SPC4xxx/5xxx/6xxx 3.8.5

Manuel d'installation et de configuration

ID document : A6V10276959-c

Date d'édition : 11.2018

Les données et la conception peuvent être modifiées sans préavis. / La fourniture du produit dépend de sa disponibilité.

© 2018 Copyright par Vanderbilt International (IRL) Ltd.

Nous nous réservons tous les droits sur ce document et sur l'objet dont il traite. Par l'acceptation de ce document, l'utilisateur reconnaît ces droits et accepte de ne pas reproduire ni diffuser le document ou des parties de ce document à des tiers sans notre accord préalable écrit et de ne pas l'utiliser à d'autres fins que celles pour lesquelles il a été fourni.

Table des matières

Table des matières 3
1 Signification des symboles 11
2 Sécurité 13
2.1 Groupe cible 13
2.2 Consignes de sécurité générales 13
2.2.1 Informations générales 13
2.2.2 Transport 13
2.2.3 Configuration 14
2.2.4 Fonctionnement 14
2.2.5 Entretien et maintenance 14
2.3 Signification des avertissements écrits 15
2.4 Signification des pictogrammes indicateurs de danger 15
3 Directives et normes 17
3.1 Directives de l'Union européenne 17
3.2 Vue d'ensemble de la conformité à la norme EN50131 17
3.2.1 Conformité aux agréments EN50131 23
3.2.2 Conformité aux agréments EN 50136-1:2012 et EN 50136-2:2014 24
3.2.3 Conformité aux agréments INCERT 25
3.2.4 Directives de conformité PD 6662:2010 26
3.2.5 Conformité aux agréments VDS 31
3.2.6 Conformité au référentiel de la certification NF&A2P incluant les exigences CYBER 32
4 Données techniques 35
4.1 SPC4000 35
4.2 SPC5000 38
4.3 SPC6000 41
4.4 SPCP355.300 44
5 Introduction 47
6 Installation du matériel 49
6.1 Montage d'un boîtier G2 49
6.2 Montage d'un boîtier G3 50
6.2.1 Montage d'un kit d'autosurveillance arrière 52
6.2.2 Installation de la batterie pour conformité EN50131 56
6.3 Montage d'un boîtier G5 57
6.3.1 Protection antisabotage 58
6.3.2 Montage du boîtier avec la protection antisabotage 59
6.3.3 Installation des batteries 61
6.4 Montage d'un clavier 62

6.5 Montage d'un transpondeur 62
7 Smart PSU 63
7.1 SPCP355.300 Smart PSU 63
7.1.1 Sorties supervisées 66
7.1.2 Batteries 66
7.1.3 Câblage de l'interface X-BUS 68
7.1.4 Conformité au référentiel de la certification NF&A2P 71
7.1.5 Témoin d'état du module d'alimentation 72
7.1.6 Restauration du système 73
8 Matériel du contrôleur 75
8.1 Matériel de la centrale 42xx/43xx/53xx/63xx 75
8.2 Matériel de la centrale SPC5350 et 6350 78
9 Transpondeur de porte 83
10 Câblage du système 85
10.1 Câblage de l'interface X-BUS 85
10.1.1 Configuration en boucle 86
10.1.2 Configuration en branche 87
10.1.3 Configuration en étoile et multipoint 88
10.1.4 Blindage 93
10.1.5 Plan câble 93
10.2 Câblage d'un transpondeur en branche 93
10.3 Câblage de la mise à la terre du système 94
10.4 Câblage de la sortie de relais 94
10.5 Câblage des entrées de zone 95
10.6 Câblage d'une sirène extérieure SAB 98
10.7 Câblage d'un buzzer interne 99
10.8 Câblage du Bris de verre 99
10.9 Installation de modules de raccordement 100
11 Alimentation du contrôleur SPC 103
11.1 Alimentation à partir de la batterie uniquement 103
12 Interface utilisateur du clavier 105
12.1 SPCK420/421 105
12.1.1 À propos du clavier LCD 105
12.1.2 Utilisation de l'interface du clavier LCD 107
12.1.3 Entrées de données sur le clavier LCD 111
12.2 SPCK620/623 111
12.2.1 À propos du clavier confort 112
12.2.2 Description des LED 115
12.2.3 Description du mode d'affichage 116

12.2.4 Touches de fonction (état repos) 116
13 Outils logiciels 119
14 Démarrage du système 121
14.1 Modes Installateur 121
14.1.1 Codes PIN installateur 121
14.2 Programmation avec le clavier 121
14.3 Configuration des paramètres de démarrage 122
14.4 Création des utilisateurs système 123
14.5 Programmation d'un badge 124
14.6 Programmation des tags sans fil 125
14.6.1 Effacement d'alertes avec la télécommande 125
15 Programmation en mode Exploitation avec le clavier 127
16 Programmation en mode Paramétrage avec le clavier 129
16.1 État du système 129
16.2 Options 130
16.3 Temporisations 134
16.4 Secteurs 138
16.5 Groupes Secteurs 140
16.6 Périph. X-BUS 140
16.6.1 Adressage du X-BUS 140
16.6.2 Rafraîchissement du X-BUS 141
16.6.3 Reconfigurer 141
16.6.4 Claviers / Transpondeurs / Contrôleurs de porte 142
16.6.5 Mode adressage 151
16.6.6 Type X-BUS 152
16.6.7 Ré-essai bus 152
16.6.8 Tempo communications 152
16.7 Radio 153
16.7.1 Ajouter des détecteurs 153
16.7.2 Éditer des détecteurs (affectation de zone) 154
16.7.3 Ajouter WPA 154
16.7.4 Éditer WPA 154
16.8 Zones 155
16.9 sur les portes 156
16.10 Sorties 160
16.10.1 Types de sortie et ports de sortie 161
16.11 Communication 165
16.11.1 Ports série 166
16.11.2 Ports Ethernet 166

16.11.3 Modems 167
16.11.4 Centre de télésurveillance 169
16.11.5 SPC Connect PRO 170
16.12 Test 171
16.12.1 Test sirène 171
16.12.2 Test de déplacement 171
16.12.3 Test zone 171
16.12.4 Test sortie 172
16.12.5 Test JDB 173
16.12.6 Options sonores 173
16.12.7 Indications visuelles 173
16.12.8 Test WPA 174
16.12.9 TEST SISMIQUE 174
16.13 Utilitaires 174
16.14 Isoler 175
16.15 Journal des événements 175
16.16 Journal des accès 175
16.17 Journal des alarmes 175
16.18 Modifier code installateur 176
16.19 Utilisateurs 176
16.19.1 Ajouter 176
16.19.2 Éditer 176
16.19.3 Effacer 179
16.20 Profils utilisateur 179
16.20.1 Ajouter 180
16.20.2 Éditer 180
16.20.3 Effacer 180
16.21 SMS 180
16.21.1 Ajouter 181
16.21.2 Éditer 181
16.21.3 Effacer 182
16.22 X-10 182
16.23 Régler date/heure 183
16.24 Texte installat. 183
16.25 Contrôle de portes 184
16.26 SPC Connect 184
17 Programmation en mode Installateur avec le navigateur 185
17.1 Infos sur le système 185
17.2 Interface Ethernet 185

17.3 Connexion USB à la centrale 187
17.4 Ouverture de session dans le navigateur 189
17.5 SPC Accueil 190
17.5.1 Vue d'ensemble du système 190
17.5.2 Vue générale des alarmes 191
17.5.3 Affichage des vidéos 192
17.6 État centrale 193
17.6.1 Etat 193
17.6.2 État X-bus 194
17.6.3 Radio 201
17.6.4 Zones 203
17.6.5 sur les portes 205
17.6.6 FlexC - État 206
17.6.7 Alertes système 208
17.7 Journaux de bord 208
17.7.1 JDB Système 208
17.7.2 Journal des accès 209
17.7.3 Journal WPA 210
17.7.4 JOURNAL DES ALARMES 210
17.8 Utilisateurs 211
17.8.1 Ajouter/Éditer un utilisateur 211
17.8.2 Ajouter/modifier des profils utilisateur 214
17.8.3 Programmation SMS 219
17.8.4 Commandes SMS 220
17.8.5 Suppression des Mots de passe Web 223
17.8.6 Paramètres de configuration Installateur 223
17.9 Configuration 225
17.9.1 Configuration des entrées/sorties du contrôleur 226
17.9.2 Périph. X-BUS 236
17.9.3 Radio 249
17.9.4 Modification des paramètres du système 256
17.9.5 Configuration des zones, des portes et des secteurs 277
17.9.6 Calendriers 292
17.9.7 Modification de son propre code PIN 296
17.9.8 Configuration des paramètres avancés 296
17.10 Configurer les communications 305
17.10.1 Paramètres de communication 305
17.10.2 FlexC® 315
17.10.3 Rapports 336

17.10.4 Outils PC 349
17.11 Gestion des fichiers 351
17.11.1 Mise à jour des fichiers 351
17.11.2 Utilisation du gestionnaire de fichiers 356
18 Accès à distance au serveur Web 357
18.1 Connexion RTC 357
18.2 Connexion GSM 359
19 Fonction alarme anti-intrusion 363
19.1 Fonctionnement mode Bancaire 363
19.2 Fonctionnement mode Évolué 363
19.3 Fonctionnement mode Simple 364
19.4 Alarmes totales et locales 364
20 Exemples de systèmes et scénarios 367
20.1 Comment utiliser un secteur commun 367
21 Détecteurs sismiques 369
21.1 Test des détecteurs sismiques 370
21.1.1 Procédures de tests manuel et automatique 370
21.1.2 Test automatique des détecteurs 371
21.1.3 Test manuel des détecteurs 372
22 Utilisation du verrouillage de blocage 375
22.1 Verrouillage de blocage 375
22.2 Activation autorisée du verrouillage de blocage 376
22.3 Élément de verrouillage 377
23 Annexe 379
23.1 Connexions du câble réseau 379
23.2 LED d'état du contrôleur 380
23.3 Alimentation des transpondeurs à partir des bornes auxiliaires 381
23.4 Calcul de la puissance nécessaire pour la batterie 382
23.5 Paramètres par défaut des modes Simple, Évolué et Bancaire 384
23.6 Câblage de l'interface X10 385
23.7 Codes SIA 386
23.8 Codes CID 391
23.9 Vue d'ensemble des types de clavier 393
23.10 Combinaisons de codes utilisateur 394
23.11 Codes utilisateur de contrainte 394
23.12 Inhibitions automatiques 394
23.12.1 Zones 394
23.12.2 Codes PIN d'accès 395
23.12.3 Accès Installateur 395

23.12.4 Déconnexion clavier de l'utilisateur 395
23.13 Raccordement du câble secteur sur le contrôleur 395
23.14 Contrôleur de maintenance 395
23.15 Maintenance Smart PSU 396
23.16 Types de zone 397
23.17 Attributs zone 404
23.18 Attributs applicables aux types de zones 408
23.19 Niveaux ATS et spécifications d'atténuation 409
23.20 Lecteurs de cartes et de formats de badges pris en charge 409
23.21 Support SPC pour périphériques E-Bus 411
23.21.1 Configuration et adressage des périphériques E-Bus 412
23.22 Glossaire FlexC 414
23.23 FlexC - Commandes 415
23.24 Tempos des catégories d' ATS 418
23.25 Tempos des catégories de Chemin 419
24 Remarques 421

1 Signification des symboles

Les pictogrammes utilisés ont la signification suivante :

Symbole	Description
SPC4xxx	Non disponible pour SPC42xx, SPC43xx.
IP	Uniquement disponible pour le contrôleur SPC avec interface IP (SPC43xx/SPC53xx/SPC63xx).
	Non disponible pour l'installation de type « Simple » dans une résidence privée.
	Uniquement disponible en mode « Pas de restriction ».
	Trouver des informations détaillées sur le niveau de sécurité, le pays ou le mode dans le texte.
	Voir l'annexe pour de plus amples informations.

2 Sécurité

Ce chapitre recouvre :

2.1 Groupe cible **13**
2.2 Consignes de sécurité générales **13**
2.3 Signification des avertissements écrits **15**
2.4 Signification des pictogrammes indicateurs de danger **15**

2.1 Groupe cible

Les instructions fournies dans ce document sont destinées aux lecteurs suivants :

Lecteurs ciblés	Qualification	Activité	État de l'équipement
Personnel chargé de l'installation	Formation technique dans le domaine de la gestion technique du bâtiment (GTB) ou des installations électriques.	Monte et installe les composants sur le site.	Composants individuels devant être assemblés et installés.
Personnel chargé de la mise en service	Formation technique appropriée couvrant les tâches et les produits, périphériques ou systèmes devant être mis en service.	Mise en service du périphérique ou système assemblé et installé sur site.	Équipement neuf assemblé et installé ou équipement modifié.

2.2 Consignes de sécurité générales

AVERTISSEMENT : avant de commencer l'installation de ce produit, merci de prendre connaissance des Consignes de sécurité. cet appareil ne doit être connecté qu'à des sources d'alimentation électrique conformes à la norme EN60950-1, chapitre 2.5 (« Source d'énergie limitée »).

2.2.1 Informations générales

- Conservez ce document pour pouvoir vous y référer ultérieurement.
- Joignez systématiquement ce document au produit.
- Veuillez également tenir compte de toute norme ou réglementation de sécurité locale spécifique au pays concernant la planification du projet, l'utilisation du produit et sa mise au rebut.

Responsabilité

- Ne branchez pas le périphérique au réseau d'alimentation de 230 V s'il est endommagé ou si l'un quelconque de ses composants est manquant.
- N'apportez à l'appareil aucune modification autre que celles expressément mentionnées dans le présent manuel et approuvées par le fabricant.
- N'utilisez que des pièces de rechange et accessoires approuvés par le fabricant.

2.2.2 Transport

Dommages sur l'unité lors du transport

- Conservez l'emballage pour pouvoir transporter l'appareil ultérieurement.
- N'exposez pas l'appareil à des vibrations mécaniques ou chocs.

2.2.3 Configuration

Interférences radioélectriques avec d'autres appareils installés dans le même environnement / EMS

- Lors de la manipulation de modules sensibles aux décharges électrostatiques, veuillez vous conformer aux consignes ESD.

Dommages résultant d'un emplacement inapproprié

- Les spécifications environnementales recommandées par le fabricant doivent être respectées. Voir *Données techniques* page 35.
- N'utilisez pas l{}'{}appareil près de sources générant de puissants rayonnements électromagnétiques.

Risque d'électrocution en raison d'un branchement inapproprié

- Ne branchez l'appareil que sur des sources d'alimentation présentant la tension spécifiée. La tension requise est indiquée sur l'étiquette signalétique du périphérique.
- Assurez-vous que l'appareil est toujours branché sur l'alimentation électrique. Un dispositif de coupure immédiatement accessible doit être fourni.
- Assurez-vous que le circuit sur lequel l'appareil est branché soit protégé par un fusible de 16 A (maxi). Ne branchez sur ce fusible aucun autre appareil d'un système différent.
- Cet appareil est conçu pour être utilisé avec les systèmes d'alimentation mis à la terre selon un schéma TN. Ne branchez pas cet appareil sur un autre système d'alimentation.
- La mise à la terre électrique doit être conforme aux normes et réglementations de sécurité locales usuelles.
- Les câbles d'alimentation primaires et les câbles secondaires ne doivent pas se croiser, ni être posés parallèlement, ni se toucher les uns les autres à l'intérieur du boîtier.
- Les câbles téléphoniques doivent être connectés séparément à l'appareil.

Risque d'endommagement du câble résultant d'une trop forte sollicitation

- Assurez-vous qu'aucun câble ou conducteur sortant n'est soumis à une contrainte excessive.

2.2.4 Fonctionnement

Situation dangereuse résultant d'une fausse alarme

- Avant de tester le système, n'oubliez pas d'en informer toutes les parties et autorités concernées.
- Avant de tester un dispositif d'alarme quel qu'il soit, informez-en systématiquement toutes les personnes présentes afin d'éviter tout mouvement de panique.

2.2.5 Entretien et maintenance

Risque d'électrocution lors de la maintenance

- Les travaux de maintenance ne peuvent être effectués que par des spécialistes qualifiés.
- Débranchez systématiquement le câble d'alimentation et les autres câbles de la source d'alimentation principale avant toute opération de maintenance.

Risque d'électrocution lors du nettoyage du périphérique

- N'utilisez pas de produits nettoyants liquides ni d'aérosols contenant de l'alcool ou de l'ammoniac.

2.3 Signification des avertissements écrits

Terme avertisseur	Type de risque
DANGER	Danger de mort ou risque de blessures corporelles graves.
AVERTISSEMENT	Danger de mort ou risque de blessures corporelles graves possible.
ATTENTION	Risque de blessures légères ou de dégâts matériels.
IMPORTANT	Risque de dysfonctionnements.

2.4 Signification des pictogrammes indicateurs de danger

AVERTISSEMENT : avertissement d’un danger

AVERTISSEMENT : avertissement d’une tension électrique dangereuse

3 Directives et normes

Ce chapitre recouvre :

3.1 Directives de l'Union européenne **17**

3.2 Vue d'ensemble de la conformité à la norme EN50131 ..... **17**

3.1 Directives de l'Union européenne

Ce produit est conforme aux exigences des directives européennes 2004/108/CE portant sur la compatibilité électromagnétique, 2006/95/CE sur les équipements basse tension et 1999/5/CE sur les équipements terminaux de radio et de télécommunications. La déclaration de conformité aux directives européennes est disponible pour les autorités compétentes sur http://pcd.vanderbiltindustries.com/doc/SPC

Directive européenne 2004/108/CE sur la compatibilité électromagnétique

Le produit a été testé conformément aux normes suivantes afin de démontrer sa conformité aux exigences de la directive européenne 2004/108/EC :

Émission CEM	EN 55022 classe B
Immunité CEM	EN 50130-4

Directive européenne 2006/95/CE sur les équipements basse tension

Le produit a été testé conformément à la norme suivante afin de démontrer sa conformité aux exigences de la directive européenne 2006/95/CE :

Sécurité	EN 60950-1

3.2 Vue d'ensemble de la conformité à la norme EN50131

Cette section vous fournit une vue générale de la conformité du SPC à la norme EN50131.

Adresse de l'organisme certificateur
VDS (approbation VdS A/C/EN/SES) AG Köln HRB 28788 Sitz der Gesellschaft : Amsterdamer Str. 174, 50735 Köln Geschäftsführer : Robert Reinermann JörgWilms-Vahrenhorst (Stv.)

Les produits SPC listés ont été testés conformément à la norme EN50131-3:2009 et à toutes les spécifications RTC pertinentes.

Type de produit	Standard
• SPC6350.320 • SPC6330.320 • SPC5350.320 • SPC5330.320 • SPCP355.300 • SPCP333.300 • SPCE652.100 • SPCK420.100 • SPCK421.100 • SPCE452.100 • SPCE110.100 • SPCE120.100 • SPCA210.100 • SPCK620.100 • SPCK623.100 • SPCN110.000 • SPCN320.000	EN50131 Grade 3
• SPC5320.320 • SPC4320.320 • SPCP332.300 • SPCW110.000 • SPCW112.000 • SPCW114.000 • SPCW130.100	EN50131 Grade 2

Les informations spécifiques en rapport avec les exigences de la norme EN50131 sont contenues dans les sections suivantes de ce document.

Exigences EN50131 (et section concernée)	Documentation Vanderbilt concernée
Plage de fonctionnement pour la température et l'humidité	Données techniques : • *SPC4000* page 35 • *SPC5000* page 38 • *SPC6000* page 41
Poids et dimensions	Données techniques : • *SPC4000* page 35 • *SPC5000* page 38 • *SPC6000* page 41
Détails d'installation	*Installation du matériel* page 49

Exigences EN50131 (et section concernée)	Documentation Vanderbilt concernée
Instructions d'installation, de mise en service et d'entretien, y compris identifications de bornes	*Installation du matériel* page 49 *Matériel du contrôleur* page 75
Type d'interconnexions (voir 8.8)	Données techniques : • *SPC4000* page 35 • *SPC5000* page 38 • *SPC6000* page 41 *Câblage de l'interface X-BUS* page 85
Détail des méthodes possibles de mise en et hors service (voir 11.7.1 à 11.7.3 et tableaux 23 à 26)	Programmation en mode Utilisateur avec le clavier : • *Mise en / hors surveillance* page 284 • *Configuration d'un transpondeur de boîtier à clé* page 241 • *Programmation des tags sans fil* page 125 • *Déclencheurs* page 298
Pièces remplaçables par l'utilisateur	Données techniques : • *SPC4000* page 35 • *SPC5000* page 38 • *SPC6000* page 41
Alimentation électrique nécessaire si pas de bloc d'alimentation intégré	Consultez les instructions d'installation pour les blocs d'alimentation des transpondeurs SPCP33x et SPCP43x.
Bloc d'alimentation intégré, informations requises par EN 50131-6 :2008, Clause 6	Données techniques : • *SPC4000* page 35 • *SPC5000* page 38 • *SPC6000* page 41
Nombre maximal pour chaque type d'ACE et de périphérique.	*Câblage de l'interface X-BUS* page 85 Données techniques : • *SPC4000* page 35 • *SPC5000* page 38 • *SPC6000* page 41
Consommation électrique du CIE et de chaque type d'ACE et de périphérique, sans et avec une condition d'alarme.	Consultez les instructions d'installation pertinentes.
Courant nominal maximal de chaque sortie électrique	Données techniques : • *SPC4000* page 35 • *SPC5000* page 38 • *SPC6000* page 41

Exigences EN50131 (et section concernée)	Documentation Vanderbilt concernée
Fonctions programmables à disposition	*Programmation en mode Paramétrage avec le clavier* page 129 *Programmation en mode Installateur avec le navigateur* page 185
Comment les indications sont rendues inaccessibles aux utilisateurs de niveau 1 lorsque les utilisateurs de niveau 2, 3 ou 4 ne peuvent plus accéder aux informations (voir 8.5.1)	*Interface utilisateur du clavier* page 105 *Paramètres du clavier LCD* page 143 *Paramètres du clavier confort* page 144 *Configuration d'un transpondeur d'indication* page 239
Masquage/réduction de l'étendue des signaux/messages traités en tant qu'événements « défaut » ou « masquage » (voir 8.4.1, 8.5.1 et tableau 11)	*Options système* page 257 *Câblage des entrées de zone* page 95 *Codes SIA* page 386 Le masquage d'un détecteur PIR est toujours signalé comme un événement masqué de zone (SIA - ZM). En outre, l'anti-masquage peut – suivant la configuration – provoquer une alarme, une alarme « dysfonctionnement », une alarme « autosurveillance », ou ne pas déclencher d'action du tout. Valeurs par défaut actuelles de l'ajout de détecteur IRP : **Irlande** Hors surveillance – Aucun En surveillance – Alarme **Royaume-Uni, Europe, Suède, Suisse, Belgique** Hors surveillance – Sabotage En surveillance – Alarme
Priorisation du traitement des signaux et messages et des indications (voir 8.4.1.2, 8.5.3)	*Utilisation de l'interface du clavier LCD* page 107 Utilisation de l'interface clavier Confort – voir *À propos du clavier confort* page 112
Nombre minimal de variations de codes PIN, touches logiques, touches biométriques et/ou touches mécaniques pour chaque utilisateur (voir 8.3).	*Combinaisons de codes utilisateur* page 394
Méthode de limitation du temps d'accès à un PA (périphérique d'avertissement) pour un niveau 3 ne possédant pas d'autorisation niveau 2 (voir 8.3.1)	Non pris en charge – L'Installateur ne peut pas accéder au système sans autorisation.
Nombre de codes PIN rejetés avec les détails (voir 8.3.2.2.1)	*Inhibitions automatiques* page 394
Détails des méthodes biométriques d'autorisation (voir 8.3.2.2.3)	Sans objet
Méthode utilisée pour déterminer le nombre de combinaisons de codes PIN, clés logiques, clés biométriques et/ou clés mécaniques 11.6)	*Combinaisons de codes utilisateur* page 394

Exigences EN50131 (et section concernée)	Documentation Vanderbilt concernée
Nombre d'entrées de code invalides avant que l'interface utilisateur ne soit désactivée (voir 8.3.2.4)	*Codes PIN d'accès* page 395
Détail des méthodes utilisées pour une autorisation temporaire d'accès pour l'utilisateur (voir 8.3.2)	Menus utilisateur – Valider accès
En cas de mise en surveillance automatique à des moments prédéterminés, détails sur les indications préalables à la mise en surveillance et sur toutes les dérogations automatiques aux oppositions à la mise en surveillance (voir 8.3.3, 8.3.3.1)	*Mise en / hors surveillance* page 284
Détails des conditions indiquées pour l'état En surveillance (voir 8.3.3.4)	*Mise en / hors surveillance* page 284 *Paramètres du clavier LCD* page 143 *Paramètres du clavier confort* page 144 *Éditer une sortie* page 228 *Types de zone* page 397
Notification des signaux ou des messages de sortie fournis (voir 8.6)	*Éditer une sortie* page 228 *Mise en / hors surveillance* page 284 *Droits d'utilisateur* page 215
Autres configurations de sortie à interfacer avec les composants I&HAS (voir 8.2)	*Éditer une sortie* page 228 *Types de zone* page 397 *Test* page 171 *Interface utilisateur du clavier* page 105
Critères pour le retrait automatique de l'attribut « Test JDB » (voir 8.3.9)	*Temporisations* page 269
Nombre d'événements débouchant sur une inhibition automatique	*Inhibitions automatiques* page 394
Si un ACE est de type A ou de type B (voir 8.7) et s'il est portatif ou déplaçable (voir 11.14)	Tous les appareils sont câblés et alimentés à partir des blocs d'alimentation du système. Consultez les données techniques pertinentes sur les blocs d'alimentation (documents séparés).
Données sur les composants des mémoires non volatiles (voir tableau 30, étape 6)	Consultez la documentation utilisateur pour les claviers SPCK420/421 et SPCK620/623.
Durée de vie de la batterie de la mémoire (voir 8.10.1)	N/A. Enregistrement dans la mémoire non volatile.
Fonctions optionnelles proposées (voir 4.1)	*Programmation en mode Paramétrage avec le clavier* page 129 *Programmation en mode Installateur avec le navigateur* page 185
Fonctions supplémentaires proposées (voir 4.2, 8.1.8)	*Grade sans restriction* page 276 *Options* page 257

Exigences EN50131 (et section concernée)	Documentation Vanderbilt concernée
Niveaux d'accès requis pour utiliser ces fonctions supplémentaires proposées	*Éditer* page 176 Configuration utilisateur (navigateur) – voir *Ajouter/Éditer un utilisateur* page 211
Détails de tout dispositif programmable qui annulerait la conformité de I&HAS avec EN 50131-1 :2006, 8.3.13 ou qui réaliserait la conformité à un niveau de sécurité inférieur, avec instructions de suppression en découlant des étiquettes de conformité (voir 4.2 et 8.3.10).	*Grade sans restriction* page 276 *Options* page 257 *Conformité aux agréments EN50131* à la page opposée

Les produits SPC listés ont été testés conformément à la norme EN50131-6 et à toutes les spécifications RTC pertinentes.

Type de produit	Standard
• SPC6350.320 • SPC6330.320 • SPC5350.320 • SPC5330.320 • SPCP355.300 • SPCP333.300 • SPCP355.300 • SPCE652.100 • SPCK420.100 • SPCK421.100 • SPCE452.100 • SPCE110.100 • SPCE120.100 • SPCA210.100 • SPCK620.100 • SPCK623.100 • SPCN110.000 • SPCN310.000	EN50131-6
• SPC5320.320 • SPC4320.320 • SPCP332.300	EN50131-6

3.2.1 Conformité aux agréments EN50131

Configuration logicielle requise

- Dans la page de paramètres **Normes & Standards**, sélectionnez **Europe** dans **Spécificités Pays** pour mettre en œuvre les exigences de l'EN50131.
- Sélectionnez **Grade 2** ou **Grade 3** pour mettre en œuvre le niveau de conformité EN50131.
- Le paramètre **Radio Supervision RF : MES impossible** doit être supérieur à 0 et inférieur à 20.
- Le paramètre **Radio Détecteur RF perdu** doit avoir une valeur inférieure à 120.
- La valeur de **Paramètres X-BUS, nouveaux essais** doit être égale à 10.
- La valeur de **Paramètres X-BUS, tempo communications** doit être égale à 5.
- Sélectionnez le **Temps de synchronisation avec la configuration Secteur** sous **Horloge** pour utiliser le secteur en tant qu'horloge maître.

- NE sélectionnez PAS l'attribut **État des MES** des paramètres de configuration **Clavier** pour les **Indications visuelles**.

Exigences matérielles

- Le kit d'anti-sabotage arrière (SPCY130) doit être installé conformément aux dispositions de la norme EN50131 Grade 3, en ce qui concerne les centrales et l'alimentation électrique.
- Les composants conformes à la norme EN50131 Grade 3 doivent être installés sur des systèmes conformes à l'EN50131 Grade 3.
- Les composants conformes à la norme EN50131 Grade 2 ou 3 doivent être installés sur des systèmes conformes à l'EN50131 Grade 2.
- Il n'est pas possible d'enregistrer un périphérique radio dont le signal a une force inférieure à 3.
- Le ratio recommandé entre les récepteurs et les transmetteurs radio est d'un maximum de 20 transmetteurs pour un récepteur.
- Le bris de vitre doit être utilisé avec une interface pour bris de vitre conforme aux normes EN.
- Pour la conformité avec EN50131-3:2009, n'activez pas ou ne désactivez pas le système utilisant le SPCE120 (transpondeur à indicateur) ou le SPCE110 (transpondeur à boîtier à clé).

Les modules SPCN110 PSTN et SPCN320 GSM/GPRS sont testés sur les centrales approuvées de Grade 2 et 3 et peuvent être utilisés avec ces centrales approuvées.

3.2.2 Conformité aux agréments EN 50136-1:2012 et EN 50136-2:2014

Les produits SPC listés ont été testés conformément aux normes EN 50136-1:2012 et EN 50136-2:2014.

3.2.3 Conformité aux agréments INCERT

Configuration logicielle requise

La sélection de Belgique (*) sous **Région** a pour effet de remplacer les exigences EN50131 par les réglementations locales ou nationales.

La sélection de **Grade 2** ou **Grade 3** entraîne la prise en compte des exigences EN50131 et de certaines exigences complémentaires INCERT :

- Seul un Installateur peut réinitialiser un événement d'autosurveillance. Pour INCERT, cela s'applique à tous les grades.
  Il ne s'agit normalement que d'une exigence pour Grade III En50131.
- Un événement d'autosurveillance d'une zone inhibée ou isolée doit être envoyé au CTS et affiché pour l'utilisateur.
  Pour INCERT, les événements d'autosurveillance sont traités pour les zones isolées. Pour toutes les autres variantes standards, les événements d'autosurveillance sont ignorés pour les zones isolées.
- Les codes utilisateur doivent être définis par plus de 4 chiffres.

Exigences matérielles

- La capacité minimale de la batterie du SPC42xx/43xx/52xx/53xx/63xx est de 10 Ah / 12 V. Si vous utilisez une batterie de 10 Ah, la batterie est tournée vers la gauche du boîtier et la patte du bas est pliée pour la retenir.
- Placez le cavalier (J12) sur le sélecteur de batterie lorsque vous utilisez une batterie de 17 à 10 Ah, et retirez-le pour une batterie de 7 Ah.
- La quantité de courant de la sortie Aux avec une batterie de 10 Ah (SPC42xx/52xx) est :

COMMS / Durée de veille	AUCUN (mA)	RTC (mA)	GSM (mA)	RTC + GSM (mA)
12 h	568	543	438	413
24 h	214	189	84	59
30 h	143	118	13	Indisponible
60 h	2	Indisponible	Indisponible	Indisponible

- La quantité de courant de la sortie Aux avec une batterie de 10 Ah (SPC43xx/SPC53xx/SPC63xx) est :

COMMS / Durée de veille	AUCUN (mA)	RTC (mA)	GSM (mA)	RTC + GSM (mA)
12 h	538	513	408	383
24h	184	159	54	29
30 h	113	88	Indisponible	Indisponible
60h	Indisponible	Indisponible	Indisponible	Indisponible

3.2.4 Directives de conformité PD 6662:2010

Ce document contient tous les critères d'installation, de mise en service et de maintenance du système SPC pour faire en sorte qu'il soit conforme à la norme PD 6662:2010.

3.2.4.1 Étendue du produit

Ce document concerne les composants suivants du système SPC :

Contrôleur Grade 2 SPC4320.320-L1	
Contrôleur Grade 2 SPC5320.320-L1	Transpondeur SPCE652.100, 8 entrées / 2 sorties
Contrôleur Grade 3 SPC5330.320-L1	Transpondeur SPCP332.300 Smart PSU avec transpondeur E/S
Contrôleur Grade 3 SPC5350.320-L1	Smart PSU avec transpondeur SPCP355.300 8 entrées / 2 sorties
Contrôleur Grade 3 SPC6330.320-L1	
Contrôleur Grade 3 SPC6350.320-L1	Smart PSU avec transpondeur E/S SPCP333.300
Clavier LCDSPCK420/421.100	Module RTC SPCN110.000
Transpondeur SPCE452.100, 8 sorties de relais	Module GSM SPCN320.000

3.2.4.2 Aperçu des normes

Les directives sont fournies pour la mise en œuvre de la conformité à PD 6662:2010 d'un système SPC, aux normes suivantes :

PD 6662:2010	BS EN 50136-1-5:2008
BS 4737-3.1:1977	BS EN 50136-2-1:1998 +A1:1998
BS 8243:2010	BS EN 50136-2-2:1998
BS 8473:2006+A1:2008	BS EN 50136-2-3:1998
BS EN 50131-1:2006+A1:2009	BS EN 50131-3:2009
BS EN 50136-1-1:1998+A2:2008	BS EN 50131-6:2008
BS EN 50136-1-2:1998	DD 263:2010
BS EN 50136-1-3:1998	DD CLC/TS 50131-7:2008

3.2.4.3 Méthodes d'obtention de l'activation et de la désactivation

Méthodes d'obtention de l'activation (BS 8243:2010 - Clause 6.3)

La fin / arrêt de la procédure complète d'activation est obtenu(e) à l'aide des méthodes suivantes :

a) Serrure de blocage posée sur la dernière porte de sortie

Une serrure de blocage doit être installée par l'installateur de la manière suivante :

un type de TEMPORISATION DE SORTIE doit être configuré pour le SPC.

Voir *Types de zone* page 397.

b) Appuyez sur le bouton-poussoir monté à l'extérieur des locaux objet de la surveillance

Connectez le bouton-poussoir à l'entrée de zone SPC de la manière suivante :

un type de TEMPORISATION DE SORTIE doit être configuré pour le SPC.

Voir *Types de zone* page 397.

c) Commutateur de protection (par exemple, contact de porte) monté sur la porte de sortie finale des locaux sous alarme ou du secteur

Connectez le commutateur au système SPC de la manière suivante :

le contact est monté sur la porte de sortie finale et est connecté à une zone d'ENTRÉE/SORTIE avec un attribut « Sortie finale ».

Voir *Types de zone* page 397 et *Attributs zone* page 404.

Il est possible de mettre en place un signal d'utilisation erronée en vous servant de la fonction d'annulation d'alarme. Cela est activé par défaut.

Voir *Options* page 130 (Clavier) et *Options* page 257 (Navigateur).

d) Clé numérique

N'est pas prise en charge par la SPC.

e) En association avec un CTS

Cette méthode d'activation est prise en charge à l'aide du logiciel SPC COM XT ou d'un autre logiciel tiers CTS prenant en charge les commandes EDP.

Méthodes d'exécution de la désactivation (BS 8243:2010 - Clause 6.4)

La conformité des méthodes de désactivation est garantie de la manière suivante :

6.4.1 Pour toutes les méthodes de désactivation dans le système SPC, l'utilisateur reçoit une indication sonore que le système a été désactivé avec succès. Cette indication prend la forme d'une séquence de bips émis par le CIE.

6.4.2 Prévention de l'entrée dans les locaux surveillés avant que le système d'alarme anti-intrusion (SAAI) soit désactivé :

a) Le déverrouillage de la porte d'entrée de départ provoque la désactivation du SAAI ;

conformité par le SPC si le type de zone CLÉ DE MES est utilisé uniquement avec l'attribut MHS. Ce type de zone ne doit pas être utilisé pour l'activation.

b) La désactivation du SAAI par l'utilisateur avant l'entrée dans les locaux supervisés cause ou permet que la porte d'entrée de départ soit déverrouillée.

Conformité du SPC par désactivation à l'aide d'un lecteur de carte d'accès sur un lecteur d'entrée à l'aide de l'option MHS ou par entrée à partir d'un système d'accès tiers sur une zone ARME PAR CLEF avec un attribut MHS.

6.4.3 Prévention de l'entrée sur des locaux surveillés avant que tous les moyens de la confirmation d'alarme anti-intrusion aient été désactivés :

a) Le déverrouillage de la porte d'entrée de départ fait que tous les moyens de confirmation sont désactivés

L'utilisation n'est pas permise par le SPC.

b) La désactivation de tous les moyens de confirmation par l'utilisateur avant d'entrer dans les locaux surveillés fait que, ou permet que, la porte d'entrée soit déverrouillée.

L'utilisation n'est pas permise par le SPC.

6.4.4 L'ouverture de la porte d'entrée de départ désactive tous les moyens de confirmation de l'alarme anti-intrusion

L'utilisation n'est pas permise par le SPC.

6.4.5 Désactivation à l'aide d'une clé numérique

a) Utilisation d'une clé numérique avant d'entrer dans les locaux surveillés (par exemple, via radio)

Le SPC est conforme à cette clause lorsque l'installateur met en place un lecteur TAG (par exemple, SPCK421) hors des locaux.

b) Utilisation d'une clé numérique après entrée dans les locaux supervisés à partir d'un site aussi proche et utilisable de la porte d'entrée de départ.

Cette fonctionnalité est fournie à l'aide d'un lecteur TAG (par exemple, SPCK421) à côté de la porte d'entrée d'un local.

Voir *Types de zone* page 397 et *Attributs zone* page 404.

AVERTISSEMENT : nous attirons votre attention sur le fait qu'en autorisant cette méthode de désactivation, si un intrus réussit à forcer la porte d'entrée de départ, la police ne sera pas appelée, quelle que soit la progression de l'intrus dans les locaux.

Cette méthode de désactivation du système d'alarme de l'intrus peut s'avérer inacceptable pour vos assureurs.

6.4.6 Désactivation en association avec un centre de télésurveillance (CTS)

Conformité du SPC utilisant un logiciel de CTS tiers. L'indication externe au bâtiment doit se faire avec un buzzer/flash minuté ou équivalent qui fonctionnera sur un système désactivé pendant une période minutée de, par exemple, 30 secondes.

Voir *Temporisations* page 134.

3.2.4.4 Exigences en matière de configuration pour la conformité avec la PD 6662:2010

Recommandations pour l'enregistrement des conditions d'alarme signalée à distance (BS 8243:2010 – Annexes G.1 et G.2)

Les conditions d'alarme peuvent être divisées en catégories pour l'analyse selon l'Annexe G, si le système SPC est configuré pour que le minuteur d'entrée soit réglé sur une valeur inférieure à 30 secondes. Le délai du minuteur est lui aussi réglé sur 30 secondes.

Consultez les sections suivantes :

- *Secteurs* page 138
- *Ajouter/Éditer un secteur* page 278
- *Temporisations* page 134

Exigences pour les systèmes utilisant des chemins d'alarme dédiés (BS EN 50136-1-2, 1998)

Le système SPC devrait être configuré pour effectuer un test automatique d'appel au CTS.

