Texte de spécification destiné aux architectes, planificateurs de travaux et conseillers

Système d’alarme anti-intrusion / contrôle d’accès SPCEvo53

Système d’alarme anti-intrusion avec contrôle d’accès intégré pour des installations de taille moyenne jusqu’à 128 zones et 16 portes.

Edition: 17-04-2025

Série SPC53 – 128 zones, 500 utilisateurs, 16 portes

Système d'alarme anti-intrusion – Généralités

Selon la taille et la structure du site à sécuriser, l'ensemble de l'installation est connecté à un ou plusieurs panneaux. Le panneau est installé dans une zone sécurisée du bâtiment et est commandé par un ou plusieurs claviers de commande et/ou lecteurs de cartes et/ou via des commandes du système de gestion externe et via une interface web intégrée. Le panneau fonctionne de manière totalement autonome et peut enregistrer séparément les événements d'intrusion et les événements d'accès, avec horodatage.

Le panneau doit répondre aux spécifications suivantes :

- Toutes les entrées doivent être surveillées par une résistance de fin de ligne et être capables de détecter une alarme, une alarme de sabotage, un court-circuit et une alarme technique. La valeur de la résistance de fin de ligne doit être réglable par entrée et prendre en charge les valeurs de différents fabricants.
- Le panneau doit être utilisable avec des détecteurs filaires et sans fil.
- Les points de détection doivent être divisibles en zones indépendamment activables. Le panneau doit également permettre l'utilisation de zones communes.
- Les zones doivent pouvoir être liées entre elles, de sorte qu'elles puissent être activées/désactivées ensemble, et que certaines zones ne puissent pas être désactivées simultanément.
- Le panneau doit permettre l'activation automatique des zones, avec possibilité de temporisation. Il doit également permettre la désactivation différée des zones, par exemple pour une chambre forte.
- La communication avec la salle de surveillance, le système de gestion et les systèmes liés au bâtiment s'effectue via une connexion TCP/IP chiffrée et/ou une connexion 2G/3G/4G. Une ligne téléphonique (PSTN) doit être disponible en tant que secours pour la connexion à la salle de surveillance. Un modem 3G/4G supplémentaire peut être utilisé comme secours pour la connexion 2G/3G/4G.
- Le panneau doit pouvoir recevoir des commandes via une connexion TCP/IP chiffrée depuis divers systèmes de gestion. Pour chaque connexion, il doit être possible de spécifier les commandes acceptées par le panneau.
- Toutes les défaillances de l'alimentation (secteur et batterie), des lignes de bus et des lignes de communication doivent être signalées.
- Le panneau est contrôlé par microprocesseur et dispose d'une fonction de surveillance (watchdog), avec une sortie physique de surveillance pour la connexion à un système (de gestion) externe.
- Le panneau peut communiquer avec un serveur NTP librement configurable pour maintenir l'heure correcte.
- Le panneau dispose d'une connexion BUS pour les composants de bus tels que les claviers de commande, les modules d'extension et les modules d'indication. Le bus peut être connecté en boucle pour la redondance, de sorte qu'en cas de déconnexion, tous les composants alimentés restent opérationnels.
- Le panneau doit offrir une fonctionnalité de contrôle d'accès, y compris la possibilité de définir des zones anti-retour (anti-passback) et d'attribuer des actions liées à la date et à l'heure, telles que les droits d'accès, l'utilisation de carte/code PIN et l'ouverture automatique des portes.
- Le panneau doit être indépendant de la marque en ce qui concerne les lecteurs de cartes et prendre en charge différents formats de lecteurs et de cartes.
- Le panneau doit être utilisable par plusieurs utilisateurs et configurable pour des codes PIN de 4, 5 ou 6 chiffres. Les droits des utilisateurs peuvent être définis et modifiés par profils. Le panneau offre un support multilingue, permettant aux utilisateurs d'utiliser le système dans leur propre langue.
- Le panneau doit pouvoir être facilement étendu à une version plus avancée via une mise à niveau de licence, évitant ainsi le remplacement complet du système en cas d'extension future.

Spécifications techniques – Détection d'intrusion

- Le système doit permettre l'utilisation d'au moins 128 entrées filaires pour des détecteurs tels que : détecteurs de mouvement, contacts magnétiques, détecteurs de bris de vitre, détecteurs sismiques, boutons de panique, etc.

