Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRÉFET DE LA ZONE DE DÉFENSE ET DE SÉCURITÉ SUD

PRÉFET
DE LA ZONE
DE DÉFENSE
ET DE SÉCURITÉ
SUD

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

ANNEXE 3 : Principes concernant le système de détection d'intrusion. 2020

Les principes de déploiement des équipements ci-dessous servent de référence aux particularités du site décrites dans le document principal

CCTP SURETE – DESCRIPTIF DU PROJET

TABLE DES MATIÈRES

1. Généralités....3
2. Architecture....3
3. CENTRALE DE GESTION....4
4. Appareillage de mise en et hors Service....4
4.1. Claviers....5
4.2. Commande asservie par contrôle d'accès....5
4.3. Commande par le logiciel de supervision....5
4.4. Commande automatique....5
5. Détection de l'intrusion....5
5.1. Câble coaxial de détection....6
5.2. Câble de détection de chocs....6
5.3. Barrière de détection infrarouge (BIR)....7
5.4. Barrière de détection Hyper-fréquence....7
5.5. Détection par vidéo analytique....8
5.6. Détecteur de présence....9
5.7. Détecteurs de choc, bris de vitre ou de vibration....9
5.8. Détecteurs d'ouverture....9
5.9. Commandes manuelles anti-agression....10
6. Sécurité....10
7. Traitement de L'information....10
7.1. Signalisation....10
7.1.1. Sirènes (extérieure – intérieure)....11
7.1.2. Transmetteur téléphonique....11
7.1.3. Télétransmission Ramsès....11
8. Règles de sécurité....11
8.1. Intégration de l'antivirus....12
8.2. Synchronisation de l'heure....12
8.3. Logiciels et firmwares....12
8.4. Journalisation....12

1. GÉNÉRALITÉS

Dans le cadre de la surveillance du site et des locaux sensibles, et afin de lutter contre la malveillance, le système de détection d'intrusion proposé sera conforme aux règles du référentiel technique d'installation **APSAD R81.**

Une installation d'alarme se compose d'un ensemble d'équipements électroniques, agencé de telle sorte qu'après mise en service du dispositif, la tentative ou l'accès aux zones surveillées sera obligatoirement détecté, et actionnera les dispositifs de signalisation.

Un système de détection d'intrusion ne peut être pleinement efficace que s'il vient compléter une protection mécanique aussi parfaite que possible.

Les qualités essentielles d'un système d'alarme reposent sur :

- La détection précoce des tentatives d'intrusion et des déplacements d'un intrus dans les zones surveillées, ainsi que les tentatives de neutralisation des matériels,
- Le déclenchement des alarmes suite à la détection,
- L'insensibilité aux phénomènes autres que ceux qu'il a pour but de détecter.

Un système de détection d'intrusion est dit « sûr », lorsqu'il remplit son rôle de façon durable, non erratique, sans erreur ou défaillance, dans les conditions d'emploi et d'installation prescrite par le constructeur.

2. ARCHITECTURE

Deux solutions sont admises :

- Soit le système de détection d'intrusion est composé d'une centrale de gestion **(NFA2P type 3)** et de coordination des points de détection et de contrôle,

- Soit les équipements de détection d'intrusion sont connectés à un système global de sûreté. Ils devront être câblés sur des interfaces entrées/sorties de ce système. Celui-ci devra disposer des entrées en nombre nécessaire et suffisant.

Dans le cas d'un système indépendant, la centrale permet la distribution par bus RS485 de tous les équipements ci-dessous :

- Claviers
- Modules d'extension
- Détecteurs (de présence, d'ouverture magnétiques, de choc ...)
- Barrières de détection (infra-rouge, hyperfréquence)
- Radars laser
- Sirènes

La programmation du système peut se faire à l'aide :

- du clavier de commande avec afficheur (code installateur)
- d'un PC sur prise USB
- d'un PC sur interface IP

Le système permettra le découpage en zones surveillées (16 minimum) activables/désactivables localement ou à distance.

Les zones doivent être programmables selon le type de déclenchement souhaité : instantané ou temporisé. Chaque zone configurée en mode temporisé peut disposer d'une temporisation d'entrée différente.

Toutes les liaisons seront filaires. Les centrales d'alarme hybrides ou radio sont proscrites, sauf spécification explicite contraire dans le document « descriptif du projet ».

