecteur et caméras) qui peuvent être mesurées spécifiquement par des tests d'intrusion.

10.3.1. LE CONTRÔLE QUANTITATIF ET QUALITATIF

Chaque matériel fourni par le titulaire sera comptabilisé et ses caractéristiques comparées à l'offre initiale.

Le titulaire s'engage à ce que la solution livrée soit protégée contre les virus et les logiciels malveillants connus au jour de l'installation.

L'origine des installations, matériels ou logiciels et de leurs mises à jour doit pouvoir être garantie.

10.3.2. LE CONTRÔLE FONCTIONNEL

Le contrôle fonctionnel portera sur le comportement du système installé.

La recette fonctionnelle comprend les tests effectués sur l'installation de manière exhaustive.

Tous ces résultats seront consignés dans le dossier de recette.

La recette sera effectuée par l'administration en présence du titulaire.

Le contrôle devra donc s'assurer :

- Du bon fonctionnement des caméras intérieures et extérieures,
- Du bon fonctionnement du système de détection d'intrusion,
- De la qualité de l'image obtenue,
- Des unités de gestions et lecteurs de badge,
- Du bon paramétrage et du bon fonctionnement des logiciels de gestion du système,
- Des fonctionnalités du système et d'enregistrement/relecture des communications,
- Des fonctionnalités de visualisation et d'automatisation des ouvertures.

10.4. PROCÈS VERBAL DE RECETTE

Le procès-verbal de recette comportera le compte-rendu des contrôles visuel et fonctionnel.

Il sera composé de deux parties distinctes :

- Infrastructure,
- Systèmes de sécurisation.

La réception définitive des travaux ne sera prononcée qu'après l'exécution de l'ensemble des essais et contrôles du système de vidéo et après la fourniture d'un dossier technique complet comprenant en particulier la nomenclature des équipements, les plans de câblage et de raccordement, les notices d'exploitation et d'entretien.

Si le procès-verbal fait état de réserves motivées par des omissions ou des imperfections, le titulaire disposera d'un délai de **15 jours** à définir avec le maître d'ouvrage pour exécuter les travaux nécessaires. Passé ce délai, le maître d'ouvrage pourra se réserver le droit de faire exécuter les travaux par une autre entreprise, aux frais, risques et périls du titulaire défaillant.

10.5. LES FICHES DE RECETTE

Les fiches de recette, fournies par le titulaire et complétées par l'administration, comprennent :

- La méthodologie et les procédures de tests,
- La description des tests,
- Les procès verbaux.

Ces trois étapes sont définies en concertation avec le titulaire.

10.6. VABF

La vérification d'aptitude et de bon fonctionnement (VABF) porte sur le respect des spécifications du CCTP et des résultats des tests. La VABF sera conduite par le titulaire, un représentant de l'administration, assistée par la MOE.

La durée de la VABF est de 30 jours ouvrés à partir de la validation de la recette.

Un procès-verbal est établi par la maîtrise d'ouvrage pour la validation de la VABF, conjointement avec le titulaire, à l'issue des opérations de validation, et propose pour l'administration une décision qui mentionne selon les cas :

- La réception sans réserve valant constat d'aptitude et de bon fonctionnement,
- La réception avec réserves (ajournement),
- Le rejet.

Ce procès-verbal cosigné est transmis au pouvoir adjudicateur, qui notifie sa décision au titulaire dans un délai de **30 jours ouvrés**.

La décision d'ajournement prévoit le délai imparti au titulaire pour remédier aux dysfonctionnements constatés. À l'issue de ce délai, une nouvelle procédure de validation de la VABF sur site est mise en place. Suite à cette nouvelle procédure, si des dysfonctionnements sont constatés, il sera procédé au rejet définitif de la prestation. Dès lors, la résiliation du marché aux torts exclusifs du titulaire peut être prononcée.

La décision d'acceptation avec réserves fixe le délai de levée des réserves. À cette issue, il sera procédé à de nouvelles vérifications. Il sera alors établi un procès-verbal de levée de réserves. Le constat d'aptitude et de conformité technique est dès lors réputé acquis à la date de l'établissement du premier procès-verbal.

10.7. VSR

La période de vérification de service régulier (VSR) est d'une durée de 60 jours ouvrés à compter de la date de réception de la VABF; elle est reconductible une fois, en cas d'ajournement. Elle est destinée à vérifier le bon fonctionnement des systèmes de sécurité dans les conditions d'exploitation définies par l'administration, avec la qualité de service définie dans le CCTP.

