Spécification architecturale et technique pour un
système de détection des intrusions périmétriques monté sur clôture

FlexZone®

Ce document est destiné à fournir les spécifications de performance et les exigences opérationnelles pour le système de détection des intrusions périmétriques FlexZone. Il est rédigé dans un format générique. Ces spécifications peuvent être recopiées telles quelles pour constituer un cahier des charges d'achat générique.

PARTIE 1 GÉNÉRALITÉS

1.1 Synthèse du système

Le contractant doit installer un système de détection des intrusions périmétriques monté sur clôture. Le système doit détecter et localiser les intrus qui tentent de couper, d'escalader ou de soulever la structure de la clôture.

Les capteurs de détection doivent consister en des câbles coaxiaux faciles à installer. Les câbles doivent se connecter à des modules processeurs du signal qui détectent et localisent les tentatives d'intrusions périmétriques en analysant les signaux électriques qui se produisent sous l'effet de vibrations infimes des câbles du capteur.

Le système doit pouvoir être intégré au système de gestion de la sécurité de l'installation.

Le système doit prendre en charge l'utilisation de capteurs sans fil pour renforcer la protection périmétrique dans les zones où les câbles filaires posent des problèmes au niveau de l'installation et/ou de l'entretien, comme dans le cas de barrières coulissantes ou battantes.

1.2 Soumissions

A. Les soumissions des contractants au propriétaire de l'installation doivent comprendre au moins les éléments suivants :

1. Rapport sur les conditions du site, conformément à l'article 3.1 ;

2. Paramètres de configuration et d'étalonnage, et schémas de sensibilité pour chaque processeur dans le système une fois l'installation et l'étalonnage terminés, conformément à l'article 3.1 ;

3. Tous les logiciels fournis par le fabricant nécessaires à l'étalonnage et au fonctionnement du système.

1.3 Pièces de rechange

A. Le contractant doit livrer au propriétaire du site des composantes du système de rechange.

B. Pour chaque composante du système, des pièces de rechange composées au minimum d'une unité ou de 10 % du nombre que comprend le système, selon le chiffre le plus élevé, doivent être fournies.

1.4 Garantie

A. Le produit doit bénéficier d'une garantie minimum de deux ans à compter de la date d'achat.

B. Le fournisseur doit mettre à disposition des composants, des pièces ou des assemblages de remplacement pendant un minimum de 10 ans à compter de la date d'achat.

1.5 Références

A. Abréviations et sigles : Les abréviations et sigles suivants sont utilisés dans ce document:

1. PIDS : Système de détection des intrusions périmétriques (*Perimeter Intrusion Detection System*)
2. MTBF : Temps moyen entre défaillances (*Mean Time Between Failures*)
3. MTTR : Temps moyen jusqu'au remplacement (Mean Time To Replace)
4. Pd : Probabilité de détection

B. Normes de référence : Les normes réglementaires et industrielles suivantes sont mentionnées dans le présent document :

1. Commission fédérale des communications : Exigences FCC 47 CFR Partie 15, sous-partie B pour les appareils de classe B.
2. Industrie Canada : Exigences ICES-003, Issue 4 pour les appareils de classe
3. Normes CE : EN 61000-6-4 / A1: 2011 (Partie 6-4 : Normes génériques - Norme sur l'émission pour les environnements industriels), EN 50130-4: 2011 (Systèmes d'alarme - Partie 4 : Compatibilité électromagnétique - Norme de famille de produits : exigences relatives à l'immunité des composants de système d'alarme de détection d'incendie, contre l'intrusion, contre les hold-up, CCTV, de contrôle d'accès et des systèmes d'alarme sociale), Directive sur la restriction de l'utilisation de substances dangereuses 2011/65/UE (RoHS2)
4. Underwriters Laboratory (UL) 50 (Évaluations environnementales) Organisation internationale de normalisation : ISO 9001:2008
5. Commission électrotechnique internationale (CEI), Ingress Protection (IP) 66
6. Règlement 1907/2006 de l'Union européenne : Enregistrement, évaluation, autorisation et restriction des substances chimiques (REACH)

PARTIE 2 PRODUITS

2.1 Système de détection des intrusions périmétriques monté sur clôture

A. Le contractant doit fournir un système télémétrique de détection des intrusions périmétriques (PIDS – *Perimeter Intrusion Detection System*) monté sur clôture.

