

ETAT - MINISTÈRE DES ARMÉES

ETABLISSEMENT DU SERVICE INFRASTRUCTURE DE LA DEFENSE DE LYON

DIVISION INVESTISSEMENT

POLE Montauban



**Extension de la capacité du chenil du CPIS
à Saint-Laurent de la Salanque**



COSI n° 460 431

Annexe de tous les lots :

« Electricité Cfo et Cfa, sureté, sonorisation et sécurité incendie »

Objet :

CYBERSECURITE DES SYSTEMES DE SURETE ET DE GTC

	Architecture des systèmes de sécurité (GTC- VIDEOSURVEILLANCE)	Juin 2024

Nombre de pages : 32

Edition du : 9 juillet 2024

Contenu

1	INTRODUCTION	5
1.1	OBJET DU DOCUMENT.....	5
1.2	BESOIN EN VIDEOSURVEILLANCE.....	5
1.3	BESOIN EN GESTION TECHNIQUE DES PV (GTC)	6
1.4	MOTS DE PASSE DES SYSTEMES VIDEO ET GTC.....	6
1.5	REMARQUES	7
1.6	ECHANGES ET MESSAGERIE ELECTRONIQUE	7
2	EXIGENCES APPLICABLES EN MATIERE DE CYBERSECURITE.....	8
2.1	RESPECT DES RECOMMANDATIONS ANSSI.....	8
2.2	INSTALLATION DES SYSTEMES	8
2.2.1	Stabilisation de l'exploitation	8
2.2.2	Compétences des intervenants	9
2.2.3	Certification des Editeurs de logiciel	10
2.3	ORGANISATION.....	10
2.4	PROPRIETE INTELLECTUELLE	10
2.5	DEVELOPPEMENT / INTEGRATION	11
2.5.1	Vidéosurveillance	11
2.5.2	La Gestion Technique Centralisée	11
2.5.3	Fiches Produits : à fournir en amont !.....	11
2.5.4	Développement – paramétrage - Intégration	12
2.6	TRAÇABILITE ET LIVRAISON.....	12
2.7	VEILLE.....	13
2.8	EXIGENCES RELATIVES AUX OUTILS ET A L'ENVIRONNEMENT DE DEVELOPPEMENT	13
2.9	INTERVENTION ET MISE EN OEUVRE	13
2.9.1	Moyens utilisés lors de la mise en œuvre	14
3	PERIMETRE TECHNIQUE	15
3.1	PRESTATIONS ATTENDUES.....	15
3.1.1	Normes et règlements applicables.....	16
3.2	L'ARCHITECTURE RESEAU.....	17
3.2.1	La matrice des flux.....	17

3.2.2	Internet.....	17
3.2.3	Interfaçage autres systèmes	17
3.2.4	Les switchs ou commutateurs réseau	17
3.2.5	Détail de la prestation	18
3.3	REPORTS DES ALARMES ET GESTION DE CONFIGURATION.....	19
3.3.1	Borniers d’interconnexion et de prise d’informations alarmes	19
3.3.2	Pré Requis au déroulement des reports d’alarmes (principe commun GTC/VMS)	19
3.3.3	Tests unitaires	19
3.3.4	Essais transverses	20
3.3.5	Livrables attendus	21
3.4	LA FORMATION : VMS + GTC.....	21
4	DOCUMENTS A FOURNIR PAR LE TITULAIRE DU MARCHE.....	22
4.1	ECHANGES D’INFORMATIONS PAR RESEAU INFORMATIQUE	22
4.2	FOURNITURE DES FICHES TECHNIQUES.....	22
5	RECEPTION DES PRESTATIONS	25
6	ASSURANCE QUALITE	26
6.1	SYSTEME QUALITE	26
7	VERIFICATION DES INSTALLATIONS, ESSAIS ET MESURES.....	28
8	NETTOYAGE ET PROTECTION DES OUVRAGES	29
8.1	TRI ET EVACUATION DES DECHETS	29
9	DOCUMENTS APPLICABLES ET DOCUMENTS DE REFERENCE	30
9.1	DOCUMENTS TECHNIQUES APPLICABLES AU MARCHE	30
9.2	LIVRABLES ATTENDUS.....	30
10	ANNEXE 1 : MATRICE DE COMPETENCES	31
11	ANNEXE 2 : TAUX HORAIRES	32

1 INTRODUCTION

1.1 OBJET DU DOCUMENT



Le présent document est une annexe au programme globale d'extension de la capacité du chenil du CPIS à Saint-Laurent de la Salanque. Il précise les règles de cybersécurité à mettre en œuvre dans le cas de fourniture et pose de systèmes informatiques : ordinateurs (PC, Serveur) et Réseau IP. C'est la raison pour laquelle il porte sur tous les lots et en particulier, sur la vidéosurveillance et la GTC.