En cas de dysfonctionnement, l'administration peut être amenée à prononcer des réserves. Le titulaire doit remédier à ces problèmes dans un délai de 15 jours ouvrés. Un procès-verbal de vérification de service régulier est établi à l'issue de cette période de VSR, après correction des éventuels dysfonctionnements, et fourniture de l'ensemble des livrables.

À l'issue, en cas de dysfonctionnements toujours constatés, l'ajournement de l'admission peut être prononcé, avec mise en demeure de les corriger. En cas de carence du titulaire dans les délais impartis, il est procédé au rejet définitif de la solution. Le rejet n'est prononcé par l'administration qu'après constat contradictoire de ces dysfonctionnements. La résiliation du marché aux torts exclusifs du titulaire, ou la mise en régie aux frais et risques de ce dernier, peut dès lors être prononcée.

En tout état de cause, la réception définitive n'est effective qu'après constat de la livraison de l'ensemble des documents requis. Elle fait l'objet d'une décision expresse de l'administration, qui intervient au plus tard dans le délai de 15 jours ouvrés à compter du constat de levée de réserves ou de levée des motifs d'ajournement prononcés dans le cadre de cette VSR. Elle est ensuite notifiée au titulaire.

10.8. RÉCEPTION DÉFINITIVE

La réception définitive de la solution n'est prononcée qu'après remise des documents permettant la prise en charge des installations par le Maître d'Ouvrage et au terme de la VSR.

Dans le cas où le Maître d'Ouvrage serait amené à prendre possession des installations sans la remise de ces documents, les installations sont exploitées suivant les instructions de l'entreprise et sous sa responsabilité, sans que cette dernière puisse prétendre à indemnisation.

11. GARANTIE

11.1. MODALITÉS

Le service demandeur doit préciser les actions à exécuter lors de la maintenance face à chaque type ou cas de panne.

La garantie débute à compter de la réception définitive de l'installation.

Elle comprend l'échange de pièces, la main d'œuvre et les déplacements, à l'exception des disques durs qui font l'objet d'un cas particulier.

Les disques durs remplacés ne peuvent en aucun cas quitter le périmètre du site et sont remis à un représentant du client (contre décharge si besoin). Aucune donnée ne peut être dupliquée sur tout support hors du site.

Durant la période de garantie, le titulaire s'engage à remplacer à l'identique, à réparer ou à modifier toutes les pièces ou éléments reconnus défectueux. Il doit corriger les erreurs constatées au sein des logiciels fournis.

Les modalités d'accès à la maintenance seront mises en place par le titulaire qui fournira la procédure de signalisation des dérangements.

Les incidents seront enregistrés sous forme de tickets numérotés qui indiqueront :

- L'identité et la localisation du demandeur,
- Le descriptif précis du dérangement,
- La date et l'heure de signalisation.

La télémaintenance est proscrite, si la résolution de l'incident n'est pas possible d'une manière simple et rapide par assistance téléphonique, le dépannage devra se faire par déplacement d'un technicien.

11.2. INTERVENTIONS PENDANT LA PÉRIODE DE GARANTIE

11.2.1. DÉFINITION DE LA GRAVITÉ DE L'INCIDENT

Deux niveaux de gravité d'incident sont définis :

1. Panne urgente:

Une panne urgente correspond à une panne rendant le système complètement inexploitable.

2. Panne non urgente:

Toutes les autres pannes sont considérées comme non urgentes.

11.2.2. GARANTIES DE TEMPS DE RÉTABLISSEMENT (GTR)

Panne urgente (option 1):

Elle devra être réparée dans les 4 heures suivant la signalisation de l'incident en heures ouvrables 5 jours sur 7 (du lundi au vendredi).

Panne urgente (option 2) :

Elle devra être réparée dans les 24 heures suivant la signalisation de l'incident en heures ouvrables 5 jours sur 7 (du lundi au vendredi).

Panne non urgente :

Elle devra être réparée dans les 48 heures suivant la signalisation de l'incident en heures ouvrables 5 jours sur 7 (du lundi au vendredi).

Le début de la période prise en compte dans le cadre des garanties de rétablissement correspond aux date et heure de signalisation d'incident (ticket horodaté).

11.3. MISES À JOUR

Pendant la période de garantie, les mises à jour préconisées par le constructeur ou permettant de corriger une anomalie pourront être installées après accord préalable de l'administration.