B. Le PIDS monté sur clôture doit détecter et localiser les intrus tentant d'ouvrir une brèche dans la clôture périmétrique en coupant, escaladant ou soulevant la structure de la clôture.

2.2 Fabricants

A. Le système FlexZone™ de Senstar Corporation (www.senstar.com) est conforme aux exigences présentées dans ce document.

2.3 Exigences en matière de réglementations

A. Le système doit être conforme aux réglementations suivantes :

1. Exigences FCC 47 CFR Partie 15, sous-partie B pour les appareils de classe B
2. CE : EN 61000-6-4/A1: 2011, EN 50130-4: 2011, RoHS2
3. Industrie Canada : Exigences ICES-003, Issue 4 pour les appareils de classe B
4. REACH

2.4 Exigences de qualité de fabrication

A. Le système de gestion de la qualité du fabricant doit être certifié conforme à la norme ISO 9001: 2008.

B. Composants extérieurs du système :

1. Tous les modules et assemblages électroniques destinés à une utilisation à l'extérieur doivent prévoir des revêtements de protection.
2. Les modules et les assemblages doivent être testés au cours de la fabrication sur l'ensemble de leur gamme de températures de fonctionnement, sur la base d'échantillons.

2.5 Exigences mécaniques

A. Câble du capteur :

1. Le câble du capteur doit offrir la possibilité d'être enveloppé dans une gaine blindée, pour être utilisé dans des zones avec un fort potentiel de dommage physique au câble.

2. Le câble du capteur doit avoir un rayon de courbure minimum qui ne dépasse pas 10 cm (4 pouces).

3. Le câble du capteur doit être fixé à la clôture de l'installation au moyen d'attaches de câble en plastique ou en métal résistantes aux UV.

4. Le câble du capteur ne doit pas nécessiter l'installation d'un conduit de câble le long du périmètre de la clôture.

B. Modules du processeur :

1. Le fabricant doit donner au propriétaire de l'installation la possibilité d'installer chaque bloc du processeur dans son propre boîtier ou d'utiliser un boîtier existant.

2. Le couvercle du boîtier du processeur doit être articulé pour permettre l'accès aux composants internes sans que le retrait ne soit nécessaire

3. Le boîtier du processeur doit pouvoir être sécurisé au moyen d'un cadenas

4. Le boîtier du module du processeur comprend des goupilles de câble pré-installées, de sorte que les techniciens d'installation n'aient pas besoin de percer leurs propres points d'entrée de câble.

5. Pour améliorer l'accessibilité lors de l'installation et de la maintenance, des borniers enfichables en deux parties doivent être utilisés.

6. Le module du processeur doit détecter et indiquer les circonstances d'altération physique, notamment :

a. Ouverture du couvercle du boîtier du processeur entraînant une intervention sur le commutateur d'activation

b. Coupure du câble du capteur

c. Court-circuit du câble du capteur

d. Débranchement du câble du capteur

2.6 Exigences en matière d'environnement

A. Plage de fonctionnement : Le processeur dans son boîtier standard doit fonctionner selon les spécifications dans les conditions environnementales suivantes :

1. Température : -40 °C à 70 °C (-40 °F à 158 °F)

2. Humidité relative : 0 % à 100 % (avec condensation)

B. Boîtier du processeur :

1. La carte du circuit du processeur doit être logée dans un boîtier en aluminium peint conforme aux exigences de la norme UL Type 4X / IP66.

2. Les ports entrée/sortie du câble doivent comprendre des goupilles de câble qui ne nécessitent aucun produit d'étanchéité supplémentaire pour assurer l'étanchéité à l'environnement des câbles gainés.

2.7 Exigences en matière de fiabilité et de maintenance

A. Câbles du capteur : Les câbles de capteurs doivent avoir une durée de vie minimale de 10 ans, hors dommages causés par des forces non environnementales.

B. Processeur :

1. Le processeur doit avoir un temps moyen entre défaillances (MTBF – *Mean Time Between Failures*) prévu de plus de 100 000 heures, tel que calculé par la procédure de prédiction de fiabilité de Telcordia, méthode par comptage des pièces à 70 °C.