- Le panneau doit pouvoir fournir des entrées virtuelles, permettant la transmission d'informations d'alarme et d'état selon différents scénarios. Cela évite de devoir relier physiquement les sorties aux entrées et simplifie les options de programmation.
- Les points de détection doivent être divisibles en au moins 16 zones indépendamment activables.
- Il doit être possible de connecter au moins 16 claviers de commande.
- Il doit être possible de connecter au moins 16 modules d'extension.
- Le panneau doit disposer d'une mémoire d'événements capable d'enregistrer 10 000 événements d'alarme ou système.
- Le panneau doit permettre l'utilisation de 500 codes PIN utilisateurs différents.
- Le panneau doit pouvoir être utilisé dans au moins 4 langues : néerlandais, français, anglais, allemand. En outre, les langues suivantes doivent être disponibles : espagnol, portugais, italien, polonais, russe, suédois, norvégien et danois.
- Le panneau doit être équipé d'une alimentation secteur qui fonctionne également comme chargeur pour une batterie au plomb 12V. Il doit pouvoir charger des batteries courantes de 7,0 Ah et 17,0 Ah. Le panneau doit tester automatiquement et régulièrement la batterie, et afficher son état : Bon, Mauvais (batterie à remplacer bientôt) ou Défaut (message d'erreur).
- Le panneau doit être équipé d'au moins 2 relais et 6 sorties collecteur ouvert pour commander des sirènes, flashs, etc. Le nombre de sorties doit être extensible jusqu'à au moins 128.
- En cas de panne de courant, le panneau doit être automatiquement alimenté par la batterie. Une autonomie conforme aux normes applicables (EN Grade 2, EN Grade 3, INCERT) doit être assurée.
- Les composants du bus doivent pouvoir être connectés en ligne ou en boucle. Ils doivent pouvoir être placés à au moins 400 mètres les uns des autres.

Spécifications techniques – Contrôle d'accès intégré

- Le panneau doit offrir une fonctionnalité de contrôle d'accès intégré pour au moins 16 lecteurs de cartes et 500 détenteurs de cartes.
- Il doit disposer d'une mémoire d'événements d'accès distincte pour au moins 10 000 événements.
- Il doit proposer 32 calendriers hebdomadaires indépendants et configurables pour attribuer des droits d'accès, définir des horaires pour l'utilisation de la carte et/ou du code PIN, et pour l'ouverture/fermeture automatique des portes.
- L'utilisation et la gestion de la partie contrôle d'accès doivent être faciles à réaliser par l'utilisateur sans logiciel supplémentaire.
- Le panneau doit permettre l'utilisation de boutons de demande de sortie et de capteurs de position de porte, ces derniers pouvant également être utilisés dans le système d'alarme anti-intrusion.
- L'ouverture et la fermeture des portes peuvent être effectuées via un lecteur de cartes, l'interface web ou un système de gestion connecté via TCP/IP.
- En cas d'incendie, des portes prédéfinies doivent pouvoir être automatiquement ouvertes par le panneau pour garantir une évacuation sécurisée.
- Au moins 500 détenteurs de cartes prédéfinis doivent pouvoir être stockés localement dans l'unité de contrôle de porte, afin de maintenir l'accès même en cas de perte de connexion avec le panneau.
- Pour les zones à haut risque, certaines portes ne doivent pouvoir être ouvertes que par deux détenteurs de cartes simultanément (principe des quatre yeux).
- Pour les sas, les portes doivent pouvoir être liées entre elles, de sorte qu'une porte reste verrouillée tant que l'autre est ouverte.
- Pour les détenteurs de cartes en situation de handicap, il doit être possible de prolonger le temps de contrôle de la porte.
- Le système doit permettre de configurer plusieurs zones anti-retour (anti-passback). Le statut anti-passback d'un détenteur de carte doit pouvoir être réinitialisé automatiquement chaque jour.
- Le panneau doit prendre en charge différents formats de lecteurs de cartes, notamment Wiegand 26 bits, Wiegand 36 bits, EM4102, Mifare Classic et Mifare DESfire. Il doit également prendre en charge différents formats de communication des lecteurs, dont Wiegand 26 bits et Clock & Data.

Certifications

Le panneau et les composants de bus connectés, tels que les claviers de commande et les modules d'extension, doivent être testés et certifiés par un organisme d'accréditation indépendant selon au moins les normes suivantes :

EN50131-1 Grade 2 et Grade 3

INCERT

VdS Classe B et Classe C (rayer les mentions inutiles si nécessaire)

La connexion TCP/IP avec la salle de surveillance doit être testée et certifiée selon la norme EN50136-1:2012 SP6 et DP4.

Le panneau doit également être testé et certifié selon la norme NF A2P Cyber RTC.