Une procédure de mise à jour sera définie pour maintenir le service opérationnel (définition d'un plan de repli pendant la mise à jour, choix d'un moment propice dans la journée).

11.4. INTERVENTIONS APRÈS LA PÉRIODE DE GARANTIE

En plus de renseigner le CRT onglet 11.GARANTIE & MAINTENANCE, **le titulaire fournira un contrat type de maintenance pour une mise à jour logicielle majeure annuelle détaillé et chiffré basé sur les éléments du système déployé.**

12. ANNEXES

Le présent CCTP est complété par une description détaillée sous forme d'annexes qui serviront à l'établissement de la proposition financière et technique, notamment par des plans de l'existant en matière de protection des bâtiments. Tout ou partie des annexes sera fournie en fonction du périmètre de la prestation demandée dans le présent CCTP.

ATTENTION !

Les annexes ci-après et celles fournies en pièces jointes font partie intégrante de ce CCTP.

A ce titre, leurs prescriptions sont à appliquer, en fonction du périmètre de la prestation demandée, aussi bien pour l'établissement de la proposition financière et technique, que lors de la réalisation des travaux.

13. ANNEXE 1 : PRINCIPES CÂBLAGE ÉQUIPEMENTS RACCORDEMENT

ANNEXE 1 – CCTP SÛRETÉ SGAMI DSIC_PRINCIPES CÂBLAGE ÉQUIPEMENTS RACCORDEMENT

14. ANNEXE 2 : CONTRÔLE D'ACCÈS

ANNEXE 2 – CCTP SÛRETÉ SGAMI DSIC_PRINCIPES CONTRÔLE ACCÈS

15. ANNEXE 3 : NORMES ET RÉGLEMENTATIONS

ANNEXE 3 – CCTP SÛRETÉ SGAMI DSIC_NORMES ET RÉGLEMENTATIONS APPLICABLES

Cette annexe présente les textes et réglementation en vigueur dans le cadre de la sécurisation des sites et vient en complément du CCTP.

Les prestations, services, matériels et installations doivent être conformes aux normes, règlements et décrets (éditions en vigueur à la date de signature du marché) et respecteront les règles de l'art applicables dans leur dernière édition complétées de leurs additifs.

Les documents de référence sont des documents pouvant être utilement consultés pour élaborer les offres et projets de contrat ainsi que pour l'exécution du contrat.

Pour chaque paragraphe de l'annexe 3, mis à part la hiérarchie des textes législatifs et réglementaire qui s'applique, les références sont citées dans leur ordre hiérarchique. En cas de contradiction, les premières références citées l'emportent sur les suivantes.

D'une manière générale, le titulaire du contrat doit respecter l'ensemble des textes réglementaires – lois, décrets, arrêtés, circulaires – et para-réglementaires – normes, document technique unifié (DTU), avis techniques et solutions techniques.

Le soumissionnaire est tenu d'informer l'administration de toute discordance entre le CCTP et les règles énoncées ou non dans cette annexe, ainsi que de toutes les questions qui pourraient être une source de litige par la suite.

16. ANNEXE 4 : DÉTECTION INTRUSION

ANNEXE 4 – CCTP SÛRETÉ SGAMI DSIC_PRINCIPES DÉTECTION INTRUSION

17. ANNEXE 5 : PRINCIPE D'EXPLOITATION

ANNEXE 5 – CCTP SÛRETÉ SGAMI DSIC_PRINCIPES D'EXPLOITATION

18. PLANS

Ils récapitulent les types et emplacements des périphériques relatifs au projet. Ils seront remis lors de la visite sur site, s'ils ont été établis (en fonction de la complexité du projet).

19. SYNOPTIQUES DU PROJET

Ils explicitent de manière graphique le fonctionnement, les types et emplacements des périphériques

relatifs au projet. Ils seront remis lors de la visite sur site, s'ils ont été établis (en fonction de la complexité du projet).

20. CADRE DE RÉPONSE TECHNIQUE

Le Cadre de Réponse Technique (CRT) est à remplir obligatoirement et vient en complément de la réponse au CCTP.

Fichier de référence :

CRT-Préfecture_TULLE-Intrusion.ods

21. DÉCOMPOSITION DU PRIX GLOBAL ET FORFAITAIRE

La Décomposition du Prix Global et Forfaitaire est à remplir obligatoirement et vient en complément de la réponse au CCTP.

Fichier de référence :

DPGF-Préfecture_TULLE-Intrusion.ods