3. CENTRALE DE GESTION

La centrale doit pouvoir mettre en œuvre :

- de 4 à 16 stations d'armement
- différents profils d'utilisateurs
- 40 codes d'accès modifiables
- de 8 à 32 zones de détection pouvant être mis en service indépendamment
- de 2 à 15 modules d'extension adressables

Elle sera équipée :

- d'interfaces : 5 entrées / 5 sorties sur relais avec ou sans alimentation,
- d'une interface IP permettant la transmission, la supervision, la maintenance et la sauvegarde du système.

L'adjonction de cartes optionnelles permettra d'augmenter la capacité initiale de la centrale.

La centrale doit disposer des caractéristiques de fonctionnement suivantes :

- Chaque adresse de périphérique d'entrée sera programmable individuellement,
- Les entrées se feront par boucles équilibrées,
- Les sorties se feront sur le bus,
- Des asservissements entre entrées et sorties seront programmables,
- Temporisation programmable sur les différentes sorties
- Elle disposera de timer pour certains automatismes,
- Elle aura une sortie pour liaison au système vidéo.

Un module radio 6 à 30 canaux à 868 Mhz peut être envisagé exceptionnellement sur accord de l'administration. Il sera associé aux périphériques radio : détecteur d'ouverture, de présence, de chocs et de bris de vitre, de fumée si ces équipements sont envisagés en lieu et place d'équipements de type filaires. Ce type d'appareillage n'est autorisé que dans les cas extrêmes en fonction des risques et de l'architecture des bâtiments à protéger. Ces périphériques radio doivent être adressables afin d'être identifiables.

La centrale et les boîtiers d'extension fonctionneront sur secteur 220V et seront équipés d'une batterie pour une autonomie supérieure à 8 heures. Ils seront alimentés à partir du tableau de distribution électrique désigné par l'administration, sur un circuit 220V-16A 2P+T, ondulé si existant, protégé par un disjoncteur différentiel 30mA dédié.

Le raccordement du câble 220V se fera impérativement sur le bornier interne.

La centrale est auto-protégée contre l'effraction et l'arrachement.

Les paramètres de configuration du site seront sauvegardés sur un emplacement disque désigné par l'administration. Le titulaire doit fournir également la procédure de sauvegarde.

A l'issue de l'installation, le titulaire fournira, en complément du DOE, un tableau regroupant les zones de détection, les équipements ainsi que leur adressage.

4. APPAREILLAGE DE MISE EN ET HORS SERVICE

4.1. Claviers

La mise en et hors service du système peut être opérée à partir de :

- claviers
- claviers avec écran LCD, munis de touches rétro-éclairées
- claviers plus lecteurs de badge Mifare Desfire EV1 ou supérieur
- claviers anti-vandale.

Les claviers munis d'écran permettront de consulter les informations issues de la centrale (indication sur les zones en service, historique des événements, alarmes, état de l'alimentation, défauts …).

Les claviers serviront aussi à l'activation, la désactivation de zones surveillées et l'isolement des équipements en défaut.

Ils seront auto-protégés à l'ouverture et à l'arrachement.

Le type et le nombre d'appareillage seront définis dans le document « descriptif du projet ».

4.2. Commande asservie par contrôle d'accès

Dans certains cas, la commande d'activation ou désactivation d'une zone, peut être commandée par un lecteur de badges du contrôle d'accès.

Le passage d'un badge autorisé ou badge+ code ouvre la porte et désactive les détecteurs de cette zone.

Le réarmement peut se faire par appui sur un bouton en sortie, par commande sur logiciel, ou en automatique après temporisation.

4.3. Commande par le logiciel de supervision

Les actions d'activation, de désactivation de zones surveillées et d'isolement des équipements en défaut sont également réalisables depuis le logiciel de supervision.

4.4. Commande automatique

Le système peut être activé automatiquement suivant une plage horaire définie par l'utilisateur.

Les plages de mise en service seront programmables.

5. DÉTECTION DE L'INTRUSION

Les zones à surveiller ainsi que la liste exhaustive des points de détection à mettre en place seront décrites dans le document « descriptif du projet ». Leur implantation sera indiquée sur les plans remis lors de la visite sur site.

Le soumissionnaire devra prendre connaissance de l'ensemble des points de détection à installer afin de proposer les détecteurs les plus appropriés à l'action à mener.

Ce système sera paramétré pour déclencher une alarme en temps réel, par tout temps, 24h/24 et 7j/7.

Dans certains cas, la détection d'intrusion sera associée à un système de caméras analytiques.