Connexions TCP/IP

Le panneau doit être équipé d'une connexion TCP/IP intégrée avec au moins un port Ethernet 100baseT, pouvant être utilisé pour :

- Une connexion sécurisée à la salle de contrôle, conforme à la norme EN50136-1:2012.
- Une connexion sécurisée à des systèmes de gestion tels que : Systèmes de gestion vidéo (VMS), systèmes de gestion des risques, systèmes de contrôle d'accès, systèmes de gestion de la sécurité physique (PSIM), systèmes de gestion technique du bâtiment, interfaces KNX, etc.
- Une connexion sécurisée au système de gestion à distance de l'installateur.

Le panneau doit pouvoir gérer au moins dix connexions TCP/IP simultanées. Pour chaque connexion, il doit être possible de : Définir quels messages d'événements sont envoyés, définir quelles commandes sont acceptées, attribuer un code d'identification unique (numéro de connexion).

Les connexions TCP/IP doivent pouvoir être chiffrées avec un cryptage AES 256 bits au minimum.

La connexion TCP/IP à la station de surveillance doit être protégée par une clé de chiffrement aléatoire après la première connexion, unique à la station et inconnue de l'installateur et de la station.

Le panneau doit pouvoir intégrer au moins un modem 2G/3G/4G pour une transmission d'alarme principale ou secondaire.

Il doit également pouvoir intégrer un deuxième modem (PSTN ou 2G/3G/4G) pour une transmission d'alarme secondaire ou tertiaire. Ces modems doivent pouvoir être réinitialisés à distance.

Le panneau doit utiliser un protocole de communication moderne pour l'interfaçage avec des systèmes (de gestion) externes. Ce protocole doit être fourni par le fabricant et utiliser un langage de balisage courant tel que XML, cURL ou Python, afin d'éviter toute dépendance à un fournisseur.

Le panneau d'alarme anti-intrusion doit pouvoir être intégré, via une connexion TCP/IP sécurisée (native ou plugin), aux systèmes suivants : Milestone XProtect et Genetec Security Center (VMS), Entelec SkyWalker, Advancis WinGuard et Prysm AppVision (PSIM).

Le panneau doit permettre la gestion à distance par l'installateur. L'accès à distance doit être autorisé par l'administrateur depuis le clavier de commande ou via l'interface web, pour une durée déterminée.
En cas de gestion à distance, l'installateur doit pouvoir : Garantir que seuls les techniciens autorisés ont accès au panneau, Suivre les modifications apportées à la programmation, Fournir les journaux d'accès à distance avec date et heure.
L'accès à distance doit permettre : Des modifications de programmation, la synchronisation automatique de la date et de l'heure, la mise à jour du firmware, la sauvegarde automatique des fichiers de configuration, la génération de rapports d'état.

De cette manière, l'installateur devrait être en mesure d'assurer une surveillance continue et une attitude proactive envers la maintenance.

Le panneau doit être opérable via une interface web intégrée. L'accès à cette interface doit pouvoir être protégé par un mot de passe alphanumérique librement définissable.

Circuits dépendants de scénarios

Le panneau doit permettre la création de circuits automatisés dépendants de scénarios, basés sur des conditions configurables. Ces circuits doivent pouvoir contrôler : des sorties, des entrées virtuelles, des zones, des portes. Les conditions suivantes doivent pouvoir être appliquées indépendamment ou combinées dans un circuit :

- État des entrées de zone
- État des zones
- Événements de porte
- Événements système
- Événements d'alarme
- Actions des utilisateurs ou des profils utilisateurs

Les conditions doivent également pouvoir être limitées selon :

- L'heure
- Un calendrier
- Une période de temps spécifiée

Claviers de commande

Les claviers doivent être équipés d'un écran graphique LCD, d'indicateurs pour l'alimentation, les alarmes et les avertissements, de touches numériques rétroéclairées et de touches de fonction. Pour la protection contre le sabotage, les claviers doivent être munis d'un contact d'autoprotection. Les claviers doivent être connectés au bus du panneau et programmables pour contrôler une, plusieurs ou toutes les zones. Il doit également être possible de restreindre l'utilisation des claviers à une période de temps spécifique. L'accès au menu doit être enregistré par utilisateur dans le journal d'événements du clavier.