Le système SPC devrait être configuré avec une sortie « Défaut Transmission ».

Consultez la section suivante :

- *Ajouter/Éditer un CTS au moyen d'un SIA ou CID* page 336

Exigences pour les équipements utilisés dans des systèmes avec communicateurs numériques utilisant un RTC (BS EN 50136-2-2, 1998)

Sortie de défaut

Le système SPC devrait être configuré avec une sortie « Défaut Transmission ».

Consultez les sections suivantes :

- *Sorties* page 160 (Clavier)
- *Configuration des entrées/sorties du contrôleur* page 226 (Navigateur)
- *Ajouter/Éditer un CTS au moyen d'un SIA ou CID* page 336

Tentatives de retransmission

Les tentatives de retransmission (tentatives de numérotation) sont configurés dans ce manuel :

- *Ajouter/Éditer un CTS au moyen d'un SIA ou CID* page 336
- *Éditer les paramètres EDP* page 347

Au minimum 1 et au maximum 12 retransmissions sont permises.

Intrusion et hold-up – conception de système (DD CLC TS 50131-7, 2008)

Mise en et hors surveillance

Le système SPC est configurable de telle manière que l'activation est terminée par « Sortie finale ».

Il est possible de configurer le SPC pour qu'un PA (périphérique d'avertissement) soit momentanément activé lors de la mise en œuvre.

Consultez les sections suivantes :

- *Temporisations* page 134
- *Attributs zone* page 404
- *Sorties* page 160 (Clavier)
- *Éditer une sortie* page 228 (Navigateur)

Alarme d'intrusion et d'agression confirmée (BS8243:2010 Désignation des signaux d'alarme d'agression (HUA) pour confirmation séquentielle)

Le système SPC est configurable afin que les scénarios de déclenchement de plus de deux minutes survenant hors des zones d'agression ou de périphérique d'agression (HD) provoquent l'envoi d'un événement confirmé d'alarme d'agression (HV pour SIA et 129 pour CID) au CIE :

- deux activations de zone d'agression
- une activation de zone d'agression et de zone de panique

Si une activation (zone d'agression et zone anti-sabotage ou zone de panique et zone anti-sabotage) survient dans le délai de deux minutes, cela déclenche également l'envoi d'un événement confirmé d'alarme d'agression.

Une agression confirmée ne réclame pas de RAZ installateur, même si cette option est activée. Tout événement d'agression confirmé est enregistré dans le journal système.

3.2.4.5 Exigences supplémentaires de mise en œuvre pour conformité à PD 6662:2010

Information à inclure dans la proposition de structure du système et dans le document correspondant à l'installation mise en place (BS 8243:2010 - Annexe F)

- Pendant l'installation, la configuration et la mise en œuvre d'un système SPC, l'installateur doit suivre les lignes directrices suivantes, comme l'exige l'annexe ci-dessus :
- il est recommandé que les chemins doubles soient utilisés pour signaler lesquels sont utilisés dans le système SPC à l'aide des options GSM, RTC et Ethernet.
- Le système SPC doit être installé et configuré pour fournir un système de confirmation efficace. Toute exception doit être mise en évidence dans le document « Comme installé ».
- Les combinaisons et les séquences contribuant à une alarme confirmée devraient être clairement notifiées à l'utilisateur final.
- L'heure de confirmation de l'intrusion devrait clairement être notifiée à l'utilisateur final.
- Les méthodes de mise en œuvre de l'activation et de la désactivation devraient clairement être décrites à l'utilisateur final, comme détaillé dans ce document.
- Assurez-vous que des accords écrits sont fournis à l'utilisateur final en cas d'échec d'un verrouillage.

Il est recommandé que l'étiquette incluse PD 6662:2010 soit fixée à un emplacement adéquat à l'intérieur du boîtier du SPC, à côté de l'étiquette du type de produit.

3.2.4.6 Informations supplémentaires

Exigences du réseau de transmission – niveaux de performance, de disponibilité et de sécurité (BS EN 50136-1-2, 1998 et BS EN 50136-1-5, 2008)

Le système SPC a été testé et approuvé selon la norme EN50136-1-1.

Les niveaux du SPC sont classifiés de la manière suivante :

Temps de transmission	D2 comme max.
Temps de transmission, valeurs maxi	M0 – M4
Temps de reporting	T3 comme max.
Disponibilité	Voir *Niveaux ATS et spécifications d'atténuation* page 409.
Niveau de sécurité de l'émission de signal	Testé selon EN50136-1-1 et classé « S0 ».

3.2.5 Conformité aux agréments VDS

Ce document contient les informations nécessaires à l'installation du produit en vue d'obtenir l'agrément VdS.

Vanderbilt

SPC42xx/43xx/53xx/63xx : numéro d'approbation VdS G112104, G112124 et G112128. Certificats VdS EN-ST000142, EN-ST000143, EN-ST000055, EN-ST000056, EN-ST000057, EN-ST000058, EN-ST000061, EN-ST000062.

Siemens

SPC42xx/43xx/53xx/ : numéro d'approbation VdS G116035. Certificats VdS EN-ST000225, EN-ST000226, EN-ST000227, EN-ST000228, EN-ST000229, EN-ST000230, EN-ST000231, EN-ST000232.

Cette section décrit la conformité de ce système avec les agréments VdS.

Configuration du logiciel pour la conformité VdS

Pour obtenir la conformité VDS lors du paramétrage du système, suivez la procédure ci-dessous :

1. connectez-vous à la centrale avec le navigateur.
2. Cliquez sur **Mode Paramétrage**.
3. Cliquez sur **Configuration > Système > Normes**.
4. Sélectionnez **Europe** dans la section **Continent** de la page.
5. Sélectionnez **Allemagne** dans la section **Pays pour la conformité** de la page.
6. Sélectionnez le grade VDS requis par votre type d'installation.

Reporting erreur matérielle — dans **Configuration > Système > Options du système**, vous devez sélectionner l'option **Validé + reporting (10 s)** de la liste déroulante du **Mode sortie watchdog**.

les défauts matériels ne sont pas signalés si l'ingénieur est connecté au système.

Matériel

La conformité VDS exige les points suivants :

- un boîtier G5 avec l'antisabotage (autosurveillance) avant mis en œuvre comme exigence minimale.
- Les claviers ne montrent pas d'information de statut si le système est armé.
- Le nombre de zones prises en charge est affiché.
  – 512 zones en configuration en anneau
  – 128 zones par X-BUS en configuration multipoint (en branche)
- Les combinaisons suivantes de résistance de fin de ligne ne sont pas conformes aux normes

VdS :

– 1k, 470 ohms

– 1k, 1k, 6k6 ohms

3.2.6 Conformité au référentiel de la certification NF&A2P incluant les exigences CYBER

Adresse de l'organisme certificateur	
CNPP Cert Route de la Chapelle Réanville CS 22265 F-27950 SAINT MARCEL www.cnpp.com	**AFNOR Certification** 11 rue François de Pressensé 93571 Saint Denis La Plaine Cedex www.marque-nf.com

Afin de satisfaire aux exigences d'installation NF et A2P, ce boîtier doit être scellé après son installation en y apposant l'étiquette infalsifiable jointe.

3.2.6.1 Conformité au référentiel de la certification NF&A2P incluant les exigences CYBER

Pour être conforme au référentiel NF&A2P et aux exigences CYBER, le serveur Web HTTP doit être dévalidé selon les instructions suivantes. La configuration du système ne pourra alors se faire qu'avec l'outil SPC Connect Pro via la prise USB de la centrale SPC.

Pour dévalider l'interface Web de la centrale SPC:

1. Passer en mode programmation et sélectionner l'option **Communications**.
2. Sous l'onglet **Services**, décocher la case **HTTP activé**.

Cela désactivera l'interface web de la centrale SPC.

3.2.6.2 Conformité au référentiel de la certification NF&A2P incluant les exigences CYBER - Les produits SPC

Les produits SPC listés ont été testés conformément à la norme NF324 - H58, avec référence aux normes RTC50131-6 et RTC50131-3 et aux certifications EN en vigueur. Voir *Conformité aux agréments EN50131* page 23.

Type de produit	Configuration	Standard	Logo
SPC6350.320 + SPCP355.300 Cert. 1233700001 + Cert.8033700002	60 h, non monitorisé	NF Grade 3, Classe 1	
SPC5350.320 + SPCP355.300 Cert. 1233700001 + Cert.8033700002	60 h, non monitorisé		
SPC6350.320 Cert. 1233700001	60 h, non monitorisé		
SPC5350.320 Cert. 1233700001	60 h, non monitorisé		
SPC6330.320 + SPCP333.300 Cert. 1232200003	60 h, non monitorisé	NF Grade 3, Classe 1	
SPC5330.320 + SPCP333.300 Cert. 1232200003	60 h, non monitorisé		
SPC6330.320 Cert. 1232200003	30 h, monitorisé		
SPC5330.320 Cert. 1232200003	30 h, monitorisé		
SPC5320.320 Cert. 1222200003	36 h, non monitorisé	NF Grade 2, Classe 1	
SPC4320.320 Cert. 1222200003	36 h, non monitorisé		

Type de produit	Configuration	Standard	Logo
SPCN110.000 SPCN320.000 SPCK420.100 SPCK620.100 SPCK623.100 SPCE652.100 SPCE452.100 SPCE110.100 SPCE120.100		NF Grades 2 et 3, Classe 1	

4 Données techniques

Ce chapitre recouvre :

4.1 SPC4000 ..... **35**
4.2 SPC5000 ..... **38**
4.3 SPC6000 ..... **41**
4.4 SPCP355.300 ..... **44**

4.1 SPC4000

Zones programmables	4
Max. nombre de codes utilisateur	100
Télécommandes	Jusqu'à 32
Modules TAG	32
Alarme panique radio	Jusqu'à 128
Historique	1 000 événements d'intrusion, 1 000 .... événements d'accès
Nombre de zones intégrées	8
Max. nombre de zones câblées	32
Max. nombre de zones radio	32 (retrancher les zones câblées)
Max. nombre de détecteurs radio Intrunet par récepteur radio (recommandé)	20
Résistance fin de ligne (EOL)	Deux 4K7 (par défaut), autres combinaisons de résistances configurables
Nombre de relais intégrés	1 flash (courant de commutation résistif 30 VCC / 1 A)
Nombre de collecteurs ouverts intégrés	2 sirènes internes/externes, 3 librement programmables (chacune avec un courant de commutation résistif maximal de 400 mA, fourni par la sortie auxiliaire)
Version du Firmware	V3.x
Capacité en portes	Max. 4 portes d'entrée ou 2 portes d'entrée/sortie
Nombre de lecteurs de badge	Max. 4

Module radio	• SPC4221 : récepteur SiWay RF intégré (868 MHz) • SPC4320.220 : optionnel (SPCW111) • SPC4320.320 : optionnel (SPCW110)
Vérification	4 zones de vérification avec au maximum 4 caméras IP et 4 appareils audio.
Vidéo	Jusqu'à 16 images pré-événement / 16 images post-événement (avec une résolution JPEG 320 x 240, 1 image/seconde maxi)
Audio	Jusqu'à 60 s. pré-événement / 60 s. enregistrement audio post-événement
Bus de terrain 1)	X-BUS sur RS-485 (307 ko/s)
Nombre de périphériques de terrain 2)	Max. 11 (4 claviers, 2 transpondeurs de porte, 5 transpondeurs d'entrée/sortie)
Tags de terrain connectables	• Claviers : SPCK42x, SPCK52x, SPCK62x • Transpondeurs de porte : SPCA210, SPCP43x • Transpondeurs avec E/S : SPCE65x, SPCE45x, SPCP33x, SPCE110, SPCE120, SPCV32x
Interfaces	• X-BUS (1 branche) • 1 RS232 • USB (connexion PC) • SPC43xx : en ajoutant 1 Ethernet (RJ45)
Contact antisabotage	Anti-effraction frontale intégrée à ressort, 2 entrées de contact anti-effraction auxiliaires
Alimentation	Type A (selon EN50131-1)
Tension secteur	230 VCA, + 10 %/ -15 %, 50 Hz
Fusible d'alimentation secteur	250 mA T (pièce remplaçable sur le bornier d'alimentation)
Consommation électrique	SPC42xx : max. 160 mA à 230 VCA SPC43xx : max. 200 mA à 230 VCA
Courant de service	Contrôleur SPC42xx : max. 160 mA à 12 VCC Contrôleur SPC43xx : max. 200 mA à 12 VCC
Courant de repos	Contrôleur SPC42xx : Max. 140 mA à 12 VCC (165 mA avec RTC, 270 mA avec GSM, 295 mA avec RTC et GSM) Contrôleur SPC43xx : Max. 170mA à 12 VCC (195mA avec RTC, 300mA avec GSM, 325mA avec RTC et GSM)
Tension en sortie	13 – 14 VCC en conditions normales (alimentation secteur et batterie totalement chargée), minimum 10,5 VCC avec alimentation par appareil secondaire (avant l'arrêt du système pour se protéger d'une décharge profonde de la batterie)
Déclencheur basse tension	7,5 VCC

Protection contre les surtensions	15,7 VCC
Ondulation crête à crête	Max. 5 % de la tension de sortie
Alimentation auxiliaire (nominale)	Max. 750mA à 12 VCC
Type de batterie (Batterie non fournie)	YUASA NP7-12FR (7Ah) - NF PowerSonic PS1270 12v/7.0Ah Yuasa Yucel Y7-12FR
Chargement de la batterie	SPC422x/4320 : max. 72 h pour 80 % de la capacité de la batterie
Protection de la batterie	Courant limité à 1 A (protection par fusible), protection contre la décharge profonde à 10,5 VCC +/- 3 %
Mise à jour du logiciel	Mise à niveau locale et à distance pour les centrales, les périphériques et les modems GSM / RTC.
Étalonnage	Aucun contrôle d'étalonnage nécessaire (étalonnage en usine)
Pièces remplaçables par l'utilisateur	Pas de pièces remplaçables par l'utilisateur
Températures de fonctionnement	Entre -10 et 50 ºC
Humidité relative	Max. 90 % (sans condensation)
Couleur	RAL 9003 (blanc signal)
Poids	SPC422x/4320 : 4,500 kg
Dimensions (l x h x p)	SPC422x/4320 : 264 x 357 x 81 mm
Boîtier	SPC4320.320 : petit boîtier métal (acier doux 1,2 mm) SPC422x.220 : petit boîtier avec base métallique (acier doux 1,2 mm) et couvercle en plastique
Le boîtier peut contenir jusqu'à	SPC422x/4320 : 1 transpondeur supplémentaire (taille 150 x 82 mm)
Indice IP	30
ATS	3
ATP	8
Profils d'événement	5
Exceptions d'événement	10
Profils de commande	5

1) Maxi 400 m entre les périphériques/câbles des types IYSTY 2 x 2 x Ø 0,6 mm (mini), UTP cat5 (âme pleine) ou Belden 9829.

2) Il est possible d'adresser davantage de transpondeurs d'E/S à la place de claviers ou de transpondeurs de porte, mais le nombre d'entrées/sorties programmables ne peut pas dépasser les limites indiquées pour le système.

4.2 SPC5000

Zones programmables	16
Max. nombre de codes utilisateur	500
Télécommandes	100 max.
Modules TAG	250
Alarme panique radio	Jusqu'à 128
Historique	10 000 événements d'intrusion, 10 000 événements d'accès
Nombre de zones intégrées	• SPC5320/5330 — 8 • SPC5350 — 16
Max. nombre de zones câblées	128
Max. nombre de zones radio	120 (retrancher les zones câblées)
Max. nombre de détecteurs radio Intrunet par récepteur radio (recommandé)	20
Résistance fin de ligne (EOL)	Deux 4K7 (par défaut), autres combinaisons de résistances configurables
Sorties de relais	• SPC5320\5330 — 1 flash (courant de commutation résistif 30 VCC / 1 A) • SPC5350 — 4 (relais de commutation unipolaire, 30 VCC / courant de commutation résistif maxi 1 A)
Sorties électroniques	• SPC5320/5330 — 5 sorties : – 2 sirènes internes/externes – 3 programmables Courant de commutation résistif maximum 400 mA par sortie, fourni par la sortie auxiliaire. • SPC5350 — 8 sorties. Courant de commutation résistif maximum 400 mA par sortie – 5 sorties d'alimentation standards – 3 sorties surveillées
Version du Firmware	V3.x
Capacité en portes	Max. 16 portes d'entrée ou 8 portes d'entrée/sortie
Nombre de lecteurs de badge	Max. 16
Module radio	Optionnel (SPCW110)
Vérification	16 zones de vérification avec au maximum 4 caméras IP et 16 appareils audio.

Vidéo	Jusqu'à 16 images pré-événement / 16 images post-événement (avec une résolution JPEG 320 x 240, 1 image/seconde maxi.)
Audio	Jusqu'à 60 s. pré-événement / 60 s. enregistrement audio post-événement
Bus de terrain 1)	X-BUS sur RS-485 (307 ko/s)
Nombre de périphériques de terrain 2)	Max. 48 (16 claviers, 8 transpondeurs de porte, 16 transpondeurs d'entrée/sortie)
Tags de terrain connectables	• Claviers : SPCK42x, SPCK52x, SPCK62x • Transpondeurs de porte : SPCA210, SPCP43x • Transpondeurs avec E/S : SPCE65x, SPCE45x, SPCP33x, SPCP35x, SPCE110, SPCE120, SPCV32x
Interfaces	• 2 X-BUS (2 branches ou 1 boucle) • 2 RS232 • 1 USB (connexion PC) • SPC53xx : en ajoutant 1 Ethernet (RJ45)
Contact antisabotage	• SPC5320/5330 : antisabotage frontal intégré à ressort, 2 entrées de contact antisabotage auxiliaires • SPC5350 : interrupteur d'autosurveillance avant/arrière
Alimentation	Type A (selon EN50131-1)
Tension secteur	230 VCA, + 10 %/ -15 %, 50 Hz
Fusible d'alimentation secteur	• SPC5320/5330 : 250 mA T (pièce remplaçable sur le bornier d'alimentation) • SPC5350 : 800 mA T (pièce remplaçable sur le bornier d'alimentation)
Consommation électrique	• SPC5320/5330 : max. 200 mA à 230 VCA • SPC5350 : max. 500 mA à 230 VCA
Courant de service	• SPC5320/5330 : contrôleur : maxi 200 mA à 12 VCC • SPC5350 : max. 210 mA à 12 VCC
Courant de repos	Contrôleur SPC53xx : max. 170 mA à 12 VCC (195 mA avec RTC, 300 mA avec GSM, 325 mA avec RTC et GSM)
Tension en sortie	13 – 14 VCC en conditions normales (alimentation secteur et batterie totalement chargée), minimum 10,5 VCC avec alimentation par appareil secondaire (avant l'arrêt du système pour se protéger d'une décharge profonde de la batterie)
Déclencheur basse tension	11 VCC
Protection contre les surtensions	• SPC5320/5330 : 15,7 VCC • SPC5350 : 15 VCC nominal
Ondulation crête à crête	Max. 5 % de la tension de sortie
Alimentation auxiliaire (nominale)	• SPC5320/5330 : max. 750mA à 12 VCC • SPC5350 : max. 2 200 mA à 12 VCC (8 sorties à fusibles séparés, 300 mA par sortie)

Type de batterie (Batterie non fournie)	SPC5320 • YUASA NP7-12FR (7Ah) - NF • PowerSonic PS1270 12v/7.0Ah • Yuasa Yucel Y7-12FR SPC5330 • YUASA NP17-12IFR (17Ah) - NF • Yuasa Yucel Y17-12FR • PowerSonic PS12170 12v/17.0Ah SPC5350 • FIAMM FGV22703 (12V 27Ah) - NF • PowerSonic PS12260FR 12v/26.0Ah • PowerSonic PS12170 12v/17.0Ah • Alarmcom AB1227-0 (12V 27Ah) • YUASA NPL24-12IFR (12V 24Ah) • Yuasa Yucel Y17-12IFR • Yuasa Yucel Y24-12FR
Chargement de la batterie	• SPC5320 : max. 72 h, • SPC5330/5350 : max. 24 h pour 80 % de la capacité de la batterie
Protection de la batterie	• SPC5320/5330 : courant limité à 1 A (protection par fusible), protection contre la décharge profonde à 10,5 VCC +/- 3 % • SPC5350 : courant limité à 2 A (protégé par fusible PTC réinitialisable), protection contre la décharge profonde à 10,5 VCC
Mise à jour du logiciel	Mise à niveau locale et à distance pour les centrales, les périphériques et les modems GSM / RTC.
Étalonnage	Aucun contrôle d'étalonnage nécessaire (étalonnage en usine)
Pièces remplaçables par l'utilisateur	• SPC5320/5330 : pas de pièces remplaçables par l'utilisateur • SPC5350 : 8 fusibles en verre (400 mA AT) pour les sorties 12 VCC
Températures de fonctionnement	Entre -10 et 50 ºC
Humidité relative	Max. 90 % (sans condensation)
Couleur	RAL 9003 (blanc signal)
Poids	• SPC5320 : 4,500 kg • SPC5330 : 6,400 kg • SPC5350 : 18,600 kg
Dimensions (l x h x p)	• SPC5320 : 264 x 357 x 81 mm • SPC5330 : 326 x 415 x 114 mm • SPC5350 : 498 x 664 x 157 mm

Boîtier	• SPC5320 : petit boîtier métal (acier doux 1,2 mm) • SPC5330 : boîtier métal articulé (acier doux 1,2 mm) • SPC5350 : boîtier métal (acier doux 1,5 mm)
Le boîtier peut contenir jusqu'à	• SPC5320 : 1 transpondeur supplémentaire • SPC5330 : 4 transpondeurs supplémentaires (taille 150 x 82 mm) • SPC5350 : 4 transpondeurs supplémentaires (taille 150 x 82 mm)
Classe IP/IK	30/06
ATS	5
ATP	15
Profils d'événement	10
Exceptions d'événement	50
Profils de commande	8

1) Maxi 400 m entre les périphériques/câbles des types IYSTY 2 x 2 x Ø 0,6 mm (mini), UTP cat5 (âme pleine) ou Belden 9829.

2) Il est possible d'adresser davantage de transpondeurs d'E/S à la place de claviers ou de transpondeurs de porte, mais le nombre d'entrées/sorties programmables ne peut pas dépasser les limites indiquées pour le système.

4.3 SPC6000

Zones programmables	60
Max. nombre de codes utilisateur	2500
Télécommandes	100 max.
Modules TAG	250
Alarme panique radio	Jusqu'à 128
Historique	10 000 événements d'intrusion, 10 000 événements d'accès
Nombre de zones intégrées	• SPC6320/6330 — 8 • SPC6350 — 16
Max. nombre de zones câblées	512
Max. nombre de zones radio	120 (retrancher les zones câblées)
Max. nombre de détecteurs radio Intrunet par récepteur radio (recommandé)	20

Résistance fin de ligne (EOL)	Deux 4K7 (par défaut), autres combinaisons de résistances configurables
Sorties de relais	• SPC6320\6330 — 1 flash (courant de commutation résistif 30 VCC / 1 A) • SPC6350 — 4 (relais de commutation unipolaire, 30 VCC / courant de commutation résistif maxi 1 A)
Sorties électroniques	• SP6320/6330 — 5 sorties : – 2 sirènes internes/externes – 3 programmables Courant de commutation résistif maximum 400 mA par sortie, fourni par la sortie auxiliaire. • SPC6350 — 8 sorties. Courant de commutation résistif maximum 400 mA par sortie – 5 sorties d'alimentation standards – 3 sorties surveillées
Version du Firmware	V3.x
Capacité en portes	Max. 64 portes d'entrée ou 32 portes d'entrée/sortie
Nombre de lecteurs de badge	Max. 64
Module radio	Optionnel (SPCW110)
Vérification	32 zones de vérification avec au maximum 4 caméras IP et 32 appareils audio.
Vidéo	Jusqu'à 16 images pré-événement / 16 images post-événement (avec une résolution JPEG 320 x 240, 1 image/seconde maxi.)
Audio	Jusqu'à 60 s. pré-événement / 60 s. enregistrement audio post-événement
Bus de terrain 1)	X-BUS sur RS-485 (307 ko/s)
Nombre de périphériques de terrain 2)	Max. 128 (32 claviers, 32 transpondeurs de porte, 64 transpondeurs d'entrée/sortie)
Tags de terrain connectables	• Claviers : SPCK42x, SPCK52x, SPCK62x • Transpondeurs de porte : SPCA210, SPCP43x • Transpondeurs avec E/S : SPCE65x, SPCE45x, SPCP33x, SPCP35x, SPCE110, SPCE120, SPCV32x
Interfaces	• 2 X-BUS (2 branches ou 1 boucle) • 2 RS232 • 1 USB (connexion PC) • SPC63xx : en ajoutant 1 Ethernet (RJ45)
Contact antisabotage	• SPC6330 : antisabotage frontal intégré à ressort, 2 entrées de contact antisabotage auxiliaires • SPC6350 : interrupteur d'autosurveillance avant/arrière
Alimentation	Type A (selon EN50131-1)
Tension secteur	230 VCA, +10 % / -15 %, 50 Hz

Fusible d'alimentation secteur	• SPC6330 : 250 mA T (pièce remplaçable sur le bornier d'alimentation) • SPC6350 : 800mA T (pièce remplaçable sur le bornier d'alimentation)
Consommation électrique	• SPC6330 : max. 200mA à 230 VCA • SPC6350 : max. 500mA à 230 VCA
Courant de service	• SPC6330 : max. 200mA à 12 VCC • SPC6350 : max. 210mA à 12 VCC
Courant de repos	Contrôleur SPC63xx : max. 170 mA à 12 VCC (195 mA avec RTC, 300 mA avec GSM, 325 mA avec RTC et GSM)
Tension en sortie	• SPC6330 : 13 – 14 VCC en conditions normales (alimentation secteur et batterie totalement chargée), minimum 10,5 VCC avec alimentation par appareil secondaire (avant l'arrêt du système pour se protéger d'une décharge profonde de la batterie) • SPC6350 : 13 – 14 VCC en conditions normales (alimentation secteur et batterie totalement chargée), minimum 10,5 VCC avec alimentation par appareil secondaire (avant l'arrêt du système pour se protéger d'une décharge profonde de la batterie)
Déclencheur basse tension	11V CC
Protection contre les surtensions	• SPC6330 : 15,7 VCC • SPC6350 : 15 VCC nominal
Ondulation crête à crête	Max. 5 % de la tension de sortie
Alimentation auxiliaire (nominale)	• SPC6330 : max. 750mA à 12 VCC • SPC6350 : max. 2 200 mA à 12 VCC (8 sorties à fusibles séparés, 300 mA par sortie)
Type de batterie (Batterie non fournie)	SPC6330 • YUASA NP17-12FR (17Ah) - NF • Yuasa Yucel Y17-12IFR • Yuasa Yucel Y24-12FR • PowerSonic PS12170 12v/17.0Ah • PowerSonic PS12260 12v/26.0Ah SPC6350 • YUASA NP17-12FR (17Ah) - NF • FIAMM FGV22703 (12V 27Ah) - NF • YUASA NPL24-12IFR (12V 24Ah) • Alarmcom AB1227-0 (12V 27Ah) • PowerSonic PS12260 12v/26.0Ah
Chargement de la batterie	SPC63xx : max. 24 h pour 80 % de la capacité de la batterie

Protection de la batterie	• SPC6330 : courant limité à 1 A (protection par fusible), protection contre la décharge profonde à 10,5 VCC +/- 3 % • SPC6350 : courant limité à 2 A (protégé par fusible PTC réinitialisable), protection contre la décharge profonde à 10,5 VCC, voyant de basse tension à 11 VCC
Mise à jour du logiciel	Mise à niveau locale et à distance pour les centrales, les périphériques et les modems GSM / RTC.
Étalonnage	Aucun contrôle d'étalonnage nécessaire (étalonnage en usine)
Pièces remplaçables par l'utilisateur	• SPC6330 : pas de pièces remplaçables par l'utilisateur • SPC6350 : 8 fusibles en verre (400 mA AT) pour les sorties 12 VCC
Températures de fonctionnement	Entre -10 et 50 ºC
Humidité relative	Max. 90 % (sans condensation)
Couleur	RAL 9003 (blanc signal)
Poids	• SPC6330 : 6,400 kg • SPC6350 : 18,600 kg
Dimensions (l x h x p)	• SPC6330 : 326 x 415 x 114 mm • SPC6350 : 498 x 664 x 157 mm
Boîtier	• SPC6330 : boîtier métal articulé (acier doux 1,2 mm) • SPC6350 : boîtier métal (acier doux 1,5 mm)
Le boîtier peut contenir jusqu'à	• SPC6330 : 4 transpondeurs supplémentaires (taille 150 x 82 mm) • SPC6350 : 6 transpondeurs supplémentaires (150 x 82 mm) ou 1 centrale supplémentaire + 4 transpondeurs
Classe IP/IK	30/06
ATS	10
ATP	30
Profils d'événement	20
Exceptions d'événement	100
Profils de commande	10

1) Maxi 400 m entre les périphériques/câbles des types IYSTY 2 x 2 x Ø 0,6 mm (mini), UTP cat5 (âme pleine) ou Belden 9829.

2) Il est possible d'adresser davantage de transpondeurs d'E/S à la place de claviers ou de transpondeurs de porte, mais le nombre d'entrées/sorties programmables ne peut pas dépasser les limites indiquées pour le système.

4.4 SPCP355.300

Nombre de zones intégrées	8

Résistance fin de ligne (EOL)	Deux 4K7 (par défaut), autres combinaisons de résistances possibles
Sorties de relais	3 (relais de commutation unipolaires, 30 VCC / courant de commutation résistif maximal 1 A)
Sorties électroniques	3 supervisés (chacun avec courant de commutation résistif maximal 400 mA),
Interfaces	X-BUS (entrée, sortie, branche)
Tension secteur	230 VCA, +10 à -15 %, 50 Hz
Courant de service	Max. 245 mA à 12 VCC (tous les relais activés)
Courant de repos	Max. 195mA à 12 VCC
Tension en sortie	13 – 14 VCC en conditions normales (alimentation secteur et batterie totalement chargée),
Alimentation auxiliaire (nominale)	Max. 2 360 mA à 12 VCC (8 sorties à fusibles séparés, maxi 300 mA par sortie)
Type de batterie (Batterie non fournie)	• FIAMM FGV22703 (12V 27Ah) - NF • YUASA NP17-12FR (17Ah) • YUASA NPL24-12IFR (12V 24Ah) • Alarmcom AB1227-0 (12V 27Ah) • PowerSonic PS12170 12v/17.0Ah • PowerSonic PS12260 12v/26.0Ah • Yuasa Yucel Y17-12IFR • Yuasa Yucel Y24-12FR
Contact antisabotage	Interrupteur d'autosurveillance avant / arrière
Températures de fonctionnement	0 à +40 °C
Boîtier	Boîtier en métal (acier doux 1,5 mm)
Couleur	RAL 9003 (blanc signal)
Dimensions	498 x 664 x 157mm
Poids (sans les batteries)	18,4 kg (boîtier avec capot), 11, 3 kg (boîtier sans capot)
Classe IP/IK	30/06

5 Introduction

Le contrôleur de la série SPC est un contrôleur hybride capable de gérer 8 zones reliées par câble et de communiquer avec les composants d'alarme intrusion.

Sa conception souple permet de combiner les composants fonctionnels (RTC/GSM/RF) et d'améliorer ainsi les capacités du système. Cette approche permet à l'installateur de réaliser le montage rapidement avec un câblage réduit au minimum.

Vue d'ensemble

Numéro	Description	Numéro	Description
1	RTC	13	Transpondeur sans fil
2	GSM	14	Module d'alimentation
3	Ethernet	15	Configuration en boucle
4	Récepteur radio	16	Réseau RTC
5	Alimentation 230 V	17	Réseau GSM
6	Batterie 12 V	18	Routeur haut débit
7	RF	19	Réseau
8	Sorties câblées (6)	20	Central
9	Entrées câblées (8)	21	LAN/WLAN
10	Claviers	22	Bureau d'assistance
11	Transpondeur E/S	23	Utilisateur à distance
12	Sortie transpondeur	24	Interfaces mobiles

6 Installation du matériel

Ce chapitre recouvre :

6.1 Montage d'un boîtier G2 ..... **49**
6.2 Montage d'un boîtier G3 ..... **50**
6.3 Montage d'un boîtier G5 ..... **57**
6.4 Montage d'un clavier **62**
6.5 Montage d'un transpondeur **62**

6.1 Montage d'un boîtier G2

Le boîtier SPC G2 est fourni avec un couvercle métallique ou en plastique. Ce couvercle est fixé sur l'embase du boîtier au moyen de 2 vis de fixation en haut et en bas du couvercle.

Pour ouvrir le boîtier, enlevez les deux vis en vous servant d'un tournevis adéquat et enlevez le couvercle directement de l'embase.

Le boîtier G2 contient la carte de circuit imprimé du contrôleur montée sur 4 colonnettes. Un module d'entrée/sortie en option peut être installé directement sous la carte du contrôleur. Une batterie de capacité maximale 7 Ah peut être montée sous le contrôleur.

Une antenne externe en option doit être montée sur les boîtiers avec capot en métal si la fonction radio est utilisée. Si une antenne est montée, elle doit être activée dans le micrologiciel.

Le boîtier SPC G2 dispose de 3 trous de vis à l'arrière pour la fixation murale.

Pour fixer le boîtier sur le mur, enlevez le couvercle et localisez le premier trou de vis dans la partie supérieure du boîtier. Repérez la position de ce trou à l'endroit voulu sur le mur à l'aide d'un crayon, puis percez le premier trou avec une perceuse. Vissez le boîtier sur le mur et marquez la position des 2 trous de vis inférieurs à l'aide d'un crayon après avoir pris soin d'aligner le boîtier à la verticale.

Il est recommandé d'employer des vis ayant au minimum une tête de 8 mm de diamètre et une tige de 4-5 mm de diamètre et 40 mm de longueur pour le montage du boîtier. Toutefois, selon la nature du mur, d'autres fixations ou des chevilles expansibles peuvent être nécessaires.

Boîtier standard

Numéro	Description
1	Antenne sans fil
2	Contrôleur SPC
3	Trous de vis pour la fixation murale

6.2 Montage d'un boîtier G3

Le boîtier SPC G3 est fourni avec un couvercle avant métallique. Ce couvercle est fixé sur l'embase du boîtier par des charnières et fixé au moyen d'une vis située à droite du couvercle avant.

Pour ouvrir le boîtier, enlevez la vis en vous servant d'un tournevis adapté et ouvrez le couvercle.

Le boîtier G3 contient la carte mère du contrôleur montée sur un support de fixation articulé. Les transpondeurs et les modules d'alimentation peuvent être montés sur la face inférieure du support de fixation articulé ou sur la paroi arrière du boîtier sous le support de fixation.

Numéro	Description
1	Transpondeurs / module d'alimentation
2	E/S Centrale
3	Transpondeurs / module d'alimentation
4	Batterie

Une antenne externe en option doit être montée sur les boîtiers avec capot en métal si la fonction radio est utilisée. Si une antenne est montée, elle doit être activée dans le micrologiciel.

Le boîtier SPC G3 dispose de 3 trous de vis à l'arrière pour la fixation murale (voir point 1 ci-dessous).

Il est recommandé d'employer des vis ayant au minimum une tête de 8 mm de diamètre et une tige de 4-5 mm de diamètre et 40 mm de longueur pour le montage du boîtier. Toutefois, selon la nature du mur, d'autres fixations ou des chevilles expansibles peuvent être nécessaires.

Pour fixer le boîtier au mur :

1. Enlevez le couvercle et repérez le premier trou de vis dans la partie supérieure du boîtier.
2. Repérez la position de ce trou à l'endroit voulu du mur à l'aide d'un crayon, puis percez le premier trou avec une perceuse.
3. Vissez le boîtier sur le mur, et marquez la position des deux trous de vis inférieurs à l'aide d'un crayon après avoir pris soin d'aligner le boîtier à la verticale.

Exigences pour l'anti-effraction arrière

Un interrupteur d'anti-effraction arrière peut être requis pour obtenir l'agrément local.

L'interrupteur d'anti-effraction arrière est livré avec les centrales SPC dans un boîtier G3 ou est disponible comme option supplémentaire avec un kit de montage (SPCY130). Les centrales EN50131 G3 (SPCxx3x.x20) sont fournies par défaut avec un kit d'autosurveillance arrière.

6.2.1 Montage d'un kit d'autosurveillance arrière

Le kit d'autosurveillance arrière dote les centrales SPC d'un dispositif d'autosurveillance à l'avant et à l'arrière.

Le kit d'autosurveillance arrière comprend les pièces suivantes :

- Bouton antisabotage
- Câbles pour connecter le bouton antisabotage au contrôleur
- Plaque de fixation murale

Montage de la plaque de fixation murale

1. Montage du SPC dans la position appropriée sur le mur à l'aide des trois fixations (voir réf. 1 ci-dessous).

2. Tracez une ligne autour de l'intérieur de la découpe de l'antisabotage (voir réf. 2 ci-dessous) qui servira de repère pour la plaque murale à fixer sur le mur. Retirez le boîtier du mur.
3. Placez la plaque murale sur le mur (voir réf. 1 ci-dessous) en la centrant précisément autour du rectangle préalablement dessiné (voir réf. 2 ci-dessous).

4. Assurez-vous que les quatre brides de la plaque murale sont encastrées dans le mur.
5. Repérez les quatre points de fixation sur la plaque murale.
6. Percez et utilisez des vis adaptées (maxi 4 mm) au matériau du mur.
7. Fixez la plaque murale sur le mur.

Mise en place du bouton antisabotage

1. Insérez le bouton antisabotage (voir réf. 2 ci-dessous) à l'arrière du boîtier de manière à ce que le plongeur soit tourné vers l'extérieur (voir réf. 1 ci-dessous).

2. Remettez en place le boîtier sur le mur à l'aide des trois fixations préalablement retirées (voir réf. 2 ci-dessous). Vérifiez visuellement que l'encastrement soit parfait entre la plaque murale et le boîtier métallique.

Numéro	Description
1	Boîtier
2	Mur
3	Plaque de fixation murale
4	Bouton antisabotage

AVERTISSEMENT : si la plaque de fixation murale n'est pas précisément alignée, le boîtier ne reposera pas correctement sur ses fixations.

Câblage du bouton antisabotage sur la centrale

Toutes les centrales disposent d'entrées supplémentaires configurées pour permettre le câblage du bouton antisabotage sans aucune programmation.

Ce bouton antisabotage est désigné « Autosurveillance Aux. 1 » par le système.

1. Connectez le contact NO du bouton antisabotage au contact T1 du contrôleur.
2. Connectez le contact COM du bouton antisabotage au contact C du contrôleur. Assurez-vous que le cavalier T2 n'est pas retiré.
3. Une fois que le bouton antisabotage est câblé, le contrôleur peut être mis en service comme habituellement.

6.2.2 Installation de la batterie pour conformité EN50131

Pour assurer la conformité EN50131, la batterie doit être fermement maintenue dans le boîtier. Pour cela, il convient de replier les pattes situées à l'arrière du boîtier articulé pour retenir la batterie.

Si vous utilisez une batterie de 7 Ah, la batterie est tournée vers la gauche du boîtier et la patte du bas est repliée pour la retenir.

Si vous utilisez une batterie de 17 Ah, la batterie est tournée vers la droite du boîtier et la patte du milieu est pliée pour la retenir.