La détection d'intrusion peut également être intégrée dans les équipements gérés par le système de contrôle d'accès.

La surveillance périmétrique et intérieure pourra s'articuler autour des équipements suivants qui seront de type **NF A2P type 2 ou supérieur**. Des équipements combinant plusieurs de ces technologies seront également acceptés.

5.1. Câble coaxial de détection

XXX

5.2. Câble de détection de chocs

Les câbles à détection de chocs sont constitués de capteurs, installés sur les panneaux de clôture, connectés à une unité d'analyse électronique appelée Unité de Gestion (UG).

Les tentatives d'escalade ou de coupure sont détectées par les capteurs et transmises à l'unité d'analyse électronique qui transmet à son tour une information d'alarme.

Les câbles à détection de chocs constituent un système de détection d'intrusion instrumentalisant une clôture existante sur le site à sécuriser.

Les câbles à détection de chocs doivent répondre aux recommandations minimales suivantes :

- capteurs installés sur chaque panneau de clôture (soit tous les 2m50) afin de pouvoir localiser précisément la source de l'alarme intrusion (tentative de franchissement) ou de l'alarme technique (coupure, dégradation, alimentation)

- capteurs à accéléromètre intégrés dans un câble standard passif (facilité d'installation) et peu de sensibilité aux conditions météorologiques (vent fort, neige, forte pluie),

- sensibilité de la détection paramétrable en fonction du niveau de détection attendu. Attribution d'un seuil de déclenchement sur l'intensité du signal mesurée par combinaison des valeurs d'accélération des trois axes géométriques (X, Y, Z) résultant des variations de mouvements d'une clôture ou d'un bardage.

- nombre d'impacts avant déclenchement d'alarme paramétrable en fonction du niveau de détection attendu.

- compatibilité électromagnétique conforme aux normes européennes (label CE)

- température d'utilisation de -35°C à + 70°C

- installable sur tous types de clôtures

Les Unités de Gestion doivent répondre aux recommandations minimales suivantes :

- serveur web intégré

- historique horodaté

- localisation du capteur en alarme

- zones de détection multiples (regroupement de plusieurs capteurs par zone)

- transmission d'alarme par contact sec, RS-485, RS-422 ou IP. Carte contacts secs intégrée pour raccordement au système d'alarme ou au système de pilotage de caméras

- visualisation temps réel de l'état du site (diagnostic de panne)

- comptabilité électromagnétique conforme aux normes européennes (label CE)

- température d'utilisation de -35°C à + 70°C

5.3. Barrière de détection infrarouge (BIR)

La barrière de type infrarouge doit répondre aux recommandations minimales suivantes :

- Etre à faisceaux multiples et synchrones,
- Etre modulable en hauteur et en nombre de faisceaux suivant le site à protéger,
- Avoir une alarme configurable suivant la coupure de 1, 2 ou 3 faisceaux,
- Pouvoir discriminer tous type d'interférences (brouillard, neige etc.),
- Posséder une temporisation réglable,
- Avoir une alimentation indépendante secourue pour chacune,
- Etre en TX et RX totalement orientables avec aide à l'alignement,
- Etre auto-protégées mécaniquement contre le vandalisme,
- Etre munies de chapeau anti-appui,
- Etre équipées de filtres anti-insectes,
- Etre chauffées et munies de thermostats,
- Etre raccordées par bus ou par contact au système d'alarme intrusion ou de contrôle d'accès.
- Générer et transmettre les alarmes d'intrusion, d'autoprotection, de non alignement et de défaut technique.

Dans le cas d'un ensemble de barrières, il sera possible d'isoler chacune des barrières individuellement.

Les barrières extérieures auront un indice de protection IP45 ou supérieur.

5.4. Barrière de détection Hyper-fréquence

La barrière de type hyper-fréquence X (9,9 Ghz) ou K (24 Ghz) doit répondre aux recommandations minimales suivantes :