2. Le processeur doit avoir un temps moyen jusqu'au remplacement (MTTR – *Mean Time to Replace*) de moins de 10 minutes.

3. Le processeur doit être capable d'effectuer des tests d'auto-diagnostic internes des circuits internes, de la continuité et de la terminaison du câble, et du traitement de la détection.

4. Le cycle d'auto-test du processeur doit pouvoir se lancer à partir de ses deux entrées contacts secs ou d'une commande émise sur le réseau, selon la configuration.

5. Le micrologiciel du processeur doit pouvoir être mis à niveau sur le terrain soit localement via une connexion USB, soit via le réseau.

2.8 Exigences en matière d'énergie

A. Chaque module du processeur doit satisfaire les exigences en matière d'énergie suivantes :

1. Source d'alimentation d'entrée : 10V à 60V DC

2. Consommation d'énergie (unité autonome) : moins de 2 W

3. Consommation d'énergie (unité mise en réseau) : moins de 2,5 W

B. Protection contre la foudre/la surtension : Le processeur doit comporter une protection contre la surtension transitoire pour protéger le système contre les coups de foudre ou les perturbations électriques.

C. Le système doit prendre en charge l'alimentation en électricité via les câbles du capteur, afin que les modules des processeurs individuels, lorsqu'ils sont connectés ensemble, puissent partager une source d'alimentation commune.

D. Le système doit être capable d'avoir jusqu'à 5 processeurs qui se partagent l'alimentation électrique à partir d'une source unique d'alimentation de 48 V (nominaux).

E. Configuration électrique de sortie et d'entrée auxiliaire :

1. Relais sortie : Chaque relais doit avoir pour capacité au moins 1 A à 30 V.

2. Entrées auxiliaires : Les valeurs de la/des résistance(s) de supervision pour chaque entrée contact sec doivent être définies à partir du logiciel de configuration.

F. Toute carte de communication optionnelle connectée à l'assemblage de processeurs sera capable d'utiliser la source d'alimentation du processeur existant et ne nécessitera aucune connexion électrique supplémentaire.

G. Le système doit pouvoir être alimenté par la fonction *Power-over-Ethernet* (PoE) si une carte de communication Ethernet est installée.

2.9 Capacités de détection

A. Le capteur du PIDS doit consister en un câble fixé à la clôture sur toute la longueur à protéger.

B. Le système doit être capable de détecter et de localiser les intrusions jusqu'à une distance de câble de 600 m (1 968 pieds) par processeur.

C. Le processeur du PIDS doit avoir les capacités de détection suivantes :

1. Traiter le signal du câble du capteur pour détecter les intrus tentant d'ouvrir une brèche dans la clôture périmétrique en coupant, escaladant ou soulevant la structure de la clôture.

2. Chaque processeur doit prendre en charge deux câbles de capteurs, chacun d'une longueur de jusqu'à 300 m (984 pieds).

3. Localiser la position d'une intrusion détectée avec une précision égale ou inférieure à 3 m (9,8 pieds) au moins 95 % du temps.

4. Détecter des intrusions multiples simultanées, lorsque chaque tentative d'intrusion est séparée par une distance de câble de capteur supérieure à 50 m (164 pieds).

5. Prendre en charge des zones de détection flexibles, définies par le logiciel. Chaque processeur doit prendre en charge jusqu'à 4 ou 60 zones distinctes dimensionnées individuellement, selon le modèle.

6. Pouvoir être étalonné pour fonctionner sur différents types de clôtures métalliques.

7. Utiliser des algorithmes de différenciation de l'environnement dans le processus de détection pour distinguer de façon optimale entre les perturbations localisées dans l'espace liées aux intrusions réelles et les perturbations réparties dans l'espace telles que la pluie et le vent.

D. Le système doit prendre en charge un circuit de communication redondant afin d'assurer le maintien de la détection des intrusions sur le périmètre en cas de coupure d'un câble.

E. Performances de détection des intrusions :

1. La probabilité de détection (Pd) d'un intrus coupant la clôture, soulevant la structure de la clôture, ou escaladant sans assistance la clôture doit être de 95 % avec un coefficient de confiance de 95 % lorsque le système est installé conformément aux indications du fabricant sur une clôture de bonne qualité.