1.2 BESOIN EN VIDEOSURVEILLANCE

La vidéosurveillance à mettre en œuvre concerne 2 systèmes vidéo :

1. une caméra en adjonction au système existant (Geutebruck)
2. Une création complète (serveur et caméra) autonome, de marque Geutebruck également, pour anticiper un besoin non exprimé à ce jour, de mise en relation avec l'ancien système.
3. Un déport vidéo à l'entrée du site (environ 250m)

Le système vidéo existant est de la marque GEUTEBRUCK, le logiciel d'exploitation vidéo est G-SIM.

S'agissant d'une adjonction à l'existant, les marques et types de matériel décrits ci-dessous sont à respecter. Le titulaire devra fournir, installer et paramétrer :

- Une caméra cylindrique AXIS Q1806-LE **Bullet Camera**
- Coffret mural en kit nid d'abeille 12U 600*600*635mm ligne 100 SOCAMONT **REF : 11266KSA** ;
- Panneau de brassage FTP SOCAMONT, 16 ports **REF : 71108** ;
- Connecteur RJ45 Jack Coccinelle One Pouce Keystone CAT 6A FTP **REF : 71009** ;
- Bandeau PDU 19 pouces 1U, 9 prises FR avec voyant **REF : 71639** ;
- Tablette fixe, prof. Coffret 600 **REF : 71107** ;
- Tiroir optique noir 1U multimode om4 équipé 6 raccords SC EKIVALAN **REF : TOLCOM4-06** ;
- Câble 6 fibres multimode om4 50/125 extérieur structure libre uni tube acier PEHD GGM FO6B4CST GIGAMEDIA **REF : GGM FO6B4CST** ;
- Câble 4 paires Catégorie 6F/UTP Résistant UVPE noir GIGAMEDIA **REF : GGM C6F4PPET3** ;

Ajout sur système existant :

Une caméra doit être installée sein du « local soin » du Bâtiment 0030. Cette caméra doit être reliée au système existant (G-SIM) afin de garder un visuel depuis le poste de contrôle sur les chiens en convalescence.

La mise à jour du système G-SIM sera fournie par le titulaire sur support de masse validé par le Maître d'ouvrage (ex : clé USB), mais son installation sera effectuée par le maître d'ouvrage.

Création nouveau système :

La seconde caméra, type fish eye, doit être installée au sein de la grande pièce du bâtiment ARDE, reportée au local préparation du même bâtiment afin d'avoir un visuel lors de l'exercice.

Ce système devra être de même marque que l'existant, mais totalement indépendant, sans connexion ou mode commun avec le système existant, une liaison optique d'un seul tenant transportera le flux vidéo afin de pallier les risques liés à la cybersécurité.

1.3 BESOIN EN GESTION TECHNIQUE DES PV (GTC)

Le système d'utilisation d'énergie photovoltaïque (GTC), devra également respecter les règles de cybersécurité décrites ci-dessous, pour toute fourniture de système de gestion informatique de l'énergie obtenue par les PV.

1.4 MOTS DE PASSE DES SYSTEMES VIDEO ET GTC

Les actions menées sur ces systèmes devront être validées par le MOA, au préalable de toute action.

Les mots de passe « administrateur » restent propriété du MOA.

Les mots de passe utilisés pour l'installation du marché devront faire l'objet d'une « Cérémonie des clés », moment lors duquel tous les mots de passe utilisés par le titulaire du marché pendant l'installation seront remplacés par les mots de passe privés du MOA, avec l'aide du Titulaire.

1.5 REMARQUES

Les règles de cybersécurité annoncées sont applicables sur tout système informatique prévu au titre de ce marché, quelque soit son lot d'origine

Ces installations sont liées au domaine technique et aux servitudes des bâtiments concernés par les travaux. Elles sont totalement indépendantes des prestations décrites pour l'usage de l'informatique des usagers du bâtiment (DIRISI – FR-OPS – INTRACED, etc)

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

R1 : les locaux techniques décrits par la DIRISI sont à l'usage exclusif de la DIRISI. Les systèmes liés aux solutions techniques installées au titre du projet, devront être installés dans des locaux indépendants des LTI dédiés à la DIRISI.