Prenez soin de replier les pattes avec précaution pour ne pas endommager la batterie. Si la batterie est endommagée ou en cas de fuite de l'électrolyte, remplacez la batterie par une batterie neuve. Éliminez l'ancienne en suivant les dispositions applicables.

6.3 Montage d'un boîtier G5

Le boîtier SPC G5 est composé d'une base métallique et d'un couvercle frontal. Ce couvercle est fixé sur l'embase du boîtier au moyen de 4 vis de fixation en haut et en bas du couvercle.

Pour ouvrir le boîtier, enlevez tous les vis en vous servant d'un tournevis, et enlevez le couvercle directement de l'embase.

Le boîtier G5 contient la carte de circuit imprimé du contrôleur et le SPCP355.300 Smart PSU, tous deux montés sur 4 colonnettes. Un transpondeur 8 entrées / 2 sorties est monté sur le module d'alimentation. Quatre colonnettes supplémentaires sont inclues pour que vous puissiez monter le transpondeur 8 entrées / 2 sorties sous le panneau du PSU dans le boîtier G5. Vous pouvez installer des transpondeurs supplémentaires dans le boîtier, comme illustré.

Numéro	Description	Numéro	Description
1	Batterie	6	Câbles de la température de la batterie
2	Bande d'attache de batterie	7	Module d'alimentation

Numéro	Description	Numéro	Description
3	Languettes de fixation	8	Positions en option du transpondeur
4	Trous de la bande d'attache	9	E/S Centrale
5	Câbles de la batterie	10	Antenne

Deux batteries d'une capacité maximale de 27 Ah peuvent être placées dans le compartiment prévu à cet effet dans le fond du boîtier.

Une antenne externe en option doit être mise en place sur un cadre métallique si la fonctionnalité radio est requise. Des orifices prépercés sont disponibles à trois emplacements de la partie supérieure du boîtier, là où vous pouvez installer l'antenne. Si une antenne est montée, elle doit être activée dans le micrologiciel.

Le boîtier SPC G5 dispose de 4 trous de vis à l'arrière pour la fixation murale.

Numéro	Description
1	Fixation en angle
2	Découpe antisabotage
3	Étagère séparant le compartiment de la batterie
4	Découpage du socle de télécommunication

6.3.1 Protection antisabotage

L'interrupteur d'autosurveillance et l'équerre d'autosurveillance arrière sont montés sur le boîtier. L'interrupteur est utilisé seul uniquement pour la protection antisabotage avant, ou bien avec l'équerre d'autosurveillance arrière pour la protection antisabotage avant et arrière. L'une des deux protections antisabotage (avant ou arrière) est nécessaire en fonction des agréments locaux.

L'équerre d'autosurveillance est fermement maintenue en place à l'aide d'une vis de calage. N'oubliez pas d'enlever cette vis si vous mettez le système en service pour la protection antisabotage arrière. Ne l'enlevez pas si vous n'utilisez que la protection avant.

6.3.2 Montage du boîtier avec la protection antisabotage

Pour monter le boîtier :

1. à l'aide du gabarit de montage fourni, marquez les 4 emplacements de perçage grâce auxquels vous allez fixer le boîtier sur le mur.
2. Percez puis installez des vis adaptées (voir le gabarit inclus) dans le mur. Laissez les vis dépasser de 1,5 cm du mur.
3. Le boîtier G5 est préconfiguré pour l'autosurveillance avant uniquement. Pour configurer le boîtier pour les deux types de dispositifs antisabotage, enlevez la vis de fixation du dispositif avant (rep. 1).

   L'équerre d'antisabotage oscille à l'extrême droite de la fente d'orientation (rep. 6).
4. Montez le boîtier G5 en position appropriée sur le mur et serrez les 4 vis de fixation. Assurez-vous que le boîtier est encastré dans le mur.
5. Déplacez l'équerre antisabotage à l'extrême gauche de la fente d'orientation et serrez la vis d'antisabotage arrière (rep. 5). L'équerre doit être perpendiculaire à la paroi arrière du boîtier.

6. Installez le couvercle sur le boîtier pour tester la connexion de l'interrupteur d'autosurveillance. Soulevez le couvercle d'environ 1 mm pour activer l'interrupteur d'autosurveillance.

Numéro	Description	Numéro	Description
1	Vis de calage d'autosurveillance avant	5	Vis d'autosurveillance arrière
2	Équerre antisabotage	6	Fente d'orientation
3	Bouton antisabotage	7	Étagère séparant le compartiment de la batterie
4	Découpe de l'autosurveillance arrière		

AVERTISSEMENT : si la vis d'autosurveillance arrière n'est pas bien fixée au mur, la protection antisabotage n'est pas garantie. Si le boîtier est retiré du mur ou déplacé, le bon fonctionnement du contact d'autosurveillance arrière doit être testé à nouveau afin de le régler si nécessaire.

6.3.2.1 Fonctionnement de l'antisabotage (autosurveillance)

Interrupteur d'autosurveillance – normal

Numéro	Description
1	Mur
2	Vis d'autosurveillance arrière
3	Paroi arrière du boîtier
4	Couvercle du boîtier
5	Contact de l'interrupteur d'autosurveillance fermé

Interrupteur d'autosurveillance – déplacé

Numéro	Description
1	Mur
2	Vis d'autosurveillance arrière
3	Paroi arrière du boîtier
4	Couvercle du boîtier

Numéro	Description
5	Contact de l'interrupteur d'autosurveillance ouvert

Si le boîtier est enlevé du mur ou déplacé, la vis de l'équerre antisabotage n'est plus fixée de manière sûre contre le mur, provoquant ainsi un pivotement de l'équerre. Cela a pour effet que l'interrupteur d'autosurveillance se détache du couvercle et ouvre le contact de l'interrupteur.

AVERTISSEMENT : si la vis d'autosurveillance n'est pas bien fixée au mur, la protection antisabotage n'est pas garantie.

6.3.3 Installation des batteries

Si vous utilisez deux batteries dans le boîtier G5, il est recommandé que les deux batteries aient la même valeur d'Ah.

Numéro	Description	Numéro	Description
1	Batterie	6	Câble de la température de la batterie
2	Bande de fixation	7	Module d'alimentation
3	Languettes de fixation de la batterie	8	Positions en option du transpondeur
4	Trous de la bande d'attache	9	E/S Centrale
5	Câbles de la batterie	10	Antenne

Installation des batteries :

1. insérez les batteries dans le compartiment correspondant.
2. Appuyez sur les languettes métalliques situées sur le haut et sur les deux côtés des batteries vers l'intérieur, vers les batteries.
3. Attachez chacune d'elles au logement à l'aide d'une bande d'attache. Assurez-vous que l'attache passe au travers des orifices correspondants situés à l'arrière du compartiment de la batterie et autour d'elle. Les deux extrémités doivent se trouver à l'avant de la batterie.
4. Attachez-les fermement à l'aide d'une bande Velcro. Assurez-vous que la bande est serrée autour de la batterie.
5. Connectez une extrémité des câbles de la batterie aux terminaux + et - et l'autre extrémité aux entrées + et - correspondantes du module d'alimentation.

ATTENTION : lorsque vous installez la batterie, connectez toujours le câble positif (+) à la batterie avant de connecter le câble négatif (-). Lorsque vous retirez la batterie, enlevez toujours le câble négatif (-) avant le positif (+).

6. Connectez les extrémités sans attaches des câbles de surveillance de la température aux entrées correspondantes du module d'alimentation.

6.4 Montage d'un clavier

Consultez les instructions d'installation correspondantes.

Les guides d'installation sont disponibles sur http://www.spcsupportinfo.com/connectspcdata/userdata.

6.5 Montage d'un transpondeur

Consultez les instructions d'installation correspondantes.

Les guides d'installation sont disponibles sur http://www.spcsupportinfo.com/connectspcdata/userdata.

7 Smart PSU

Cette section décrit les composants et le câblage du Smart PSU.

7.1 SPCP355.300 Smart PSU

Le SPCP355.300 Smart PSU est un module d'alimentation combiné avec un transpondeur 8 entrées / 2 sorties, contenu dans un boîtier G5. Il est pourvu d'une sauvegarde par deux batteries de 24 Ah ou 27 Ah et fournit huit sorties d'alimentation et quatre sorties logiques.

Le transpondeur surveille les surintensités, les défauts de fusible, la tension secteur, les communications et la sortie batterie dans le module d'alimentation. Le transpondeur est alimenté par le module d'alimentation et reçoit des données de celui-ci via un câble de connexion. Il interagit également avec le transpondeur SPC via le X-BUS SPX.

Numéro	Description
SPCP355.300 Smart PSU	
1	Entrée secteur et bloc de fusibles
2	Transformateur d'entrée
3	CA IN — entrée d'alimentation CA
4	SECTEUR — LED d'alimentation secteur
5	BATT1 — LED de l'état de charge de la batterie 1
6	BATT2 — LED de l'état de charge de la batterie 2

Numéro	Description
7	FUSIBLE — LED de panne de fusible
8	LIMITE — LED de limite de courant
9	ÉTAT — LED d'état
10	S2 — sortie de courant 14,5 V. • Pas de prise en charge de secours par la batterie • Protégée par un fusible réinitialisable par PTC de 300 mA (repère n°23 de l'image ci-dessus).
11	A1 — se connecte à l'entrée d'alimentation (+/-) sur le SPC5350/6350.
12	COMM1 — interface à 4 broches du transpondeur. Se connecte au repère 32 (connexion d'alimentation et de données de l'image ci-dessus) à l'aide d'un câble traversant.
13	Référence horloge — se connecte à la référence de l'horloge sur le SPC5350/6350.
14	T1, T2 — entrées de l'interrupteur d'autosurveillance. Connectez celles-ci à l'interrupteur d'autosurveillance avant/arrière. Voir *Montage du boîtier avec la protection antisabotage* page 59.
15	Interrupteur d'autosurveillance avant/arrière. Voir *Montage du boîtier avec la protection antisabotage* page 59.
16	NO/NF — sortie de relais logique NO/NF configurable. Consultez *Câblage des sorties* page 70 pour plus d'informations.
17	Fusibles de verre — fusibles en T de 400 mA pour les sorties 1 à 8.
18	OP 6 – 8 et SW 6 – 8 — sorties combinées d'alimentation (OP) et logiques (SW). Sorties d'alimentation standards en 12 VCC combinées avec des sorties logiques configurables à drainage ouvert (résistance de fin de ligne 4k7 supervisée / non supervisée).
19	OP 1 – 5 — sorties d'alimentation CC standard de 12 VCC. Voir l'avertissement sous le tableau pour des informations supplémentaires.
20	BTE2 — entrée de surveillance de la température de la batterie 2.
21	BATT1 et BATT2 — connecteurs de la batterie 1 et 2.
22	BTE1 — entrée de surveillance de la température de la batterie 1.
23	Fusibles PTC — Fusibles de 300 mA. Protègent les sorties A1 et A2. Pour plus d'informations, consultez *Restauration du système* page 73.
24	Fusible PTC — fusible de 5 A. Protège l'entrée d'alimentation CA (repère 3 de l'image ci-dessus). Pour plus d'informations, consultez *Restauration du système* page 73.
25	Interrupteur de relance du module d'alimentation — pour plus d'informations, consultez *Restauration du système* page 73.
Transpondeur	

Numéro	Description
26	NO/NF — sorties de relais logiques. Le transpondeur dispose de deux sorties de relais logiques NO/NF. Pour plus d'informations, consultez *Câblage des entrées* page 69.
27	I 1 – 8 — entrées. Le transpondeur possède 8 entrées intégrées à la carte pouvant être configurées comme des zones d'alarme anti-intrusion sur le système SPC. Pour plus d'informations, consultez *Câblage des entrées* page 69.
28	Alimentation auxiliaire 12 V — ne pas utiliser. Le transpondeur est alimenté par COMM1 sur le SPCP355.300 Smart PSU.
29	Alimentation d'entrée X-BUS — ne pas utiliser. Le transpondeur est alimenté par COMM1 sur le SPCP355.300 Smart PSU.
30	Interface X-BUS — le bus de communication connecte les transpondeurs sur le système SPC.
31	Cavalier de terminaison — ce cavalier est toujours mis en place, par défaut. Pour plus d'informations, consultez *Câblage de l'interface X-BUS* page 68.
32	Interface à 4 broches du module d'alimentation — se connecte au COMM1 du SPCP355.300 SMART PSU (repère 12 de l'image ci-dessus), à l'alimentation et au connecteur de données à l'aide d'un câble traversant droit.
33	Interrupteur d'autosurveillance avant — non utilisé. L'antisabotage avant/arrière connecté à T1 et T2 du SPCP355.300 Smart PSU est le seul dispositif antisabotage dont a besoin cette installation.
34	JP1 — il faut mettre en place le mécanisme permettant de passer outre l'antisabotage avant.
35	Buzzer — activé pour localiser le transpondeur. Consultez *Localiser* page 142 pour plus d'informations.
36	JP6 — bypass de l'antisabotage arrière. Doit être mis en place.
37	Commutateurs d'adressage manuel — active le paramètrage manuel de l'ID du transpondeur.
38	Témoin d'état X-BUS — indique l'état de l'X-BUS lorsque le système est en Mode Paramétrage, comme illustré ci-dessous : • clignotement lent (toutes les 1,5 seconde) — l'état de communication X-BUS est OK. • Clignotement rapide (toutes les 0,2 seconde) — indique une des choses suivantes : – Indique le dernier transpondeur en ligne pour les configurations en branche. – Indique un problème de communication entre deux transpondeurs. Si deux transpondeurs adjacents clignotent rapidement, le problème se trouve entre ces deux transpondeurs.
39	LED : pas utilisé
40	Témoin d'état module d'alimentation électrique

AVERTISSEMENT : le courant de charge maximal combiné de toutes les sorties 12 VCC (OP 1 – 8) plus COMM1 ne doit pas dépasser 2,4 A. Chacune des sorties individuelles et la sortie A2 ne doit pas dépasser 300 mA. Si le courant de l'appareil nécessite plus de 300 mA, nous vous recommandons de monter les sorties en parallèle.

Ajout de transpondeurs supplémentaires

Si vous ajoutez des transpondeurs supplémentaires dans le boîtier G5, vous devez vous assurer que les antisabotages avant et arrière sont désactivés en mettant en place les cavaliers adéquats. Dans le boîtier G5, les antisabotages avant et arrière sont traités par le boîtier lui-même et par le SPCP355.300 Smart PSU.

7.1.1 Sorties supervisées

Le SPCP355.300 Smart PSU prend en charge trois sorties logiques de drain vers la sortie pouvant être surveillées pour la détection de sabotage. La détection de sabotage de la sortie est activée par la configuration. Elle est activée en connectant une résistance de fin de ligne 4k7 en parallèle avec l'appareil de charge, comme une sirène externe. Une diode d'alimentation (1N4001 par exemple, ou similaire) est également requise si elle n'est pas déjà présente dans le périphérique externe.

Numéro	Description
1	Sorties standard d'alimentation 12 V
2	Sortie commutée configurable et supervisée 12 V CC.

7.1.2 Batteries

Cette section recouvre :

7.1.2.1 Installation des batteries

Cette section décrit l'installation des batteries pour le SPCP355.300 Smart PSU et le boîtier G5.

Numéro	Description
1	Batterie
2	Bande d'attache de batterie
3	Orifices de fixation
4	Trous de la bande d'attache
5	Câbles de la batterie
6	Câbles de la température de la batterie
7	Module d'alimentation / transpondeur
8	Emplacements de montage pour transpondeurs supplémentaires.

Nous vous recommandons d'utiliser deux batteries. Elles doivent avoir le même type et la même capacité.

1. Installez les batteries dans le compartiment prévu à cet effet.
2. Fixez chacune des batteries à l'aide des bande d'attache fournies en vous assurant que la bande passe au travers des orifices prévus à cet effet pour faire le tour de la batterie en passant par l'arrière.
3. Fixez les deux extrémités de la bande devant la batterie, en vous assurant que la bande est fermement serrée.
4. Connectez les câbles du SPCP355.300 Smart PSU aux batteries dans l'ordre suivant :

   – connectez tout d'abord le câble du + (rouge).

   – connectez ensuite le câble du - (noir).

DANGER : lorsque vous retirez les câbles de la batterie, déconnectez toujours le - (noir) en premier avant de déconnecter le + (rouge).

7.1.2.2 Test de la tension de la batterie

Le SPCP355.300 Smart PSU effectue un test de charge sur chacune des batteries en plaçant une résistance de charge entre les bornes de la batterie et en mesurant la tension qui en résulte. Ce test de la batterie a lieu toutes les cinq secondes.

7.1.2.3 Protection contre la décharge profonde

Si l'alimentation secteur du SPCP355.300 Smart PSU est coupée pendant une période prolongée, chacune des batteries fournit du courant 12 VCC au module d'alimentation pendant un temps déterminé. Les batteries finiront par se décharger. Pour éviter qu'une batterie ne se décharge trop et qu'elle ne devienne inutilisable, le SPCP355.300 Smart PSU la déconnecte si la tension mesurée passe au-dessous de 10,5 VCC. La batterie peut alors être rechargée après le retour de l'alimentation secteur.

7.1.2.4 Durée de veille de la batterie

Consultez *Calcul de la puissance nécessaire pour la batterie* page 382 pour des informations sur la veille de la batterie.

7.1.3 Câblage de l'interface X-BUS

L'interface X-BUS connecte les transpondeurs et les claviers au contrôleur SPC. Le X-BUS peut être câblé selon plusieurs configurations différentes en fonction des besoins d'installation.

Le tableau suivant fait la liste des types et des distances de câblage recommandés :

longueur maximale du câble = (nombre de transpondeurs et de claviers dans le système) x (distance maximale pour chacun des types de câble).

Type de câble	Distance
Câble d'alarme CQR standard	200m

Type de câble	Distance
UTP Cat-5 à âme pleine	400m
Belden 9829	400m
IYSTY 2x2x0,6 (min)	400m

Le diagramme suivant montre un exemple de câblage de l'X-BUS :

Numéro	Description
1	Sorties SPCP355.300 Smart PSU
2	Centrale SPC
3	Transpondeur entrée/sortie SPCP355.300
4	Transpondeur suivant
5	Transpondeur suivant

7.1.3.1 Câblage des entrées

Le transpondeur comprend 8 entrées de zone intégrées pouvant être configurées de la manière suivante :

- Sans fin de ligne (NEOL)
- Fin de ligne simple (SEOL)
- Fin de ligne double
- Infrarouge anti-masquage (PIR)

Configuration par défaut

Le diagramme suivant montre la configuration par défaut, avec fin de ligne double 4k7 :

Numéro	Description
1	Entrée 1
2	COM
3	Autosurveillance
4	Alarme
5	4k7
6	EOL 4k7

Infrarouge anti-masquage (PIR)

Le diagramme suivant montre la configuration infrarouge anti-masquage INFRAROUGE :

Numéro	Description
1	Entrée 2
2	COM
3	Autosurveillance
4	Alarme
5	4k7
6	Détecteur de défaut
7	2K2
8	EOL 4k7

7.1.3.2 Câblage des sorties

Les sorties logiques de relais du transpondeur et du module d'alimentation peuvent être affectées à n'importe laquelle des sorties du système SPC. Les sorties du relais peuvent commuter une tension nominale de 30 VCC à 1 A (charge non inductive).

Lorsque le relais est activé, la connexion du terminal « commune » (COM) passe du terminal « Normally Closed (Normalement fermé, NF) » au terminal « Normally Open (Normalement ouverte, NO) ».

Le diagramme suivant montre le câblage d'une sortie haute active.

Numéro	Description
1	Borne normalement ouverte
2	Connexion de terminal commune (COM)
3	Terminal Normalement fermé (NF)

7.1.4 Conformité au référentiel de la certification NF&A2P

Adresse de l'organisme certificateur	
CNPP Cert Route de la Chapelle Réanville CS 22265 F-27950 SAINT MARCEL www.cnpp.com	**AFNOR Certification** 11 rue François de Pressensé 93571 Saint Denis La Plaine Cedex www.marque-nf.com

Afin de satisfaire aux exigences d'installation NF et A2P, ce boîtier doit être scellé après son installation en y apposant l'étiquette infalsifiable jointe.

Les produits SPC listés ont été testés conformément à la norme NF324 - H58, avec référence aux normes RTC50131-6 et RTC50131-3 et aux certifications EN en vigueur, voir *Conformité aux agréments EN50131* page 23.

Type de produit	Configuration	Standard	Logo
SPC6350.320 + SPCP355.300 Cert. 1233700001 + Cert.8033700002	60 h, non monitorisé	NF Grade 3, Classe 1	
SPC5350.320 + SPCP355.300 Cert. 1233700001 + Cert.8033700002	60 h, non monitorisé		
SPC6330.320 + SPCP333.300 Cert. 1232200003	60 h, non monitorisé	NF Grade 3, Classe 1	
SPC5330.320 + SPCP333.300 Cert. 1232200003	60 h, non monitorisé		

7.1.5 Témoin d'état du module d'alimentation

Le tableau suivant fournit une liste des informations sur l'état du module d'alimentation Smart PSU :

TÉMOIN	ALIMENTATION	BATT 1 et 2	FUSIBLE	LIMITE	ÉTAT
COULEUR	Vert	Vert	Rouge	Rouge	Vert
Condition					
Normal	Actif	Actif	Inactif	Inactif	Actif
Alimentation OK, batterie en charge	Actif	Flash			Actif
Alimentation principale en panne, batterie OK	Inactif	Actif			Actif
Alimentation principale OK, batterie en panne ou absente	Actif	Inactif			Actif
Alimentation principale OK, batterie en panne, absente ou en mode de protection contre la décharge profonde	Tous les témoins sont éteints.				
Panne de fusible			Actif		Actif
Courant de charge total dépassé				Actif	Actif
Panne du commutateur du module d'alimentation	Inactif	Inactif	Inactif	Inactif	Flash

7.1.6 Restauration du système

Panne d'alimentation secteur et de la batterie

Dans le cas où l'alimentation secteur et la batterie sont en panne toutes les deux, le bouton de relance du module d'alimentation (repère 25 dans *SPCP355.300 Smart PSU* page 63) permet de redémarrer le système avec seulement le courant de la batterie. Pour relancer le système, effectuez les opérations suivantes :

Prérequis

- l'alimentation du secteur est en panne
- l'alimentation de la batterie est en panne
- De nouvelles batteries sont disponibles

1. Raccordez les câbles de la batterie.
2. Appuyez sur le bouton de relance du module d'alimentation et maintenez-le enfoncé.

   Tous les témoins clignotent.
3. Maintenez le bouton enfoncé jusqu'à ce que les témoins arrêtent de clignoter.
4. Relâchez le bouton de relance.

Réinitialisation d'un fusible PTC

Si l'un des fusibles PTC en verre se réinitialise, vous devez le déconnecter manuellement avant de rétablir les connexions secteur et celles de la batterie.

8 Matériel du contrôleur

Cette section décrit le matériel de la centrale.

Voir également

Alimentation des transpondeurs à partir des bornes auxiliaires page 381

Câblage de l'interface X-BUS page 85

Câblage d'un buzzer interne page 99

Câblage des entrées de zone page 95

LED d'état du contrôleur page 380

Alimentation des transpondeurs à partir des bornes auxiliaires page 381

Câblage de l'interface X-BUS page 85

Câblage d'un buzzer interne page 99

Câblage des entrées de zone page 95

8.1 Matériel de la centrale 42xx/43xx/53xx/63xx

Cette section décrit la centrale pour les modules SPC42xx, 43xx, 53 xx et 63xx. Les SPC5350 et 6350 sont décrits dans *Matériel de la centrale SPC5350 et 6350* page 78.

Le contrôleur SPC dispose de 8 zones embarquées câblées et de zones radio optionnelles.

Numéro	Nom	Description
1	Module radio en option	La carte mère de la centrale peut être équipée en usine d'un module radio utilisable avec les capteurs radio (868 MHz).
2	LED de statut du contrôleur SPC	Ces 7 LED indiquent l'état de plusieurs paramètres système décrits dans *LED d'état du contrôleur* page 380.
3	Entrée d'alimentation CA	Entrée secteur CA : La tension secteur CA est appliquée sur ce connecteur deux broches via un transformateur installé dans le boîtier SPC. Le conducteur de terre est relié à un point de raccordement sur le boîtier métallique. Référence d'horloge* : un signal de référence d'horloge peut aussi être appliqué à ce connecteur deux broches pour garantir la précision du temps système.
4	Bouton de réinitialisation	• Pour réinitialiser le contrôleur : – Appuyez une fois sur cet interrupteur. • Pour restaurer la configuration par défaut et redémarrer la centrale : – Maintenez pressé le bouton jusqu'à ce qu'on vous demande si vous désirez une réinitialisation aux valeurs d'usine par défaut. – Sélectionnez OUI pour rétablir les valeurs d'usine par défaut. **Avertissement :** le fait d'attribuer à la centrale les paramètres d'usine par défaut supprime tous les fichiers de configuration, y compris les sauvegardes, enregistrés sur la centrale. Toutes les isolations et les inhibitions sont également supprimées. Nous vous recommandons de sauvegarder votre configuration sur un PC avant d'attribuer les valeurs par défaut à la centrale. **Remarque :** cette fonction n'est pas disponible si le mode verrouillage installateur est actif.
5	Borne de connexion à la terre	Cette borne n'est pas nécessaire et ne doit pas être connectée.
6	Sortie auxiliaire 12V	Le contrôleur SPC fournit une sortie auxiliaire de 12 VCC utilisable pour alimenter les transpondeurs et les périphériques tels que les gâches, les sirènes, etc. Voir *Alimentation des transpondeurs à partir des bornes auxiliaires* page 381. Elle peut délivrer un courant maximal de 750 mA. **Remarque :** le courant consommé dépend de la durée d'utilisation avec la batterie.
7	Interface X-BUS	Bus de communication du SPC utilisé pour mettre les transpondeurs en réseau dans le système. Voir *Câblage de l'interface X-BUS* page 85. Le SPC4000 n'est équipé que d'une seule interface X-BUS.
8	Sorties intégrées	Les sorties OP4, OP5 et OP6 sont des sorties 12 V résistives à collecteur ouvert qui partagent un courant nominal de 400 mA avec la sortie auxiliaire 12 V. Si les sorties ne sont pas raccordées à la borne 12 V du contrôleur et sont alimentées par une source externe, la borne 0 V de la source externe doit être raccordée sur la borne 0 V du contrôleur et la source externe ne peut pas dépasser 12 V.
9	Sortie de relais	Le contrôleur SPC possède un relais de commutation unipolaire de 1 A, utilisable pour alimenter la sortie de flash sur la sirène externe.

Numéro	Nom	Description
10	Sirène intérieure / sirène extérieure	Les sorties des sirènes intérieure et extérieure (INT+, INT-, EXT+, EXT-) sont des sorties résistives avec un courant nominal de 400 mA. Les sorties BHO (Bell Hold Off = Retenue de sirène), TR (Tamper Return = Retour antieffraction) et EXT sont utilisées pour connecter une sirène extérieure au contrôleur. Les bornes INT+ et INT- permettent de se raccorder à des périphériques internes tels qu'un buzzer interne. Voir *Câblage d'un buzzer interne* page 99.
11	Entrées de zone	Le contrôleur dispose de 8 entrées de zone intégrées qui peuvent être surveillées à l'aide de différentes configurations de supervision. Ces configurations peuvent être programmées à partir du système. La configuration par défaut est Fin de ligne double (DEOL) en utilisant des valeurs de résistance de 4k7. Voir *Câblage des entrées de zone* page 95.
12	Bornes anti-effraction	La centrale possède deux bornes supplémentaires d'entrée antieffraction servant à connecter des dispositifs antisabotage supplémentaires pour augmenter la protection. Ces bornes doivent être mises en court-circuit lorsqu'elles ne sont pas utilisées.
13	Bornier de connexion port série 2	Le bornier de connexion port série 2 (TX, RX, GND) peut être utilisé pour s'interfacer avec un modem externe ou un programme de terminal PC. Le port série 2 partage un canal de communication avec le modem de secours. Si un modem de secours est installé, assurez-vous qu'aucun périphérique n'est connecté à ce port série.
14	IP LED de connectivité Ethernet	Les deux LED Ethernet indiquent le statut de la connexion Ethernet. La LED gauche indique l'activité des données sur le port Ethernet ; la LED droite indique que le lien Ethernet est actif.
15	IP Interface Ethernet	L'interface Ethernet permet le raccordement du contrôleur à un PC afin de pouvoir programmer le système.
16	Interface USB	L'interface USB est utilisée pour accéder à la programmation du navigateur ou un programme de terminal.
17	Port série 2	Le port série RS232 peut être utilisé pour s'interfacer avec un modem externe ou un programme de terminal PC. Le port série 2 partage un canal de communication avec le modem de secours. Si un modem de secours est installé, assurez-vous qu'aucun périphérique n'est connecté à ce port série.
18	Port série 1	Le port série RS232 peut être utilisé pour s'interfacer avec un appareil de protocole X10.
19	Modules de raccordement optionnels	Un module principal (emplacement gauche) et un module de secours (emplacement droit) peuvent être raccordés sur le contrôleur. Ces modules peuvent être un modem GSM ou un modem RTC qui augmentent les possibilités de communication. Le modem de secours ne doit pas être connecté si le port série 2 est raccordé à un modem externe ou à un autre périphérique.
20	Antieffraction avant	Ce contact antieffraction frontal (interrupteur et interrupteur) protège le boîtier contre les tentatives de sabotage. **Remarque :** l'antieffraction avant n'est pas utilisée dans le boîtier G5.

Numéro	Nom	Description
21	Sélecteur de la batterie	J12 : placez un cavalier pour l'utilisation d'une batterie 17 Ah et retirez-le pour l'utilisation d'une batterie 7 Ah. Veuillez noter que ce sélecteur n'est disponible que sur la carte mère version 2.3 du contrôleur. (Pas applicable aux centrales SPC5350 et SPC5360.)
22	Entrée d'alimentation auxiliaire	Entrée 12 V de la batterie ou du module d'alimentation**.

* Configuration par défaut pour les centrales SPC5350 et SPC5360

** Le module d'alimentation est valable uniquement pour les centrales SPC5350 et SPC6350.

8.2 Matériel de la centrale SPC5350 et 6350

Cette section décrit le SPC5350 et le SPC6350.

Le transpondeur qui est connecté à l'alimentation dans le G5 est réglé sur ID1 par défaut. Ce paramétrage ne doit pas être modifié.

Numéro	Nom	Description
1	Module radio en option	La carte mère de la centrale peut être équipée en usine d'un module radio utilisable avec les capteurs radio (868 MHz).
2	LED de statut du contrôleur SPC	Ces 7 LED indiquent l'état de plusieurs paramètres système décrits dans *LED d'état du contrôleur* page 380.
3	Référence d'horloge	Un signal de référence d'horloge peut aussi être appliqué à cette borne de connexion à 2 broches pour garantir la précision du temps système. Connectez-vous à la référence d'horloge CN17 sur le SPCP355.300 Smart PSU.
4	Bouton de réinitialisation	• Pour réinitialiser le contrôleur : – Appuyez une fois sur cet interrupteur. • Pour restaurer la configuration par défaut et redémarrer la centrale : – Maintenez pressé le bouton jusqu'à ce qu'on vous demande si vous désirez une réinitialisation aux valeurs d'usine par défaut. – Sélectionnez OUI pour rétablir les valeurs d'usine par défaut. **Avertissement :** le fait d'attribuer à la centrale les paramètres d'usine par défaut supprime tous les fichiers de configuration, y compris les sauvegardes, enregistrés sur la centrale. Toutes les isolations et les inhibitions sont également supprimées. Nous vous recommandons de sauvegarder votre configuration sur un PC avant d'attribuer les valeurs par défaut à la centrale. **Remarque :** cette fonction n'est pas disponible si le mode verrouillage installateur est actif.
5	Borne de connexion à la terre	Cette borne n'est pas nécessaire et ne doit pas être connectée.
6	Interface X-BUS	Bus de communication du SPC utilisé pour mettre les transpondeurs en réseau dans le système. Voir *Câblage de l'interface X-BUS* page 85. Les bornes 1B et 1A doivent être connectées aux bornes 2B et 2A du transpondeur d'E/S SPCP355.300, respectivement. Ces deux terminaux, 2A et 2B, doivent être connectés respectivement sur les terminaux 2A et 2B du transpondeur suivant du X-BUS.
7	Sorties intégrées	Les sorties OP4, OP5 et OP6 sont des sorties 12 V résistives à collecteur ouvert avec un courant nominal de 300 mA. La charge OP4 doit être connectée au SPCP355.300 Smart PSU.
8	Sortie de relais	Le contrôleur SPC possède un relais de commutation unipolaire de 1 A, utilisable pour alimenter la sortie de flash sur la sirène externe.
9	Mise en attente de la sirène (BHO) et retour d'anti-effraction (TR)	Les sorties BHO (Bell Hold Off = Retenue de sirène), TR (Tamper Return = Retour antieffraction) et EXT sont utilisées pour connecter une sirène extérieure au contrôleur. Voir *Câblage d'un buzzer interne* page 99.

Numéro	Nom	Description
10	Sirène intérieure (négatif)	La borne INT- permet de connecter des périphériques internes tels qu'un buzzer interne. L'alimentation du buzzer interne doit être connectée au SPCP355.300 Smart PSU.
11	Sirène extérieure (négatif)	La borne Ext- est utilisée pour se connecter à des périphériques externes, tels qu'une sirène externe. L'alimentation de la sirène externe doit être connectée au SPCP355.300 Smart PSU.
12	ne pas utiliser.	ne pas utiliser.
13	Entrées de zone	Le contrôleur dispose de 8 entrées de zone intégrées qui peuvent être surveillées à l'aide de différentes configurations de supervision. Ces configurations peuvent être programmées à partir du système. La configuration par défaut est Fin de ligne double (DEOL) en utilisant des valeurs de résistance de 4k7. Voir *Câblage des entrées de zone* page 95.
14	Bornes anti-effraction	La centrale possède deux bornes supplémentaires d'entrée antieffraction servant à connecter des dispositifs antisabotage supplémentaires pour augmenter la protection. Ces bornes doivent être mises en court-circuit lorsqu'elles ne sont pas utilisées.
15	Bornier de connexion port série 2	Le bornier de connexion port série 2 (TX, RX, GND) peut être utilisé pour s'interfacer avec un modem externe ou un programme de terminal PC. Le port série 2 partage un canal de communication avec le modem de secours. Si un modem de secours est installé, assurez-vous qu'aucun périphérique n'est connecté à ce port série.
16	LED de connectivité Ethernet	Les deux LED Ethernet indiquent le statut de la connexion Ethernet. La LED gauche indique l'activité des données sur le port Ethernet ; la LED droite indique que le lien Ethernet est actif.
17	Interface Ethernet	L'interface Ethernet permet le raccordement du contrôleur à un PC afin de pouvoir programmer le système.
18	Interface USB	L'interface USB est utilisée pour accéder à la programmation du navigateur ou un programme de terminal.
19	Port série 2	Le port série RS232 peut être utilisé pour s'interfacer avec un modem externe ou un programme de terminal PC. Le port série 2 partage un canal de communication avec le modem de secours. Si un modem de secours est installé, assurez-vous qu'aucun périphérique n'est connecté à ce port série.
20	Port série 1	Le port série RS232 peut être utilisé pour s'interfacer avec un appareil de protocole X10.
21	Modules de raccordement optionnels	Un module principal (emplacement gauche) et un module de secours (emplacement droit) peuvent être raccordés sur le contrôleur. Ces modules peuvent être un modem GSM ou un modem RTC qui augmentent les possibilités de communication. Le modem de secours ne doit pas être connecté si le port série 2 est raccordé à un modem externe ou à un autre périphérique.
22	Batterie d'horloge en temps réel	Batterie pour horloge en temps réel (HTR).

Numéro	Nom	Description
23	Entrée d'alimentation auxiliaire	Entrée 12 V d'A1 sur le SPCP355.300 Smart PSU.

Voir également

Alimentation des transpondeurs à partir des bornes auxiliaires page 381

9 Transpondeur de porte

Les deux transpondeurs de porte peuvent gérer deux portes et deux lecteurs de badge. Le mode de fonctionnement est configuré via les deux E/S de porte. Chacune des deux E/S de porte prend en charge la fonctionnalité de deux entrées et d'une sortie pour le contrôleur de porte. Un numéro de porte spécifique peut être affecté à une E/S de porte, ce qui permet d'obtenir la fonctionnalité prédéfinie pour les entrées et la sortie. Si aucun numéro de porte n'est affecté à aucune des E/S de porte (l'option « Zones » est sélectionnée), les entrées et sorties du contrôleur de porte peuvent être utilisées comme des entrées et sorties sur la centrale. Aucune fonctionnalité d'accès ne sera donc disponible sur ce contrôleur double porte.

Si un numéro de porte est affecté uniquement aux E/S de la première porte du contrôleur double porte, le premier lecteur est utilisé comme lecteur d'entrée pour cette porte. Si un deuxième lecteur est disponible, il est utilisé comme lecteur de sortie pour la porte configurée. Deux entrées et une sortie ont des fonctionnalités prédéfinies ; elles peuvent être configurées par l'utilisateur. En outre, l'entrée du détecteur de position de la première porte est utilisable en tant que zone d'intrusion, mais uniquement avec des fonctions limitées.

Si un numéro de porte est attribué à chacune des deux E/S de porte, celles-ci sont traitées indépendamment. Le premier lecteur de badge est utilisé comme lecteur d'entrée pour la première porte, et le deuxième lecteur de badge est utilisé comme lecteur d'entrée pour la deuxième porte. Toutes les entrées et sorties ont une fonctionnalité prédéfinie. Les entrées du détecteur de position des deux portes peuvent de plus être utilisées comme zones d'intrusion, mais uniquement avec des fonctions limitées.

Consultez *Lecteurs de cartes et de formats de badges pris en charge* page 409 pour un complément d'information sur les lecteurs de badge et les formats de badge.

Chaque numéro disponible peut être attribué à une zone. Cette attribution n'est pas fixe. Si une zone a été affectée au numéro de zone 9 et si un transpondeur d'entrée ayant l'adresse 1 est connecté au X-BUS (lequel utilise les numéros de zone 9 à 16), la zone affectée à partir du contrôleur double porte est déplacée vers le prochain numéro disponible. La configuration est adaptée en conséquence.

10 Câblage du système

Ce chapitre recouvre :

10.1 Câblage de l'interface X-BUS **85**

10.2 Câblage d'un transpondeur en branche **93**

10.3 Câblage de la mise à la terre du système **94**

10.4 Câblage de la sortie de relais **94**

10.5 Câblage des entrées de zone **95**

10.6 Câblage d'une sirène extérieure SAB **98**

10.7 Câblage d'un buzzer interne **99**

10.8 Câblage du Bris de verre **99**

10.9 Installation de modules de raccordement **100**

10.1 Câblage de l'interface X-BUS

L'interface X-BUS sert à connecter les transpondeurs au contrôleur. Le X-BUS peut être câblé selon plusieurs configurations différentes en fonction des besoins d'installation. Le débit en bauds de l'interface X-BUS est de 307 kb/s.

REMARQUE : le X-BUS est un bus RS-485 dont le débit en bauds est de 307 kb/s. La performance maximale n'est possible que dans les configurations de câblage en boucle (voir *Configuration en boucle* à la page suivante) et en branche (voir *Configuration en branche* page 87) ; la meilleure qualité de signal est obtenue avec la configuration en guirlande des sections isolées, avec 1 transmetteur / 1 récepteur et des résistances d'extrémité équilibrées à chaque extrémité.