L'utilisateur doit pouvoir effectuer les fonctions suivantes via le clavier :

- Armement et désarmement des zones, partiel ou total
- Armement et désarmement de groupes de zones
- Désactivation temporaire d'une entrée de zone
- Inhibition d'un détecteur défectueux
- Réinitialisation d'une alarme
- Test des sorties (flashs, sirènes)
- Contrôle des sorties
- Visualisation des entrées de zone ouvertes
- Consultation des journaux d'alarme et de contrôle d'accès
- Modification des codes
- Ajout, modification et suppression d'utilisateurs
- Passage du panneau en mode test de marche
- Retardement de l'armement automatique
- Autorisation d'accès local ou distant à l'installateur pour une durée déterminée

Le panneau doit permettre la création de profils utilisateurs multiples, permettant d'attribuer des droits d'utilisation et des plages horaires à des groupes d'utilisateurs.

En plus des codes PIN, les claviers doivent pouvoir être utilisés avec des cartes ou tags EM4102, Mifare et Mifare DESFire EV2.

Modules d'extension

Le panneau doit pouvoir être étendu avec des modules d'extension pour : augmenter le nombre d'entrées de zones, augmenter le nombre de sorties, fournir des points d'alimentation supplémentaires avec alimentation de secours, intégrer des unités de contrôle de porte pour le contrôle d'accès.

Les modules d'extension doivent être connectés au bus du panneau et adressables librement sur le bus, permettant une numérotation logique des zones.

Les modules d'extension pour entrées de zones doivent prendre en charge les configurations de résistances de fin de ligne de différents fabricants.

Modules d'extension pour entrées de zones : Équipés d'au moins 8 entrées de zone et 2 sorties relais (30 VDC, 1A), installés dans un boîtier robuste avec contact d'autoprotection.

Modules d'extension avec alimentation : Équipés d'au moins 8 entrées de zone, 2 sorties relais (30 VDC, 1A), une alimentation intelligente avec au moins 2 sorties protégées par fusible (total d'au moins 1,5 A @ 12 VDC), un circuit de charge de batterie pour batterie de 7,0 Ah ou 17,0 Ah (rayer la mention inutile), installés dans un boîtier métallique avec contact d'autoprotection, pouvant accueillir au moins deux modules d'extension supplémentaires.

Modules d'extension pour sorties supplémentaires : Équipés d'au moins 8 sorties relais (30 VDC, 1A), installés dans un boîtier robuste avec contact d'autoprotection.

Unités de contrôle de porte : Équipées d'au moins 2 connexions pour lecteurs (entrée/sortie ou entrée + sortie), 2 sorties relais (30 VDC, 1A), 4 entrées pour signalisation de position de porte et boutons de demande de sortie, installées dans un boîtier robuste avec contact d'autoprotection ou dans un boîtier métallique avec alimentation intelligente et alimentation de secours.

Sans fil

Pour les extensions sur site où le câblage n'est pas envisageable, le panneau doit pouvoir être étendu avec des capteurs et alarmes sans fil. Les options doivent inclure : des contacts de fenêtre/porte, des détecteurs de mouvement infrarouge passifs (PIR), des détecteurs de fumée optiques.

Les composants sans fil doivent : communiquer via un chemin de communication bidirectionnel chiffré, envoyer un accusé de réception au transmetteur, utiliser la bande de fréquence 868 MHz, permettre la modification des paramètres depuis le système d'alarme, afin de réduire les coûts d'ajustement après installation.

La durée de vie des batteries des composants sans fil doit être d'au moins 5 ans.

Application mobile

Si le niveau de sécurité et/ou la compagnie d'assurance le permet, le système d'alarme anti-intrusion doit pouvoir être commandé via une application mobile. Cette application doit répondre aux critères suivants :

- Compatible avec Apple iOS et Google Android.
- L'accès à l'application doit être sécurisé par un code PIN, distinct de celui du smartphone.
- Pour un niveau de sécurité supplémentaire, l'application doit pouvoir être protégée par un identifiant et un mot de passe uniques, d'au moins 8 caractères alphanumériques ou spéciaux.
- L'application doit permettre la gestion de plusieurs systèmes d'alarme (multi-sites).
- Elle doit permettre : l'activation/désactivation du système, le pontage des entrées de zone, la consultation des journaux, le contrôle des sorties, l'ouverture/fermeture des portes d'accès, si nécessaire.
- L'application doit utiliser une connexion sécurisée AES 256 bits vers un serveur sécurisé, sans nécessiter de connexion directe au système d'alarme.
- Elle doit fonctionner via une connexion mobile, sans dépendre du Wi-Fi.
- Chaque utilisateur doit pouvoir disposer de son compte personnel, avec des droits d'utilisation configurables.

- Les actions telles que l’armement/désarmement, l’ouverture des portes et le contrôle des sorties via l’application doivent être enregistrées dans le système d’alarme, avec l’identification de l’utilisateur concerné.
- L’utilisation de l’application doit pouvoir être verrouillée à distance en cas de perte du smartphone.