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

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

1.6 ECHANGES ET MESSAGERIE ELECTRONIQUE

Tous les plans et documents portant des informations de configurations ou autre plan de situation ou de câblage devront être envoyés sous conteneur crypté, si la messagerie électronique est utilisée.

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

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

2 EXIGENCES APPLICABLES EN MATIERE DE CYBERSECURITE

Les exigences s'appliquent, de manière générique, à tous les systèmes de gestion inclus au programme Extension de la capacité du chenil du CPIS.

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

2.1 RESPECT DES RECOMMANDATIONS ANSSI

Pour mémoire, le système d'information concerné (Vidéosurveillance) est un système d'information d'importance vitale (au sens des articles L.1332-1 et L.1332-2 du code de la défense), de fait les règles de sécurité applicables sont réglementairement définies dans l'arrêté du 8 septembre 2017 (NOR : PRMD1722149A) ;

Le système d'information concerné appartient à une administration de l'Etat, auquel cas il doit aussi respecter la PSSIE (circulaire du Premier ministre n° 5725/SG du 17 juillet 2014.), notamment ses objectifs 8 et 9 ;

Dans tous les cas, le minimum attendu est la mise en œuvre des mesures recensées dans les guides et notes techniques de l'ANSSI.

2.2 INSTALLATION DES SYSTEMES

RAPPEL :

Le système de vidéosurveillance à installer au titre de ce marché est une évolution du système existant sur le site (Geutebruck), ainsi que l'installation d'un nouveau. Aucun lien informatique, ou réseau, qu'il soit logique ou physique ne doit être effectué avec un autre système (GTC ou incendie ou autre) au titre du présent marché.

Cette installation devra faire l'objet d'une description détaillée dans le livrable que devra fournir l'entreprise : « Spécifications techniques et fonctionnelles détaillées » CF chapitre [9.2 Livrables attendus](#).

2.2.1 Stabilisation de l'exploitation

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

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

Deux niveaux de gravité sont à prendre en compte : panne bloquante et fonctionnement altéré.

- En cas de panne bloquante, une intervention à J+1 sera à effectuer.
- En cas d'altération du fonctionnement, une intervention sous 48h sera à prévoir.

Les délais seront validés au cas par cas, par le MOA.

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

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

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

Ces prestations comprennent :

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

2.2.2 Compétences des intervenants

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

- Automaticien : GTC / Panneau-photovoltaïques
- Electricien
- Spécialiste de la sureté, et tout autre nécessaire à la réalisation de cette opération.

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

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

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

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

2.2.3 Certification des Editeurs de logiciel

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

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

2.3 ORGANISATION

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

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

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

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

2.4 PROPRIETE INTELLECTUELLE

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

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

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

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

2.5 DEVELOPPEMENT / INTEGRATION

S'agissant d'un site en exploitation, il est indispensable que toute intervention soit parfaitement maîtrisée et coordonnées pour ne pas entraîner de rupture dans l'exploitation du système et affaiblir la sécurisation de l'emprise.

2.5.1 Vidéosurveillance

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

Une prestation d'extension et de mise à jour (selon la date d'installation) du cœur de système doit être prévue. Comme précisé plus haut, aucune dégradation de fonctionnement ne sera tolérée, une procédure de non-régression sera donc à fournir au préalable de toute action.

S'agissant d'un système neuf et dédié à la vidéosurveillance, ainsi que la mise à jour du système existant à l'identique, le titulaire devra le cœur de réseau, le cœur de système, l'application centralisée et toutes les servitudes associées

2.5.2 La Gestion Technique Centralisée

Les règles de cybersécurité et de gestion sont identiques à celles décrites plus haut pour la vidéosurveillance.

S'agissant d'un système neuf et dédié à la gestion des panneaux photovoltaïques, le titulaire devra le cœur de réseau, le cœur de système, l'application centralisée et toutes les servitudes associées.

2.5.3 Fiches Produits : à fournir en amont !

En amont de tout approvisionnement (et à fortiori, d'installation), le titulaire doit soumettre à la validation du MOE la liste et les caractéristiques de l'ensemble des équipements qu'il souhaite installer sur le site.