- Réglage de l'alignement par buzzer et LED,
- Etre à canaux multiples,
- Etre adaptée à la distance à couvrir, de 50 à 250m,
- Etre installée dans une zone dégagée,
- Etre équipée de l'anti-masquage dynamique numérique interdisant toute tentative de masquage du signal
- Etre protégée contre toutes les perturbations électromagnétiques, y compris celles générées par les radars militaires et civils, les lignes électriques très haute tension, les émetteurs de forte puissance.
- Avoir une alimentation indépendante, intégrée dans chacun des boîtiers ,émetteur et récepteur
- Etre dotée d'une mémorisation de l'historique des évènements,
- Pouvoir discriminer tout type d'interférences (brouillard, neige etc.),
- Etre auto-protégée mécaniquement contre le vandalisme (couvercle des radômes, boîtiers de connexion),
- Etre paramétrable par ordinateur via liaison RS232/RS485,
- Etre capable de s'adapter automatiquement aux variations atmosphériques (thermostat et résistances)
- Etre capable de détecter tout individu dans toutes les configurations (rampantes, roulantes, ...), équipé de tenues de camouflages sur des mouvements, même très lents,
- Disposer d'une alarme technique (signal insuffisant, etc.),
- Disposer d'un lobe de détection réglable en hauteur/largeur adapté à la scène,
- Etre raccordées par bus ou par contact au système d'alarme intrusion ou de contrôle d'accès.
- Générer et transmettre les alarmes d'intrusion, d'autoprotection, de non alignement et de défaut technique.

Dans le cas d'un ensemble de barrières, il sera possible d'isoler chacune des barrières individuellement.

Les barrières extérieures auront un indice de protection IP45 ou supérieur.

5.5. Détection par vidéo analytique

Dans certains cas décrits dans le document « descriptif du projet », le système anti-intrusion sera complété par les détections issues de caméras optiques ou thermiques.

Dans les zones périmétriques sous éclairées, les caméras optiques peuvent être associées à des caméras thermiques. Ces dernières permettront de détecter toute présence non identifiable dans une zone déterminée. Les caméras thermiques devront toujours être calibrées après installation.

Le système permet la définition de zones géographiques d'alarmes avec des conditions de déclenchement paramétrables selon l'événement (intrusion, déplacement dans la zone…). Il inclut des règles de paramétrage du départ, du sens, de la taille d'un objet suivi. Il inclut la définition d'une géométrie adaptée à des formes complexes telles que celles rencontrées sur des toits non plats.

Il doit avoir la capacité d'estimer le volume d'un objet en fonction de son éloignement par rapport à la caméra.

Il doit intégrer la notion de temps afin de permettre de réagir sur des déplacements même très lents.

Le système d'analyse d'images permet de détecter automatiquement, en tout point des zones d'analyses, et à 98% tout individu évoluant dans les zones de détection définies. Ce pourcentage n'est pas limité pour les déplacements lents.

Ces performances doivent se vérifier pour toute approche d'un individu, quelque soit sa vitesse de déplacement et son mode de progression (rampé, roulé, course).

Ces performances sont assurées même si l'individu porte des tenues classiques de camouflage et dispose d'accessoires de fraude spécifiques.

Sont considérées comme fausses alarmes, les déclenchements dus :

- Aux variations de lumières naturelles et artificielles et projections d'ombres (nuages…),
- Aux variations de températures de l'environnement naturel,
- Aux nappes de brouillard ou fumée,
- Aux faibles chutes de pluie ou de neige,
- Aux mouvements de la végétation située dans le champ des caméras et cela dans des conditions normales d'entretien des extérieurs,
- A des défaillances techniques de la caméra ou du système,
- Aux oiseaux n'évoluant pas sur l'axe horizontal du capteur.

Si le taux de fausses alarmes est important, le titulaire doit procéder aux étalonnages et aux modifications nécessaires dans un délai d'une semaine, selon les prescriptions et exigences de l'administration.

Chaque intervention doit faire l'objet d'un rapport, à transmettre à l'administration, qui précisera toutes les modifications apportées, notamment les éléments suivants :

- Modification de la taille de la cible,
- Modification de la taille de la zone,
- Modification de la vitesse de déplacement,
- Modification de filtre (neige, pluie…).

Le titulaire propose des détecteurs analytiques, matériels optiques performants pour respecter les contraintes sur la probabilité de détection et le taux de fausses alarmes définies par l'administration.

Le couplage entre la solution analytique et la solution vidéo est réalisé par l'utilisation de trames IP.

L'enregistrement vidéo permanent des caméras thermiques est nécessaire.

Si la détection d'intrusion est faite à partir de capteur vidéo traditionnel à vision IR, l'illumination de la zone par l'éclairage sera adaptée au volume de la zone observée.