La performance en configuration de câblage en étoile ou multipoint (voir *Configuration en étoile et multipoint* page 88) est limitée, compte tenu de l'absence de conditions optimales pour la caractéristique du bus RS-485 (qualité du signal réduite due au montage de plusieurs récepteurs/transmetteurs en parallèle avec des résistances d'extrémité non équilibrées).

REMARQUE : il est fortement recommandé d'utiliser une configuration en boucle (voir *Configuration en boucle* à la page suivante) ou en branche (voir *Configuration en branche* page 87).

Le tableau ci-dessous montre les distances maximales entre le contrôleur/transpondeur ou transpondeur/transpondeur pour tous les types de câbles en configuration en boucle ou en branche.

Type de câble	Distance
Câble d'alarme CQR standard	200 m
UTP cat. 5 (âme pleine)	400 m
Belden 9829	400 m
IYSTY 2 x 2 x 0,6 (min)	400 m

Chaque périphérique possède 4 bornes (1A, 1B, 2A, 2B) utilisées pour connecter des transpondeurs via le câble X-BUS. La centrale lance une procédure de détection après le démarrage pour déterminer le nombre de transpondeurs connectés au système et leur typologie.

Câblage des transpondeurs

Numéro	Description
1	Transpondeur précédent
2	Transpondeur suivant
3	Contrôleur SPC

La plupart des transpondeurs sont équipés de bornes supplémentaires 3A/3B et 4A/4B pour le câblage du transpondeur en branche. Voir *Câblage d'un transpondeur en branche* page 93 pour les instructions sur le câblage d'un transpondeur en branche.

10.1.1 Configuration en boucle

REMARQUE : 4990 le SPC42xx/43xx n'accepte pas la configuration en boucle (un seul port X-BUS).

REMARQUE : tous les transpondeurs/claviers sont équipés d'un cavalier de terminaison par défaut. Pour une configuration en boucle, il est impératif que ces cavaliers soient montés.

Le câblage en boucle (ou anneau) offre la plus grande sécurité tout en permettant des communications tolérant les erreurs sur le X-BUS. Tous les claviers et transpondeurs sont parcourus par un courant de garde permanent, et, en cas de défaut ou de panne du X-BUS, le système continue de fonctionner. Tous les détecteurs sont ainsi surveillés. Cela est obtenu en connectant 1A, 1B sur le contrôleur à 2A, 2B sur le premier clavier ou transpondeur. Le câblage se poursuit avec la connexion de 1A, 1B sur 2A, 2B sur le transpondeur suivant, et ainsi de suite jusqu'au dernier clavier ou transpondeur. La dernière connexion va

de 1A, 1B sur le dernier transpondeur jusqu'à 2A, 2B sur le contrôleur. Consultez la configuration de câblage dans l'illustration ci-dessous.

Numéro	Description
1	E/S Centrale
2-4	Transpondeurs

10.1.2 Configuration en branche

REMARQUE : les versions SPC52xx/53xx/63xx prennent en charge deux branches (2 ports X-BUS).

La version SPC42xx/43xx prend en charge une branche (1 port X-BUS).

REMARQUE : tous les transpondeurs/claviers sont équipés d'un cavalier de terminaison par défaut. Pour une configuration en branche, il est impératif que ces cavaliers soient montés.

La méthode de câblage en branche (ou boucle ouverte) offre un niveau élevé de tolérance aux défauts et peut être adaptée à certaines installations. En cas de défaut ou de coupure du X-BUS, tous les transpondeurs et détecteurs en amont du défaut continuent d'être surveillés.

Dans cette configuration, le contrôleur SPC utilise seulement le port X-BUS (1A/1B ou 2A/2B) pour prendre en charge un groupe de transpondeurs. Consultez la configuration de câblage dans l'illustration ci-dessous. Dans une configuration en boucle ouverte, le dernier transpondeur n'est pas câblé en retour sur le contrôleur et peut être identifié par le clignotement rapide du voyant LED (un clignotement toutes les 0,2 secondes environ) en mode Paramétrage.

En mode automatique, la numérotation des transpondeurs commence avec celui situé le plus près du contrôleur et se termine avec celui qui en est le plus éloigné. Par exemple, si 6 transpondeurs sont connectés dans une configuration en boucle ouverte, le transpondeur le plus proche de la connexion X-BUS aura le numéro 1, le deuxième le numéro 2, etc., le transpondeur câblé le plus loin du contrôleur ayant le numéro 6.

Tous les transpondeurs/claviers sont équipés par défaut de cavaliers de terminaison, ce qui offre une terminaison sur tous les appareils. Cela est impératif pour la configuration en branche (chaîne), car le cavalier se comporte comme une terminaison résistive qui supprime les échos sur la ligne.

Dans une configuration en boucle, tous les transpondeurs/claviers sont équipés par défaut d'un cavalier, ce qui offre une terminaison sur l'appareil.

Configuration en branche

Numéro	Description
1	E/S Centrale
2-4	Transpondeurs

10.1.3 Configuration en étoile et multipoint

REMARQUE : voir *Exemples de câblage correct* page 91, *Exemples de câblage incorrect* page 92 et *Blindage* page 93 avant de commencer l'installation.

Les méthodes de câblage en étoile et multipoint permettent de conserver les fils existants à l'aide de câbles 4 conducteurs posés dans les petits bâtiments (généralement les maisons) générant un faible bruit électrique. Ces méthodes de câblage sont limitées aux spécifications ci-dessous :

	SPC42xx/SPC43xx	SPC52xx/SPC53xx/SPC63xx
Max. transpondeurs/claviers	8	16 (8 par port X-BUS)
Longueur totale de câble	200 m	200 m

REMARQUE : la performance du câblage en étoile ou multipoint est limitée compte tenu de l'absence de conditions optimales pour la caractéristique du bus RS-485 (qualité du signal réduite due au montage de plusieurs récepteurs/transmetteurs en parallèle avec des résistances d'extrémité non équilibrées).

Configuration en étoile

REMARQUE : tous les transpondeurs/claviers sont équipés d'un cavalier de terminaison par défaut. En configuration étoile, il est impératif de **retirer** ces cavaliers.

En configuration étoile, les transpondeurs ont une liaison de retour vers le même port X-BUS sur le contrôleur SPC. En fonction du type de contrôleur, il peut y avoir deux ports (1A/1B, 2A/2B), mais un seul port (1A/1B) est utilisé sur chaque clavier ou transpondeur.

En cas de coupure du X-BUS, seul le port est déconnecté et tous les autres transpondeurs et détecteurs continuent d'être surveillés. En cas de court-circuit sur le câble, tous les transpondeurs sont désactivés.

Configuration en étoile

Configuration en étoile 2

Numéro	Description
1	Contrôleur SPC
2-4	Transpondeurs

Configuration multipoint

REMARQUE : tous les transpondeurs/claviers sont équipés d'un cavalier de terminaison par défaut. En configuration multipoint, il est impératif de **retirer** ces cavaliers, à l'exception de celui correspondant au dernier clavier ou transpondeur.

Dans une configuration multipoint, les transpondeurs utilisent le même canal de communication : chaque transpondeur est relié au suivant et tous utilisent le même canal d'entrée. Voir la configuration multipoint dans la deuxième illustration.

En cas de coupure du X-BUS, tous les transpondeurs et détecteurs en amont du défaut continuent d'être surveillés. En cas de court-circuit sur le câble, tous les transpondeurs sont désactivés.

Configuration multipoint

Configuration multipoints 2

Numéro	Description
1	Contrôleur SPC
2-4	Transpondeurs

10.1.3.1 Exemples de câblage correct

Câblage en étoile

Câblage multipoint

Câblage mixte

10.1.3.2 Exemples de câblage incorrect

REMARQUE : une configuration mixte étoile/multipoint n'est autorisée que si le point en étoile est situé au niveau du port du contrôleur X-BUS. Dans ce cas, tous les transpondeurs/claviers doivent être câblés en configuration multipoint, sans autre point en étoile dans le câblage.

Il est interdit de relier un second point en étoile

REMARQUE : si la configuration mixte n'est pas correctement câblée, la réduction de la qualité du signal peut entraîner une lenteur de réaction des périphériques connectés (par exemple, le fonctionnement du clavier), voire même une perte de communication avec les périphériques. Dans une telle situation, une configuration de câblage en boucle OU en étoile est fortement recommandée.

10.1.4 Blindage

Les bornes de blindage (SHLD) ne doivent être utilisées que pour les câbles blindés (par exemple, Belden 9829). Si un blindage est nécessaire (sur les sites connaissant d'importantes interférences de champ électrique), raccordez le blindage du câble aux bornes SHLD du contrôleur et de tous les transpondeurs en réseau. S'il est nécessaire de relier le blindage à la terre, connectez un câble pour relier la borne SHLD du contrôleur au plot de mise à la terre du châssis. Ne reliez à la terre la borne SHLD d'AUCUN des transpondeurs.

REMARQUE : pour les câblages en étoile et multipoints

Il n'est pas recommandé d'utiliser des câbles blindés à cause de leurs mauvaises caractéristiques électriques (capacitance élevée) pour les configurations en étoile et multipoints. Toutefois, si un blindage est requis (sur les sites connaissant d'importantes interférences de champ électrique), il faudra mettre en œuvre un nouveau câblage avec une configuration correcte en boucle ou en branche, avec un câble approprié à la configuration de l'installation.

10.1.5 Plan câble

L'identification et l'ordre de numérotation des transpondeurs et des claviers diffèrent selon qu'il s'agit d'un adressage automatique ou manuel des transpondeurs. Pour toute information sur la configuration manuelle et automatique, consultez *Périph. X-BUS* page 140.

Pour un système avec adressage manuel, les transpondeurs et les claviers ont une séquence de numérotation séparée et sont définis manuellement par l'Installateur. Ainsi, les transpondeurs sont numérotés 01, 02, 03, etc. en fonction du besoin. Les claviers peuvent recevoir les mêmes numéros en fonction du besoin.

En configuration manuelle, le système affecte automatiquement des zones à chaque transpondeur. C'est pourquoi les appareils sans zone, comme les transpondeurs 8 sorties, doivent être adressés en dernier.

Pour un système avec adressage automatique, les transpondeurs et les claviers appartiennent au même groupe de numérotation et sont affectés par le contrôleur. Ainsi, les transpondeurs et les claviers sont numérotés ensemble 01, 02, 03, selon leur ordre de détection par rapport à l'emplacement du contrôleur.

10.2 Câblage d'un transpondeur en branche

Le câblage de l'interface X-BUS avec 8 bornes 1A/1B à 4A/4B permet la connexion d'un transpondeur en branche supplémentaire.

Si la branche n'est pas utilisée, les bornes 1A/1B servent alors à se connecter au transpondeur/clavier suivant. Les bornes 3A/3B et 4A/4B ne sont alors pas utilisées.

Les modules suivants prennent en charge le câblage d'un transpondeur en branche (bornes supplémentaires 3A/B et 4A/B) :

- Transpondeur 8 entrées, 2 sorties
- Transpondeur 8 sorties
- Module d'alimentation / transpondeur

- Transpondeur sans fil
- Transpondeur 2 portes

Câblage d'un transpondeur en branche

Numéro	Description
1	Transpondeur précédent
2	Transpondeur connecté à la branche
3	Transpondeur suivant
4	Transpondeur sans branche

10.3 Câblage de la mise à la terre du système

Le 0 V des Smart PSU, claviers et transpondeurs doit être raccordé au 0 V (système GND) du contrôleur SPC.

10.4 Câblage de la sortie de relais

Le contrôleur SPC possède un relais de commutation unipolaire 1 A intégré pouvant être affecté à chacune des sorties du système SPC. La sortie du relais prend en charge une tension nominale de 30 VCC (charge non inductive).

Quand le relais est activé, la borne commune (COM) commute de la borne **N**ormalement **F**ermée (NF) à la borne **N**ormalement **O**uverte (NO).

Câblage standard

NO	Borne normalement ouverte
COM	Connexion de borne commune
NC	Borne normalement fermée

10.5 Câblage des entrées de zone

Le contrôleur SPC possède 8 entrées de zone intégrées. Par défaut, ces entrées sont surveillées à l'aide de la supervision fin de ligne. L'installateur peut choisir parmi l'une des configurations suivantes lors du câblage des entrées :

- Sans fin de ligne (NEOL)
- Fin de ligne simple (SEOL)
- Fin de ligne double (DEOL)
- Infrarouge anti-masquage (PIR)

Configuration par défaut (DEOL 4k7)

Numéro	Description
1	Autosurveillance
2	Alarme
3	EOL 4k7
4	EOL 4k7

Configuration infrarouge anti-masquage

Numéro	Description
1	Autosurveillance
2	Alarme
3	EOL 4k7
4	Défaut
5	EOL 2K2
6	EOL 4k7

Le tableau ci-dessous montre les résistances associées à chaque configuration:

Résistances de fin de ligne uniques

Type d'EOL	À l'état de repos			Alarme		
	Min	Nom	Max	Min	Nom	Max
AUCUNE	0 Ω (-100 %)	150 Ω	300 Ω (+100 %)	300 Ω (+100 %)	Indisponible	Infinie
UNIQUE_1K	700 Ω (-30 %)	1 kΩ	1,3 kΩ (+30 %)	23 kΩ	Indisponible	Infinie
UNIQUE_1K5	1,1 kΩ (-27 %)	1,5 kΩ	2,1 kΩ (+40 %)	23 kΩ	Indisponible	Infinie
UNIQUE_2K2	1,6 kΩ (-28 %)	2,2 kΩ	2,9 kΩ (+32 %)	23 kΩ	Indisponible	Infinie
UNIQUE_4K7	3,1 kΩ (-22 %)	4,7 kΩ	6,3 kΩ (+24 %)	23 kΩ	Indisponible	Infinie

Type d'EOL	À l'état de repos			Alarme		
	Min	Nom	Max	Min	Nom	Max
UNIQUE_10K	7 kΩ (-30 %)	10 kΩ	13 kΩ (+30 %)	23 kΩ	Indisponible	Infinie
UNIQUE_12K	8,5 kΩ (-30 %)	12 kΩ	15,5 kΩ (+30 %)	23 kΩ	Indisponible	Infinie

Double résistance fin de ligne avec masquage infrarouge et défaut

Type d'EOL	À l'état de repos			Alarme		
	Min	Nom	Max	Min	Nom	Max
Mask_1K_1K_6K8 (1K / 1K / 6K8)	700 Ω (-30 %)	1 kΩ	1,3 kΩ (+30 %)	1,5 kΩ (-25 %)	2 kΩ	2,5 kΩ (+25 %)
Mask_1K_1K_2K2 (1K / 1K / 2K2)	700 Ω (-30 %)	1 kΩ	1,3 kΩ (+30 %)	1,5 kΩ (-25 %)	2 kΩ	2,6 kΩ (+30 %)
Mask_4K7_4K7_2K2 (4K7 / 4K7 / 2K2)	3,9 kΩ (-18 %)	4,7 kΩ	5,6 kΩ (+20 %)	8,4 kΩ (-11 %)	9,4 kΩ	10,3 kΩ (+10 %)

Type d'EOL	Défaut			Masquage		
	Min	Nom	Max	Min	Nom	Max
Masque_1K_1K_6K8	2700Ω (-69 %)	8,8 kΩ	12,6 kΩ (+20 %)	-	-	-
Masque_1K_1K_2K2	2,8k (-13%)	3,2k	3,6k (+13%)	3,8k (-10%)	4,2k	4,8k (+15)
Masque_4K7_4K7_2K2	6k (-14%)	6,9k	7,8k (+14%)	10,8k (-7%)	11,6k	12,6k (+9%)

Double résistance fin de ligne

Type d'EOL	À l'état de repos			Alarme		
	Min	Nom	Max	Min	Nom	Max
DOUBLE_1K0_470	400Ω (-20 %)	470Ω	700 kΩ (+40 %)	1,1 kΩ (-27 %)	1,5 kΩ	2 kΩ (+34 %)
DOUBLE_1K0_1K0	700 Ω (-30 %)	1 kΩ	1,3 kΩ (+30 %)	1,5 kΩ (-25 %)	2 kΩ	2,6 kΩ (+30 %)
DUAL_1k0_2k2	1,6 kΩ (-28 %)	2,2 kΩ	2,9 kΩ (+32 %)	2,3 kΩ (-29 %)	3,2 kΩ	4,2 kΩ (+32 %)
DUAL_1k5_2k2	1,6 kΩ (-28 %)	2,2 kΩ	2,9 kΩ (+32 %)	2,7 kΩ (-28 %)	3,7 kΩ	4,8 kΩ (+30 %)
DOUBLE_2K2_2K2	1,6 kΩ (-28 %)	2,2 kΩ	2,9 kΩ (+32 %)	3,4 kΩ (-23 %)	4,4 kΩ	5,6 kΩ (+28 %)

Type d'EOL	À l'état de repos			Alarme		
	Min	Nom	Max	Min	Nom	Max
DOUBLE_2k2_4k7	4,1 kΩ (-13 %)	4,7 kΩ	5,4 kΩ (+15 %)	6 kΩ (-14 %)	6,9 kΩ	7,9 kΩ (+15 %)
DOUBLE_2K7_8K2	7,2 kΩ (-13 %)	8,2 kΩ	9,2 kΩ (+13 %)	9,9 kΩ (-10 %)	10,9 kΩ	11,9 kΩ (+10 %)
DOUBLE_3K0_3K0	2,1 kΩ (-30 %)	3,0 kΩ	3,9 kΩ (+30 %)	4,5 kΩ (-25 %)	6 kΩ	7,5 kΩ (+25 %)
DOUBLE_3K3_3K3	2,3 kΩ (-26 %)	3,3 kΩ	4,3 kΩ (+31 %)	4,9 kΩ (-26 %)	6,6 kΩ	8,3 kΩ (+26 %)
DOUBLE_3K9_8K2	7,0 kΩ (-15 %)	8,2 kΩ	9,5 kΩ (+16 %)	10,5 kΩ (-14 %)	12,1 kΩ	13,8 kΩ (+15 %)
DOUBLE_4K7_2K2	1,6 kΩ (-28 %)	2,2 kΩ	2,9 kΩ (+32 %)	5 kΩ (-28 %)	6,9 kΩ	8,8 kΩ (+28 %)
DOUBLE_4K7_4K7	3,3 kΩ (-30 %)	4,7 kΩ	6,1 kΩ (+30 %)	7 kΩ (-26 %)	9,4 kΩ	11,9 kΩ (+27 %)
DOUBLE_5K6_5K6	4,0 kΩ (-26 %)	5,6 kΩ	7,2 kΩ (+29 %)	8,3 kΩ (-26 %)	11,2 kΩ	14,1 kΩ (+26 %)
DOUBLE_6K8_4K7	3,3 kΩ (-30 %)	4,7 kΩ	6,1 kΩ (+30 %)	8,1 kΩ (-30 %)	11,5 kΩ	14,9 kΩ (+30 %)
DOUBLE_2k2_10K	9,2 kΩ (-8 %)	10 kΩ	10,8 kΩ (+8 %)	11,3 kΩ (-8 %)	12,2 kΩ	13,2 kΩ (+9 %)
DOUBLE_10k_10k	7,5 kΩ (-25 %)	10 kΩ	12,5 kΩ (+25 %)	17 kΩ (-15 %)	20 kΩ	23 kΩ (+15 %)

Pour tous les types de résistances de fin de ligne, une résistance inférieure à 300 Ω est considérée comme un court-circuit. Si la résistance n'est pas entre les seuils indiqués, elle est traitée comme une déconnexion.

10.6 Câblage d'une sirène extérieure SAB

Sur une sirène extérieure raccordée à la carte du contrôleur SPC, la sortie de relais est reliée à l'entrée du flash pendant que Bell Hold Off (BHO, retenue de la sirène) et Tamper Return (TR, retour d'autosurveillance) sont reliés à leurs entrées respectives de l'interface de la sirène.

Une résistance (2K2) est pré-installée sur la carte du contrôleur entre les bornes BHO et TR. Pour le câblage d'une sirène extérieure, connectez cette résistance en série de la borne TR du contrôleur à la borne TR de l'interface de la sirène.

Câblage d'une sirène extérieure

Étiquette	Description
A	Flash +
B	Flash -
C	Intervalle de suppression
D	Retour autosurveillance
E	Sirène -
F	Sirène +

10.7 Câblage d'un buzzer interne

Pour brancher un buzzer interne sur la contrôleur SPC, reliez les bornes IN+ et IN– directement à l'entrée 12 V du buzzer.

Câblage d'un buzzer interne (12 V)

IN–	IN– (contrôleur SPC)
IN+	IN+ (contrôleur SPC)

10.8 Câblage du Bris de verre

Le SPC prend en charge l'interface de bris de vitre RI S 10 D-RS-LED combinée à des détecteurs de bris de vitre GB2001.

Le diagramme suivant montre comment l'interface de bris de vitre est connectée à la centrale SPC pour l'alimentation en courant ou bine à un transpondeur de 8 entrées / 2 sorties :

pour plus d'information sur le câblage de l'interface de bris de vitre à une zone, voir la documentation spécifique au produit.

Pour plus d'information sur le câblage des capteurs de bris de vitre à l'interface de bris de vitre, voir la documentation spécifique au produit.

10.9 Installation de modules de raccordement

Deux modems (RTC ou GSM) peuvent être installés sur la carte du contrôleur pour améliorer ses fonctionnalités. L'image ci-dessous montre deux emplacements disponibles pour chaque modem, l'emplacement principal (à gauche) et l'emplacement de secours (à droite).

Si les deux emplacements sont disponibles, installez toujours le premier module d'extension dans l'emplacement gauche (module primaire) ; le système essaie toujours de faire les appels RTC ou GSM en utilisant le modem installé dans l'emplacement primaire avant d'utiliser le modem de secours.

AVERTISSEMENT : les modems ne sont pas du type « Plug and play ». Vous devez vous connecter à la centrale en mode Paramétrage avant de mettre le transpondeur sous tension et d'installer, retirer ou déplacer des modems d'un endroit vers un autre. Une fois terminée votre intervention sur le modem, reconnectez le système à l'alimentation électrique et reconnectez-vous au contrôleur en mode Paramétrage. Configurez et enregistrez la configuration. Si vous ne suivez pas cette procédure, vous obtiendrez une erreur CRC.

Modules d'extension

Numéro	Description
1	Emplacement du récepteur radio
2	Emplacement du modem primaire
3	Emplacement du modem de secours

Pour les détails d'installation, veuillez vous reporter au manuel d'instructions correspondant.

Les guides d'installation sont disponibles sur http://www.spcsupportinfo.com/connectspcdata/userdata.

11 Alimentation du contrôleur SPC

Le contrôleur SPC est alimenté par deux sources d'énergie : le secteur 230 V et la batterie intégrée. Le branchement au secteur doit être confié à un électricien qualifié. L'alimentation secteur doit être branchée sur une ligne de dérivation isolable. Consultez *Raccordement du câble secteur sur le contrôleur* page 395 pour toutes les informations nécessaires au dimensionnement des câbles électriques, des fusibles, etc.

Le contrôleur SPC doit être mis sous tension dans l'ordre suivant : 1 – alimentation secteur, 2 – batterie intégrée. Pour assurer la conformité aux normes EN, installez une seule batterie de la capacité appropriée.

11.1 Alimentation à partir de la batterie uniquement

En cas d'alimentation d'un système uniquement avec la batterie, il est recommandé que celle-ci soit totalement rechargée (> 13 V). Le système ne pourra être mis en marche si vous utilisez une batterie d'une tension inférieure à 12 V sans alimentation principale.

REMARQUE : la batterie continuera à alimenter le système jusqu'à ce que son niveau de décharge profonde (situé entre 10,5 V et 10,8 V) ait été détecté. La durée de maintien du système lorsqu'il fonctionne sur batterie dépend de la charge externe et de la capacité nominale en Ah de la batterie.

12 Interface utilisateur du clavier

Le modèle suivant de claviers sont disponibles :

- SPCK420/421 — appelé dans ce document « clavier LCD »
- SPCK620/623 — appelé dans ce document « clavier confort »

12.1 SPCK420/421

Cette section recouvre :

12.1.1 À propos du clavier LCD **105**

12.1.2 Utilisation de l'interface du clavier LCD **107**

12.1.3 Entrées de données sur le clavier LCD **111**

12.1.1 À propos du clavier LCD

Le clavier LCD est un dispositif d'interface à montage mural permettant aux :

- **installateurs** de programmer le système à l'aide des menus de programmation des installateurs (protégés par mot de passe) et pour la MES/MHS du système. L'utilisateur peut commander le système sur une base journalière.
- **utilisateurs** d'accéder aux menus de programmation des utilisateurs (protégés par mot de passe) et d'utiliser le système (MES/MHS). (Voir le *Manuel de l'utilisateur du SPCK420/421* pour plus de détails sur la programmation par l'utilisateur.)

Le clavier LCD inclut un interrupteur frontal d'autosurveillance et un afficheur de 2 lignes x 16 caractères. Il possède une touche de navigation intuitive permettant d'accéder rapidement aux options, ainsi que deux touches programmables contextuelles (à droite et à gauche) sous l'écran pour sélectionner un menu ou un paramètre. 3 témoins LED fournissent une information sur l'alimentation électrique, les alertes système et l'état des communications.

Le clavier LCD peut être équipé en usine d'un lecteur de badge de proximité compatible avec les périphériques PACE (Portable ACE) (voir *Vue d'ensemble des types de clavier* page 393).

Clavier LCD

Numéro	Nom	Description
1	Affichage LCD	L'afficheur du clavier (2 lignes x 16 caractères) affiche tous les messages d'alerte et d'avertissement et constitue une interface visuelle pour la programmation du système (programmation par l'installateur uniquement). Vous pouvez définir le contraste et les conditions d'activation du rétroéclairage.
2	Touches alphanumériques	Le pavé alphanumérique permet d'entrer du texte et des valeurs numériques pendant la programmation. Les caractères alphabétiques sont sélectionnés en effectuant le nombre approprié d'appuis sur les touches. Pour passer des caractères majuscules aux caractères minuscules, appuyez sur la touche dièse (#). Pour saisir un chiffre, appuyez sur la touche appropriée pendant 2 secondes.
3	Languettes d'accès basculantes	Les languettes d'accès basculantes permettent d'accéder aux clips de l'ensemble arrière du clavier. Vous pouvez décrocher ces clips de l'avant en insérant un tournevis de 5 mm dans les encoches et en poussant doucement.
4	Vis de fixation de l'ensemble arrière	Cette vis permet de fixer les ensembles avant et arrière sur le clavier. Elle doit être retirée pour ouvrir le clavier.
5	Voyants d'état LED	Les voyants d'état LED donnent des informations sur l'état du système selon les détails du tableau ci-dessous.
6	Touches de fonction programmables	Les touches de fonction programmables gauche et droite sont des touches contextuelles qui permettent de naviguer dans les menus et la programmation.

Numéro	Nom	Description
7	Récepteur du lecteur de badge de proximité	Si le clavier est équipé d'un lecteur de badge de proximité (voir *Vue d'ensemble des types de clavier* page 393), présentez le badge, le périphérique ou la télécommande à moins de 1 cm de cette zone pour effectuer la MES/MHS du système.
8	Touche de navigation multifonction	La touche de navigation multifonction offre, en association avec l'affichage du clavier, une interface pour la programmation du système.

TÉMOIN		Etat
Alimentation 230 V (Vert)	∿	Indique la présence ou l'absence de l'alimentation 230 V CLIGNOTEMENT : détection défaut alimentation 230 V ALLUMÉ EN CONTINU : alimentation 230 V OK
Alerte système (Jaune)	⚠	Signale une alerte système CLIGNOTEMENT : alerte système détectée ; l'affichage précise la localisation et la nature de l'alerte. Si le système est EN SURVEILLANCE, AUCUNE indication n'est donnée sur les alertes système DÉSACTIVÉ : pas d'alerte détectée ; si un clavier est affecté à plus d'un secteur, la LED n'indique pas de condition d'alerte si l'un de ces secteurs est EN SURVEILLANCE
État X-BUS (Rouge)	⊖	Indique l'état des communications du X-BUS lors de la programmation en MODE PARAMÉTRAGE Clignotement régulier (environ toutes les 1,5 secondes) : indique que l'état des communications est OK Clignotement rapide (environ toutes les 0,25 secondes) : indique que le clavier est le dernier transpondeur sur le X-BUS Le témoin LED reste allumé quand le clavier est installé pour la première fois et s'il est mis sous tension avant que la connexion avec l'interface X-BUS du contrôleur soit établie

12.1.2 Utilisation de l'interface du clavier LCD

Afficheur du clavier

Numéro	Nom	Description
1	TOUCHE PROGRAMMABLE DROITE	Cette touche est utilisée pour sélectionner l'option présentée sur le côté droit de la ligne du bas. Les valeurs possibles sont : • SÉLECTIONNER pour choisir l'option affichée sur la ligne supérieure • ENTRER pour saisir les données affichées sur la ligne supérieure • SUIVANT pour afficher l'alerte qui suit celle affichée sur la ligne supérieure • EFFACER pour annuler l'alerte affichée sur la ligne supérieure • ENREGISTRER pour sauvegarder un paramétrage
2	OK	Le bouton OK sert de touche de SÉLECTION pour l'option de menu affichée sur la ligne supérieure, mais aussi de touche ENTRER/ENREGISTRER pour les données affichées sur la ligne supérieure.
3	▶	En mode Programmation, la touche Flèche droite permet à l'utilisateur de dérouler le menu de la même manière qu'en appuyant sur l'option SÉLECTIONNER (touche programmable droite). En mode Entrée de données, appuyez sur cette touche pour déplacer le curseur d'une position vers la droite.
4	▼	En mode Programmation, la touche Flèche vers le bas permet à l'utilisateur d'accéder à l'option de programmation suivante dans le même niveau de menu. Appuyez sur cette touche de manière continue pour faire défiler toutes les options de programmation disponibles sur le niveau de menu actuel. En mode alphanumérique, appuyez sur cette touche pour qu'un caractère en majuscules passe en minuscules. Quand des alertes sont affichées, la touche Flèche vers le bas permet d'atteindre le message d'alerte suivant par ordre de priorité. (Consultez *Priorisation des messages affichés* à la page opposée.)
5	◀	En mode Programmation, la touche Flèche gauche permet à l'utilisateur de revenir au niveau de menu précédent. Si vous appuyez sur cette touche alors que vous êtes dans le niveau de menu supérieur, vous quittez la programmation. En mode Entrée de données, appuyez sur cette touche pour déplacer le curseur d'une position vers la gauche.
6	▲	En mode Programmation, la touche Flèche vers le haut permet à l'utilisateur d'accéder à l'option de programmation précédente dans le même niveau de menu. Appuyez sur cette touche de manière continue pour faire défiler toutes les options de programmation disponibles sur le niveau de menu actuel. En mode alphanumérique, appuyez sur cette touche pour qu'un caractère en minuscules passe en majuscules.
7	TOUCHE PROGRAMMABLE GAUCHE	Cette touche est utilisée pour sélectionner l'option présentée sur le côté gauche de la ligne du bas. Les valeurs possibles sont : • QUITTER pour quitter la programmation • RETOUR pour revenir au menu précédent

Numéro	Nom	Description
8	LIGNE INFÉRIEURE DE L' AFFICHEUR	À l'état REPOS, cette ligne est vide. En mode Programmation, cette ligne affiche les options disponibles pour l'utilisateur. Ces options s'alignent au-dessus des touches programmables gauche et droite pour pouvoir être sélectionnées.
9	LIGNE SUPÉRIEURE DE L' AFFICHEUR	À l'état REPOS, affiche la date et l'heure. En mode Programmation, cette ligne affiche l'un des éléments suivants : • La fonction de programmation à sélectionner • Le paramétrage actuel de la fonction sélectionnée • La nature de l'alerte en cours pendant une condition d'alerte. (Consultez *Priorisation des messages affichés* ci-dessous.)

Priorisation des messages affichés

Les messages d'anomalie et les alertes s'affichent sur le clavier dans l'ordre suivant :

- Zone
  - Alarmes
  - Autosurveillance
  - Anomalie
- Alertes secteur
  - Échec MES
  - Temporisation d'entrée
  - Code autosurveillance
- Alertes système
  - Alimentation 230 V
  - Batterie
  - Défaut alim.
  - Défaut auxiliaire
  - Fusible sirène extérieure
  - Fusible sirène intérieure
  - Autosurveillance sirène
  - Autosurveillance boîtier
  - Autosurveillance Aux. 1
  - Autosurveillance Aux. 2
  - Brouillage radio
  - Défaut modem 1
  - Ligne modem 1
  - Défaut modem 2
  - Ligne modem 2
  - Défaut de transmission
  - Panique utilis.

  - XBUS Défaut câble
  - XBUS Défaut communication
  - XBUS Défaut alimentation secteur
  - XBUS Défaut alimentation batterie
  - XBUS Défaut alimentation électrique
  - XBUS Défaut fusible
  - XBUS Défaut antipiratage
  - XBUS Défaut antenne
  - XBUS Brouillage radio
  - XBUS Panique
  - XBUS Incendie
  - XBUS Médical
  - XBUS Ligne d'alimentation
  - XBUS Autosurveillance sortie
  - XBUS Basse tension
  - Réinitialisation Installateur nécessaire
  - Armement automatique
- Informations du système
  - Zones en test
  - Zones ouvertes
  - État du secteur
  - Batterie faible (capteur)
  - Capteur perdu
  - WPA Batterie faible
  - WPA perdu
  - WPA Test non reçu
  - Camera offline
  - Batterie tag faible
  - Surintensité Xbus
  - Nom de l'installateur
  - N° téléphone de l'installateur
  - Accès Installateur validé
  - Accès Constructeur validé
  - Redémarrage
  - Défaut matériel
  - Surconsommation aux.
  - Batterie faible
  - Liaison Ethernet
  - Nom du système

12.1.3 Entrées de données sur le clavier LCD

L'interface de programmation facilite la saisie de données et la navigation dans les menus du clavier LCD. L'utilisation de l'interface pour chaque type d'opération est détaillée ci-dessous.

Saisie des valeurs numériques

En mode Saisie numérique, seuls des chiffres (0 – 9) peuvent être saisis.

- Pour déplacer le curseur d'un caractère vers la gauche ou vers la droite, appuyez respectivement sur les touches Flèche gauche et Flèche droite.
- Pour quitter la fonction sans enregistrer, appuyez sur la touche de menu ARRIÈRE.
- Pour enregistrer les paramètres programmés, appuyez sur ENTRER ou OK.

Saisie de texte

En mode Saisie de texte, il est possible de saisir des caractères alphabétiques (A – Z) et des chiffres (0 – 9).

- Pour entrer un caractère alphabétique, appuyez une ou plusieurs fois sur la touche correspondante.
- Pour entrer un caractère spécial utilisé dans certaines langues, (ä, ü, ö…) appuyez sur la touche 1, pour passer en revue ces caractères spéciaux.
- Pour entrer un caractère d'espacement ou spécial (+, -./[ ]), appuyez sur la touche 0.
- Pour saisir un chiffre, appuyez sur la touche correspondante pendant deux secondes, puis relâchez.
- Pour déplacer le curseur d'un caractère vers la gauche ou vers la droite, appuyez respectivement sur les touches Flèche gauche et Flèche droite.
- Pour quitter la fonction sans enregistrer, appuyez sur ARRIÈRE.
- Pour enregistrer les paramètres programmés, appuyez sur ENTRER ou OK.
- Pour modifier la casse d'un caractère alphabétique, appuyez sur les touches Flèches vers le haut/bas lorsque le caractère est mis en surbrillance par le curseur.
- Pour passer des majuscules aux minuscules pour tous les caractères suivants, appuyez sur la touche dièse (#).
- Pour supprimer un caractère à gauche du curseur, appuyez sur la touche *.

Sélection d'une option de programmation

En mode Navigation, l'Installateur/Utilisateur choisit une option de programmation prédéfinie dans une liste.

- Pour parcourir la liste des options disponibles avant de faire votre choix, appuyez sur les touches Flèches vers le haut/bas.
- Pour quitter la fonction sans enregistrer, appuyez sur ARRIÈRE.
- Pour enregistrer l'option sélectionnée, appuyez sur SAUVER ou OK.

12.2 SPCK620/623

Cette section recouvre :

12.2.1 À propos du clavier confort **112**
12.2.2 Description des LED **115**
12.2.3 Description du mode d'affichage **116**
12.2.4 Touches de fonction (état repos) **116**

12.2.1 À propos du clavier confort

Le clavier confort est une interface murale permettant :

- aux installateurs de programmer le système à l'aide des menus de programmation des installateurs (protégés par mot de passe) et de mettre en ou hors surveillance le système ; il est possible de commander le système sur une base journalière,
- aux utilisateurs d'accéder aux menus de programmation des utilisateurs (protégés par mot de passe) et d'utiliser le système (MES/MHS). (Voir le *Manuel de l'utilisateur du SPC620/623* pour plus de détails sur la programmation par l'utilisateur.)

Le SPCK620 possède des touches programmables et un écran LCD graphique facilitant l'utilisation. La fonctionnalité peut être améliorée avec un transpondeur à boîtier à clé SPCE110 ou un transpondeur d'indication SPCE120.

Le SPCK623 comporte un lecteur de badge de proximité (125 kHz EM 4102) facilitant l'accès des utilisateurs, des touches programmables, un grand écran graphique LCD et une fonction d'annonces vocales. La fonctionnalité peut être améliorée avec un transpondeur à boîtier à clé SPCE110 ou un transpondeur d'indication SPCE120.

Numéro	Nom	Description
1	Voyants d'état LED	Les voyants d'état LED donnent des informations sur l'état du système comme précisé dans *Description des LED* page 115.

Numéro	Nom	Description
2	Affichage LCD	L'afficheur affiche tous les messages d'alerte et d'avertissement et constitue une interface visuelle pour la programmation du système (programmation par l'installateur uniquement). (Voir *Priorisation des messages affichés* ci-dessous.) Vous pouvez configurer les conditions d'activation du rétroéclairage.
3	Touches de fonction programmables	Touches tactiles contextuelles pour naviguer à travers les menus et la programmation.
4	Touche Entrée	Confirmer l'affichage ou l'entrée.
5	Touche de retour au menu	Revenir au menu. Réinitialiser les buzzers, la sirène et les alarmes dans la mémoire.
6	Récepteur du lecteur de badge de proximité	Uniquement pour le SPCK 623 : si le clavier est équipé d'un lecteur de badge de proximité, présentez le badge, le périphérique ou la télécommande à moins de 1 cm de ce secteur.
7	Touches alphanumériques	Le pavé alphanumérique permet d'entrer du texte et des valeurs numériques pendant la programmation. Les caractères alphabétiques sont sélectionnés en effectuant le nombre approprié d'appuis sur les touches. Pour passer des caractères majuscules aux caractères minuscules, appuyez sur la touche dièse (#). Pour saisir un chiffre, appuyez sur la touche appropriée pendant 2 secondes.
8	Touche de navigation multifonctions	Navigation à travers les menus et les messages d'alerte. (Consultez *Priorisation des messages affichés* ci-dessous.)
9	Touche Information	Affiche des informations.