Une « fiche produit » type (une page A4) sera fournie pour description des matériels. Ces « fiches produits », rédigées en français, accompagnées de la fiche technique du fabricant, feront l'objet d'une liste et intégrées au DOE.

2.5.4 Développement – paramétrage - Intégration

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

Le titulaire doit prévoir la création de comptes personnels et nominatifs pour accéder au système. Ils devront être associés à des droits spécifiques (Entreprise, Administrateur, Utilisateur, autre...) pour permettre la traçabilité des actions sur les logiciels qu'il installe (VS, CA, DI, GTC, SSI etc).

Le titulaire devra également respecter la gestion des comptes utilisateur installée, ou la faire évoluer vers les contraintes suivantes (**si le maître d'ouvrage en fait la demande**) :

- verrouillage après 3 tentatives infructueuses.
- Les mots de passe devront être complexes (14 caractères pour les administrateurs : majuscules, minuscules, chiffres, caractères spéciaux)
- et changés tous les 90 jours, au plus tard.

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

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

Tous les mots de passe d'origine, de tous les outils de gestion, des systèmes et des équipements industriels, doivent être changés au profit de nouveaux. Ceux-ci seront fournis au MOA sous enveloppe cachetée à la réception du marché.

2.6 TRAÇABILITE ET LIVRAISON

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

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

2.7 VEILLE

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

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

Le jour de la réception du marché, tous les logiciel et firmware de tous les systèmes doivent être à jour de la dernière version en vigueur, l'antivirus et ses banques de données, à jour et fonctionnelles.

2.8 EXIGENCES RELATIVES AUX OUTILS ET A L'ENVIRONNEMENT DE DEVELOPPEMENT

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

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

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

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

2.9 INTERVENTION ET MISE EN OEUVRE

Les prestations effectuées dans l'emprise devront être organisées et ceci pour tous les intervenants réalisant des activités de mise en service (Titulaire, sous-traitants, etc) au titre de ce marché.

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

2.9.1 Moyens utilisés lors de la mise en œuvre

Les interventions sur l'installation des équipements dédiés au système de sureté ou à la GTC doivent être réalisées avec des outils validés.

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

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

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

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

Les coordonnées du point de contact au niveau de l'ESID seront transmises au titulaire, en début de marché.

3 PERIMETRE TECHNIQUE

Compte-tenu des installations, il est important de respecter la notion de cyber sécurité par profil d'équipement.

- Les installations dédiées à la sûreté (détection intrusion, vidéosurveillance),
- Les équipements dédiés à tous les autres systèmes, tels que la GTC, le système de sécurité incendie, et tous systèmes fonctionnant sur le réseau Ethernet (informatique en général)
- L'architecture réseau filaire et système à mettre en œuvre
- L'administration centralisée des systèmes et des utilisateurs

3.1 PRESTATIONS ATTENDUES

Fourniture et installation de :

- une caméra en adjonction au système existant (Geutebruck)
- Une création complète (serveur et caméra) autonome de marque Geutebruck également pour anticiper un besoin non exprimé à ce jour, de mise en relation avec l'ancien système.
- Un déport vidéo à l'entrée du site (environ 250m)

Le système vidéo existant est de la marque GEUTEBRUCK, le logiciel d'exploitation vidéo est G-SIM.

S'agissant d'une adjonction à l'existant, les marques et types de matériel décrits ci-dessous sont à respecter. Le titulaire devra fournir, installer et paramétrer :

- Une caméra cylindrique AXIS Q1806-LE **Bullet Camera**
- Coffret mural en kit nid d'abeille 12U 600*600*635mm ligne 100 SOCAMONT REF : **11266KSA** ;
- Panneau de brassage FTP SOCAMONT, 16 ports REF : **71108** ;
- Connecteur RJ45 Jack Coccinelle One Pouce Keystone CAT 6A FTP REF : **71009** ;
- Bandeau PDU 19 pouces 1U, 9 prises FR avec voyant REF : **71639** ;
- Tablette fixe, prof. Coffret 600 REF : **71107** ;
- Tiroir optique noir 1U multimode om4 équipé 6 raccords SC EKIVALAN REF : **TOLCOM4-06** ;
- Câble 6 fibres multimode om4 50/125 extérieur structure libre uni tube acier PEHD GGM FO6B4CST GIGAMEDIA REF : **GGM FO6B4CST** ;
- Câble 4 paires Catégorie 6F/UTP Résistant UVPE noir GIGAMEDIA REF : **GGM C6F4PPET3** ;