La levée de doute est réalisée par des dômes dont la motorisation est asservie sur le point de détection. Le complément d'éclairage IR, impératif, du dôme permet d'identifier la cause de l'intrusion de nuit comme de jour. Ce complément d'éclairage IR est donc adapté pour permettre l'identification d'un individu (visage) sur toute la profondeur observée.

Une personne qui a des habits de la même couleur que le fond (toits) est détectée.

Une personne cachée par un dispositif de la même couleur que le fond (toits) est détectée.

Le système est configuré pour qu'une personne soit toujours détectée, de jour comme de nuit, et dans toutes les configurations calendaires (saisons / horaires).

5.6. Détecteur de présence

Ces détecteurs de présence, à double technologie, seront réservés et adaptés à la détection de mouvement, de franchissement de limite sur certaines zones à surveiller et devront avoir les caractéristiques minimales suivantes :

- Détection double technologie, hyperfréquence et infrarouge passif,
- Immunité aux passages des animaux domestiques (caractérisés par la corpulence d'un animal),
- Délimitation précise de la zone à surveiller,
- Protection anti-masquage,
- Réglage sensibilité hyperfréquence et IR,
- Protection anti-ouverture,
- Protection anti-arrachement,

5.7. Détecteurs de choc, bris de vitre ou de vibration

Pour être alerté d'une tentative de pénétration par ouverture ou bris de vitre d'un ouvrant (fenêtre ou porte), les détecteurs devront avoir les caractéristiques minimales suivantes :

- Double contrôle de sensibilité,
- Sensibilité ajustable,
- Niveau de choc compatible avec les fenêtres et les portes,
- Adaptable à l'environnement,
- Compensation en température,
- Protection anti-arrachement,
- A masselotte ou inertie.

5.8. Détecteurs d'ouverture

Les contacts d'ouverture, de type magnétique, peuvent être montés en saillie, en feuillure, en zone protégée. Leur positionnement sera ajusté à l'aide de jeux de cales adaptées.

Les détecteurs d'ouverture auront les caractéristiques minimales suivantes :

- Autoprotection à l'ouverture,
- Autoprotection à l'arrachement,
- Distance d'ouverture 1,5 cm minimum.

Les détecteurs d'ouverture, adaptés aux supports sur lesquels ils seront installés, permettront la surveillance des ouvrants (porte bois ou métal, fenêtre, porte basculante, etc...) et délivreront les informations minimales suivantes :

- Alarme ouverture,
- Autoprotection.

NB : Les portes à double vantail posséderont un contact d'ouverture par vantail.

5.9. Commandes manuelles anti-agression

Elles seront assurées par des pédales d'alarme, des boutons coup-de-poing ou des boutons poussoir d'alarme (BPA), avec ou sans clé de réarmement.

Dans les zones sensibles, ces équipements seront IK10. Ils seront fixés à l'aide de vis anti-vandales.

6. SÉCURITÉ

Le coffret de la centrale sera auto-protégée par surveillance à l'ouverture et à l'arrachement. Tout défaut d'alimentation sera également signalé sur l'afficheur du clavier.

Tous les boîtiers d'extension, d'équipements de raccordement, de commande ou de détection sont auto-protégés. Une perte de liaison, un passage en mode dégradé d'un équipement est une alarme prioritaire.

En cas d'effraction ou de défaut, le système affichera sur le clavier la cause du déclenchement : Le détecteur en cause et le type d'anomalie.

Sur un système centralisé, ces informations seront remontées comme alarmes techniques au superviseur et enregistrées dans le journal d'événements.

La durée de conservation des événements devra être paramétrable jusqu'au seuil maximum de 90 jours.

La centrale doit réagir à toutes tentatives d'intrusion dans son système informatique et générer une alerte dans le journal d'événements.

Par ailleurs, le système de détection doit pouvoir éviter au maximum les « fausses alarmes » par un réglage optimum des paramètres de détection des équipements de détection intrusion.

La fausse alarme est définie par un déclenchement d'alarme sans rapport avec un fait générateur de type intrusion ou tentative d'intrusion. Elle peut donc être le fait d'une défaillance physique ou d'un logiciel.

Si des alarmes intempestives sont constatées à l'issue de l'installation, l'installateur devra procéder aux modifications nécessaires pour aboutir au fonctionnement optimal de l'installation.

La centrale d'alarme ainsi que les boîtiers d'extension doivent être installés dans des zones sécurisées désignées ou validées par l'administration.