2. Taux de fausses alarmes : Le taux maximum d'alarmes générées par des processus électroniques internes des processeurs (câbles non compris) doit être inférieur à un par zone et par an, en moyenne sur le nombre total de zones dans le système.

3. Alarmes (causées par l'environnement) intempestives :

a. Le système, lorsqu'il est étalonné conformément aux directives du fabricant, ne doit pas connaître d'alarmes intempestives causées par les sources suivantes :

1. Variations de température

2. Déplacement d'objets ou de végétation proches qui ne heurtent pas la clôture

3. Agitation des eaux de surface ou souterraines

4. Lever/coucher du soleil

5. Vibrations sismiques provoquées par la circulation de véhicules ou de trains à proximité

6. Effets acoustiques ou magnétiques

7. Neige

8. Brouillard

b. Le système doit utiliser la technologie de traitement adaptatif dérivé de l'environnement (EDAPT – *Environmentally Derived Adaptive Processing Technology)* pour tenir compte du niveau de bruit environnemental aux environs d'une perturbation avant de générer une alarme, afin de réduire au minimum la probabilité de fausses alarmes provenant des sources suivantes :

1. Vent
2. Pluie et grêle
3. Tempêtes de sable

F. Compatibilité avec les clôtures :

1. Le système doit être compatible avec l'installation sur les types de clôtures métalliques suivants :
   a. Mailles losangées
   b. Treillis en métal déployé
   c. Treillis soudés standard
   d. Concertina et/ou barbelé à lames
   e. Mailles losangées recouvertes de vinyle
   f. Palissade
2. Le système doit fonctionner comme prévu dans des installations à passage unique sur des grillages de bonne qualité de jusqu'à 4,3 m (14 pieds) de hauteur.
3. Il doit être possible d'utiliser des passages multiples du câble du capteur pour obtenir la performance de détection spécifiée, quelle que soit la hauteur de la clôture.
4. Le fabricant doit fournir des indications d'installation concernant le type et la hauteur des clôtures pouvant être protégées avec un, deux ou plusieurs passages de câble du capteur.

G. Compatibilité avec les barrières :

1. Le câble du capteur doit pouvoir être installé sur les barrières battantes.
2. Le câble du capteur doit pouvoir être dérivé sur les barrières coulissantes.
3. Le processeur doit être capable de fournir de l'énergie (2 W) de sorte que les dispositifs auxiliaires tels que les capteurs infrarouge passif (PIR – *Passive InfraRed*) puissent être alimentés au niveau des barrières.
4 Le processeur doit pouvoir communiquer avec un capteur de barrière sans fil FlexZone de Senstar afin de protéger les barrières sans qu'il soit nécessaire d'acheminer des câbles électriques ou de capteur jusqu'aux sections mobiles de la barrière.
5. Le processeur doit pouvoir alimenter un système de détection des intrusions à micro-ondes UltraWave de Senstar.
6. Le processeur doit pouvoir fournir une connectivité des données, afin que les dispositifs auxiliaires comme UltraWave de Senstar puissent être intégrés au réseau des capteurs au niveau des barrières.

7. Le système doit avoir l'option d'utiliser des connecteurs « de déconnexion rapide » pour les barrières rarement utilisées (battantes ou coulissantes), de sorte que le câble du capteur puisse être installé normalement sur la barrière et déconnecté temporairement si besoin.

H. Stockage intégré : Le processeur doit pouvoir utiliser une carte mémoire Secure Digital (SD) disponible dans le commerce pour enregistrer une copie locale des données de réponse du capteur.

2.10 Capacités externes d'entrée/sortie

A. Sorties d'alarme du processeur :

1. Le processeur du capteur doit avoir un minimum de quatre sorties relais de forme C pour indiquer les situations d'alarme.