3.1.1 Normes et règlements applicables

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

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

- **norme NF C15.100** : installations électriques à basse tension,
- **norme C18.510** : installations courants faibles et forts,
- **norme NF C63.410** : ensembles d'appareillages basse tension montés en usine,
- **norme NF C91.101** : perturbations radioélectriques et systèmes d'antiparasitage, textes officiels concernant le matériel alimenté en réseau de première catégorie et dont le rayonnement direct est faible,
- **norme NF C91.104** : perturbations radioélectriques et systèmes d'antiparasitage et textes officiels concernant les appareils servant aux réceptions individuelles ou collectives des émissions et radiodiffusion sonore ou visuelle,
- **norme NF C92.130** : appareils électroniques et appareils associés à usage domestique ou à usage général analogue, reliés à un réseau de règles de sécurité.
- **norme NF P25.362** : fermetures pour baies libres et portails, Spécifications techniques, Règles de sécurité,
- **norme C32.321** : conformité des câbles de distribution basse tension,
- **norme C32.201** : conformité du conducteur de protection,
- **norme C32.310** : conformité des câbles basse tension résistant au feu,
- **Directive SEVESO** : comptage des personnes en zone à risque
- **Déclaration CNIL**: obligatoire pour le contrôle d'accès et la biométrie
- **Titres de transport anonymes (CNIL AU-015)** : Etanchéité des identifiants entre les applications/les services quand le titre de transport est utilisé pour le contrôle d'accès
- **RoHS** : Respect des directives européennes qui interdisent certaines matières dans les cartes, composant électroniques
- **Guide ANSSI** : « Référentiel Général de Sécurité » (RGS) du 26 janvier 2010 : conformité avec un cryptage AES128 bits minimum
- **Guide ANSSI** : « SECURITE DES TECHNOLOGIES SANS-CONTACT POUR LE CONTROLE DES ACCES PHYSIQUES » du 19/11/2012 : conformité avec ce document
- **Guide ANSSI** : « Profil de protection d'un commutateur industriel » Version 1.0 court-terme du 13 juillet 2015 : conformité sur la compatibilité des automates industrielles avec 802.1x

3.2 L'ARCHITECTURE RESEAU

L'architecture réseau, objet de ce marché, est exclusivement dédiée au système de vidéosurveillance. L'ancien système ne devra pas être modifié, seule une caméra doit être ajoutée et le VMS G-SIM mis à jour (par le MOA). Le réseau du nouveau système G-SIM sera autonome, sans aucune liaison vers un autre système.

Le système de GTC à installer devra communiquer sur des switches qui lui sont propres, indépendants de ceux de la vidéosurveillance et exclusivement dédiés GTC.

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

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

3.2.1 La matrice des flux

Elle devra être établie sur la base des exigences de cybersécurité (tout flux non autorisé est interdit).

3.2.2 Internet

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

3.2.3 Interfaçage autres systèmes

Le principe de report des alarmes en **contacts secs exclusivement** devra être utilisé, si besoin, pour permettre l'interfaçage des systèmes suivants :

- Détection incendie (si ces informations sont demandées lors de la collecte des besoins effectué par le titulaire, elles devront être intégrées au système par des contacts secs exclusivement, et en aucun cas par une liaison Ethernet (IP).
- Alarme NFA2P
- Alarmes techniques

Toutes ces informations et leur méthode et schéma de câblage devront être précisées dans le document des Spécifications Techniques et Fonctionnelles.

3.2.4 Les switches ou commutateurs réseau

Si le MOA en fait la demande, le réseau informatique de sécurité doit être étendu et les règles propagées sur les 3 réseaux : VS existante – VS nouvelle – GTC/PV.

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

Remarque :

Toutes les précautions devront être prises lors du tirage et du raccordement du câble optique. La communication devra faire l'objet de tests qui permettront de vérifier la qualification et de valider la recette de l'ouvrage.

3.2.5 Détail de la prestation

Fourniture, pose et raccordement d'un câble optique extérieur : Câble 6 fibres multimode om4 50/125 extérieur structure libre uni tube acier PEHD GGM FO6B4CST GIGAMEDIA REF : GGM FO6B4CST

Nota : Dans chaque chambre de tirage, le câble optique sera étiqueté (règle de nommage à proposer) et protégé par une gaine ICTA.