Priorisation des messages affichés

Les messages d'anomalie et les alertes s'affichent sur le clavier dans l'ordre suivant :

- Zone
  - Alarmes
  - Autosurveillance
  - Anomalie
- Alertes secteur
  - Échec MES
  - Temporisation d'entrée
  - Code autosurveillance
- Alertes système
  - Alimentation 230 V
  - Batterie
  - Défaut alim.
  - Défaut auxiliaire
  - Fusible sirène extérieure
  - Fusible sirène intérieure

  – Autosurveillance sirène
  – Autosurveillance boîtier
  – Autosurveillance Aux. 1
  – Autosurveillance Aux. 2
  – Brouillage radio
  – Défaut modem 1
  – Ligne modem 1
  – Défaut modem 2
  – Ligne modem 2
  – Défaut de transmission
  – Panique utilis.
  – XBUS Défaut câble
  – XBUS Défaut communication
  – XBUS Défaut alimentation secteur
  – XBUS Défaut alimentation batterie
  – XBUS Défaut alimentation électrique
  – XBUS Défaut fusible
  – XBUS Défaut antipiratage
  – XBUS Défaut antenne
  – XBUS Brouillage radio
  – XBUS Panique
  – XBUS Incendie
  – XBUS Médical
  – XBUS Ligne d'alimentation
  – XBUS Autosurveillance sortie
  – XBUS Basse tension
  – Réinitialisation Installateur nécessaire
  – Armement automatique
- Informations du système
  – Zones en test
  – Zones ouvertes
  – État du secteur
  – Batterie faible (capteur)
  – Capteur perdu
  – WPA Batterie faible
  – WPA perdu
  – WPA Test non reçu
  – Camera offline
  – Batterie tag faible

– Surintensité Xbus
– Nom de l'installateur
– N° téléphone de l'installateur
– Accès Installateur validé
– Accès Constructeur validé
– Redémarrage
– Défaut matériel
– Surconsommation aux.
– Batterie faible
– Liaison Ethernet
– Nom du système

12.2.2 Description des LED

Description	Symbole	Couleur	Fonctionnement	Description
Informations	i	Bleu	Actif	Le système ou le secteur ne peut pas être activé. L'activation peut être forcée (les défauts ou les zones ouvertes peuvent être inhibés).
			Clignotant	Le système ou le secteur ne peut pas être activé ou forcé (les défauts ou les zones ouvertes ne peuvent pas être inhibés).
			Inactif	Le système ou le secteur peut être activé.
		Orange	Clignotant	Installateur sur site.
Utilisateur		Vert	Actif	Le secteur affecté n'est pas mis en surveillance.
			Clignotant	Le secteur affecté est mis en surveillance partielle A/B
			Inactif	Le secteur affecté est totalement mis en surveillance
Alarme		Rouge	Actif	Alarme
			Clignotant	-
			Inactif	Aucune alarme
Système		Orange	Actif	-
			Clignotant	Anomalie
			Inactif	Pas d'anomalie
Alimentation		Vert	Actif	Système OK
			Clignotant	Défaut secteur
			Inactif	Pas de connexion du bus

REMARQUE : les témoins LED d'information, d'état du secteur, d'alarme et de défaut sont désactivés lorsque le clavier est au repos. Un code d'accès d'utilisateur valide doit être entré. Il peut être modifié lorsque l'indication de mise sous tension signale que le système est au repos.

12.2.3 Description du mode d'affichage

Deux modes d'affichage sont disponibles (automatiques) :

- Affichage de plusieurs secteurs : l'utilisateur a accès à plusieurs secteurs. L'affichage des secteurs est effectué au moyen de groupes de secteurs. Si aucun groupe de secteurs n'est configuré, seul le groupe général « Tous les secteurs » s'affiche.
- Affichage d'un secteur unique : l'utilisateur n'a des droits que pour un seul secteur. Dans la vue Affichage d'un secteur unique, un seul secteur est affiché en gros caractères et il peut être contrôlé directement.

Les droits d'un utilisateur peuvent être limités par les paramètres de l'utilisateur ou par les paramètres du clavier sur lequel l'utilisateur est connecté. Le secteur ne s'affiche que si l'utilisateur et le clavier utilisé pour la connexion possèdent un droit sur ce secteur. Si l'utilisateur possède des droits sur plusieurs secteurs, mais le clavier sur un seul, l'utilisateur ne verra aussi qu'un seul secteur.

12.2.4 Touches de fonction (état repos)

Urgence

Plusieurs touches d'urgence sont affichées suivant la configuration active. Un appui simultané sur les touches déclenche un appel d'urgence.

	Alarme Panique
	Alarme incendie
	Alarme Médical

La procédure déclenchée dépend de la configuration du système. Consultez l'installateur pour plus de détails.

Paramètres directs

L'option de MES directe est affichée suivant la configuration. Une MES / MES partielle du secteur auquel le clavier est attribué est possible sans code.

13 Outils logiciels

Les outils logiciel exécutables sur PC suivants sont disponibles pour la gestion distante d'une centrale SPC :

- **SPC Manager**
  Permet la création, le contrôle et la modification à distance du protocole basé sur l'accès dans le système SPC.

14 Démarrage du système

ATTENTION : le système SPC doit être monté par un installateur approuvé.

1. Connectez le clavier à l'interface X-BUS du contrôleur.
2. Activez le mode de programmation Installateur en saisissant le code d'installateur par défaut (1111). Pour plus d'informations, consultez *Codes PIN installateur* ci-dessous.

14.1 Modes Installateur

Le système SPC fonctionne selon 2 modes de programmation utilisables par les installateurs autorisés : Paramétrage et Exploitation. Dans le navigateur, la déconnexion n'est autorisée qu'en mode Exploitation.

Mode Paramétrage

Tous les défauts, alertes et autoprotections doivent d'abord être isolés ou annulés avant de pouvoir quitter le mode Paramétrage.

Le mode Paramétrage permet d'accéder à toutes les fonctionnalités de programmation. Néanmoins, la programmation en mode Paramétrage désactive dans le système la programmation de tous les paramètres d'alarme, des rapports et des sorties. Pour connaître la totalité des options du menu Paramétrage, consultez *Programmation en mode Paramétrage avec le clavier* page 129.

Mode Exploitation

Le mode Exploitation permet d'accéder à un nombre plus faible de fonctions de programmation et n'affecte pas les sorties programmées dans le système. Pour connaître la totalité des options du menu Exploitation, consultez *Programmation en mode Exploitation avec le clavier* page 127.

14.1.1 Codes PIN installateur

Le code de programmation de démarrage par défaut de l'installateur est 1111.

Si une installation est modifiée de Grade 2 en Grade 3 à tout moment après le démarrage, tous les codes reçoivent le préfixe 0. Le code par défaut de l'installateur devient donc 01111.

L'augmentation du nombre de chiffres du code (voir *Options* page 257) provoque l'ajout de zéros à gauche du code existant (par exemple, 001111 pour un code à six chiffres).

REMARQUE : si le code utilisateur par défaut 1111 est par exemple activé pour une nouvelle installation du SPC, il faut modifier le code d'installateur sur la centrale. Si vous ne modifiez pas votre code, un message d'information apparaîtra vous obligeant à changer votre code par défaut avant de sortir du mode Paramétrage.

14.2 Programmation avec le clavier

Le clavier permet un accès rapide sur place aux menus et à la programmation du système. L'installateur autorisé doit paramétrer les configurations initiales par défaut à l'aide du clavier. La programmation du lecteur de badge de proximité et l'attribution aux utilisateurs sont également effectuées à l'aide du clavier.

14.3 Configuration des paramètres de démarrage

Les paramètres de démarrage suivants peuvent être modifiés ultérieurement lors de la programmation des fonctionnalités du système.

Lors de la mise en marche de la centrale, le numéro de version du système SPC s'affiche sur le clavier.

Prérequis

- Pour initialiser la configuration de démarrage, appuyez sur le bouton de réinitialisation de la carte pendant 6 s au moins.

1. Appuyez sur une touche du clavier.

   – Appuyez sur SUIVANT pour naviguer entre les paramètres.
2. Choisissez la langue d'affichage de l'assistant de configuration.
3. Choisissez le PAYS approprié.

   – EUROPE, SUÈDE, SUISSE, BELGIQUE, ESPAGNE, R-U, IRLANDE, ITALIE, , , , CANADA, É.-U.
4. Choisissez un TYPE d'installation :

   – SIMPLE : adapté à une utilisation domestique (maisons et appartements).

   – ÉVOLUÉ : offre des types de zones supplémentaires et des descriptions par défaut de zones commerciales pour les huit premières zones.

   – BANCAIRE : conçu pour les banques et autres institutions financières. Inclut des fonctions telles que la MES automatique, la programmation horaire des verrouillages, des groupes d'interverrouillage et un type de zone sismique.

   Pour les détails des descriptions de zone par défaut, voir .*Paramètres par défaut des modes Simple, Évolué et Bancaire* page 384
5. Choisissez le niveau de sécurité de votre installation.
6. LANGUE Voyez les langues disponibles par défaut sur le système. Les langues ci-dessous sont disponibles en fonction de la région :

   – IRLANDE/R-U : anglais, français, allemand

   – EUROPE/SUISSE/ESPAGNE/FRANCE/ALLEMAGNE : anglais, français, allemand, italien, espagnol

   – BELGIQUE : anglais, néerlandais, flamand, français, allemand

   – SUÈDE : anglais, suédois, danois, français, allemand

   REMARQUE : si le système est remis à zéro et que la région est modifiée au démarrage, seules les langues configurées pour la région précédente seront disponibles pour la nouvelle région.
7. Sélectionnez les langues dont vous avez besoin pour votre installation. Les langues sélectionnées sont précédées d'un astérisque (*). Pour supprimer ou sélectionner une langue, appuyez sur le dièse (#) du clavier.

Les langues non sélectionnées sont supprimées du système et ne seront pas disponibles si vous rétablissez les valeurs par défaut du système.

Pour ajouter d'autres langues sur la centrale, consultez *Mise à jour des langues* page 354. Pour ajouter d'autres langues sur un clavier, consultez sa documentation. Les guides d'installation sont disponibles sur http://www.spcsupportinfo.com/connectspcdata/userdata.

8. Saisissez la DATE et l'HEURE.

   Le système scanne le X-BUS à la recherche de modems.

9. Activez SPC CONNECT pour autoriser une centrale à communiquer avec https://www.spcconnect.com après configuration de l'adresse IP.
10. Activez le DHCP pour attribuer automatiquement une adresse IP réseau à la centrale. Si les fonctions SPC CONNECT (CONNECTER SPC) et DHCP sont activées, un système de transmission SPC CONNECT est ajouté au PC pour effectuer la connexion avec https://www.spcconnect.com.
11. Pour les PC avec DHCP activé, l'adresse IP attribuée automatiquement est affichée dans le menu Adresse IP. Si DHCP n'est pas activé, une adresse IP par défaut est affichée. Choisir SELECT (SÉLECTIONNER) pour continuer. En mode Paramétrage, dans le menu COMMUNICATIONS, il faut entrer manuellement l'adresse IP statique pour le PC.
12. Choisissez le mode d'adressage X-BUS :

    – MANUEL : mode recommandé pour la plupart des types d'installation, en particulier si une préconfiguration est effectuée.

    – AUTO : recommandé seulement pour des installations de très petite taille.

13. Choisissez la topologie d'installation : BOUCLE (anneau) ou BRANCHE (chaîne).

    Le système balaye le système pour déterminer la quantité de claviers, transpondeurs, contrôleurs de portes et les entrées de zone disponibles.

14. Appuyez sur SUIVANT pour scanner tous les périphériques X-BUS.

    Le MODE DE PROGRAMMATION est affiché.

    La configuration de démarrage est terminée.

15. Vérifiez les alertes dans le menu ÉTAT DU SYSTÈME > ALERTES. Sinon, vous ne serez pas autorisé à quitter le mode Installateur.
16. Configurez le système par le clavier ou le navigateur Web.

Voir également

Paramètres par défaut des modes Simple, Évolué et Bancaire page 384

14.4 Création des utilisateurs système

Par défaut, seuls les installateurs sont autorisés à accéder au système SPC. L'installateur doit créer des Utilisateurs pour que les utilisateurs sur site puissent activer, désactiver et effectuer des opérations fondamentales sur le système. Par affectation d'un profil, les utilisateurs n'ont accès qu'à une série déterminée d'opérations sur la centrale.

Tous les codes d'accès utilisateur ayant la syntaxe correcte sont acceptés : par exemple, si un code d'accès à 4 chiffres est utilisé, tous les codes entre 0000 et 9999 sont admis.

Voir *Utilisateurs* page 176 ou *Utilisateurs* page 211.

Un éventuel accès du fabricant au système (par ex. pour mise à niveau du micrologiciel de la centrale) doit être configuré comme un droit d'utilisateur affecté à un profil d'utilisateur. Pour permettre à un utilisateur d'effectuer des mises à niveau du micrologiciel, assurez-vous que le profil correct lui a été affecté.

Voir également

Codes PIN installateur page 121

14.5 Programmation d'un badge

Le clavier SPC peut être configuré avec un lecteur de badge/appareil de proximité. Les utilisateurs dont les profils sont configurés « utilisateur » peuvent activer ou désactiver le système à distance, et effectuer une programmation en fonction du niveau du profil. Lorsqu'un lecteur de proximité a été programmé sur le clavier, l'utilisateur peut activer ou désactiver le système ou enregistrer sa programmation en présentant l'appareil à moins de 1 cm de la zone de réception sur le clavier.

Zone de réception sur le clavier

Pour programmer un badge ou un tag sur le clavier :

1. Saisissez le code PIN de l'installateur. (La valeur par défaut est 1111. Consultez *Codes PIN installateur* page 121.)
2. Allez sur UTILISATEURS.
3. appuyez sur SELECT.
4. Sélectionnez ÉDITER, puis sélectionnez USER1 dans la liste.
5. Allez sur PACE et appuyez sur SELECT.
6. Vous pouvez passer de ACTIVER à DÉSACTIVER pour la fonctionnalité PACE.

   PACE PRÉSENT s'affiche en clignotant sur la ligne supérieure du clavier.
7. Positionnez le tag PACE à moins d'un centimètre de la zone de réception du clavier.

   Le clavier indique que l'appareil a été enregistré en affichant PACE CONFIGURÉ.

Pour désactiver un badge ou un tag avec le clavier :

1. Saisissez le code PIN de l'installateur. (La valeur par défaut est 1111. Consultez *Codes PIN installateur* page 121.)
2. Allez sur UTILISATEURS.
3. appuyez sur SELECT.
4. Sélectionnez ÉDITER, puis sélectionnez USER1 dans la liste.
5. Allez sur PACE et appuyez sur SELECT.

6. Passez sur DÉSACTIVÉ.

   Le clavier indique MIS À JOUR.

14.6 Programmation des tags sans fil

Si un module récepteur sans fil de 868 MHz est installé sur le clavier ou le contrôleur, une télécommande radio peut être programmée au clavier.

Pour programmer une télécommande radio dans le système :

1. Saisissez le code PIN de l'installateur. (La valeur par défaut est 1111. Consultez *Codes PIN installateur* page 121.)
2. Utilisez les touches de direction bas/haut jusqu'à ce que l'option UTILISATEURS soit affichée.
3. Appuyez sur SELECT.
4. Sélectionnez l'option ÉDITER, puis appuyez sur SELECT.
5. Choisissez l'utilisateur préférentiel et appuyez sur SELECT.
6. Allez sur l'option TÉLÉCOMMANDE RADIO et appuyez sur SELECT.
7. Passez le paramètre sur ACTIVÉ et appuyez sur SELECT.

   Le message APPUYER TOUCHE SUR TÉLÉCOMMANDE clignote sur la ligne supérieure.
8. Placez la télécommande à moins de 8 m du clavier et appuyez sur l'une des touches.

   Le message TÉLÉCOMMANDE CONFIGURÉE s'affiche pour indiquer que l'appareil a bien été enregistré.

Pour désactiver une télécommande radio dans le système :

1. Saisissez le code PIN de l'installateur. (La valeur par défaut est 1111. Consultez *Codes PIN installateur* page 121.)
2. Utilisez les touches de direction bas/haut jusqu'à ce que l'option UTILISATEURS soit affichée.
3. Sélectionnez l'option ÉDITER, puis appuyez sur SELECT.
4. Choisissez l'utilisateur préférentiel et appuyez sur SELECT.
5. Allez sur l'option TÉLÉCOMMANDE RADIO et appuyez sur SELECT.
6. Passez sur DÉSACTIVÉ et appuyez sur ENREGISTRER.

Si le récepteur sans fil de 868 MHz est détecté sur le système, l'option TÉLÉCOMMANDE RADIO ne s'affiche pas dans le menu du clavier.

Nombre de télécommandes radio par utilisateur : une seule télécommande peut être programmée pour chaque utilisateur. Pour modifier la répartition des télécommandes parmi les utilisateurs, répétez la procédure de programmation pour les nouveaux appareils. Les anciennes télécommandes peuvent alors être affectées à différents utilisateurs.

14.6.1 Effacement d'alertes avec la télécommande

Les alertes déclenchées par le système SPC sont normalement effacées à l'aide de l'option RESTAURER du clavier. L'effacement des alertes peut également être réalisé à l'aide de la télécommande radio.

Quand une alerte active est affichée sur le clavier alors que le système est en état MHS, elle peut être effacée ou remise à zéro en appuyant sur le bouton d'arrêt de la télécommande cinq secondes après le désarmement du système.

Pour activer ce protocole, l'option RAZ AL. TELEC. doit être activée dans Options Système :

1. Se connecter au clavier avec le code Installateur.
2. Sélectionnez MODE PARAMETRAGE > OPTIONS.
3. Appuyez sur SELECT.
4. Allez sur RAZ TÉLÉCOMMANDE et appuyez sur SELECT.
5. Passez le paramètre sur ACTIVÉ et appuyez sur ENREGISTRER.

15 Programmation en mode Exploitation avec le clavier

Cette section décrit les options de programmation en mode Exploitation disponibles avec le clavier LCD.

Pour chaque option de menu, le clavier doit être en mode Programmation :

1. Entrez un code Installateur valable. (La valeur par défaut est 1111. Pour plus d'informations, consultez *Codes PIN installateur* page 121.)
2. Utilisez les touches de direction bas/haut jusqu'à ce que l'option de programmation voulue soit affichée.
3. Il est également possible de sélectionner une option de programmation en utilisant les touches numériques du clavier, entrez le code d'installateur suivi du numéro indiqué dans le tableau ci-dessous.

   Si vous changez une des opérations de programmation, le message MISE A JOUR est affiché pendant un court instant.

Numéro	Nom	Description
1	ARMEMENT	Permet de mettre le système à l'ARRET, en MES TOTALE, ou en MES PARTIELLE.
2	INHIBER	Affiche une liste des zones inhibées du système.
3	ISOLER	Permet à l'installateur d'isoler des zones choisies. Voir *Isoler* page 175.
4	JOURNAL DE BORD	Affiche une liste des événements les plus récents sur le système. Voir *Journal des événements* page 175.
5	ACCES JDB	Affiche une liste des derniers accès au système. Voir *Journal des accès* page 175.
6	JOURNAL DES ALARMES	Affiche la liste des alarmes récentes. Voir *Journal des alarmes* page 175.
7	CHANGER SON CODE	Permet à l'installateur de modifier le code d'accès d'installateur. Voir *Modifier code installateur* page 176.
8	GESTION UTILISAT	Permet à l'installateur de créer, de modifier ou d'effacer des utilisateurs. Voir *Utilisateurs* page 176.
9	SMS	Permet à l'utilisateur d'ajouter, d'éditer ou de supprimer les détails de SMS pour les utilisateurs. Voir *SMS* page 180.

Voir également

Test page 171

Contrôle de portes page 184

Programmation en mode Paramétrage avec le clavier page 129

Texte installat. page 183

Régler date/heure page 183

SMS page 180

16 Programmation en mode Paramétrage avec le clavier

Cette section décrit les options de programmation en mode Paramétrage disponibles avec le clavier LCD.

Pour chaque option de menu, le clavier doit être en mode de programmation MODE PARAMETRAGE.

1. Entrez un code Installateur valable. (La valeur par défaut est 1111. Pour plus d'informations, consultez *Codes PIN installateur* page 121.)
2. Appuyez sur SELECT pour une programmation en mode PARAMÉTRAGE.
3. Utilisez les touches de direction bas/haut jusqu'à ce que l'option de programmation voulue soit affichée.
4. Une fonction de sélection rapide est disponible. Appuyez sur # pour sélectionner un paramètre (par exemple, un attribut de zone). Le paramètre sélectionné est affiché avec le signe * (par exemple *Inhiber).

   Lorsque vous terminez les opérations de programmation, le message MISE A JOUR est affiché pendant un court instant.

16.1 État du système

La fonction État du système affiche tous les défauts sur le système.

Pour visualiser ces défauts :

1. Allez sur ÉTAT DU SYSTÈME.
2. appuyez sur SELECT.

   L'état des différents éléments est affiché.

   Cliquez sur chacun des éléments pour afficher des détails supplémentaires.

AFF. ZONE OUVERT	Affiche toutes les zones ouvertes.
ALERTES	Affiche les alertes en cours dans le système.
TEST	Affiche toutes les zones en test JDB.
ISOLATIONS	Affiches les zones isolées.
ÉCHEC MES	Affiche toutes les zones dont l'activation a échoué. Sélectionnez chacune des zones pour afficher des détails sur la raison de la non-activation.
BATTERIE	Affiche l'autonomie, la tension et le courant de la batterie. Vous devez entrer les valeurs de **Capacité de la batterie** et **Courant maxi** dans OPTIONS pour voir s'afficher sur le clavier l'autonomie de la batterie en cas de panne secteur. Le temps s'affiche sous le menu ÉTAT < BATTERIE < TEMPS BATT. Ce menu signale également les pannes de batterie.
AUXILIAIRE	Affiche le voltage et le courant de la batterie.

REMARQUE : les utilisateurs ne peuvent pas quitter le mode PROGRAMMATION s'il existe des conditions de défaut. Le premier défaut s'affiche sur le clavier lorsque vous essayez de quitter le mode Installateur. Vous pouvez visualiser et isoler les défauts dans le menu État du système sous Alertes et Zones ouvertes.

16.2 Options

1. Allez sur OPTIONS et appuyez sur SELECT.
2. Allez sur l'option de programmation désirée :

   Les options affichées dans le menu OPTIONS varient en fonction du niveau de sécurité du système (voir la colonne de droite).

AVERTISSEMENT : pour modifier le pays sur votre centrale, nous vous recommandons fortement de réinitialiser votre centrale aux valeurs par défaut et de sélectionner un nouveau pays avec l'assistant de démarrage.

Variable	Description	Défaut
NIVEAU SÉCURITÉ	Détermine le niveau de sécurité de l'installation SPC. • Irlande et Europe : – EN50131 Grade 2 – EN50131 Grade 3 – Sans restriction • Royaume-Uni : – PD6662 (basé sur EN50131 Grade 2) – PD6662 (basé sur EN50131 Grade 3) – Sans restriction • Suède : – SSF1014:3 Larmclass 1 – SSF1014:3 Larmclass 2 – Sans restriction • Belgique : – TO-14 (basé sur EN50131 Grade 2) – TO-14 (basé sur EN50131 Grade 3) – Sans restriction • Suisse : – SWISSI Cat 1 – SWISSI Cat 2 – Sans restriction • Espagne – EN50131 Grade 2 – EN50131 Grade 3 • Allemagne – VdS classe A – VdS classe C – Sans restriction • France – NFtyp2 – NFtyp3 – Sans restriction	Grade 2 Pays : N/A

Variable	Description	Défaut
PAYS	Détermine les contraintes locales spécifiques auxquelles répond l'installation. Les options sont ROYAUME-UNI, IRLANDE, EUROPE, SUÈDE, SUISSE, BELGIQUE, ALLEMAGNE et FRANCE	
TYPE D'INSTAL.	Détermine si le SPC est destiné à une utilisation dans des locaux commerciaux ou une résidence privée. Choisissez ÉVOLUÉ (voir *Fonctionnement mode Simple* page 364), SIMPLE (voir *Fonctionnement mode Évolué* page 363) ou BANCAIRE.	Simple

Voir *Options* page 257 pour plus de détails sur les OPTIONS suivantes.

MES PART. A	RENOMMER TEMPORISÉ Z. ACCÈS -> TEMPO Z. TEMPO -> IMMÉDIAT ALARME LOCALE
MES PART. B	RENOMMER TEMPORISÉ Z. ACCÈS -> TEMPO Z. TEMPO -> IMMÉDIAT ALARME LOCALE
MSG SI APPEL CTS	AFFICHER MESSAGE (ACTIVÉ/DÉSACTIVÉ)
CONFIRMATION	VDS DD243 : GARDA EN50131-9
CONFIRMER ZONES	Sélectionnez LE NOMBRE DE ZONES.
RAZ ALARME AUTO	VALIDE/DEVALIDE
RAZ AL. TÉLÉC.	VALIDE/DEVALIDE
CONTRAINTE UTILISATEUR	DEVALIDE CODE +1 CODE +2
REDECL.SIRENE	VALIDE/DEVALIDE
SIRÈNE IMMÉDIATE	VALIDE/DEVALIDE
SIR. ÉCHEC MES	VALIDE/DEVALIDE
FLASH ÉCHEC MES	VALIDE/DEVALIDE
ALARME EN SORTIE	VALIDE/DEVALIDE Uniquement possible en mode CONFIGURATION INSTALLATEUR car le paramétrage n'est pas conforme à l'EN50131.

LANGUE	LANGUE SYSTÈME LANGUE AU REPOS
TAILLE DES CODES	4 CHIFFRES 5 CHIFFRES 6 CHIFFRES 7 CHIFFRES 8 CHIFFRES
RAZ AL. CODE	VALIDE/DEVALIDE
ACCÈS WEB	VALIDE/DEVALIDE Autorise/restreint l'accès au navigateur Web.
AFF. ZONE OUVERT	VALIDE/DEVALIDE
AUTOR. INSTALLAT.	VALIDE/DEVALIDE
CONSTRUC. AUTORI. *	VALIDE/DEVALIDE
AFF. ÉTAT SURV.	VALIDE/DEVALIDE
RESIST. FIN LIGNE	AUCUN 1 RÉSIST. 1K 1 RÉSIST. 1K5 1 RÉSIST. 2K2 1 RÉSIST. 4K7 1 RÉSIST. 10K 1 RÉSIST. 12K 2 RÉSIST. 1K / 470R 2 RÉSIST. 1K / 1K 2 RÉSIST. 2K2 / 1K0 2 RÉSIST. 2K2 / 1K5 2 RÉSIST. 2K2 / 2K2 2 RÉSIST. 2K2 / 4K7 2 RÉSIST. 2K7 / 8K2 2 RÉSIST. 2K2/ 10K 2 RÉSIST. 3K0 / 3K0 2 RÉSIST. 3K3 / 3K3 2 RÉSIST. 3K9 / 8K2 2 RÉSIST. 4K7 / 2K2 2 RÉSIST. 4K7 / 4K7 2 RÉSIST. 5K6 / 5K6 2 RÉSIST. 6K8 / 4K7 2 RÉSIST. 10K / 10K MASK_1K_1K_6K8 MASK_1K_1K_2K2 MASK_4K7_4K7_2K2

MODE AUTH. SMS	CODE SEULEMENT ID APPELANT SEUL CODE + ID APPELANT CODE SMS SEUL CODE PIN SMS + ID APPELLANT
TAG ET CODE	VALIDE/DEVALIDE
RAZ à la MHS	VALIDE/DEVALIDE **Remarque :**pour être conforme à PD6662, vous devez désactiver cette option.
RAZ INSTALLATEUR	VALIDE/DEVALIDE
AUTOSURVEILLANCE ZONE OFFLINE	VALIDE/DEVALIDE
VERROU INSTALLAT	VALIDÉ/DÉVALIDÉ Si cette option est active, le système ne peut pas être réinitialisé avec le bouton jaune du contrôleur si le code d'installateur n'est pas entré sur le clavier.
CODE IMPOSÉ	VALIDE/DEVALIDE
PARAM. HORLOGE	ÉTÉ/HIVER AUTO SYNCHRO SUR 50 HZ
SUSPICION AUDIBLE	VALIDE/DEVALIDE
AFF. CAMÉRAS	VALIDE/DEVALIDE
TEST SISM. SI MES	VALIDE/DEVALIDE
ALERTE EMPÊCH. MES	VALIDE/DEVALIDE
ANTIMASQUE MES	DEVALIDE AUTOSURVEILLANCE DÉFAUT ALARME
ANTIMASQUE MHS	DEVALIDE AUTOSURVEILLANCE DÉFAUT ALARME
CONTRAINTE REDÉCLENCHABLE	VALIDE/DEVALIDE
PANIQUE REDÉCLEN.	VALIDE/DEVALIDE
SILENCE SI ÉCOUTE	VALIDE/DEVALIDE
SORTIE PROGR.	VALIDE/DEVALIDE

* Non disponible pour SPC42xx, SPC43xx.

16.3 Temporisations

1. Allez sur TEMPORISATIONS et appuyez sur SELECT.
2. Allez sur l'option de programmation désirée :

Temporisations

Désignation des fonctions dans l'ordre suivant :

- 1re ligne : Web
- 2e ligne : clavier

Durée	Description	Défaut
Audible		
Sirènes intérieures DUREE SIRENE INT	Durée d'activation des sirènes intérieures lorsqu'une alarme est activée. (0 – 999 minutes ; 0 = jamais)	15min
Sirènes extérieures DUREE SIRENE EXT	Durée d'activation des sirènes extérieures lorsqu'une alarme est activée. (0 – 999 minutes ; 0 = jamais)	15min
Retard sirènes extérieures RETARD SIRÈNE EXT.	Cela provoque un décalage du déclenchement de la sirène extérieure. (0–999 secondes)	0 s
Carillon DUREE CARILLON	Durée d'activation en secondes de la sortie Carillon quand une zone avec l'attribut Carillon est déclenchée. (1-10 secondes)	2 s
Confirmation		
Confirmer TEMPS DE CONFIRM	**Remarque :** cette option n'est disponible que pour certaines combinaisons d'options de **Grade** et **Confirmation**. (Voir *Options* page 257 et *Normes* page 274.) Ce temporisateur s'applique à la fonction de confirmation d'alarme. Il définit la durée maximale entre les alarmes de deux zones différentes qui ne se chevauchent pas, avant qu'une alarme confirmée soit déclenchée. (0-60 minutes)	30 min
Agression confirmée	**Remarque :** cette option n'est disponible que pour certaines combinaisons d'options de **Grade** et **Confirmation**. (Voir *Options* page 257 et *Normes* page 274.) Ce temporisateur s'applique à la fonction de confirmation d'alarme. Il définit la durée maximale entre les alarmes de deux zones différentes qui ne se chevauchent pas, avant qu'une alarme confirmée soit déclenchée. (480-1200 minutes)	480 min

Durée	Description	Défaut
Délai de numérotation DÉLAI DE NUMÉROTATION	Lorsqu'il est programmé, le délai de numérotation provoque un temps d'attente prédéfini avant que le système n'appelle le Centre de télésurveillance (CTS). Ce décalage est destiné à limiter les interventions injustifiées du Centre de télésurveillance et de la police. En cas de déclenchement d'une deuxième zone, le délai de numérotation est ignoré et l'appel a lieu immédiatement. (0–999 secondes)	30 s
Annulation d'alarme ANNULATION D'ALARME	Temps après la transmission d'une alarme durant lequel un message d'annulation d'alarme peut être transmis. (0–999 secondes)	30 s
MES		
Autorisation MES AUTORISATION MES	Période de temps pendant laquelle l'autorisation MES est valide. (10-250 secondes)	20 s
Dernière issue DERNIÈRE ISSUE	La temporisation Dernière issue correspond au nombre de secondes pendant lequel l'armement est retardé après la fermeture d'une zone programmée avec l'attribut de dernière issue. (1-45 secondes)	7 s
Sirène si MES totale SIRÈNE SI MES TOTALE	Déclenche momentanément la sirène extérieure pour indiquer une condition de MES totale. (0-10 secondes)	0 s
Échec MES ÉCHEC MES	Nombre de secondes durant lequel le message Échec MES sera affiché sur le clavier (0 jusqu'à la saisie d'un code valide). (0–999 secondes)	10 s
Flash si MES totale FLASH SI MES TOTALE	Déclenche momentanément le flash de la sirène extérieure pour indiquer une condition de MES totale. (0-10 secondes)	0 s
Alarme		
Double déclenchement DOUBLE DÉCLENCH.	Délai maximal entre des activations de zones ayant l'attribut Double déclenchement pour déclencher une alarme. (1-99 secondes)	10 s
Test JOURS TEST JDB	Nombre de jours durant lequel une zone reste en test avant de revenir automatiquement en fonctionnement normal. (1–99 jours)	14 jours
Période de test sismique AUTOTEST SISMIQUE	Période moyenne entre les tests automatiques du détecteur sismique. (12–240 heures) **Remarque :** pour activer le test automatique, l'attribut **Test auto détecteur** doit être activé pour la zone sismique.	168 heures

Durée	Description	Défaut
Durée du test sismique DURÉE TEST SISM.	Temps maximum (secondes) d'attente du déclenchement du détecteur sismique lorsqu'il est sollicité par l'activation de la sortie Test sismique. (3-120 secondes)	30 s
Retard RAZ alarme auto	Délai avant une RAZ alarme auto lorsqu'un secteur est revenu à son état normal. (0-9999 secondes)	0 s
Verrouillage post-alarme VERROUILLAGE POST-ALARME	Le temps nécessaire pour que l'utilisateur puisse obtenir l'accès après une alarme. (1-120 minutes)	0min
Durée d'accès après alarme	Période pendant laquelle l'accès après alarme est autorisé pour un utilisateur après l'écoulement du temps de verrouillage d'accès. (10-240 minutes)	
Flash sirène extérieure DURÉE FLASH	Durée d'activation de la sortie flash lorsqu'une alarme est activée. (1 – 999 minutes ; 0 = indéfiniment)	15min
Alertes		
Tempo défaut 230 V DÉLAI DÉF. 230 V	Le temps de déclenchement d'une alerte par le système après qu'un défaut secteur a été détecté. (0-60 minutes)	0 min
Durée du brouillage radio	Le temps de déclenchement d'une alerte par le système après qu'un brouillage radio a été détecté. (0–999 secondes)	0 min
Installateur		
Accès Installateur ACCES INSTALLAT.	La temporisation d'Accès installateur démarre dès que l'utilisateur active l'Accès installateur. (0 – 999 minutes ; 0 indique que l'accès au système n'est pas limité dans le temps.)	0 min
Déconnexion installateur automatique DÉCONNECT. AUTO	La durée d'inactivité après laquelle l'installateur sera automatiquement déconnecté. (0–300 minutes)	0 min
Clavier		
Temps de saisie clavier TEMPS DE SAISIE CLAVIER	Le nombre de secondes pendant lequel un clavier attend une saisie avant de quitter le menu en cours. (10-300 secondes)	30 s
Langue clavier LANGUE CLAVIER	Temps d'attente en secondes avant qu'un clavier revienne à la langue par défaut. (0 – 9 999 secondes ; 0 = jamais)	10 s
Feu		

Durée	Description	Défaut
Pré-alarme incendie PRE-ALARME INCENDIE	Nombre de secondes d'attente avant l'envoi d'une alarme incendie pour les zones où l'attribut « Pré-alarme incendie » est activé. Consultez *Édition d'une zone* page 277. (1–999 secondes)	30 s
Confirmation incendie CONFIRMATION INCENDIE	Délai supplémentaire avant l'envoi du fichier d'alarme pour les zones où les attributs Pré-alarme incendie et Confirmation incendie sont activés. Consultez *Édition d'une zone* page 277. (1–999 secondes)	120 s
Code PIN		
Code PIN valide CODE PIN VALIDE	Période de temps pendant laquelle le code est valide (1-330 jours)	30 jours
Nbre maxi de changements de code NBRE MAXI DE CHANGEMENTS DE CODE	Nombre de changement du code dans la période de validité. (1–50)	5
Avertissement code AVERTISSMT. CODE	Temps avant que le code n'expire, démarrant la signalisation à l'utilisateur que son code va expirer (1-14 jours)	5 jours
Paramètres généraux		
Durée activation sortie RF SORTIE RADIO	Temps d'activation de la sortie RF dans le système. (0–999 secondes)	0 s
Limite de la Synchro d'heure LIMITE DE LA SYNCHRO D'HEURE	Durée limite pendant laquelle la synchronisation horaire n'a pas lieu. La synchronisation horaire n'a lieu que si l'heure et la date du système sont hors de cette limite. (0-300 secondes)	0 s
Tempo déf. liaison TEMPO DÉF. LIAISON	Temps avant l'apparition de Défaut liaison Ethernet (0–250 secondes ; 0 = Désactivé)	0 s
Camera Offline CAMERA OFFLINE	Délai avant info caméra Offline. (10-9999 secondes)	10 s

Durée	Description	Défaut
Fréquent FRÉQUENT (!)	Cet attribut ne s'applique qu'aux services à distance. Le nombre d'heures d'ouverture d'une zone si cette zone est programmée avec l'attribut **Fréquent**. (1-9999 heures)	336 h (2 semaines)
Contrainte silencieuse	Temps pendant lequel la contrainte reste silencieuse et non restaurable depuis le clavier. (0-999 minutes)	0 min
Agression/Panique silencieuse	Nombre de minutes pendant lequel une agression/panique reste silencieuse et non restaurable depuis le clavier. (0-999 minutes)	0 min

Les temps par défaut dépendent de la configuration Installateur. Les temps par défaut indiqués peuvent être admissibles ou pas et dépendent de la configuration effectuée par l'installateur.

Les paramétrages/plages valides peuvent dépendre du grade de sécurité spécifié sous **Configuration > Système > Standards**.

16.4 Secteurs

1. Allez sur SECTEURS et appuyez sur SELECT.
2. Allez sur l'option de programmation désirée :

AJOUTER	Pour les modes Simple et Évolué, le type de secteur par défaut est Standard. En mode Bancaire, sélectionnez le type de secteur : STANDARD, DAB, CHAMBRE FORTE ou AVANCÉ. Saisissez le nom du secteur et la temporisation d'entrée / de sortie choisie.

EDITER	Éditez les réglages suivants : • LIBELLÉ • ENTREE SORTIE – DELAI ENTREE – TEMPO SORTIE – PAS TEMPO SORTIE – MHS RADIO LIMITE • MES PART. A/B – ACTIVÉ/DÉSACTIVÉ – TEMPORISÉ – Z. ACCÈS -> TEMPO – Z. TEMPO -> IMMÉDIAT – LOCALE – AUCUNE SIRÈNE • SECTEURS LIES – SECTEUR – MES TOTALE – MES TOTALE DE TOUS – EMPÊCHE MES TOTALE – EMPÊCHE MES TOTALE DE TOUS – MHS – MHS DE TOUS – EMPÊCHE MHS – EMPÊCHE MHS DE TOUS • CALENDRIER – CALENDRIER – MES/MHS AUTOMATIQUE – TEMPS VERROUILLÉ – ACCÈS COFFRE • REPORTING – MES TROP TÔT – MES TROP TARD – MHS TROP TÔT – MHS TROP TARD • MES/MHS – PRÉSIGN. MES AUTO – ANNUL. UTILISATEUR – DÉROG. UTILISAT. – INTER. CLÉ – INTERVAL. DÉROG. – NBRE DE DÉROG. – MHS RETARDÉE – DURÉE MHS TEMPOR. – INTERVERROUILLER – DOUBLE CODE • SORTIE RADIO
EFFACER	Sélectionnez le secteur à effacer.

Voir pour de plus amples informations sur ces options.*Ajouter/Éditer un secteur* page 278

16.5 Groupes Secteurs

1. Passez à GROUPES SECTEURS et appuyez sur SELECT.
2. Allez sur l'option de programmation désirée :

AJOUTER	Entrez le nom du groupe de secteur.
EDITER	GROUP NAME - renommez le groupe si nécessaire. SECTEURS – naviguez jusqu'au secteur et sélectionnez-le. Sélectionnez ACTIVÉ ou DÉSACTIVÉ selon le besoin pour l'ajouter ou l'enlever du groupe. Un astérisque (*) indique si un secteur est inclus dans le groupe.
EFFACER	Sélectionnez le secteur à effacer.