2. Pour chaque relais, il doit être possible d'affecter une ou plusieurs conditions de la liste suivante pour l'activation du relais :

a. Alarme de zone (début et fin de zone configurable)

b. Alarme de supervision côté A

c. Alarme de supervision côté B

d. Violation du boîtier

e. Perte de l'alimentation d'entrée

f. Défaut matériel interne

g. Sécurité intégrée (maintenue en cas de perte totale de puissance)

h. Alarmes d'intrusion, de supervision et de diagnostic du capteur de barrières sans fil FlexZone

B. Entrées contacts secs :

1. Le processeur doit avoir au moins deux entrées contacts secs configurables pour accepter la notification des conditions d'alarme détectées ou générées par des appareils tiers.

2. Le processeur doit pouvoir surveiller sans fil l'état des contacts des barrières via le capteur de barrière sans fil Senstar.

2.11 Capacités d'installation et de configuration

A. Le système doit être simple à installer et avoir au minimum les caractéristiques suivantes :

1. Le câble du capteur doit pouvoir être fixé directement à la clôture sans qu'il soit nécessaire de le mettre dans un conduit.

2. Le câble du capteur doit pouvoir être fixé directement à la clôture avec des attaches de câble standard résistantes aux UV (en plastique ou en métal).

3. Il doit être possible de monter le processeur directement sur un poteau de clôture faisant partie de la clôture à protéger.

4. Il doit être possible de connecter le câble du capteur directement au processeur sans qu'un câble intermédiaire ne soit nécessaire.

5. Toutes les connexions électriques au processeur, y compris les câbles du capteur, doivent être effectuées avec des borniers à vis sur les connecteurs amovibles.

B. Le système doit être disponible dans différentes configurations pour les sites ayant des exigences de zonage différentes :

1. Le processeur doit être disponible dans une configuration qui prend en charge jusqu'à 4 zones sur un seul processeur.

2. Le processeur doit être disponible dans une configuration qui prend en charge jusqu'à 60 zones sur un seul processeur.

C. Le système doit prendre en charge les caractéristiques de configuration et d'étalonnage suivantes :

1. Le processeur doit fournir un port USB standard pour une connexion à un PC sous Microsoft Windows.

2. La configuration et l'étalonnage doivent être effectués via un outil logiciel basé sur Windows doté d'une interface utilisateur graphique.

3. Le logiciel d'étalonnage doit prendre en charge un nivellement de sensibilité sur une base d'un mètre (3 pieds).

4. Le logiciel d'étalonnage doit permettre la création de zones sans détection où les évènements de vibration sont ignorés (par exemple, près de barrières ou de zones où la détection des intrusions n'est pas nécessaire).

5. Le logiciel d'étalonnage doit inclure un mode graphique en temps réel pour afficher les données de réponse de la clôture en direct.

6. Le logiciel d'étalonnage doit inclure des paramètres pour optimiser les niveaux de sensibilité pour les constructions de clôture flexibles et rigides.

7. Les paramètres de configuration et d'étalonnage doivent pouvoir être stockés dans un fichier informatique à des fins d'archivage et être disponibles pour être réutilisés lors de la configuration de processeurs supplémentaires ou de remplacement.

2.12 Capacités de mise en réseau

A. Le système doit pouvoir fonctionner dans une configuration autonome ou en réseau :

1. Le système doit prendre en charge une configuration autonome (non connectée à un Silver Network). Dans cette configuration, les informations sur les alarmes et de supervision doivent être communiquées via les relais sortie du processeur.

2. Le système doit prendre en charge une configuration en réseau. Les processeurs doivent utiliser le protocole Silver Network pour relayer les informations sur les alarmes, les états et de supervision via les câbles du capteur vers le gestionnaire réseau. Le gestionnaire réseau communique ensuite les informations à un système de gestion de la sécurité.

3. Le système doit prendre en charge la notification d'alarmes de zones individuelles ainsi que des informations de supervision et d'état à des modules relais E/S compatibles avec Silver Network.

B. Quand un système capable de fonctionner en réseau est nécessaire, les exigences de la présente section (2.12) s'appliquent.