3.2.5.1 *Les Têtes optiques : soudées*

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

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

- le respect des rayons de courbure des fibres et des câbles
- un passage des fibres limitant tout risque de cassures, de macros ou micro-courbures postérieures à l'installation
- une identification des différentes connexions et des différentes fibres afin de faciliter l'utilisation et l'évolution du réseau
- des valeurs de soudures et de composants (pigtaills, raccords) respectant le budget optique

3.2.5.1.1 La soudure fibre optique ou épissurage par fusion

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

Cette prestation exige la méthodologie et la compétence nécessaires afin de les pertes associées. Le cahier de recette des brins optiques doit être fourni **AVANT** mis en œuvre de la solution de vidéosurveillance, pour exclure les fausses pannes VMS.

Après la pose du câble optique :

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

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

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

3.3 REPORTS DES ALARMES ET GESTION DE CONFIGURATION

3.3.1 Borniers d'interconnexion et de prise d'informations alarmes

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

Ces modules seront dédiés aux alarmes techniques ainsi que quelques contacts secs directs. Ils seront installés dans des coffrets auto-protégés (contacts d'ouverture).

3.3.2 Pré Requis au déroulement des reports d'alarmes (principe commun GTC/VMS)

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

Les actions intermédiaires à valider sont les suivantes :

- la création et la gestion du carnet de brassage,
- la préparation, l'organisation et le suivi des essais de report,
- la réalisation des essais unitaires et transverses.

Deux types d'essais sont demandés :

- les essais unitaires permettant de valider les modifications et le câblage réalisés,
- les essais transverses (ou d'intégration) permettant de valider chaque alarme depuis le capteur jusqu'au poste d'exploitation de la GTC et/ou de la vidéosurveillance.

3.3.3 Tests unitaires

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

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

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

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

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

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

3.3.4 Essais transverses

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

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

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

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

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

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

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

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

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

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

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

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

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

3.3.5 Livrables attendus

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

3.4 LA FORMATION : VMS + GTC

Le titulaire établit un plan de formation afin de permettre le transfert de compétences et la formation complète aux systèmes installés au terme de la prestation de l'installation de tous les systèmes.

Pour le logiciel de vidéo surveillance, s'agissant de la fourniture d'une mise à jour de version, qui sera effectuée par le MOA, le transfert de compétence, s'il est toutefois nécessaire, pourra être concentré sur une heure ou deux (la durée doit être argumentée par le candidat).

Pour la partie gestion des panneaux photovoltaïque, la formation est estimée comme suit :

Formation Administrateur/Utilisateur : 1 session de deux personnes - 1 jour

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

- Plan de formation
- Manuel de formation
- Dossier système

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

4 DOCUMENTS A FOURNIR PAR LE TITULAIRE DU MARCHÉ

4.1 ECHANGES D'INFORMATIONS PAR RESEAU INFORMATIQUE

La transmission des documents avec le Maître d'Œuvre, se fera uniquement par voie postale, aucun document technique ou plan ne devra transiter par la messagerie.

- mettre à jour les plans de liaisons
- créer des schémas de raccordement des armoires automates déportés sous format Microstation

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

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

Ils seront rédigés exclusivement en français.

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

PENDANT LA PERIODE DE PREPARATION

- Le planning d'intervention ;
- Le planning d'approvisionnement et de délais de fabrication. Ce planning comporte le délai entre l'approbation des plans et des matériaux et leur arrivée sur le site.
- Le planning des tâches en y incorporant les essais et la mise en service provisoire de réception des installations et de levée des réserves.
- Les décompositions et sous détails de prix ;
- Le plan de prévention,
- Le Dossier d'Assurance Qualité
- Le plan de Management Qualité
- Le plan Qualité Logiciel
- La liste prévisionnelle des documents et plans

4.2 FOURNITURE DES FICHES TECHNIQUES

Avant travaux :

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

Au fur et à mesure de la réalisation :

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

APRES ACHEVEMENT DES TRAVAUX

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

- Les plans de recollement ;
 - Plans mis à jour
 - Plans des constructeurs ;
- Procès-verbaux des essais réalisés ;
- Code constructeur.
- Notices d'entretien des matériels ;
- Recettes des matériels ;
- Rapports des mesures.
- les fiches de contrôles et essais,
- Document des spécifications techniques et fonctionnelles : en Word et PDF.