16.6 Périph. X-BUS

1. Allez sur X-BUS et appuyez sur SELECT.
2. Allez sur les options de programmation désirées.

16.6.1 Adressage du X-BUS

Les indications contenues dans cette section vous permettent de configurer, localiser et surveiller les transpondeurs, les claviers et les zones consécutives. Vous pouvez également accéder aux paramètres X-BUS – comme le type, les temps de communication et les nouvelles tentatives – à l'aide de ce menu.

Les illustrations ci-dessous montrent l'emplacement des interrupteurs rotatifs, chaque interrupteur rotatif ayant une flèche pointant vers un chiffre l'identifiant (dans l'exemple : 3 et 8). L'interrupteur droit correspond au chiffre des unités et l'interrupteur gauche au chiffre des dizaines. Dans l'illustration ci-dessous, le transpondeur est identifié par le nombre 38.

Roues codeuses d'adressage

Numéro	Description
1	Interrupteurs rotatifs identifiant le transpondeur comme n° 38.

Pour un système avec adressage automatique, les transpondeurs et les claviers appartiennent à la même tranche de numérotation. Par exemple, les transpondeurs et les claviers sont automatiquement numérotés 01, 02, 03, etc. par le contrôleur dans l'ordre de leur détection, c'est-à-dire en fonction de leur position relative par rapport au contrôleur. Dans cette configuration, les zones sont affectées à chaque transpondeur d'entrée.

Les transpondeurs adressés automatiquement ne sont pas pris en charge par SPC41xx.

16.6.2 Rafraîchissement du X-BUS

L'utilitaire de rafraîchissement X-Bus recherche l'état courant du X-Bus et affiche sa configuration courante.

Pour rafraîchir l'état du X-Bus :

1. Passez à XBUS REFRESH.
2. appuyez sur SELECT.

   Le nombre de claviers en ligne est affiché.
3. Appuyez sur la touche programmable droite après chacun des affichages pour voir les transpondeurs, les zones et les éléments hors ligne.
4. Réappuyez sur cette touche pour sortir.

Rafraîchir ne modifie pas le système, mais est utile pour détecter les erreurs système, telles que les connexions lâches ou les transpondeurs inactifs avant d'exécuter une **Reconfiguration**.

16.6.3 Reconfigurer

REMARQUE : la fonction Reconfigurer s'applique uniquement aux zones reliées à un transpondeur par câble. Les zones sur un transpondeur et les zones de contrôleur qui sont sans fil ne sont pas mises en service après une reconfiguration. Pour activer les zones de la centrale, attribuez à la zone un type autre que « Inutilisé » en utilisant le menu Zones du clavier ou du navigateur Web.

Si le système compte plusieurs types de transpondeurs (avec et sans interrupteurs rotatifs), le système ne peut alors qu'être reconfiguré automatiquement. Si tous les transpondeurs du système possèdent un interrupteur rotatif, le système peut toujours être reconfiguré automatiquement : les interrupteurs rotatifs ne sont pas pris en compte et les transpondeurs sont adressés automatiquement.

Nous vous recommandons d'exécuter un **rafraîchissement** avant une **reconfiguration**.

Pour reconfigurer les claviers / transpondeurs :

1. Allez sur RECONFIGURER.
2. appuyez sur SELECT.

   Le nombre de claviers en ligne est affiché.
3. Appuyez sur SUIVANT.

   Le nombre de transpondeurs en ligne est affiché.
4. Appuyez sur SUIVANT

   Le nombre de zones en ligne est affiché.
5. Appuyez sur RETOUR pour quitter.

16.6.4 Claviers / Transpondeurs / Contrôleurs de porte

16.6.4.1 Localiser

Pour localiser un clavier/transpondeur/contrôleur de porte :

1. Allez sur CLAVIERS, TRANSPONDEUR ou CONTRÔLEUR DE PORTE et appuyez sur SELECT.
2. Allez sur LOCALISER et appuyez sur SELECT.
3. Allez sur le transpondeur/clavier/contrôleur de porte à localiser et appuyez sur SELECT.

   L'appareil sélectionné bipe et la LED clignote, ce qui permet à l'Installateur de le localiser.
4. Appuyez sur RETOUR pour quitter.

   Localisez les claviers avec les mêmes menus en suivant le cheminement du clavier au lieu de celui du transpondeur.

16.6.4.2 Moniteur

Pour consulter l'état des claviers/transpondeurs/contrôleurs de porte connectés au système :

1. Allez sur CLAVIERS, TRANSPONDEUR ou CONTRÔLEUR DE PORTE et appuyez sur SELECT.
2. Allez sur SURVEILLER et appuyez sur SELECT.
3. Allez sur l'option de programmation de surveillance désirée.
4. appuyez sur SELECT.

   La liste des claviers/transpondeurs détectés s'affiche.
5. Parcourez la liste et appuyez sur SELECT lorsque vous avez choisi le transpondeur / clavier / contrôleur de porte.

   Les paramètres et les propriétés affichés, le cas échéant, sont descrits dans le tableau ci-dessous.

ÉTAT	En ligne ou hors ligne
N° série	Numéro de série (utilisé pour suivre et identifier)
VER	Version du Firmware
MARCHE	Paramètres d'alimentation : valeurs de tension et courant en temps réel
INFO ADRESSE	Le mode d'adressage et l'adresse du clavier / transpondeur / contrôleur de porte.
FUS.AUX	L'état du fusible auxiliaire sur le transpondeur / contrôleur de porte

Module d'alimentation	Le type et l'état du module d'alimentation. (Uniquement pour les transpondeurs du PSU.) Faites défiler pour afficher la tension et la charge de courant sur les sorties, ainsi que l'état de la batterie. L'option Mode lien est également disponible (elle montre le paramétrage du cavalier sur la centrale pour la valeur Ah choisie). Les options sont 7 Ah et 17 Ah. (Ce cavalier n'est pas présent sur les modèles 5350 ou 6350) Si vous utilisez le SPC 5360 ou 6350, ce menu affiche l'état de la batterie et celui des fusibles sur les sorties.
BATTERIE	Tension batterie : niveau de tension de la batterie (ne concerne que les transpondeurs du PSU)
ETAT ENTREE	État de chaque entrée de zone associée à un transpondeur : C : fermé, O : ouvert, D : déconnecté, S : court-circuit (uniquement pour les transpondeurs avec des entrées)

6. Appuyez sur RETOUR pour quitter.

16.6.4.3 Éditer les claviers

Pour éditer les claviers :

1. Allez sur KEYPADS > EDIT.
2. appuyez sur SELECT.
3. Sélectionnez le périphérique à modifier et appuyez sur SELECT.

   Les paramètres de configuration pour un clavier standard et un clavier confort sont décrits dans les sections ci-dessous.
4. Appuyez sur RETOUR pour sortir du menu.

Paramètres du clavier LCD

Configurez les paramètres du clavier suivants.

MES	Description
Description	Saisissez une description unique pour identifier le clavier.
Touches de fonction (état repos)	
Panique	Sélectionnez Activé, Désactivé ou Silencieux validé. Si elle est activée, l'alarme panique entre en fonction en appuyant simultanément sur les deux touches programmables.
Vérification	Si une zone de vérification a été assignée au clavier, en cas de déclenchement d'une alarme de panique, il suffit de deux touches simultanément ou de saisir un code de contrainte pour activer les événements audio et vidéo.
Indications visuelles	
Rétro-éclairage (Backlight)	Sélectionnez quand le rétroéclairage du clavier doit être actif. Les options sont les suivantes : Lorsqu'une touche est pressée ; Toujours En service ; Toujours Hors service.
Voyants	Activez ou désactivez les témoins sur le clavier.
Etat des MES	Sélectionnez si l'état de surveillance doit être indiqué au repos.
Indications sonores	

MES	Description
Avertisseur sonore	Activez ou désactivez le buzzer sur le clavier.
Buzzer avec MES partielle	Activez ou désactivez le buzzer pendant la temporisation de sortie de la MES partielle.
Appui sur une touche	Sélectionnez si le volume du haut-parleur doit être activé lors d'un appui sur une touche.
Désactivation	
Calendrier	Sélectionnez si le clavier doit être protégé par calendrier. Voir *Calendriers* page 292.
Interaction logique	Sélectionnez si le clavier doit être protégé par une interaction logique.
Boîtier à clé	Sélectionnez si le clavier doit être protégé par un boîtier à clé.
Entrée TAG	Cochez cette case pour désactiver les touches du clavier pendant la temporisation d'entrée lorsqu'un TAG est configuré sur le clavier.
Secteurs	
Emplacement	Sélectionnez le secteur sécurisé où est placé le clavier.
Secteurs	Sélectionnez depuis le clavier les secteurs à contrôler.
Options	
Tempo MEST	Sélectionnez pour configurer un décalage de l'activation sur tous les claviers. L'emplacement du clavier est ignoré et tous les secteurs exécutent un décompte complet de la temporisation de sortie.

REMARQUE : un secteur ne doit être affecté à un clavier que si celui-ci se trouve à l'intérieur du secteur affecté et si un chemin d'entrée/sortie est défini. Si un secteur est affecté, lorsque celui-ci est mis en ou hors surveillance, les temporisations d'entrée et de sortie sont utilisées (si elles sont configurées). Les autres fonctions liées aux chemins d'entrée/sortie deviennent également accessibles. Si aucun secteur n'est affecté, le secteur est mis en ou hors service immédiatement et les autres fonctions d'entrée/sortie ne sont plus accessibles

Paramètres du clavier confort

Configurez les paramètres suivants pour le clavier confort.

MES	Description
Description	Saisissez une description unique pour identifier le clavier.
Touches de fonction (état repos)	
Panique	Sélectionnez Activé, Désactivé ou Silencieux validé. Si elle est activée, l'alarme panique entre en fonction en appuyant simultanément sur les deux touches programmables F1 et F2.
Feu	Activez pour permettre la mise en fonction de l'alarme incendie en appuyant simultanément sur les touches programmables F2 et F3.

MES	Description
Médical	Activez pour permettre la mise en fonction de l'alarme médicale en appuyant simultanément sur les touches programmables F3 et F4.
MES totale	Activez pour permettre la mise en fonction de la MES totale en appuyant deux fois sur la touche F2.
MES Partielle A	Activez pour permettre l'activation de la MES Partielle A en appuyant deux fois sur la touche F3.
MES Partielle B	Activez pour permettre l'activation de la MES Partielle B en appuyant deux fois sur F4.
Vérification	Si une zone de vérification est assignée au clavier confort, lorsqu'un événement médical, panique ou incendie est déclenché ou si un utilisateur saisit un code de contrainte, les événements audio et vidéo sont activés.
Voyants indicateurs	
Rétro-éclairage (Backlight)	Sélectionnez quand le rétroéclairage du clavier doit être actif. Les options sont les suivantes : Lorsqu'une touche est pressée ; Toujours En service ; Toujours Hors service.
NIV.RETROECLAIR	Sélectionnez l'intensité lumineuse du rétroéclairage. Plage 1 – 8 (élevé).
Voyants	Activez ou désactivez les témoins sur le clavier.
Etat des MES	Sélectionnez si l'état de surveillance doit être indiqué au repos. (LED)
Logo	Sélectionnez si le logo doit être visible au repos.
Montre analogique	Sélectionnez si la position de la montre doit être visible au repos. Les options sont : Aligné à gauche, Aligné au centre, Aligné à droite ou Désactivé.
Urgence	Activez si les touches de fonction Panique, Incendie et Médical doivent figurer sur l'afficheur LCD.
MES directe	Activez si les touches fonctions de MES Totale et Partielle doivent figurer sur l'afficheur LCD.
Indications sonores	
Alarmes	Sélectionnez le volume du haut-parleur pour les indications d'alarme.
Entrée/sortie	La plage est de 0 à 7 (volume maximal).
Carillon	Sélectionnez le volume du haut-parleur pour les indications d'entrée et sortie, ou désactivez le son.
Appui sur une touche	La plage est de 0 à 7 (volume maximal).
Annonce Vocale	Sélectionnez le volume du haut-parleur pour le carillon, ou désactivez le son.
Buzzer avec MES partielle	La plage est de 0 à 7 (volume maximal).
Désactivation	
Calendrier	Sélectionnez si le clavier doit être protégé par calendrier. Voir calendrier.
Interaction logique	Sélectionnez si le clavier doit être protégé par une interaction logique.

MES	Description
Boîtier à clé	Sélectionnez si le clavier doit être protégé par un boîtier à clé.
Entrée TAG	Cochez cette case pour désactiver les touches du clavier pendant la temporisation d'entrée lorsqu'un TAG est configuré sur le clavier.
Secteurs	
Emplacement	Sélectionnez le secteur sécurisé où est placé le clavier.
Secteurs	Sélectionnez depuis le clavier les secteurs à contrôler.
Options	
Tempo MEST	Sélectionnez pour configurer un décalage de l'activation sur tous les claviers. L'emplacement du clavier est ignoré et tous les secteurs exécutent un décompte complet de la temporisation de sortie.

REMARQUE : un secteur ne doit être affecté à un clavier que si celui-ci se trouve à l'intérieur du secteur affecté et si un chemin d'entrée/sortie est défini. Si un secteur est affecté, lorsque celui-ci est mis en ou hors surveillance, les temporisations d'entrée et de sortie sont utilisées (si elles sont configurées). Les autres fonctions liées aux chemins d'entrée/sortie deviennent également accessibles. Si aucun secteur n'est affecté, le secteur est mis en ou hors service immédiatement et les autres fonctions d'entrée/sortie ne sont plus accessibles.

16.6.4.4 Éditer les transpondeurs

Pour éditer les transpondeurs :

1. Allez sur TRANSPONDEURS > ÉDITER.
2. appuyez sur SELECT.
3. Sélectionnez le périphérique à modifier et appuyez sur SELECT.

   Les paramètres et les propriétés, si applicables, sont affichés pour être modifiés.
4. Appuyez sur RETOUR pour sortir du menu.

Pour l'appellation et l'identification, les transpondeurs sont des zones attribuées (par groupe de 8) avec des identités consécutives allant de 1 à 512. (Le numéro le plus élevé pour l'identification de zone est 512.) Ainsi, tout transpondeur identifié par un numéro supérieur à 63 n'est attribué à aucune zone.

Édition des transpondeurs E/S

Le tableau suivant contient la liste des options disponibles pour les transpondeurs E/S :

Fonction	Description
Description	Édition de la description du transpondeur.

Édition des transpondeurs audio.

Le tableau suivant fournit une liste des options disponibles dans le menu **Edition** pour les transpondeurs audio :

Nom	Description
LIBELLÉ	Saisissez ou éditez une description du transpondeur audio.
INPUT (ENTRÉE)	Sélectionnez les entrées de zone.
LIMITE DU VOLUME	Sélectionnez la limite du volume.

Éditez les transpondeurs radios.

Le tableau suivant contient la liste des options disponibles pour les transpondeurs radio :

Fonction	Description
Description	Édition de la description du transpondeur.

Édition des transpondeurs E/S analysés

Le tableau suivant contient la liste des options disponibles pour les transpondeurs ESA :

Nom	Description
Description	Édition de la description du transpondeur.

Édition des modules de transpondeur d'indication

Le tableau suivant contient la liste des options disponibles pour les transpondeurs d'indication :

Nom	Description
LIBELLÉ	Saisissez ou éditez une description du transpondeur.
LOCALISATION	Sélectionnez un emplacement pour le transpondeur dans la liste des secteurs disponibles.
TOUCHES FONCTION	Vous permettent d'affecter une action à des touches spécifiques pour des zones spécifiques. Sélectionnez un secteur et affectez une des options suivantes à ce secteur : • Néant • Mise hors surveillance • MES Partielle A • MES Partielle B • MES totale • Alterne MHS/MES Tot • Alterne MHS/MES PartA • Alterne MHS/MES PartB • All Okay • Autorisation avant MES/MHS

Nom	Description
Indications visuelles (Mode flexible uniquement)	Vous permet d'affecter un comportement spécifique à chaque LED sur le module des voyants. Chacune des LED dispose des options suivantes : • FONCTION — les options suivantes sont disponibles : – BOÎTIER À CLÉ — sélectionnez un boîtier à clé et la position de la clé. – DÉSACTIVÉ — sélectionnez pour désactiver la LED. – SYSTÈME — sélectionnez le type d'alarme déclenchant la LED. – SECTEUR — sélectionnez le secteur déclenchant la LED. – ZONE — sélectionnez la zone déclenchant la LED. – PORTE — sélectionnez la porte et l'option de porte déclenchant la LED. • MARCHE - COULEUR — spécifiez la couleur de l'activation • MARCHE – CLIGNOT. — spécifiez le comportement de la LED en état actif. Les options disponibles sont les suivantes : – Permanent — toujours allumé. – Clignotement rapide / moyen / lent — variation de la vitesse du clignotement. • HORS - COULEUR — spécifiez la couleur de l'activation • ARRÊT – CLIGNOT. — spécifiez le comportement de la LED en état inactif. Les options disponibles sont les suivantes : – Permanent — toujours allumé. – Clignotement rapide / moyen / lent — variation de la vitesse du clignotement.
LED TOUJOURS	Active le fait que les voyants LED restent actifs si les touches sont désactivées.
IND. SONORES (Mode flexible uniquement)	Sélectionnez les signaux sonores pour les alarmes, l'entrée / sortie et l'activation de touche.
DESACTIVATION (Mode flexible uniquement)	Choisissez une ou plusieurs parmi les options suivantes de désactivation : • Calendrier – sélectionnez un calendrier parmi les options disponibles. • Boîtier à clé – sélectionnez un boîtier à clé parmi les options disponibles. • Clavier - sélectionnez un clavier parmi les options disponibles. • Lecteur de badges - activez ou désactivez la désactivation à l'aide du clavier.
MODE	Sélectionnez Lié ou Flexible. Le mode Lié réduit le nombre d'options disponibles dans le menu Éditer transpondeur.
INPUT (ENTRÉE)	Sélectionnez la zone

Édition des transpondeurs à boîtier à clé

Le tableau suivant fournit la liste des optons disponibles pour les transpondeurs à boîtier à clé :

Nom	Description
LIBELLÉ	Saisissez ou éditez une description du transpondeur.
LOCALISATION	Sélectionnez un emplacement pour le transpondeur dans la liste des secteurs définis.
VERROU	Activez ou désactivez le verrou à l'emplacement de la clé.

Nom	Description
Indications visuelles (Mode Flexible seulement)	Vous permet d'affecter un comportement spécifique à chaque LED sur le transpondeur à boîtier à clé. Chacune des LED dispose des options suivantes : • FONCTION — les options suivantes sont disponibles : – BOÎTIER À CLÉ — sélectionnez un boîtier à clé et la position de la clé. – DÉSACTIVÉ — sélectionnez pour désactiver la LED. – SYSTÈME — sélectionnez le type d'alarme déclenchant la LED. – SECTEUR — sélectionnez le secteur déclenchant la LED. – ZONE — sélectionnez la zone déclenchant la LED. – PORTE — sélectionnez la porte et l'option de porte déclenchant la LED. • MARCHE - COULEUR — spécifiez la couleur de l'activation • MARCHE – CLIGNOT. — spécifiez le comportement de la LED en état actif. Les options disponibles sont les suivantes : – Permanent — toujours allumé. – Clignotement rapide / moyen / lent — variation de la vitesse du clignotement. • HORS - COULEUR — spécifiez la couleur de l'activation • ARRÊT – CLIGNOT. — spécifiez le comportement de la LED en état inactif. Les options disponibles sont les suivantes : – Permanent — toujours allumé. • Clignotement rapide / moyen / lent — variation de la vitesse du clignotement.
DESACTIVATION (Mode Flexible seulement)	Sélectionnez une méthode de désactivation à partir des options disponibles : • Calendrier — sélectionnez un calendrier.
POSITIONS CLE	Vous permet d'affecter un comportement aux positions de clé spécifiques pour des secteurs spécifiques. Sélectionnez un secteur pour la position de clé et affectez une des options suivantes à ce secteur : • Néant • Mise hors surveillance • MES Partielle A • MES Partielle B • MES totale • Alterne MHS/MES Tot • Alterne MHS/MES PartA • Alterne MHS/MES PartB • All Okay • Autorisation avant MES/MHS

16.6.4.5 Éditer les contrôleurs de porte

Pour plus d'informations sur les contrôleurs de porte, voir *Transpondeur de porte* page 83.

1. Allez sur CONTRÔLEURS DE PORTE > ÉDITER.
2. appuyez sur SELECT.

3. Sélectionnez le périphérique à modifier et appuyez sur SELECT.

   Les paramètres et les propriétés affichés, le cas échéant, sont décrits dans le tableau ci-dessous.

LIBELLÉ	Nom du contrôleur de porte
PORTES	Configuration de l'E/S de la porte 1 et de l'E/S de la porte 2.
LECTEURS	Configuration des profils de lecteur

Pour éditer une E/S de porte :

1. Allez sur PORTES.
2. appuyez sur SELECT.
3. Allez à la Porte E/S que vous voulez modifier en utilisant les touches de direction bas/haut et appuyez sur SELECT.

   Les paramètres et les propriétés affichés, le cas échéant, sont descrits dans le tableau ci-dessous.

ZONES	Aucune fonctionnalité d'accès n'est exécutée. Les entrées et sorties peuvent être utilisées normalement.
PORTE 1 – PORTE 64	Le numéro de porte sélectionnée est affecté à l'E/S DE PORTE.

Si l'option « ZONE » est sélectionnée pour une E/S DE PORTE, les deux entrées de cette E/S de porte doivent être configurées :

Pour éditer les deux zones d'une E/S de porte :

1. Allez à l'E/S DE PORTE que vous voulez modifier et appuyez sur SELECT.

   L'option « Zones » est sélectionnée.
2. appuyez sur SELECT.
3. Sélectionnez la zone qui doit être modifiée (zone DPS ou DRS).
4. appuyez sur SELECT.

   Les paramètres et les propriétés affichés, le cas échéant, sont descrits dans le tableau ci-dessous.

NON AFFECTÉE	Cette zone n'est pas affectée et ne peut pas être utilisée.
ZONE 1 – ZONE 512	La zone qui est modifiée est affectée à ce numéro de zone. Si la zone est affectée à un numéro de zone spécifique, elle peut être configurée comme une zone normale.

Les zones peuvent être affectées à chaque numéro de zone disponible. Cette attribution n'est pas fixe. Si la zone a été affectée au numéro de zone 9 et si un transpondeur d'entrée ayant l'adresse 1 est connecté au X-BUS (lequel utilise les numéros de zone 9 à 16), la zone affectée à partir du contrôleur double porte est déplacée vers le prochain numéro disponible. La configuration est adaptée en conséquence.

Pour modifier un PROFIL LECTEUR :

1. Allez sur LECTEURS.
2. appuyez sur SELECT.
3. Allez sur le LECTEUR à modifier et appuyez sur SELECT.

   Sélectionnez l'un des profils suivants pour le lecteur :

1	Pour les lecteurs ayant une LED verte/rouge.
2	Pour les lecteurs VANDERBILT ayant une LED jaune (AR618X).
3	Le profil 3 est utilisé avec les lecteurs HID qui envoient un code PIN à la centrale en tant que lecture de badge avec un code site prédéfini (0).
4	Le profil 4 est utilisé avec les lecteurs HID qui envoient un code PIN à la centrale en tant que lecture de badge avec un code site prédéfini (255).
5	Effectuez ce choix pour activer les lecteurs Sesam. Pour l'homologation VDS, assurez-vous de sélectionner l'option **Forcer profil lecteur** sur le navigateur pour obtenir un retour d'informations durant la configuration.

Voir également

Transpondeur de porte page 83

16.6.5 Mode adressage

L'adressage X-BUS peut être configuré de deux manières :

Adressage automatique

En mode d'adressage automatique, le contrôleur ignore les interrupteurs rotatifs et attribue automatiquement un numéro d'identification (adresse) séquentiel aux transpondeurs et aux claviers du système.

Adressage manuel

L'adressage manuel permet à l'installateur d'attribuer lui-même un numéro d'identification aux transpondeurs/claviers. Après avoir installé tous les périphériques à leur endroit de destination, l'installateur attribue les numéros d'identification manuellement à l'aide des interrupteurs rotatifs. Les ID de zone peuvent être déterminées en utilisant la formule suivante : [(valeur d'ID X 8) + 1] = numéro de la première zone suivi des numéros séquentiels des 7 zones suivantes. Par exemple [(ID2 x 8) + 1] = 17. La zone 17 est attribuée à l'entrée 1 sur ID2. Chacune des entrées reçoit le numéro séquentiel de zone suivant, dans ce cas jusqu'à la zone 24.

Remarque : limite d'ID pour l'affectation de zone pour le SPC 4000 : ID transpondeur 1–3. SPC 5000 : ID transpondeur 1–15. SPC 6000 : ID transpondeur 1-63.

ID	Zone	ID	Zone	ID	Zones	ID	Zones	ID	Zones
1	9-16	14	113-120	27	217-224	40	321-328	53	425-432
2	17-24	15	121-128	28	225-232	41	329-336	54	433-440
3	25-32	16	129-136	29	233-240	42	337-344	55	441-448
4	33-40	17	137-144	30	241-248	43	345-352	56	449-456
5	41-48	18	145-152	31	249-256	44	353-360	57	457-464
6	49-56	19	153-160	32	257-264	45	361-368	58	465-472
7	57-64	20	161-168	33	265-272	46	369-376	59	473-480
8	65-72	21	169-176	34	273-280	47	377-384	60	481-488
9	73-80	22	177-184	35	281-288	48	385-392	61	489-496
10	81-88	23	185-192	36	289-296	49	393-400	62	497-504

ID	Zone	ID	Zone	ID	Zones	ID	Zones	ID	Zones
11	89-96	24	193-200	37	297-304	50	401-408	63	505-512
12	97-104	25	201-208	38	305-312	51	409-416		
13	105-112	26	209-216	39	313-320	52	417-424		

Si deux périphériques du même type (par exemple, deux transpondeurs) ont la même adresse, les deux émettent un bip après la configuration et le témoin LED clignote pour indiquer un conflit. Après une réinitialisation des interrupteurs, le système passe à nouveau en revue les périphériques présents.

Si les deux interrupteurs rotatifs d'un périphérique sont réglés sur zéro (0, 0), l'adressage est automatique.

Pour sélectionner le mode d'adressage:

1. Sélectionnez MODE ADRESSAGE.
2. Appuyez sur SELECT.
3. Choisissez le mode d'adressage voulu : AUTOMATIQUE ou MANUEL
4. Appuyez sur SELECT pour mettre à jour le paramètre.

16.6.6 Type X-BUS

Pour programmer le type X-BUS depuis le clavier :

1. Allez sur TYPE X-BUS.
2. appuyez sur SELECT.
3. Sélectionnez la configuration voulue :
   – BOUCLE
   – BRANCHE
4. Appuyez sur SELECT pour mettre à jour le paramètre.

16.6.7 Ré-essai bus

Pour programmer le nombre de tentatives de retransmission des données via l'interface X-BUS avant qu'une erreur de communication soit générée :

1. Allez sur RÉ-ESSAI BUS.
2. Appuyez sur SELECT.
3. Entrez le nombre souhaité de tentatives de retransmission des données.
4. Appuyez sur SELECT pour mettre à jour le paramètre.

16.6.8 Tempo communications

Pour indiquer le délai avant qu'un défaut de communication ne soit enregistré :

1. Allez sur TEMPO COMMUNICATIONS.
2. Appuyez sur SELECT.
3. Saisissez la durée que vous souhaitez.
4. Appuyez sur ENTRÉE pour mettre à jour le paramètre.

16.7 Radio

1. Allez sur RADIO et appuyez sur SELECT.
2. Allez sur l'option de programmation désirée :

DÉTECTEURS	Il peut être nécessaire de modifier le type de détecteur programmé dans le système s'il n'a pas été correctement identifié pendant la phase de programmation. Si aucun détecteur radio n'a été programmé, le clavier affiche PAS DE DÉTECTEURS ACTIFS. Les options suivantes sont disponibles pour les détecteurs : • AJOUTER Consultez *Ajouter des détecteurs* ci-dessous • ÉDITER (modifier l'affectation de zone) Consultez *Éditer des détecteurs (affectation de zone)* à la page suivante • RETIRER Sélectionnez le périphérique ou le détecteur à supprimer.
WPA	Ajouter, éditer ou retirer un WPA (alarme personnelle sans fil). • AJOUTER Consultez *Ajouter WPA* à la page suivante • ÉDITER Consultez *Éditer WPA* à la page suivante • RETIRER Sélectionnez le WPA à supprimer.
ANTENNE EXTERNE	Activer ou désactiver l'antenne externe
SUPERVISION	Activer ou désactiver la supervision d'autosurveillance.
FILTRE SIGNAL BAS	Activer ou désactiver le filtre signal bas (force du signal RF 0 et 1).
DÉTECT. PB RF	Activer ou désactiver le brouillage RF.
PANIQUE RADIO	Activer ou désactiver la panique radio ou activer le mode silencieux pour la panique radio.
PLANIFICATION TEST WPA	Saisissez un délai maximal (en jours) entre deux tests WPA. Le maximum est 365 jours.
DÉLAI PRÉV. MES	Saisissez un temps en minutes au-delà duquel, si le détecteur ou le WPA n'envoie pas de signal, une activation est empêchée pour le secteur où se trouve la zone radio. Le délai maximal est 720 minutes.
DÉLAI RADIO PERDU	Saisissez le nombre de minutes au-delà duquel l'appareil sans fil est considéré comme perdu s'il n'envoie pas de signal. (Le minimum est 20 et le maximum 720 minutes)

16.7.1 Ajouter des détecteurs

Pour ajouter un détecteur radio :

1. Allez sur AJOUTER et appuyez sur SELECT.

   Le message ACTIVER ENREG. s'affiche.
2. Appuyez sur SELECT.

La ligne supérieure de l'écran clignote en affichant le texte ACTIVER APPAREIL.

3. Activez l'appareil sans fil entre trois et cinq fois successivement pour permettre au récepteur du clavier de détecter la transmission sans fil de l'appareil.

   L'écran indique que l'appareil a bien été détecté en faisant clignoter le texte TROUVÉ DÉTECTEUR. Le TYPE et l'ID de l'appareil s'affichent alternativement.

4. Appuyez sur ENREG.

   Un message s'affiche pour vous inviter à sélectionner le type de zone.

5. Appuyez sur SELECT.
6. Allez sur le type de zone voulu et appuyez sur SELECT.

Pour ajouter un appareil avec AUTOSUR. ENREG., allez sur cette option dans l'étape 2. La procédure d'enregistrement est identique, mais il vous est demandé de définir un type de secteur avant le type de zone.

16.7.2 Éditer des détecteurs (affectation de zone)

Il peut être nécessaire de modifier l'affectation de zone d'un détecteur enregistré sur le système.

Pour modifier l'affectation de zone d'un détecteur radio :

1. Allez sur ÉDITER et appuyez sur SELECT.
2. Allez sur le détecteur à modifier et appuyez sur SELECT.
3. Allez sur ZONE.
4. Sélectionnez le numéro de zone approprié (seuls les numéros de zone disponibles sont affichés).
5. appuyez sur SELECT.

16.7.3 Ajouter WPA

AVERTISSEMENT : vous ne pouvez configurer un WPA ou vérifier son statut que s'il y a un module radio installé sur la centrale ou sur l'un de ses transpondeurs et si la centrale dispose d'une licence pour le type de module(s) installé(s).

Un WPA n'est pas affecté à un utilisateur. Généralement, un WPA est partagé entre plusieurs personnes, par exemple des gardes de sécurité qui travaillent en équipe ; il peut également être fixé de manière permanente sur une surface, par exemple sous un bureau ou derrière une caisse enregistreuse.

Un maximum de 128 WPA est autorisé pour chaque centrale.

Pour configurer un WPA à partir du clavier :

1. Sélectionnez RADIO, puis WPA.
2. Sélectionnez ÉDITER pour ajouter un WPA.
3. Sélectionnez MANUELLEMENT pour saisir manuellement une ID WPA.
   L'ID peut aussi être saisie automatiquement par la centrale en sélectionnant l'option APPRENDRE WPA. L'un des boutons WPA doit être pressé lorsque le message ACTIVER WPA s'affiche pour que la centrale puisse identifier le WPA. La centrale n'accepte pas un WPA dont l'ID est une copie d'un WPA déjà configuré.
4. Quittez le menu AJOUTER et sélectionnez le menu ÉDITER pour configurer le WPA.

16.7.4 Éditer WPA

Pour configurer un WPA à partir du clavier :

1. Sélectionnez RADIO, puis WPA.
2. Sélectionnez ÉDITER pour configurer un WPA.

LIBELLÉ	Saisissez une description pour identifier de manière unique le WPA.
ID TRANSMETTEUR	Saisir l'ID du WPA. La centrale n'accepte pas un WPA dont l'ID est une copie d'un WPA déjà configuré.
FONCT DES BOUTON	Utilisez cette section pour assigner des fonctions à des associations de boutons. Les fonctions disponibles sont les suivantes : Panique, Panique silencieuse, Agression, Suspicion, Sortie RF utilisateur, Médical. Il est possible de sélectionner plusieurs combinaisons de boutons pour la même fonction. Par exemple : • Jaune – Suspicion● • Rouge + Vert – Hold-up • Pour les installations Évolué ou Simple, la valeur par défaut est : Rouge + Vert – Panique **Remarque :** si aucune fonction n'a été assignée à une combinaison de boutons, il est encore possible d'affecter cette combinaison à un déclencheur. Voir *Déclencheurs* page 298.
SUPERVISION	Le WPA peut être configuré pour envoyer des signaux de supervision périodique. Si la supervision est activée sur le WPA (avec le cavalier), le WPA envoie un message de supervision environ toutes les 7,5 minutes. Le délai entre deux messages est randomisé pour limiter le risque de collision avec les autres WPA. La fonction de supervision doit également être activée sur la centrale pour le WPA concerné afin de permettre un fonctionnement correct de la supervision. Si la centrale ne reçoit pas de signal de supervision, elle déclenche une alarme qui s'affiche dans le clavier et est journalisée. Si la supervision n'est pas activée, le WPA envoie un message de supervision environ toutes les 24 heures pour indiquer l'état de la batterie du WPA à la centrale. Ce message est également randomisé pour limiter le risque de collision avec les autres WPA. Sélectionnez ACTIVER si la supervision est activée pour ce WPA particulier.
TEST	Active la fonction de test du signal WPA.

Voir également

Déclencheurs page 298

Radio page 153

Test WPA page 174

16.8 Zones

1. Allez sur ZONES et appuyez sur SELECT.
2. Allez sur la zone désirée (ZONE 1-x).
3. Allez sur l'option de programmation désirée :

LIBELLÉ	Aide à identifier la zone: entrez un nom descriptif individuel.
TYPE DE ZONE	Détermine le type de zone. Voir *Types de zone* page 397.

ATTRIBUTS	Détermine les attributs pour la zone. Voir *Attributs zone* page 404.
AU SECTEUR	Détermine quelle zone est rattachée à quel secteur. Cette option de menu ne s'affiche que si plusieurs secteurs sont définis sur le système. La sélection de cette fonction permet aux utilisateurs de créer un ensemble de zones qui sont identifiées avec un secteur particulier dans le bâtiment.

Le nombre et le type d'attributs affichés dans les menus du clavier pour une zone particulière varient en fonction du type de zone sélectionnée.

16.9 sur les portes

1. Allez sur DOORS et appuyez sur SELECT.
2. Allez sur la porte que vous voulez programmer et appuyez sur SELECT.
3. Les paramètres et les propriétés affichés peuvent être modifiés. Ce sont les suivants :

   - Description

   – Entrées de porte

   – Groupe de portes

   – Attributs de porte

   – Temporisateurs porte

   – Données lecteur (affichage seul : format du dernier badge lu avec le lecteur configuré)

Entrées de porte

Chaque porte dispose de deux entrées avec deux fonctionnalités prédéfinies. Ces deux entrées – le détecteur de position et le bouton d'ouverture de la porte – peuvent être configurées.

Nom	Description
Zone	L'entrée de détecteur de position de porte peut aussi être utilisée pour les fonctions « intrusion ». Si l'entrée de détecteur de position de porte est utilisée pour les fonctions « intrusion », sélectionnez le numéro de zone auquel l'entrée est attribuée. Si le détecteur de position de la porte est utilisé uniquement pour la partie accès, l'option « NON AFFECTÉE » doit être sélectionnée. Si le détecteur de position de la porte est affecté à une zone d'intrusion, il peut être configuré comme une zone normale, mais uniquement avec des fonctionnalités limitées (par exemple, tous les types de zones ne peuvent pas être sélectionnés). Si un secteur ou le système est activé avec le lecteur de badge, l'entrée du détecteur de position de la porte doit être affectée à un numéro de zone et au secteur/système qui doit être activé.
Description (Web uniquement)	Description de la zone à laquelle est affecté le détecteur de position de la porte.

Nom	Description
Type de zone (Web uniquement)	Type de zone pour la zone à laquelle le détecteur de position de porte est affecté (tous les types de zones ne sont pas disponibles).
Attributs zone (Web uniquement)	Les attributs de la zone à laquelle est affecté le détecteur de position de porte peuvent être modifiés.
Zone (Web uniquement)	Le secteur auquel la zone et le lecteur de badge sont affectés. (Si le lecteur de badge est utilisé pour l'activation et la désactivation, ce secteur sera activé/désactivé.)
Position porte (web) Résistance fin de ligne DPS (claviers)	La résistance utilisée avec le détecteur de position de porte. Sélectionnez une résistance / une association de résistances.
DPS normalement ouvert	Indique si le bouton d'ouverture de porte est une entrée normalement ouverte ou non.
Libération porte (Web) DRS RES.FIN LIGN (claviers)	La résistance utilisée avec le bouton d'ouverture de porte. Sélectionnez une résistance / une association de résistances.
DRS normalement ouvert	Indique si le bouton d'ouverture de porte est une entrée normalement ouverte ou non.
Pas de DRS (Web uniquement)	Sélectionnez pour ignorer le DRS. Si un DC2 est utilisé sur la porte, cette option DOIT être sélectionnée. Si elle n'est pas sélectionnée, la porte s'ouvrira.
Localisation du Lecteur (Entrée/Sortie) (Web uniquement)	Sélectionnez l'emplacement des lecteurs d'entrée et de sortie.
Formats de lecture (web) INFO LECTEUR (claviers)	Affiche le format du dernier badge lu avec chaque lecteur configuré.

Chaque numéro disponible peut être attribué à une zone, mais l'affectation n'est pas déterminée. Si le numéro 9 est affecté à une zone, celle-ci et un transpondeur d'entrée avec l'adresse 1 sont connectés au X-BUS (qui utilise les numéros de zones compris entre 9 et 16). La zone affectée à partir du contrôleur double porte est déplacée vers le prochain numéro disponible. La configuration est adaptée en conséquence.

Groupes de portes

Chaque porte peut être affectée à un groupe de portes. Cela est nécessaire si l'une des fonctionnalités suivantes est activée :

- Gardien
- Antipassback soft
- Antipassback avec blocage
- Verrouillage

Attributs de porte

Si aucun attribut n'est actif, on peut utiliser une carte en cours de validité.