C. Outils de gestion de réseau : Le logiciel de gestion de réseau du système doit fournir les outils suivants pour faciliter le suivi, la mise en service et la résolution de problèmes du système :

1. Un outil d'état du système qui fournit un affichage visuel de l'état de tous les processeurs du système ;

2. Un outil de journal des évènements système qui fournit un journal interrogeable de ces évènements ;

3. Un outil de schéma du système qui stocke et rappelle les données de réponse pour tous les capteurs en réseau et affiche un schéma de la réponse pour un minimum de 8 zones de capteurs simultanément ;

4. Un outil audio qui génère un signal sonore représentant les données de réponse du capteur pour chaque zone.

D. Auto-test du processeur mis en réseau : Il doit être possible de lancer un auto-test sur le réseau.

E. Intégration et communications du réseau :

1. Les processeurs doivent être capables de communiquer les informations sur les alarmes, les états et la configuration vers et depuis un emplacement central sur un réseau de capteurs intégré.

2. Les informations sur les alarmes, les états et la configuration doivent pouvoir être communiquées via les câbles de capteur, permettant ainsi à

un système à processeurs multiples de nécessiter une seule connexion au réseau et/ou aux systèmes de gestion de la sécurité de l'installation.

3. Les processeurs doivent prendre en charge les options de médias physiques suivantes pour la communication avec le réseau de capteurs intégré :

   a. Câble EIA-422

   b. Câble à fibre optique multimode

   c. Câble à fibre optique monomode

   d. Ethernet avec fonction PoE (*Power over Ethernet*).

4. Le réseau de capteurs doit pouvoir être connecté dans une configuration en boucle et être interrogé à partir des deux extrémités de la boucle afin de fournir des voies de communication redondantes à chaque processeur.

5. Les processeurs doivent conserver une file d'attente interne des alarmes en cas d'interruption du réseau. Les alarmes doivent être renvoyées automatiquement lorsque la connectivité du réseau est rétablie.

6. Mise en réseau des relais d'entrée et de sortie auxiliaires :

   a. L'état des entrées contacts secs auxiliaires du processeur doit être communiqué sur le réseau de capteurs intégré.

   b. Les relais sortis du processeur doivent être contrôlables via le réseau de capteurs intégré.

F. Gestion du réseau :

1. Le système doit inclure un logiciel de gestion du réseau pour gérer les communications sur le réseau de capteurs. Le logiciel de gestion du réseau doit fonctionner sur un PC Windows standard.

2. Le logiciel de gestion de réseau du système doit fournir les interfaces suivantes :

   a. Interface basée sur le protocole TCP/IP pour communiquer les données sur les alarmes, les états et la configuration depuis et vers les systèmes de gestion de la sécurité. Le fournisseur du système doit apporter une documentation complète de cette interface pour faciliter l'intégration avec les systèmes de gestion de la sécurité.

   b. Interface sérielle et basée sur le protocole TCP/IP pour communiquer les données des alarmes, des états et de la configuration vers et depuis les systèmes de gestion de la sécurité en utilisant des chaînes de caractère au format ASCII.

c. Interface basée sur le protocole TCP/IP qui sera utilisée par l'outil d'étalonnage et de configuration du logiciel sur PC du système pour effectuer l'étalonnage et la configuration de tous les paramètres du processeur à partir d'un emplacement central.

PARTIE 3 EXÉCUTION

3.1 Évaluation du site

A. Avant que l'installation ne commence, le contractant responsable de l'installation doit fournir un rapport au propriétaire du site afin de documenter toute condition du site risquant d'empêcher le système de fonctionner de manière satisfaisante. Des exemples de ces conditions incluent une structure de clôture lâche, des barrières mal ajustées ou des objets tels que des panneaux ou des branches d'arbres heurtant la clôture.

3.2 Installation du système

A. Le système doit être installé conformément aux procédures recommandées par le fabricant, telles que définies dans la documentation du fabricant concernant le système.

3.3 Étalonnage du système

A. Le contractant responsable de l'installation doit étalonner le système conformément aux procédures recommandées par le fabricant, telles que définies dans le guide produit du fabricant.

B. Le contractant responsable de l'installation doit soumettre au propriétaire les paramètres d'étalonnage et de configuration pour le système.

C. Le contractant responsable de l'installation doit soumettre au propriétaire un schéma de la réponse pour chaque zone dans le système.

3.4 Formation

A. Le contractant ou fournisseur responsable de l'installation doit former le personnel d'entretien du propriétaire aux procédures d'étalonnage et de maintenance du système, telles qu'indiquées par la documentation produit du fabricant.