Le Dossier des Ouvrages Exécutés (DOE) suivant un reproductible, trois tirages et une clé USB de l'ensemble du dossier

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

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

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

Cette liste n'est pas exhaustive.

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

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

5 RECEPTION DES PRESTATIONS

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

Ces cahiers seront principalement constitués :

- des fiches de tests unitaires et des fiches d'essais transverses,
- des fiches de réception des modifications matérielles et logicielles des équipements existants,
- des carnets de câbles validés,
- des schémas de câblage des armoires ou coffrets modifiés.

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

6 ASSURANCE QUALITE

6.1 SYSTEME QUALITE

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

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

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

Ce système qualité comprend :

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

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

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

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

Cette organisation devra être décrite dans le PAQ du titulaire.

7 VERIFICATION DES INSTALLATIONS, ESSAIS ET MESURES

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

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

8 NETTOYAGE ET PROTECTION DES OUVRAGES

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

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

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

8.1 TRI ET EVACUATION DES DECHETS

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

9 DOCUMENTS APPLICABLES ET DOCUMENTS DE REFERENCE

9.1 DOCUMENTS TECHNIQUES APPLICABLES AU MARCHÉ

- Le présent programme ;
- Les DTU et les normes en vigueur ;
- Le Code Civil ;
- Le Code du Travail ;
- Les documents cités dans cette section.

9.2 LIVRABLES ATTENDUS

Le prestataire devra fournir

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

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

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

Le prestataire devra fournir

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

Le prestataire devra fournir

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

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

10 ANNEXE 1 : MATRICE DE COMPETENCES

Le fichier Excel
est fourni pour
faciliter la saisie
des
informations.

13/07/2024					
MATRICE DES COMPETENCES TECHNIQUES et SYSTEMES					
Compétences	Nb total intervenants	Profil 1 Expert	Profil 2 Ingénieur	Profil 3 Technicien	Profil 4 Débutant
Gestion de projet					
Suivi et gestion de projet					
Sécurité organisationnelle					
Gestion des risques					
Audit Organisationnel					
Audit LPM					
Conseil et gouvernance					
Matériel réseaux :					
Alcatel					
Hirschmann					
Scalance					
HP					
Cisco					
Moxa					
Dlink					
Checkpoint, Fortinet					
Solutions CA-DI-VS					
TIL-TECHNOLOGIE					
NEDAP					
SYNCHRONIC					
GUINNEBO					
CASTEL					
STENTOFON					
TRAKA					
autres					
ajoutez toutes marques présentées dans votre réponse					
SOLUTION DE VIDEOSURVEILLANCE (Systèmes et marques)					
GENETEC					
MILESTONE					
BOSCH					
AXIS					
GUINNEBO					
GEUTEBRUCK					
SAMSUNG					
autres					
ajoutez toutes marques présentées dans votre réponse					
Administration Windows :					
Windows 7					
Win US					
Windows Server 2008					
Windows Server 2012 R2					
Windows Server 2019 / 22					
Expertise Linux et systèmes UNIX					
Réseau Informatique					
Certification du constructeur proposé					
Fonctions avancées (802.1Q, 802.1X, VLAN Trunking Protocol,...)					
...					
Informatique Industrielle : GTC/GTB					
VxWorks					
PC industriels, contrôle-commande					
Superviseur industriel PANORAMA E2 et P2					
PC Vue					
Rétro ingénierie de protocole					
Fuzzing de protocole					
Bureautique :					
MS/office (Word, Excel, Powerpoint, Access, project)					
...					
Développement :					
Scripts système					
C, Python, C++, Go, Git					
CFI-CFS :					
Courants Faibles Industriels et de sécurité					
Ces compétences et profils sont donnés ici à titre d'exemple seulement. Le candidat pourra ajouter, modifier selon son besoin. En revanche, chaque logiciel ou matériel proposé par le candidat devra être intégré dans cette matrice de compétences.					

11 ANNEXE 2 : TAUX HORAIRES

Le fichier Excel est fourni pour faciliter la saisie des informations

TAUX HORAIRES ET COEFFICIENT DE PEINES ET SOINS APPLICABLES

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

Coefficient de peines et soins

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

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

FIN DU DOCUMENT