Attribut	Description
Badge inutilisé	Le badge est bloqué provisoirement.
Groupe de portes	Utilisé lorsque plusieurs portes sont assignées au même secteur ou quand les fonctionnalités antipassback, gardien ou interverrouillage sont requises.
Badge et code	L'accès est possible seulement avec un badge et un code PIN.
Code seulement	Un code PIN est requis. Le badge n'est pas accepté.
Code PIN ou Badge	L'accès est possible seulement avec un badge ou un code PIN.
Code pour sortir	Code requis sur le lecteur de sortie. La porte doit posséder un lecteur d'entrée et un lecteur de sortie.
Code pour MES/MHS	Le code PIN est requis pour armer (MES) ou désarmer (MHS) le secteur lié. Le badge doit être présenté avant de saisir le code.
MHS à l'extérieur (navigateur)	Le secteur sera mis à l'arrêt lorsqu'un badge est présenté sur le lecteur d'entrée.
MHS à l'intérieur (navigateur)	Le secteur sera mis à l'arrêt lorsqu'un badge est présenté sur le lecteur de sortie.
Accès si MES	L'accès est autorisé si le secteur est en MES et que la porte est de type zone d'alarme ou zone d'entrée.

Attribut	Description
MES à l'extérieur (navigateur)	Le secteur sera mis en surveillance lorsqu'un badge est présenté deux fois sur le lecteur d'entrée.
MES sur lecteur de sortie	Le secteur sera mis en surveillance lorsqu'un badge est présenté deux fois sur le lecteur de sortie.
Forcer MES totale	Si l'utilisateur possède les droits correspondants, il peut forcer le réglage du lecteur d'entrée.
Urgence	La porte est déverrouillée automatiquement en cas de détection d'un incendie dans le secteur attribué.
Évacuat. globale	Un incendie dans un secteur quelconque déverrouille la porte.
Escorte	La fonction Escorte permet à des détenteurs de badge à accès privilégié d'escorter d'autres détenteurs de badge à travers certaines portes. Quand cette fonction est appliquée à une porte, un badge avec des « droits d'escorte » doit être présenté en premier, puis les autres détenteurs de badge ne possédant pas ce privilège peuvent ouvrir cette même porte. Le délai entre la présentation du badge d'escorte et celle du badge normal est configuré pour chacune des portes.
Anti-passback*	La fonction antipassback (protection physique) doit être activée sur la porte. Toutes les portes doivent posséder un lecteur d'entrée et un lecteur de sortie, et doivent faire partie d'un groupe de portes. Dans ce mode, les détenteurs de badge doivent utiliser leur badge pour entrer et sortir d'un espace défini par un groupe de portes. Si un détenteur de badge valide présente son badge pour entrer dans un espace mais qu'il ne le présente pas pour en sortir, il viole les règles d'antipassback. La prochaine fois qu'il tentera de pénétrer dans le même espace, une alarme d'antipassback réelle est déclenchée, l'empêchant ainsi d'entrer dans le groupe de portes.
Antipassback soft*	Les violations des règles d'antipassback sont seulement journalisées. Toutes les portes doivent posséder un lecteur d'entrée et un lecteur de sortie, et doivent faire partie d'un groupe de portes. Dans ce mode, les détenteurs de badge doivent utiliser leur badge pour entrer et sortir d'un espace défini par un groupe de portes. Si un détenteur de badge valide présente son badge pour entrer dans un espace mais qu'il ne le présente pas pour en sortir, il viole les règles d'antipassback. La prochaine fois qu'il tentera de pénétrer dans le même groupe de portes, une alarme d'antipassback logiciel est déclenchée. Cependant, le détenteur de badge pourra entrer dans ce groupe de portes.
Gardien*	La fonction Gardien permet à un détenteur de badge ayant le privilège de gardien (le gardien) d'accompagner dans une pièce d'autres détenteurs de badge n'ayant pas ce privilège. Le gardien doit pénétrer dans une pièce en premier. Les autres personnes ne sont autorisées à entrer dans la pièce que si le gardien s'y trouve déjà. Le gardien n'est pas autorisé à quitter la pièce tant qu'il reste un non-gardien.
Buzzer porte	Le buzzer monté sur la carte de circuit imprimé du contrôleur de porte retentit en cas d'alarme sur une porte.
Ignorer les portes forcées	L'ouverture forcée d'une porte est ignorée.

Attribut	Description
Group. Interver. * (navigateur)	Une seule porte d'un seul secteur peut être ouverte à la fois. Groupe Portes requis.
Préfixe de MES	Utilisation des touches (A, B, * ou #) en préfixe pour armer le système
* Groupe Portes requis.	

Timers porte

Durée	Min.	Max.	Description
Accès autorisé	1 s	255 s	Durée pendant laquelle la porte reste ouverte après que l'accès est autorisé.
Accès refusé	1 s	255 s	Durée après laquelle le contrôleur sera de nouveau prêt, après un événement invalide.
Porte ouverte	1 s	255 s	Temps avant lequel la porte doit être fermée pour éviter une alarme « Porte ouverte trop longtemps ».
Porte restée ouverte	1 min	180 min	Temps avant lequel la porte doit être fermée pour éviter une alarme « Porte laissée ouverte ».
Extension de temps	1 s	255 s	Temps additionnel après avoir autorisé l'accès à un badge disposant d'un attribut d'extension de temps.
Escorte	1 s	30 s	Durée pendant laquelle, après avoir présenté un badge avec un attribut Escorte en accompagnement d'un utilisateur sans droit d'escorte, il est possible de franchir la porte.

16.10 Sorties

Chaque type de zone sur le système SPC a son type de sortie associé (un drapeau ou un indicateur interne). Lorsqu'un type de zone est activé – p. ex., si une porte ou une fenêtre s'ouvre, de la fumée est détectée, une alarme se déclenche, etc. –, la sortie correspondante est activée.

1. Allez sur SORTIES et appuyez sur SELECT.
2. Allez sur CONTRÔLEUR ou TRANSPONDEUR et appuyez sur SELECT.
3. Allez sur le transpondeur / la sortie que vous voulez programmer et appuyez sur SELECT.

   Si les activations de sortie sont enregistrées dans le journal des événements système (activés, éléments enregistrés/désactivés, éléments), les options de programmation indiquées dans le tableau ci-dessous deviennent possibles.

NOMS	Aide à identifier la sortie : entrez un nom descriptif individuel.
TYPE DE SORTIE	Détermine le type de sortie ; voir le tableau dans *Types de sortie et ports de sortie* à la page opposée pour la description des types de sorties.
MODE SORTIE	Détermine le mode de sortie : en continu, impulsion ou intermittent.
POLARITÉ	Indique si la sortie est activée sur une polarité positive ou négative.

JOURNAL DE BORD	Indique si le journal système est activé ou désactivé.

Pour la procédure de test des sorties, consultez *Test sortie* page 172.

16.10.1 Types de sortie et ports de sortie

Chaque type de sortie peut être attribué à un des 6 ports de sortie physiques sur le contrôleur SPC ou à une sortie de l'un des transpondeurs connectés. Les types de sortie qui ne sont pas attribués à des sorties physiques servent d'indicateurs d'événements sur le système et peuvent être enregistrés et/ou renvoyés vers des centres de télésurveillance éloignés si nécessaire.

Les ports de sortie des transpondeurs sont tous des sorties de type relais unipolaire (NO, COM, NC) ; par conséquent, les tags de sortie ont besoin d'une source d'alimentation externe s'ils sont reliés à des sorties de transporteur.

L'activation d'un certain type de sortie dépend du type de zone (voir *Types de zone* page 397) ou de l'alerte qui déclenche l'activation. Si plusieurs secteurs sont définis, les sorties du SPC sont groupées en sorties système et sorties secteur ; les sorties système sont activées pour indiquer un événement au niveau du système (par exemple une panne de courant) alors que les sorties secteur indiquent des événements détectés dans au moins un secteur. Chaque secteur dispose de son propre ensemble de sorties secteur ; si le secteur est commun à d'autres secteurs, ces sorties indiqueront alors l'état de tous les secteurs avec lesquels il est commun, y compris son propre état. Par exemple, si le secteur 1 est commun avec les secteurs 2 et 3, et que la sirène ext. du secteur 2 est activée, alors la sirène ext. du secteur 1 sera aussi activée.

Certains types de sortie ne peuvent indiquer que des événements au niveau du système (aucun événement spécifique à un secteur). Voir le tableau ci-dessous pour de plus amples informations.

Type de sortie	Description
Sirène extérieure	Ce type de sortie est utilisé pour activer la sirène extérieure du système. La sortie est active quand une sirène extérieure du secteur est active. Par défaut, cette sortie est attribuée à la première sortie sur la carte de la centrale (EXT+, EXT-). **Remarque :** une sortie de sirène extérieure est activée automatiquement chaque fois qu'une zone programmée comme une zone d'alarme déclenche une alarme en mode MES Totale ou MES Partielle.
Flash sirène extérieure	Ce type de sortie est utilisé pour activer le flash sur la sirène extérieure du système. La sortie est active quand un flash du secteur est actif. Par défaut, cette sortie est attribuée à la sortie de relais de flash (sortie 3) sur la carte du contrôleur (NO, COM, NC). **Remarque :** une sortie de flash sirène extérieure est activée automatiquement chaque fois qu'une zone programmée comme une zone d'alarme déclenche une alarme en mode MES Totale ou MES Partielle. Le flash de la sirène extérieure est activé après un « Échec MES » si ce flash est sélectionné (case cochée) pour l'option « Échec MES » dans les options système.

Type de sortie	Description
Sirène intérieure	Ce type de sortie est utilisé pour activer la sirène intérieure du système. La sortie est active quand une sirène intérieure du secteur est active. Par défaut, cette sortie est attribuée à la deuxième sortie sur la carte de la centrale (INT+, INT-). **Remarque :** une sortie de sirène intérieure est activée automatiquement chaque fois qu'une zone programmée comme un type de zone d'alarme déclenche une alarme en mode MES Totale ou MES Partielle. La sirène intérieure est activée après un « Échec MES » si la sirène est sélectionnée (case cochée) pour l'option « Échec MES » dans les options système.
Alarme	Cette sortie est activée après qu'une zone d'alarme a été activée dans le système ou dans l'un des secteurs définis.
Alarme Confirmée	Cette sortie est activée en cas de confirmation d'une alarme. Une alarme est confirmée quand 2 zones indépendantes du système (ou faisant partie du même secteur) sont activées pendant un intervalle de temps défini.
Panique*	Cette sortie est activée après qu'une zone d'alarme de panique a été activée dans l'un des secteurs. Une alarme de panique est également déclenchée si un événement « Contrainte utilisateur » est déclenché ou si l'option Panique est activée sur le clavier.
Agression	Cette sortie est activée chaque fois qu'une zone programmée avec le type « Agression » déclenche une alarme dans un secteur.
Feu	Cette sortie est activée après qu'une zone d'incendie a été activée dans le système (ou toute autre zone).
Autosurveillance	Cette sortie est activée quand une condition de sabotage est détectée dans le système. Pour un système de niveau 3, si la communication avec un périphérique XBUS est perdue pendant plus de 100 s, une alarme pour sabotage est générée et les événements signalés par le SIA et le CIR enverront une alerte pour sabotage.
Médical	Cette sortie est activée si une zone médicale est activée.
Défaut	Cette sortie est activée quand une erreur technique est détectée.
Technique	Cette sortie surveille les activités dans une zone technique.
Défaut secteur*	Cette sortie est activée quand l'alimentation secteur tombe en panne.
Défaut batterie*	Cette sortie est activée en cas de défaut de la batterie de secours (secondaire). Elle est aussi activée dès que la tension passe sous le seuil des 11 V. L'option « Restaurer » pour ce genre de défaut est accessible uniquement si la tension remonte à au moins 11,8 V.
MES Partielle A	Cette sortie est activée si le système ou un secteur est en mode de surveillance partielle A.
MES Partielle B	Cette sortie est activée si le système ou un secteur est en mode de surveillance partielle B.
MES totale	Cette sortie est activée quand le système est en mode de surveillance totale.
Échec MES	Cette sortie est activée si le système ou un secteur n'a pas pu être mis en surveillance. Elle est libérée après la remise à zéro de l'alerte.
Entrée/sortie	Cette sortie est activée quand une zone de type Entrée/Sortie est activée, c'est-à-dire dès qu'un temporisateur d'entrée ou de sortie du système ou d'un secteur est exécuté.

Type de sortie	Description
Mémoire	La sortie est activée selon la configuration des sorties du système de gâches (voir *Configuration des sorties du système de gâches et de la MES automatique* page 234). Cette sortie peut être utilisée pour la remise à zéro des détecteurs verrouillés tels que les détecteurs de fumée ou d'inertie.
Issues de secours	Cette sortie est activée quand une issue de secours est activée.
Carillon	Cette sortie est activée brièvement quand une zone ayant l'attribut Carillon est ouverte.
Fumée	Cette sortie est activée brièvement (3 secondes) quand un utilisateur met le système hors surveillance. Elle peut être utilisée pour réinitialiser les détecteurs de fumée. La sortie sera également activée lorsque le secteur est restauré. Lorsque vous utilisez le secteur pour réinitialiser les détecteurs de fumées verrouillés, la première saisie du code ne désactivera pas la sortie de la fumée, mais rendra silencieuses les sirènes. Avec la saisie suivante du code, si le secteur de feu est encore en mode ouvert, la sortie destinée au feu sera activée momentanément. Ce processus peut être répété jusqu'à la fermeture du secteur de feu.
Test déplacement*	Cette sortie est activée brièvement quand un test de déplacement est effectué et qu'une zone est activée. Cette sortie peut être utilisée, par exemple, pour activer les tests fonctionnels des détecteurs branchés (si cette fonction est disponible).
Mise en service automatique	Cette sortie est activée quand la fonction de mise en service automatique est active.
Code contrainte	Cette sortie est activée si un état « Contrainte utilisateur » est déclenché (l'utilisateur tape le code + 1 sur le clavier).
Masquage détecteur	Cette sortie est activée en cas de présence d'une zone infrarouge masquée dans le système. Elle génère une sortie de panne sur la LED du clavier. Cette sortie est verrouillée de façon à rester active jusqu'à ce qu'elle soit rétablie par un utilisateur de niveau 2. Le masquage détecteur est enregistré par défaut dans le journal. Le nombre d'entrées de journal ne dépasse pas 8 entre les périodes d'armement.
Zone omise	Cette sortie est activée en cas de présence d'une zone désactivée, isolée, ou de déplacement dans le système.
Echec de communication	Cette sortie est activée en cas d'échec de la communication avec le centre de télésurveillance.
Test Homme Mort (PTI)	Cette sortie active un tag de détresse activé lors d'un test de cette fonction.
Mise hors surveillance	Cette sortie est activée quand le système est en mode MHS.
Annulation d'alarme	Cette sortie est activée en cas d'annulation d'alarme, par exemple par saisie d'un code valide par le clavier à la suite d'une alarme confirmée ou non. Elle est utilisée, par exemple, avec un composeur externe de numéros (SIA, CID, FF).

Type de sortie	Description
TEST SISMIQUE	Cette sortie sert à activer un test manuel ou automatique en zone sismique. Les détecteurs sismiques sont munis d'un petit capteur vibrant qui est fixé sur la même paroi que le détecteur et relié par câble à la centrale ou à l'un des transpondeurs. Au cours du test, la centrale attend 30 secondes l'ouverture de la zone sismique. Si celle-ci ne s'ouvre pas, le test aboutit à un échec. Si elle s'ouvre dans les 30 secondes, la centrale attend que la zone se referme dans le délai de 10 secondes. Si celle-ci ne se referme pas, le test aboutit à un échec. La centrale attend encore 2 secondes avant de transmettre le résultat du test. Que le test soit manuel ou automatique, le résultat est sauvegardé dans le JDB.
Alarme Locale	Cette sortie est activée en cas d'alarme d'intrusion locale.
Sortie Radio	Sortie activée quand on appuie sur un bouton de la télécommande ou du WPA.
Défaut ligne Modem 1	Cette sortie est activée en cas de défaut de ligne du modem principal.
Modem 1 en Panne	Cette sortie est activée en cas de défaut du modem principal.
Défaut ligne Modem 2	Cette sortie est activée en cas de défaut de ligne du modem secondaire.
Modem 2 en Panne	Cette sortie est activée en cas de défaut du modem secondaire.
Batterie faible	Cette sortie est activée en cas de bas niveau de charge de la batterie.
Comité d'accueil Vert	Cette entrée est activée si une procédure d'entrée « Tout va bien » est lancée et qu'aucune alarme n'est générée, par exemple, si le bouton « Tout va bien » est pressé dans le délai configuré après la saisie du code utilisateur.
Comité d'accueil Rouge	Cette entrée est activée si une procédure d'entrée « Tout va bien » est lancée et qu'une alarme discrète est générée, par exemple, si le bouton « Tout va bien » n'est pas pressé dans le délai configuré pour cela après la saisie du code utilisateur.
MES possible	Cette sortie devient active lorsqu'un secteur est prêt à être activé.
Acquis de MES	Cette sortie indique l'état de la configuration. La sortie commute pendant 3 secondes pour signaler que le paramétrage a échoué. La sortie reste pendant 3 secondes si le paramétrage est couronné de succès.
MES totale faite	Cette sortie est activée pendant 3 secondes pour signaler que le système a été complètement mis en service.
Blockschloss 1	Utilisé pour les appareils Blockschloss normaux. Lorsque toutes les zones du secteur sont fermées et qu'il n'y a aucun défaut en cours, la sortie « Bockschloss 1 » est activée. Si le verrou du Blockschloss est fermé, une entrée « Clé de MES » est activée, le secteur en question est activé et la sortie « Acquis de MES » est activée pendant 3 secondes pour indiquer que le paramétrage a réussi. « Blockschloss 1 » n'est pas désactivé. Si le Blockschloss est déverrouillé, l'appareil Blockschloss désactive l'entrée de la clé de mise en service (fermée) et le secteur est mis hors surveillance. « Blockschloss 1 » est alors désactivé.

Type de sortie	Description
Blockschloss 2	Utilisé pour le type d'appareil Blockschloss - Bosch Blockschloss, Sigmalock Plus, E4.03. Lorsque toutes les zones d'un secteur sont fermées et qu'aucun défaut n'est en cours, la sortie « Blockschloss 2 » est activée. Si le verrou du Blockschloss est fermé, une entrée « Clé de MES » est activée, le secteur en question est activé et la sortie « Acquis de MES » est activée pendant 3 secondes pour indiquer que le paramétrage a réussi. « Blockschloss 2 » est alors désactivé. Si le Blockschloss est déverrouillé, la zone de clé de mise en service est mise en position de désactivation (fermée) et le secteur est mis hors surveillance. « Blockschloss 2 » est activé (si le secteur est prêt à être mis en surveillance).
Elément de verrouillage	S'active si l'élément de verrouillage est en position « verrouillé ».
Élément de déverrouillage	S'active si l'élément de verrouillage est en position « déverrouillé ».
Code autosurveillance	S'active s'il existe un code anti-effraction dans le secteur. Disparaît lorsque l'état est réinitialisé.
Anomalie	S'active si une des zones a un état indiquant un problème.
Lien Ethernet	S'active s'il existe un problème sur le lien Ethernet.
Défaut réseau	S'active s'il existe un défaut de communication EDP.
RAZ Bris de vitre	Utilisé pour commander l'alimentation du détecteur de bris de vitre, ce qui permet de réinitialiser le détecteur en coupant son alimentation. La sortie est réinitialisée si l'utilisateur saisit son code, la zone n'est pas en état fermé et les sirènes sont désactivées.
Agression Confirmée	Active les scénarios suivants pour conformité avec PD6662 : • deux activations de zone d'agression à plus de deux minutes d'intervalle • l'activation d'une zone d'agression et d'une zone de panique à plus de deux minutes d'intervalle • Si l'activation d'une zone d'agression et d'une zone anti-sabotage ou d'une zone de panique et d'une zone anti-sabotage) survient dans le délai de deux minutes
Mode paramétrage	Activer si l'installateur est sur le site et que le système est en mode paramétrage.

Ce type de sortie ne peut indiquer que des événements au niveau du système (aucun événement spécifique à un secteur).

Voir également

Configuration des sorties du système de gâches et de la MES automatique page 234

16.11 Communication

1. Allez sur COMMUNICATION et appuyez sur SELECT.
2. Allez sur l'option de programmation désirée.

16.11.1 Ports série

Les ports série permettent de connecter d'anciens PC au système ou à d'autres périphériques comme les imprimantes.

1. Allez sur PORTS SÉRIE.
2. appuyez sur SELECT.
3. Allez sur le port série à programmer.
4. Sélectionnez l'option de programmation désirée dans le tableau ci-dessous.

TYPE	Détermine si le type est TERMINAL (information système) ou IMPRIMANTE (journal d'événements SPC).
DÉBIT EN BAUDS	Détermine la vitesse de communication entre la centrale et le périphérique. Important : le débit en bauds doit être configuré de manière identique sur les deux composants.
BITS_ DONNEES	Détermine la longueur du paquet de données à transférer entre la centrale et le périphérique. Important : les bits de données doivent être configurés de manière identique sur les deux composants.
BITS DE STOP	Détermine le nombre de bits d'arrêt à la fin du paquet de données. Important : les bits d'arrêt doivent être configurés de manière identique sur les deux composants.
PARITÉ	Détermine la parité (paire/impaire) du paquet de données. Important : la parité doit être configurée de manière identique sur les deux composants.
CONTRÔLE FLUX	Indique si les données sont contrôlées par le matériel (RTS, CTS) ou par le logiciel (Aucun). Important : le contrôle de flux doit être configuré de manière identique sur les deux composants.

5. Appuyez sur RETOUR pour quitter.

16.11.2 Ports Ethernet

Pour programmer le port Ethernet :

1. Allez sur PORT ETHERNET.
2. appuyez sur SELECT.

   L'option ADRESSE IP affiche XXX.XXX.XXX.XXX. Complétez les chiffres inférieurs à 100 par des zéros significatifs à gauche, par exemple 001.
3. Appuyez sur SELECT et saisissez l'adresse IP préférentielle.

   Lorsque la touche ENTRER est pressée, le système bipe deux fois et indique MIS À JOUR si l'adresse IP est valide. Si l'adresse IP est assignée manuellement, elle doit être unique sur le LAN ou le VLAN connecté à la centrale. La valeur n'est pas prise en compte si l'option DCHP est utilisée.
4. Allez sur Masque de sous-réseau.
5. Appuyez sur SELECT. Entrez le masque de sous-réseau sous la forme XXX.XXX.XXX.XXX. Complétez les chiffres inférieurs à 100 par des zéros significatifs à gauche, par exemple 001. Lorsque la touche ENTRER est pressée, le système bipe deux fois et indique MIS À JOUR si le MASQUE DE SOUS-RÉSEAU est valide.
6. Allez sur PASSERELLE. Notez que la passerelle doit être programmée pour pouvoir y accéder de l'extérieur du réseau (utilisation avec le portail).

7. Appuyez sur SELECT. Entrez la PASSERELLE sous la forme XXX.XXX.XXX.XXX. Complétez les chiffres inférieurs à 100 par des zéros significatifs à gauche, par exemple 001. Lorsque la touche ENTRER est pressée, le système bipe deux fois et indique MIS À JOUR si la PASSERELLE est valide.
8. Allez sur DHCP. Le DHCP est activé si le LAN dispose d'un serveur DHCP pour assigner l'adresse IP. L'adresse IP doit être activée manuellement. Notez que la passerelle doit être programmée si l'on doit pouvoir accéder à la centrale de l'extérieur du réseau (service avec le portail).
9. Appuyez sur SELECT. Entrez la PASSERELLE sous la forme XXX.XXX.XXX.XXX. Complétez les chiffres inférieurs à 100 par des zéros significatifs à gauche, par exemple 001.

   Lorsque la touche ENTRER est pressée, le système bipe deux fois et indique MIS À JOUR si la PASSERELLE est valide.

   L'option DHCP s'affiche.
10. Choisissez votre option entre DHCP ACTIVÉ et DHCP DÉSACTIVÉ.
11. appuyez sur SELECT.

16.11.3 Modems

Le système SPC prend en charge les intelli-modems SPC pour la communication avec les lignes analogiques et l'interfaçage du réseau mobile pour des communications et une connectivité performantes. Le système SPC doit être configuré en conséquence.

16.11.3.1 Supervision de l'interface réseau de transmission

La centrale SPC envoie un polling au récepteur SPC Com XT qui répond avec un acquittement (ACK). Après réception de l'acquittement du polling (ACK), la centrale SPC passe le statut du chemin en OK et relance son intervalle de polling (en fonction de la catégorie de l'ATP).
Si la centrale SPC ne reçoit pas l'acquittement de polling (ACK) dans le délai imparti (en fonction de la catégorie d'ATP), la centrale passe le statut du chemin en TOMBÉ.

SPC supporte les interfaces de transmission suivantes:

- Ethernet
- GSM avec GPRS validé
- Modem RTC.

REMARQUE : avant de modifier le code ou d'installer une nouvelle carte SIM, assurez-vous que toutes les sources de courant sont débranchées (alimentation secteur et batterie), sinon la nouvelle carte ne sera pas activée.

REMARQUE : lorsqu'elle est en configuration usine, la centrale détecte, pendant la phase de réglage initial du système avec le clavier, si elle est équipée d'un modem primaire ou de secours, affiche dans ce cas le type de modem et l'active (ou les active) automatiquement avec la configuration par défaut. Aucune autre configuration de modem n'est autorisée à ce stade.

16.11.3.2 Configuration des modems

Pour configurer un modèle GSM ou RTC :

1. Allez sur MODEMS et appuyez sur SELECT.
2. Alternez entre PRIMAIRE et SECOURS pour trouver l'emplacement correct du modem, puis appuyez sur SELECT.

   L'option VALIDER MODEM s'affiche.
3. VALIDER ou DÉVALIDER le modem selon les besoins.

4. Sélectionnez ETAT MODEM, TYPE, VERSION FIRMWARE et NIVEAU RECEPTION puis appuyez sur SELECT pour afficher les données du modem.
5. Configurez les paramètres suivants du modem depuis le menu comme suit et appuyez sur ENTRÉE après chaque sélection :

Option de menu	Description
CODE PAYS	Sélectionnez un pays dans la liste.
CODE PIN GSM	(Modem GSM seulement) Entrez un CODE PIN GSM pour la carte SIM.
MODE RÉPONSE	Sélectionnez MODE RÉPONSE pour choisir le mode selon lequel le modem doit traiter les appels reçus : NE RÉPOND JAMAIS ou RÉPOND TOUJOURS.
CODE SMS RÉP. TECHN. ACC.	Sélectionnez VALIDER pour répondre uniquement quand l'accès ingénieur est activé.
RÉGLAGES SMS	Sélectionnez VALIDER SMS pour accepter les SMS pour ce MODEM. **Modem RTC seulement** Sélectionnez Serveur SMS pour saisir un numéro de téléphone correct du fournisseur de service SMS avec couverture sur votre site, si nécessaire. Ce numéro affiche automatiquement le numéro par défaut pour le SMS dans le pays sélectionné. Pour tester manuellement les SMS, sélectionnez TEST SMS puis entrez le n° de SMS. Pour tester automatiquement les SMS avec des intervalles de temps définis, sélectionnez TEST AUTOMATIQUE, sélectionnez un INTERVALLE DE TEST, puis entrez le N° DE SMS.
PRÉFIXE	**Modem RTC seulement** Entrez le préfixe à composer avant le nº de SMS, le cas échéant.
SURVEIL. LIGNE	**Modem RTC seulement** Activez cette fonction pour surveiller la tension de la ligne reliée au modem. **Modem GSM seulement** Activez cette fonction pour surveiller le niveau de signal émis par le GSM branché sur le modem. Sélectionnez un mode de contrôle (TOUJOURS ACTIF, MES TOTALE, DÉSACTIVÉ). L'option MES TOTALE n'est efficace que si MES TOTALE est active dans le système. Entrez le nombre de secondes pour le TEMPORISATEUR de surveillance (0 – 9 999 s). **Remarque :** confirmation de la configuration EN 50131-9 Afin que la confirmation EN50131-9 fonctionne correctement, il faut que la surveillance de ligne soit activée. (Consultez *Options système* page 257.)
Code USSD	**Modem GSM seulement** Rentrez le code Données de services supplémentaires non structurées (**USSD**) de votre opérateur pour activer une vérification de crédit avec SMS gratuits pour les cartes SIM prépayées. Remarque : cette fonction n'est pas disponible partout. Veuillez consulter votre opérateur pour vérification.

Option de menu	Description
VÉRIF. CRÉDIT SIM	Activez cette fonction pour recevoir des informations sur votre suivi de consommation pour les cartes SIM prépayées (si elle est proposée par votre opérateur).

Modem GSM seulement

En mode SMS, si un code incorrect est entré sur la carte SIM trois fois de suite, la carte SIM sera bloquée. Vanderbilt recommande dans ce cas que la carte SIM soit retirée et débloquée à l'aide d'un téléphone mobile. Si la carte SIM est remplacée sur le module GSM ou si une carte SIM est utilisée avec un code, Vanderbilt recommande de programmer le code avant de placer la carte SIM dans son logement. Cela permet de garantir que des codes incorrects ne sont pas envoyés à la carte SIM. Toutes les sources de courant (alimentations secteur et batterie) doivent être débranchées au moment d'installer la carte SIM dans l'emplacement SIM.

16.11.4 Centre de télésurveillance

Cette section recouvre :

16.11.4.1 Ajouter

Pour programmer les paramètres de la station centrale :

1. Allez sur CENTRE DE TÉLÉSURVEILLANCE > AJOUTER.
2. Appuyez sur SELECT.
3. Sélectionnez l'option de programmation désirée dans le tableau ci-dessous.

N° IDENTIFICATION	Cette information doit être disponible sur la station réceptrice et sert à identifier les utilisateurs chaque fois qu'ils effectuent un appel vers le CTS.
NOM DU CTS	Description du Centre de télésurveillance éloigné.
PROTOCOLE	Le protocole de communication à utiliser (SIA, Contact ID, Fast Format).
1ER N° TÉLÉPHONE	Le premier numéro à appeler pour contacter le CTS.
2EME N° TÉLÉPHONE	Le deuxième numéro de téléphone à composer pour joindre le CTS. Il s'agit du deuxième numéro de téléphone composé pour joindre le CTS si le premier numéro n'a pas abouti.
PRIORITE	Le modem (primaire ou secours) à utiliser pour communiquer avec le CTS.

4. À la fin de la programmation, l'option d'effectuer un appel d'essai au centre est affichée sur le clavier.

16.11.4.2 Éditer

Pour éditer les paramètres de la station centrale :

1. Allez sur CENTRE DE TÉLÉSURVEILLANCE > ÉDITER.
2. appuyez sur SELECT.
3. Sélectionnez l'option de programmation désirée dans le tableau ci-dessous.

N° IDENTIFICATION	Cette information doit être disponible sur la station réceptrice et sert à identifier les utilisateurs chaque fois qu'ils effectuent un appel vers le CTS.
NOM DU CTS	Description du Centre de télésurveillance éloigné.
PROTOCOLE	Le protocole de communication à utiliser (SIA, Contact ID, Fast Format).
1ER N° TÉLÉPHONE	Le premier numéro à appeler pour contacter le CTS.
2EME N° TÉLÉPHONE	Le deuxième numéro de téléphone à composer pour joindre le CTS. Il s'agit du deuxième numéro de téléphone composé pour joindre le CTS si le premier numéro n'a pas abouti.
NBRE DE TENTATIVES	Saisissez le nombre de fois où le système tentera de faire un appel vers le récepteur.
INTERVALLE NUM.	Saisissez le nombre de secondes d'attente après un échec de numérotation. (0-999)
Affecter secteur	Affectez les secteurs pour lesquels des événements sont rapportés au CTS.
INFOS TRANSMISES	Définit les types d'événements signalés au CTS.
PRIORITE	Le modem (primaire ou secours) à utiliser pour communiquer avec le CTS.
TEST CYCLIQUE	Définit une planification pour le test de la connexion vers le CTS. La plage peut aller de toutes les heures à tous les 30 jours.

4. À la fin de la programmation, l'option d'effectuer un appel d'essai au centre est affichée sur le clavier.

16.11.4.3 Effacer

Vous permet de supprimer un CTS configuré.

16.11.4.4 Faire appel test

Vous permet de tester la connexion avec le CTS.

Pour passer un appel test, suivez la procédure ci-après :

1. Sélectionnez FAIRE APPEL TEST.
2. Sélectionnez le nom du CTS.
3. Cliquez sur Sélectionner.
4. Sélectionnez le modem à utiliser pour l'appel test.

   L'appel test est effectué.

16.11.5 SPC Connect PRO

SPC Connect PRO est une application de bureau destinée à l'installation et la maintenance des systèmes SPC. Grâce à SPC Connect PRO, vous pouvez créer et configurer des installations avant d'arriver sur un site. Cet outil peut également être utilisé en association avec le service de cloud SPC Connect pour se connecter à distance aux sites des clients et leur apporter une assistance technique.

Pour activer et configurer le support SPC Connect PRO :

1. Allez sur SPC Connect PRO, puis appuyez sur SELECT.
2. Activez l'option SPC CONNECT PRO.
3. Allez sur INTERFACES et appuyez sur SELECT.
4. Activez/désactivez les interfaces ETHERNET, USB, SERIAL (X10) et MODEM selon le besoin.
5. Pour activer l'interface TCP, sélectionnez TCP PORT puis saisissez le numéro du port et appuyez sur SELECT.

16.12 Test

1. Allez sur TEST et appuyez sur SELECT.
2. Allez sur l'option de programmation désirée.

16.12.1 Test sirène

Pour effectuer un test sirène :

1. Allez sur TEST > TEST SIRÈNE.
2. Appuyez sur SELECT.

   Lorsque TEST SIRÈNE est sélectionné, les options suivantes sont disponibles : SIRÈNES EXTÉRIEURES, FLASH, SIRÈNES INTÉRIEURES et BUZZER. L'appareil déclenche chaque système pour en vérifier le bon fonctionnement lorsqu'il est sélectionné.

16.12.2 Test de déplacement

Un test de déplacement permet de vérifier que tous les détecteurs du système SPC sont opérationnels.

Pour effectuer un test de déplacement :

1. Allez sur TEST > TEST DE DÉPLACEMENT.
2. appuyez sur SELECT.
3. L'affichage indique le nombre de zones à tester sur le système avec le texte À TESTER XX (où XX correspond au nombre de zones valides pour le test de déplacement). Placez le détecteur sur la première zone et activez-le (ouvrez la porte ou la fenêtre).

   Le buzzer du clavier retentit en continu pendant environ deux secondes pour indiquer que l'activation de zone a été détectée ; le nombre de zones qui restent à tester (affiché sur le clavier) baisse alors.
4. Poursuivez avec les autres zones du système jusqu'à ce qu'elles aient toutes été testées. Si l'activation d'une zone n'est pas enregistrée par le système, vérifiez le câblage du détecteur et/ou remplacez-le si nécessaire par un nouveau détecteur.

REMARQUE : toutes les zones peuvent être inclues dans un test de déplacement Installateur.

16.12.3 Test zone

L'option Test zone affiche les informations d'état sur chacune des zones du système.

Pour afficher les informations d'état d'une zone :

1. Allez sur TEST > TEST ZONE.
2. appuyez sur SELECT.

3. Allez sur la zone choisie et appuyez sur SELECT.

   L'état de la zone et sa valeur de résistance associée s'affichent.

4. Appuyez sur SUIVANT pour localiser la zone (par exemple, CONTRÔLEUR 1 = première zone du contrôleur).

   Consultez le tableau ci-dessous pour mettre en corrélation les informations d'état (valable pour les doubles résistances fin de ligne).

État des zones	Abréviation
INCONNU	Royaume-Uni
FERMÉ	FE
OUVERT	OU
COURT-CIRCUIT	CC
DÉCONNECTÉ	DI
NBRE IMPULSIONS	PU
COUP BRUTAL	GR
MASQUÉ	AM
DÉFAUT	DF
Subst. DC	DC
HORS LIMITES	HL
ZONE INSTABLE EN MES	ZONE INSTABLE EN MHS

Il est possible de vérifier le bon fonctionnement de toutes les zones d'un système en effectuant un test de zone.

Pour effectuer un test de zone :

1. Allez sur TEST ZONE.
2. appuyez sur SELECT.
3. Allez sur la zone choisie et appuyez sur SELECT, ou saisissez directement le numéro de la zone.

   Si la zone est située à côté du clavier, l'état de la zone peut être visualisé en cours de modification. L'état et la valeur de résistance de la zone s'affichent en haut à droite.

4. Modifiez l'état du détecteur ; par exemple, pour un détecteur de contact de porte, ouvrez la porte.

   Le buzzer du clavier retentit et l'état du détecteur passe de FE (Fermé) à OU (Ouvert). La valeur de résistance correspondante est modifiée et prend une valeur qui dépend de la configuration des résistances fin de ligne.

Nous vous conseillons de vérifier le bon fonctionnement de toutes les zones du système après achèvement de l'installation. Pour localiser la zone, sélectionnez SUIVANT (en bas à droite) sur le clavier. Les valeurs d'état de zone CC et DI signifient respectivement que la zone est en court-circuit ou déconnectée.

16.12.4 Test sortie

Pour tester les sorties :

1. Allez sur TEST SORTIE.
2. appuyez sur SELECT.

3. Sélectionnez l'une des options CONTRÔLEUR ou TRANSPONDEUR.
4. Pour tester les sorties du contrôleur, sélectionnez la sortie voulue puis appuyez sur SELECT. Pour tester les sorties du transpondeur, sélectionnez le transpondeur et ensuite la sortie.

   L'état actuel de la sortie est affiché dans la première ligne du clavier.
5. Activez ou désactivez la sortie en sélectionnant SORTIE / PAS DE SORTIE.
6. Vérifiez que le périphérique connecté à la sortie sélectionnée change d'état conformément à la sélection.

16.12.5 Test JDB

Le test JDB est un moyen de tester des zones choisies. Les zones soumises au test JDB ne déclenchent pas d'alarme mais les événements sont consignés dans le journal des événements. Le test JDB continue dans les zones concernées jusqu'à ce que le temporisateur de test JDB configuré dans les valeurs par défaut des temporisateurs (14 jours) expire.

Pour effectuer un test JDB :

1. Allez sur TEST JDB et appuyez sur SELECT.
2. Sélectionnez ACTIVER TEST ou ANNULER TEST selon l'option voulue.
3. Sélectionnez la zone voulue et appuyez sur SELECT.

   Un message confirme que le test JDB est en cours dans la zone.

REMARQUE : tous les types de zones peuvent être inclus dans un test JDB.

16.12.6 Options sonores

Les options sonores sont utilisées en tant qu'indications au cours d'un test de déplacement.

Pour paramétrer les options sonores :

1. Aller sur OPTIONS SONORES.
2. Appuyez sur SELECT.
3. Allez sur l'une des options suivantes : TOUTES, SIRÈNE INTÉRIEURE, SIRÈNE EXTÉRIEURE, CLAVIER.
4. Appuyez sur ENREGISTRER.
5. Appuyez sur RETOUR pour quitter.

16.12.7 Indications visuelles

Ce test est utilisé pour tester tous les pixels du clavier LCD et tous les pixels et voyants LED du clavier confort, du module de voyants et du boîtier à clé.

Pour tester un clavier :

1. Passez à IND. VISUELS.
2. appuyez sur SELECT.
3. Appuyez sur Activer.

Sur le clavier LCD sont affichées deux rangées de caractères modifiés en permanence.

Sur le clavier confort, tous les voyants LED sont allumés et tous les pixels de l'écran sont affichés.