7. TRAITEMENT DE L'INFORMATION

7.1. Signalisation

La signalisation et la transmission de l'alarme peuvent être réalisées à l'aide des équipements décrits dans les paragraphes ci-dessous.

Le dispositif sera spécifié dans le document « descriptif du projet ».

7.1.1. Sirènes (extérieure – intérieure)

La sirène répondra aux normes **NF A2P type 2**. Elle sera de puissance **100 dB** minimum **à 1 mètre** et de durée paramétrable. La sirène doit être équipée d'une alimentation indépendante avec batterie de secours. La sirène sera auto-protégée contre l'ouverture et l'arrachement.

Les sirènes auront un indice de résistance au choc IK08 ou supérieur, et un indice de protection IP44 ou supérieur.

7.1.2. Transmetteur téléphonique

Le titulaire se conformera aux directives de l'Administration : des numéros internes ou externes pourront être mémorisés en tant que destinataires des alarmes.

7.1.3. Télétransmission Ramsès

Le système doit pouvoir transmettre les alarmes aux services de Police.

L'information est transmise *via* les boîtiers RAMSES de l'administration.

Ces boîtiers sont interfacés par un ou plusieurs contact (s) sec (s) (ToR) avec la solution du titulaire.

La transmission est faite par le réseau du Ministère de l'Intérieur. L'activation de RAMSES se fera par l'ouverture d'une **boucle sèche normalement fermée (N/F)**, d'une durée de l'ordre de 2 secondes, commandée par la centrale.

La fourniture, l'installation et la mise en service de ces boîtiers seront effectuées par les techniciens du SGAMI DSIC

Le câble de liaison entre la centrale et le boîtier RAMSES sera fourni par le titulaire.

8. RÈGLES DE SÉCURITÉ

Le système doit être sécurisé par l'application des mesures habituelles de sécurité des systèmes d'information.

Pour tous les matériels constituant le système, les règles suivantes doivent être observées :

- Les modes de communication par liaison sans fil (WIFI ou autre) ainsi que les fonctionnalités associées doivent être désactivés.
- De la même manière, les équipements par liaison sans fil sont à proscrire
- Un cloisonnement logique doit être établi entre les sous-systèmes. L'interconnexion entre les sous-systèmes s'opèrent uniquement par l'intermédiaire d'un dispositif de routage/filtrage.
- Les codes par défaut doivent être remplacés par des codes spécifiques.
- Les mots de passe applicatifs par défaut doivent être remplacés par des mots de passe spécifiques et robustes. Les systèmes doivent pouvoir gérer des mots de passe d'une longueur minimale de 10 caractères, avec des caractères alphabétiques minuscules et majuscules, des chiffres et des symboles.
- Les possibilités de communications vers des serveurs « internet » doivent être désactivées (ex : mise à jour, dns ….)
- Les fonctions et interfaces d'administration ainsi que les services non utilisés doivent être désactivés

Il est impératif que la solution respecte les contraintes sur les flux et les contraintes de sécurité.

Tous les flux générés par les équipements doivent être identifiés et décrits dans l'offre présentée par le soumissionnaire du marché.

8.1. Intégration de l'antivirus

Dans le cas où l'installation a accès à la plate-forme de l'antivirus de l'administration, les postes d'exploitation faisant partie de l'installation doivent intégrer l'antivirus McAfee. L'antivirus est en mode géré. L'agent McAfee ainsi que le logiciel antivirus seront fournis par l'administration.

8.2. Synchronisation de l'heure

Dans le cas où l'installation a accès au serveur NTP de l'administration, les équipements IP faisant partie de l'installation doivent être synchronisés avec ce dernier. Les paramètres IP de synchronisation seront fournis par l'administration.

Si l'installation n'accède pas au serveur NTP de l'administration, un serveur de temps de référence doit être installé sur un des équipements de l'installation. Les autres équipements IP se synchronisent avec ce serveur de temps.

8.3. Logiciels et firmwares

Les équipements doivent disposer de la version la plus récente des logiciels et firmwares. Les mises à jours doivent être effectuées en atelier chez le titulaire avant l'implantation sur site.

8.4. Journalisation

Le système doit gérer la journalisation des événements.

La journalisation des événements est un processus automatique qui a pour but d'enregistrer toutes opérations menées sur un système en identifiant l'auteur, la date, l'heure ainsi que la nature de l'opération.

Les historiques relatifs aux déclenchements d'alarmes, aux activation/désactivation des zones, aux remontées techniques sont également conservés dans le journal d'événements.