1. Appuyez sur RETOUR pour désactiver le test.
2. Appuyez sur RETOUR pour quitter.

16.12.8 Test WPA

REMARQUE : ce test doit être effectué exclusivement par un installateur ou un utilisateur en possession du droit de test du WPA. Voir *Droits d'utilisateur* page 215.

Pour tester le WPA depuis le clavier :

1. Allez sur TEST WPA et appuyez sur SELECT.
2. Quand un message demande ACTIVER WPA, appuyez simultanément sur les trois boutons du WPA.

   Si le test aboutit, un message OK *n* WPA est affiché, où *n* est le nombre de WPA testés.
3. Répétez le test si nécessaire.
4. Appuyez sur RETOUR ou X pour terminer le test.

16.12.9 TEST SISMIQUE

Pour effectuer un test sismique :

1. Allez sur TEST > TEST SISMIQUE.
2. appuyez sur SELECT.
3. Sélectionnez TESTER TOUS LES SECTEURS, ou sélectionnez un secteur particulier à tester.
4. Si vous sélectionnez un secteur particulier à tester, vous pouvez sélectionner TESTER TOUTES LES ZONES ou sélectionner une zone sismique spécifique à tester.

   Le message « TEST SISMIQUE » s'affiche sur le clavier en cours de test.

   Si le test échoue, le message « ÉCHEC DU TEST SISMIQUE » s'affiche. Si la touche « i » ou VOIR est pressée, vous verrez s'afficher une liste de toutes les zones en défaut que vous pourrez balayer.

   Si le test réussit, le message « TEST SISMIQUE OK » s'affiche.

Voir également

Test des détecteurs sismiques page 370.

16.13 Utilitaires

1. Allez sur UTILITAIRES et appuyez sur SELECT.
2. Allez sur l'option de programmation désirée :

LOGICIEL SYSTÈME	Pour afficher la version actuelle du logiciel.
PAR DÉFAUT	Pour réinitialiser les utilisateurs ou reconfigurer le système avec les paramètres d'usine.
BACKUP CONFIG.	Pour sauvegarder une configuration.
RESTAURER CONFIG.	Pour restaurer une configuration.
REDÉMARRAGE SYSTÈME	Pour redémarrer le système.
LICENCE	Entrez un numéro de licence pour changer la licence du SPC. Le système n'enregistre pas et ne signale pas les changements de licence.

16.14 Isoler

Les zones, les alertes système et les alertes liées aux périphériques X-BUS peuvent être isolées manuellement à l'aide du clavier. L'isolation d'une zone retire cette zone du système jusqu'à ce que l'utilisateur annule l'isolation.

Pour isoler des zones, des alertes système ou des alertes liées aux périphériques X-BUS :

1. Allez sur ISOLER et appuyez sur SELECT.
2. Allez sur l'option désirée dans le tableau ci-dessous et appuyez sur SELECT.

ZONE	Sélectionnez la zone requise et passez le paramétrage de NON ISOLÉ à ISOLÉ.
SYSTÈME	Isole l'alerte système désirée.
X-BUS	Isole l'alerte désirée provenant des TRANSPONDEURS ou des CLAVIERS : • COMM. X-BUS PERDUE • DÉFAUT FUS. X-BUS (uniquement pour les transpondeurs) • AUTOSURVEILLANCE X-BUS
VOIR ISOLÉES	Pour afficher une liste des zones, alertes système et alertes de périphériques X-BUS isolées.

16.15 Journal des événements

Les événements récents sur le système s'affichent dans l'option JOURNAL DES ÉVÉNEMENTS. Les événements s'affichent en clignotant toutes les secondes.

1. Allez sur JOURNAL DES ÉVÉNEMENTS et appuyez sur SELECT.
2. Pour afficher un événement correspondant à une date particulière, saisissez la date avec les touches numériques.

   Les événements les plus récents s'affichent sur la dernière ligne de l'écran. Tous les événements précédents s'affichent à tour de rôle pendant une seconde.

16.16 Journal des accès

Les accès de zone sur le système s'affichent dans l'option JOURNAL DES ACCÈS.

1. Allez sur JOURNAL DES ACCÈS et appuyez sur SELECT.
2. Sélectionnez une porte du système pour lequel vous souhaitez afficher les événements d'accès.

   Les événements d'accès les plus récents s'affichent avec la date et l'heure.
3. Parcourez les événements d'accès ou saisissez une date et appuyez sur ENTRÉE pour chercher un événement d'accès particulier.

16.17 Journal des alarmes

Alarme JDB affiche une liste des événements d'alarme.

- Sélectionnez **JDB > JDB système > JDB alarme**.

Les types suivants sont affichés dans ce journal :

- Zones

  – Alarme

– Panique

- EVENEMENTS SYSTEME

  – Alarme confirmée

  – Contrainte utilisateur

  – X-BUS Panique

  – Panique utilisateur

  – WPA Panique

16.18 Modifier code installateur

Pour modifier le code installateur :

1. Sélectionnez CHANGER SON CODE puis appuyez sur SELECT.

   Un code généré de manière aléatoire apparaît.

2. Entrez un nouveau code, le cas échéant, en réécrivant (écrasant) le code affiché puis appuyez sur ENTRÉE.

   Le nombre minimal de caractères requis pour un code dépend du niveau de sécurité configuré pour le système ou de la longueur du code choisie dans le navigateur (**Paramètres centrale > Paramètres du système > Options**). Le système n'accepte pas de code plus court que le nombre de chiffres configuré.

3. Confirmez le nouveau code et appuyez sur ENREGISTRER.

4. appuyez sur RETOUR pour retourner à l'écran précédent pour changer le code.

   En cas de dépassement du délai accordé pour changer le code, l'ancien code reste valable.

16.19 Utilisateurs

Seuls les utilisateurs disposant des droits à cet effet dans leur profil peuvent ajouter, modifier ou supprimer des utilisateurs.

16.19.1 Ajouter

Pour ajouter des utilisateurs sur le système :

1. Allez sur UTILISATEURS > AJOUTER.

   Sélectionnez une ID utilisateur dans la liste des ID système disponibles puis appuyez sur SELECT.

2. Appuyez sur ENTRÉE pour accepter le nom d'utilisateur par défaut ou entrez un nom de votre choix puis appuyez sur ENTRÉE.

3. Sélectionnez le type de profil utilisateur souhaité et appuyez sur ENTRÉE.

   Le système génère un code par défaut pour chaque nouvel utilisateur.

4. Appuyez sur ENTRÉE pour accepter le code utilisateur par défaut ou entrez un code de votre choix puis appuyez sur ENTRÉE.

Le clavier confirme la création du nouvel utilisateur.

16.19.2 Éditer

Pour éditer les utilisateurs dans le système :

1. Allez sur UTILISATEURS > ÉDITER.

2. appuyez sur SELECT.

3. Modifiez le paramètre utilisateur désiré (voir tableau ci-dessous).

CHANGER LE NOM	Modifiez le nom actuel de l'utilisateur
PROFIL D'UTILISATEUR	Sélectionnez le profil du nouvel utilisateur.
CONTRAINTE UTILISATEUR	Activez ou désactivez l'option Contrainte pour le nouvel utilisateur.
LIMITÉ ENTRE 2 DATES	Activez cette option pour limiter l'accès au système à une période fixée d'avance. Entrez les dates de début et de fin de la période souhaitée et appuyez sur ENTRÉE.
PACE	Activez ou désactivez la capacité PACE
TELECOMMANDE	Permet d'activer ou de désactiver l'accès par télécommande radio (clavier radio, télécommande)
MOD-TRAVAI-ISOLE	Active le test d'alerte accident.
CONTRÔLE D'ACCÈS	Si aucun badge n'est affecté à l'utilisateur : • AJOUT BADGE • RECONNAÎTRE UN BADGE Si un badge est affecté à l'utilisateur : • ÉDITER BADGE – NUMÉRO BADGE – ATTRIBUTS DU BADGE (voir Contrôle d'accès) • RAZ BADGE • EFFACER BADGE
LANGUE	Sélectionnez une langue pour cet utilisateur.

16.19.2.1 Contrôle d'accès

Un badge d'accès peut être affecté à chacun des utilisateurs sur la centrale.

Pour configurer le contrôle d'accès pour un utilisateur :

1. Allez sur UTILISATEURS > ÉDITER.
2. Appuyez sur SELECT.
3. Sélectionnez l'utilisateur qui doit être configuré et appuyez sur SELECT.
4. Allez sur CONTRÔLE D'ACCÈS et appuyez sur SELECT.

Les sections suivantes vous indiquent les étapes de programmation correspondant à l'option de contrôle d'accès de l'utilisateur sélectionné.

Ajouter un badge manuellement

Si le format du badge ou le numéro de badge n'est pas connu, le badge peut être créé manuellement.

Le code du site du badge est configuré pour le profil affecté à cet utilisateur.

1. Allez sur AJOUTER BADGE
2. Appuyez sur SELECT.

   Un badge vide a été ajouté et peut maintenant être modifié.

Reconnaître un badge

REMARQUE : seuls les badges ayant des formats pris en charge peuvent être enregistrés dans le système.

Si le numéro de badge ou le format du badge n'est pas connu, le badge peut être lu et ses informations prises en compte.

1. Allez sur RECONNAÎTRE BADGE.
2. Appuyez sur SELECT.
3. Sélectionnez la porte sur laquelle le badge sera présenté.
4. Appuyez sur SELECT.

   REMARQUE : le nouveau badge peut être présenté sur le lecteur d'entrée ou de sortie de la porte sélectionnée.

5. Présentez le badge sur le lecteur de badge de la porte sélectionnée.

   Les informations du nouveau badge sont prises en compte.

Editer badge

Si un badge est déjà attribué à un utilisateur, il peut être modifié à l'aide du clavier :

1. Allez sur ÉDITER BADGE.
2. Appuyez sur SELECT.
3. Modifiez le paramètre d'utilisateur désiré montré dans le tableau dans *Contrôle d'accès* ci-dessous.
4. Appuyez sur RETOUR pour quitter.

Contrôle d'accès

Attribut	Description
Numéro badge	Saisissez le numéro de badge. Saisissez 0 pour désaffecter ce badge.
Badge inutilisé	Cocher pour désactiver temporairement ce badge
Extension de temps	Prolongation des temporisations de porte quand ce badge est utilisé.
Sans code	Permet d'accéder à une porte possédant un lecteur de code sans utiliser le code.

Attribut	Description
Prioritaire	Les badges prioritaires sont enregistrés localement sur les contrôleurs de porte. Ceci permet d'accéder à une zone même en cas de défaut technique si le contrôleur de porte ne peut communiquer avec la centrale. Le nombre maximal d'utilisateur prioritaire est : • SPC4xxx – tous les utilisateurs • SPC5xxx – 512 • SPC6xxx – 512
Escorte	La fonction Escorte permet à des détenteurs de badge à accès privilégié d'escorter d'autres détenteurs de badge à travers certaines portes. Quand cette fonction est activée sur une porte, le badge avec le privilège « escorte » doit être présenté en premier, puis les autres détenteurs de badge ne possédant pas ce privilège présentent leur badge et peuvent ouvrir cette porte. Le délai entre la présentation du badge d'escorte et celle du badge normal est configuré pour chacune des portes.
Gardien	La fonction Gardien force un détenteur de badge avec privilège de gardien (le gardien) à accompagner dans une pièce (groupe de portes) des personnes n'ayant pas ce privilège. Le gardien doit pénétrer dans une pièce en premier. Les autres personnes sont autorisées à entrer dans la pièce uniquement si le gardien s'y trouve déjà. Le gardien n'est pas autorisé à quitter la pièce tant qu'il reste un porteur de badge non-gardien dans celle-ci. Identifie ce détenteur de badge en tant que gardien. L'utilisateur ayant l'attribut Gardien doit entrer dans une pièce (groupe de portes) avant les autres personnes et la quitter en dernier.

Effacer badge

Si un badge n'est plus utilisé, il peut être effacé à l'aide du clavier :

1. Allez sur SUPPRIMER BADGE.
2. Appuyez sur SELECT.

Réinitialisation badge

Si la fonction Antipassback est activée dans une salle et que l'utilisateur quitte cette salle sans utiliser le lecteur de sortie, il ne sera pas autorisé à revenir dans la salle. Le badge de l'utilisateur peut être réinitialisé pour lui permettre de présenter une fois son badge sans vérification passback.

Pour réinitialiser le badge par le clavier :

1. Allez sur RÉINITIALISER BADGE.
2. Appuyez sur SELECT.

16.19.3 Effacer

Pour supprimer des utilisateurs dans le système :

1. Allez sur UTILISATEURS > SUPPRIMER.
2. appuyez sur SELECT.

   Un message s'affiche demandant confirmation de la suppression.
3. Appuyez sur OUI pour supprimer l'utilisateur.

16.20 Profils utilisateur

Voir également

Ajouter/modifier des profils utilisateur page 214

16.20.1 Ajouter

Pour ajouter des profils d'utilisateurs au système :

Le créateur doit avoir un type de profil d'utilisateur ADMINISTRATEUR.

1. Passer à PROFILS UTILS. > Ajouter.

   L'option NOUVEAU NOM est affichée. Appuyez sur SELECT.
2. Saisissez un nom de profil d'utilisateur personnalisé et appuyez sur ENTRÉE.

   Le clavier confirme la création du nouveau profil d'utilisateur.

16.20.2 Éditer

Pour modifier des profils d'utilisateur dans le système :

1. Passer à PROFILS UTILS. > Modification.
2. appuyez sur SELECT.
3. Modifiez le paramètre de profil d'utilisateur désiré dans le tableau ci-dessous.

CHANGER LE NOM	Éditez le nom du profil si nécessaire.
CHANGER LES SECTEURS	Sélectionnez les secteurs correspondants à ce profile.
CALENDRIER	Sélectionnez un calendrier configuré ou AUCUN.
DROIT	Activez ou désactivez les fonctions du système pour ce profil. Voir *Droits d'utilisateur* page 215.
PORTE	Sélectionnez le type d'accès disponible à ce profil pour les portes configurées. Les options sont AUCUN, AUCUNE LIMITE ou CALENDRIER.
CODE SITE	Saisissez un code de site pour toutes les badges utilisant ce profil.

16.20.3 Effacer

Pour effacer des profils d'utilisateur du système :

1. Passer à PROFILS UTILS. > SUPPRIMER.
2. Naviguez entre les profils d'utilisateur pour atteindre le profil requis.
3. Appuyez sur SELECT.

   On vous demandera de confirmer la suppression.
4. Appuyez sur SELECTIONNER pour supprimer le profil d'utilisateur.

16.21 SMS

Le système SPC prend en charge la communication d'alertes SMS de la centrale vers les téléphones portables de l'installateur et de certains utilisateurs sélectionnés (événements SMS), ce qui permet en outre aux utilisateurs de commander le système SPC à distance (contrôle par SMS). Ces deux fonctions combinées permettent à l'utilisateur de commander la centrale par SMS : il peut réagir sans avoir besoin de se déplacer physiquement.

32 (SPC4xxx), 50 (SPC5xxx) ou 100 (SPC6xxx) ID SMS au maximum peuvent être configurées pour chaque centrale. Un modem compatible SMS et une configuration système et utilisateur correcte sont requis pour activer les communications SMS.

En fonction du mode d'authentification SMS choisi (voir *Options* page 130), l'authentification peut être configurée par différentes combinaisons du code PIN et de l'ID appelant ou du code PIN SMS et de l'ID appelant.

La notification par SMS peut fonctionner avec un modem RTC si l'opérateur réseau prend en charge le service SMS dans son réseau RTC. En revanche, le contrôle par SMS requiert l'installation d'un modem GSM dans la centrale. Un modem GSM prend en charge la notification et le contrôle par SMS.

Contrôle par SMS

La fonction de contrôle par SMS est configurable de manière qu'un utilisateur distant puisse envoyer un message SMS à la centrale pour déclencher l'une des actions suivantes :

- Mise en/hors surveillance
- Activation/désactivation Installateur
- Activation/désactivation accès Constructeur.
- Interactions logiques activées/désactivées.

Événements SMS

La notification par SMS peut être paramétrée pour signaler toute une série d'événements qui se produisent sur le système, comme :

- Déclenchement d'alarme
- Alarmes confirmées
- Défaut et autoprotection
- Mise en et hors surveillance
- Inhibition et isolation
- Tous les autres types d'événements

16.21.1 Ajouter

Pour ajouter un utilisateur

Prérequis

- Un modem est installé et identifié par le système.
- La fonction **Authentification SMS** est activée dans OPTIONS (voir *Options* page 130).

1. Allez sur SMS -> AJOUTER et appuyez sur SELECT.
2. Sélectionner un utilisateur à ajouter pour l'utilisation de SMS.
3. Entrez un numéro de SMS pour cet utilisateur et appuyez sur Entrée.
4. Entrez un numéro de SMS pour cet utilisateur et appuyez sur Entrée.

   Le clavier indique que les détails SMS sont mis à jour.

16.21.2 Éditer

Prérequis

- Un modem est installé et identifié par le système.
- La fonction **Authentification SMS** est activée dans OPTIONS (voir *Options* page 130).

1. Allez sur SMS > ÉDITER et appuyez sur SELECT.
2. Sélectionnez un ID SMS d'ingénieur ou d'utilisateur à éditer.

N° SMS	Entrez le numéro de destination du SMS (avec l'indicatif du pays à trois chiffres). **Remarque :** le numéro SMS Installateur peut être supprimé en fixant la valeur à 0. Les numéros SMS Utilisateur ne peuvent pas être supprimés.
ÉDITER UTILIS.	Sélectionnez un nouvel utilisateur pour cette ID SMS Utilisateur, le cas échéant.
FILTRE D'ÉVÉNEMENT	Sélectionnez les événements centrale devant être envoyés par SMS à l'utilisateur ou à l'installateur. Sélectionnez ACTIVÉ ou DÉSACTIVÉ. Les événements qui sont activés sont signalés par un astérisque (*) placé avant l'événement dans la liste.
DROITS COMMANDES	Sélectionnez les opérations pouvant être effectuées à distance sur la centrale par SMS. Consultez *Commandes SMS* page 220

REMARQUE : les événements HOLD-UP ne sont pas transmis par SMS.

Si la ligne téléphonique est connectée au réseau RTC via un PBX, il est nécessaire d'insérer le chiffre approprié pour l'accès à la ligne avant le numéro du destinataire. Assurez-vous que le service **C**alling **L**ine **I**dentity (CLI) est actif sur la ligne choisie pour effectuer l'appel sur le réseau SMS. Pour les détails, consultez l'administrateur du PABX.

16.21.3 Effacer

1. Allez sur SMS > SUPPRIMER.
2. Passez à l'ID de SMS requis.
3. appuyez sur SELECT.

   Le clavier indique que les informations de SMS sont mises à jour.

16.22 X-10

X-10 est en maintenance à partir de la version 3.4. La fonctionnalité est conservée pour le produit, afin que la compatibilité en arrière soit maintenue.

X-10 est un protocole de communication permettant au système de commander des périphériques tels que des lampes ou des actionneurs, et d'utiliser les événements système pour adresser des sorties sur les périphériques X-10. Le contrôleur SPC possède un port série dédié (port série 1) servant d'interface directe pour les périphériques X-10 standard.

1. Sélectionnez X-10 en utilisant les touches de direction bas/haut et appuyez sur SELECT.
2. Allez sur l'option de programmation désirée :

VALIDER X-10	Permet d'activer ou de désactiver X-10.

PÉRIPHÉRIQUES	Permet d'ajouter, de modifier et d'effacer des périphériques X-10.
ENREGISTREMENT	Permet d'activer ou de désactiver la journalisation des événements X-10.

16.23 Régler date/heure

La date et l'heure peut être saisies manuellement sur le système. Les informations de date et d'heure s'affichent sur le clavier et le navigateur et sont utilisées pour les fonctions nécessitant une horloge.

1. Allez sur RÉGLER DATE/HEURE, puis appuyez sur SELECT.

   La date s'affiche sur la ligne supérieure de l'écran.
2. Pour saisir une nouvelle date, appuyez sur les touches numériques correspondantes. Pour déplacer le curseur vers la gauche ou vers la droite, appuyez respectivement sur les touches Flèche gauche et Flèche droite.
3. Appuyez sur ENTRER pour enregistrer la nouvelle date.

   Si vous saisissez une date invalide, le texte VALEUR INVALIDE s'affiche pendant une seconde et l'utilisateur est invité à saisir une date valide.
4. Pour saisir une nouvelle heure, appuyez sur les touches numériques correspondantes. Pour déplacer le curseur vers la gauche ou vers la droite, appuyez respectivement sur les touches Flèche gauche et Flèche droite.
5. Appuyez sur ENTRER pour enregistrer la nouvelle heure.

   Si vous saisissez une heure invalide, le texte VALEUR INVALIDE s'affiche pendant une seconde et l'utilisateur est invité à saisir une heure valide.

16.24 Texte installat.

Ce menu permet à l'installateur d'entrer des informations sur le système et ses données de contact.

1. Allez sur TEXTE INSTALLAT. et appuyez sur SELECT.
2. Allez sur l'option de programmation désirée :

NOM DU SITE	Utilisé pour identifier le système ; saisissez un nom clair et descriptif.
NUMÉRO DU SITE	Permet d'identifier l'installation quand elle est connectée à un centre de télésurveillance (10 caractères maxi).
NOM INSTALLATEUR	Utilisé pour contacter l'installateur.
TÉL. INSTALLATEUR	Utilisé pour contacter l'installateur.
AFFICH. INSTALLATEUR	Permet d'afficher les données de l'installateur pendant les périodes d'inactivité.

Les données de contact de l'installateur entrées dans ce menu doivent également être inscrites sur la fiche signalétique déroulante du clavier à la fin de l'installation.

16.25 Contrôle de portes

Cette option vous permet de contrôler toutes les portes du système.

1. Allez sur CONTRÔLE DE PORTES et appuyez sur SELECT.
2. Sélectionnez la porte qui doit être contrôlée et appuyez sur SELECT.
3. Sélectionnez l'un des statuts de porte listé ci-dessous en tant que nouveau statut de porte et appuyez sur SELECT.

NORMALE	Cette porte est en mode de fonctionnement normal. Un badge possédant les droits d'accès correspondants est nécessaire pour ouvrir la porte.
TEMPORAIRE	La porte est ouverte pendant un certain temps pour permettre l'accès.
VERROUILLÉE	La porte est verrouillée. La porte reste fermée jusqu'à ce qu'un badge possédant les droits d'accès correspondants soit présenté.
DÉVERROUILLÉE	La porte est déverrouillée.

16.26 SPC Connect

Ajoute un ATS (système de transmission d'alarme) de SPC Connect pour instaurer une liaison entre une centrale et le site Web SPC Connect https://www.spcconnect.com. Cela permet à un utilisateur d'enregistrer et d'accéder à sa centrale à distance par le biais du site Web SPC Connect. Si SPC Connect n'est pas activé au cours de la séquence de l'assistant de démarrage, ce menu permet d'ajouter un ATS de SPC Connect. Si SPC Connect a été activé au cours du démarrage, ce menu affiche l'ID d'enregistrement pour un PC.

AJOUTER	Si CONNEXION SPC était désactivé pendant l'exécution de l'assistant de démarrage, le menu ADD s'affiche. Sélectionnez AJOUTER pour créer un système de transmission SPC Connect. Cela permet à un utilisateur d'enregistrer une centrale et d'y accéder à distance depuis le site Web SPC Connect https://www.spcconnect.com.
ID ENREGISTREMENT	Si SPC CONNECT était activé pendant l'exécution de l'assistant de démarrage, l'écran ID d'enregistrement de la centrale s'affiche. Fournissez ces informations à un utilisateur final pour lui permettre d'enregistrer sa centrale sur le site Web Connexion SPC https://www.spcconnect.com, afin de disposer d'un accès distant.
ID SOCIÉTÉ	Pour utilisation ultérieure.
EFFACER	Pour supprimer un système de transmission d'alarme SPC Connect d'une centrale, sélectionnez SUPPRIMER.

17 Programmation en mode Installateur avec le navigateur

Vous pouvez avoir accès aux options de programmation d'accès Installateur sur la centrale SPC avec n'importe lequel des navigateurs Web standard, à partir d'un PC. Elles sont protégées par un code.

Vous pouvez avoir accès au mode de programmation Installateur en entrant le code d'installateur par défaut (1111). Pour plus d'informations, consultez *Codes PIN installateur* page 121.

Ce serveur Web permet d'accéder à toutes les fonctions de programmation disponibles pour installer et configurer le système SPC.

L'accès aux fonctions de programmation devrait être réservé aux installateurs autorisés du système SPC.

Les fonctions de programmation destinées à l'installateur du SPC sont subdivisées en deux catégories :

Fonctions mode Exploitation

Ces fonctions peuvent être programmées sans désactiver le système d'alarme ; elles sont accessibles directement en accédant au mode Installateur.

Fonctions mode Programmation

Ces fonctions ne peuvent être programmées qu'en désactivant au préalable le système d'alarme ; elles sont accessibles dans le menu Programmation.

REMARQUE : si l'option Sortie mode Paramétrage est activée, l'installateur peut sortir du mode Paramétrage avec des alertes actives, mais il doit accepter toutes les alertes listées sur le clavier ou sur le navigateur avant de basculer du mode Paramétrage au mode Exploitation.

Le serveur Web sur la centrale SPC est accessible via l'interface Ethernet ou USB.

Dans le navigateur Web, les modifications doivent être enregistrées expressément en cliquant sur le bouton **Enregistrer**.
Pour consulter les valeurs de programmation actives sur une page Web, cliquez sur **Rafraîchir**.

17.1 Infos sur le système

Cliquez sur l'icône **?** pour afficher le menu Aide qui vous donne des informations actualisées sur la centrale et les fonctionnalités actuellement autorisées sur le système.

17.2 Interface Ethernet

IP

Connect

Numéro	Description
1	JP9 ~~SPC4xxx~~
2	Port Ethernet
3	Vers le port Ethernet du PC

Si l'interface Ethernet du SPC est connectée à un réseau local (LAN) existant, consultez l'administrateur de ce réseau avant de connecter ce dernier à la centrale. Adresse IP par défaut : 192.168.1.100.

Branchez le câble

- Connectez un câble Ethernet à partir de l'interface Ethernet du PC vers le port Ethernet de la carte du contrôleur
  – OU –
  Si vous vous connectez directement à partir d'un PC, vous pouvez utiliser un câble null modem. Voir *Connexions du câble réseau* page 379.

  Les LED situées à la droite de l'interface Ethernet indiquent le succès de la connexion de données (LED droite éclairée) et du trafic de données Ethernet (LED gauche clignotante).

Déterminez l'adresse IP du contrôleur SPC

1. Passage au mode Paramétrage (voir *Codes PIN installateur* page 121).
2. En vous servant des touches de déplacement vers le haut et vers le bas, allez jusqu'à l'option COMMUNICATION et appuyez sur SELECT.
3. Allez sur PORT ETHERNET et appuyez sur SELECT.
4. Allez sur ADRESSE IP et appuyez sur SELECT.

17.3 Connexion USB à la centrale

Si la centrale est réinitialisée lorsque le câble USB est connecté, le câble doit être débranché puis rebranché.

Le port USB de la centrale est relié au PC à l'aide d'un câble USB A/B. La connexion USB entre la centrale et le PC requiert l'installation de pilotes.

Prérequis

- Un câble USB doit connecter votre PC à la centrale.

1. Reliez la centrale à un port USB du PC en utilisant un câble USB.

   L'assistant **Nouveau matériel détecté** est affiché.
2. Cliquez sur **Next**.

   Windows XP détecte un concentrateur USB générique.
3. Cliquez sur **Finish**.

   Windows XP détecte le système avancé de sécurité – SPC sur le port COM N (N représentant le numéro du port COM affecté au périphérique).
4. Notez le port COM affecté au périphérique. Vous en aurez besoin plus tard.

   L'assistant **Nouveau matériel détecté** est affiché à nouveau.
5. Sélectionnez **Installer le logiciel automatiquement**.
6. Si l'assistant d'installation de pilote de Windows XP vous demande de sélectionner le meilleur choix dans une liste, choisissez l'option suivante :

   Connexion locale USB Vanderbilt Intrunet SPC
7. Cliquez sur **Next**.

   Une boîte de dialogue relative à la certification Windows est affichée. Vanderbilt considère qu'il est possible de continuer. Pour toute question, adressez-vous à l'administrateur réseau ou à un technicien Vanderbilt.
8. Cliquez sur **Continuer**.

   L'installation est terminée.
9. Cliquez sur **Finish**.

   Le pilote est installé.

Configuration de la connexion sur Windows XP

Pour créer une nouvelle connexion sur le PC :

1. Cliquez sur la commande **Démarrer**.
2. Sélectionnez **Connexion > Afficher toutes les connexions > Créer une nouvelle connexion.**
3. Dans l'assistant Nouvelle Connexion, sélectionnez **Configurer une connexion ou un réseau**.
4. Sélectionnez l'option **Connexion directe à un autre ordinateur**.
5. Sélectionnez **Invité** pour identifier le PC.
6. Nommez la connexion dans ce champ.
7. Sélectionnez un port série disponible pour la connexion. Ce port devrait être le port COM utilisé par le périphérique USB.
8. Choisissez si la connexion est disponible pour tous les utilisateurs ou si elle vous est réservée.

9. Cliquez sur **Terminer**.
10. Le PC vous invite à indiquer votre nom d'utilisateur et votre mot de passe pour la connexion USB. Entrez les données suivantes :

    – Nom d'utilisateur : SPC

    – Mot de passe : password (par défaut)
11. Cliquez sur **Se connecter.**

    Le PC génère une liaison de données avec le contrôleur. Lorsque la liaison a été établie, une icône de connexion apparaît sur la barre de tâches en bas de l'écran du PC.
12. Faire un clic droit sur le lien et sélectionnez **État**.

    Une adresse IP de serveur s'affiche dans la fenêtre des détails.
13. Entrez cette adresse dans la barre d'adresse du navigateur Web en utilisant le protocole sécurisé HTTP (Hyper Text Transfer Protocol), par exemple : https://192.168.5.1.
14. Connectez-vous à l'explorateur SPC en entrant votre code utilisateur.

Votre code utilisateur par défaut doit être changé dès la première utilisation. N'oubliez pas de le noter. Si vous oubliez votre code utilisateur, il faut exécuter un RAZ usine, ce qui entraîne une mise à zéro de la configuration du système. Les paramètres programmés peuvent être rétablis si une sauvegarde est disponible.

Windows 7

Prérequis

- Vous devez avoir les droits locaux d'administrateur pour exécuter les actions dans cette tâche.

1. Ouvrez le panneau de contrôle de Windows 7.
2. Sélectionnez **Téléphone et modem**.

   La page **Téléphone et modem** s'affiche.
3. Sélectionnez l'onglet **Modems** et cliquez sur **Ajouter**.

   La page **Assistant Ajout de matériel – Installer un nouveau modem** s'affiche.
4. Cliquez deux fois sur **Suivant**.

   L'assistant **Ajouter un nouveau matériel** affiche une liste de modems.
5. Sélectionnez **Communications cable between two computers**.
6. Cliquez sur **Next**.
7. Cliquez sur **Suivant**, puis sur **Terminer**.
8. Retournez à l'onglet **Modems** de la page **Téléphone et modem**.
9. Sélectionnez le nouveau modem et cliquez sur **Propriétés**.

   La page **Propriétés de Communications cable between two computers** s'affiche.
10. Dans l'onglet **Général**, cliquez sur **Modifier les paramètres** pour permettre la modification des propriétés.
11. Sélectionnez l'onglet **Modem**.
12. Modifiez la valeur dans **Vitesse maximale du port** à **115200** et cliquez sur **OK**.
13. Dans le **Panneau de contrôle** , ouvrez **Centre Réseau et partage**.
14. Cliquez sur **Modifier les paramètres de l'adaptateur**. Si un nouveau modem est présent dans la liste des connexions disponibles, passez à l'étape 22. Si le modem n'est *pas* présent, exécutez les actions suivantes :
15. dans le **Centre Réseau et partage**, cliquez sur **Configurer une connexion ou un réseau**.

16. Sélectionnez **Configurer une connexion par modem à accès à distance** puis cliquez sur **Suivant**.
17. Saisissez des valeurs dans les champs **Numéro de téléphone**, **Nom d'utilisateur** et **Mot de passe** et saisissez un nom dans le champ **Nom de la connexion**.
18. Cliquez sur **Se connecter.**

    Windows 7 crée la connexion.
19. Passez outre l'étape **Test de la connexion Internet**.
20. Cliquez sur **Fermer.**
21. Dans le **Centre Réseau et partage**, cliquez sur **Modifier les paramètres de l'adaptateur**.
22. Double-cliquez sur le nouveau modem.

    La page **Connecter*nomdeconnexion*** s'ouvre ; le *nomdeconnexion* est le nom que vous avez défini pour le modem.
23. Cliquez sur **Propriétés**.
24. Assurez-vous que le champ **Se connecter avec :** contient les informations correctes, Communications cable between two computers (COM3), par exemple.
25. Ouvrez votre explorateur et saisissez l'adresse IP du contrôleur en vous servant de https comme protocole de connexion.
26. Cliquez sur **Continuer** si le navigateur affiche une page d'erreur de certificat.
27. Connectez-vous à la centrale.

17.4 Ouverture de session dans le navigateur

Pour ouvrir une session dans le navigateur :

1. Après avoir établi une liaison Ethernet ou USB et trouvé l'adresse IP de la centrale, ouvrez le navigateur Web.
2. Entrez l'adresse IP dans la barre d'adresse du navigateur en utilisant le protocole sécurisé HTTP de transfert de texte. (Par exemple, https:// 192.168.1.100.) Voir le tableau dans *Adresses par défaut du serveur Web* à la page suivante.

   Une page contenant un message de sécurité s'affiche.
3. Cliquez sur **Continuer vers se site Web**.

   La page de connexion apparaît.

4. Entrez les données suivantes :
   – **ID utilisateur** : nom de l'utilisateur ou de l'installateur
   – **Mot de passe** : code de l'utilisateur ou de l'installateur.
5. Sélectionnez la langue d'affichage des pages du navigateur. Le paramètre de langue par défaut « Auto » chargera automatiquement la langue affectée à cette ID d'utilisateur.
6. Cliquez sur **Connexion.**

Adresses par défaut du serveur Web

Connexion	Adresse IP du serveur Web
Ethernet	192.168.1.100 (par défaut)
RS232	192.168.2.1 (fixé)
Modem de secours/RS232	192.168.3.1 (fixé)
Modem principal	192.168.4.1 (fixé)
USB	192.168.5.1 (fixé)

17.5 SPC Accueil

La page SPC Accueil présente les onglets **Résumé système**, **Alarmes** et **Vidéo**.

17.5.1 Vue d'ensemble du système

L'onglet **État du système** est organisé selon les trois sections suivantes :

- **Système :** affiche l'état de tous les secteurs, les alertes système actives ainsi que les avertissements et les informations pour le système.
- **Secteurs :** affiche l'état de chaque secteur défini dans le système avec 20 événements d'alarme au maximum. On peut armer ou désarmer un secteur et les états de secteur affichés ici.
- **Inhibition et isolation :** liste toutes les zones isolées et permet de retirer l'isolation ou le contournement (bypass) avant les réglages.

REMARQUE : si des alarmes sont activées sur le système, le message d'information **Voir l'onglet Alarmes** s'affiche.

17.5.2 Vue générale des alarmes

L'onglet **Alarmes** affiche l'information système suivante :

- **État d'alarme définie** – indique si le système était en MES totale ou partielle au moment du déclenchement de l'alarme.
- **État Alarme** – affiche le type d'alarme (alarme, alarme confirmée, etc.)
- **Sirènes actives** – indique si l'alarme a activé les sirènes. Cliquez sur **Sirènes silencieuses** pour annuler.

Pour chaque secteur, les états suivants sont affichés : **État d'armement**, **État alarme**, **Activations d'alarme** et **JDB alarme**. Les **Activations d'alarme** affichent une liste de zones en état d'alarme commandées par l'activation. Cliquez sur le bouton **Restauration** pour vider la liste. L'option **JDB alarme** affiche jusqu'à 20 événements.

17.5.3 Affichage des vidéos

L'onglet **Vidéo** affiche des images de 4 caméras IP maximum.

- Dans les modes Paramétrage, Exploitation et Utilisateur, sélectionnez **SPC Accueil > Vidéo**.

  Toutes les caméras configurées et opérationnelles (quatre maximum) sont affichées sur la page **Caméras vidéo**. Seules deux caméras sont disponibles dans l'exemple suivant.

Les images sont automatiquement rafraîchies en fonction de l'intervalle de temps défini pour la caméra. (Consultez *Configuration de la vidéo* page 301.)

Cliquez sur le bouton **Stop rafraîchissement** pour garder l'image actuelle sur l'écran et stopper le rafraîchissement. Cliquez sur le bouton **Reprise rafraîchissement** pour autoriser la centrale à reprendre le rafraîchissement des images.

Remarque :assurez-vous que la résolution de 320 x 240 est sélectionnée pour les caméras dont les images doivent être affichées sur le navigateur. Si ce n'est pas le cas, l'affichage pourrait ne pas être satisfaisant. La résolution plus élevée de 640 x 480 peut être utilisée avec SPC Com.

Transmission de défaut vidéo

Un rapport de défaut vidéo est affiché au-dessus de l'image de la caméra. Le tableau ci-dessous fournit une liste des messages possibles :

Message	Description
OK	La caméra se comporte normalement.
Délai	La délai de connexion de la caméra est arrivé à expiration.
Socket Invalide	Erreur interne de traitement de connecteur
Image trop petite	L'image reçue est trop petite
Tampon trop petit	L'image reçue est trop grande. Diminuez la résolution dans la configuration de la caméra.
Format incorrect	Format reçu incorrect.
Abandonner	Connexion TCP déconnectée
Interne	La centrale d'alarme dispose d'une mémoire insuffisante pour répondre à la demande.
Requête erronée	Une requête a été envoyée sous une forme erronée à la caméra. Vérifiez vos paramètres de caméra.
Erreur client	La caméra a renvoyé une erreur client. Vérifiez vos paramètres de caméra.
Erreur d'autorisation	Le nom d'utilisateur et/ou le mot de passe sont incorrects

Message	Description
Inconnu	Une erreur inconnue a été renvoyée. Le modèle de caméra peut ne pas être pris en charge.

17.6 État centrale

Cette section recouvre :

17.6.1 Etat **193**
17.6.2 État X-bus **194**
17.6.3 Radio **201**
17.6.4 Zones **203**
17.6.5 sur les portes **205**
17.6.6 FlexC - État **206**
17.6.7 Alertes système **208**

17.6.1 Etat

Cette page fournit l'état et un résumé des informations sur les composants principaux du SPC, notamment le système, l'alimentation, le X-BUS et les communications.

1. Sélectionnez **État > Hardware > État Centrale**.
2. Consultez les sections ci-dessous pour de plus amples informations.

Actions exécutables

Les actions suivantes ne sont possibles que si une connexion a été établie.

Effacer toutes les alertes	Efface toutes les alertes actives sur la centrale. Ces messages d'alerte s'affichent en rouge en face de l'élément concerné.
Rafraîchir	Intègre toutes les modifications dans l'état de la centrale. Vous devez rafraîchir le statut de la page pour afficher l'état en cours de la centrale à un moment particulier.
Paramétrage/Exploitation	Pour basculer entre les modes Paramétrage et Exploitation. En mode Paramétrage, les alarmes sont désactivées pour éviter d'envoyer des événements au centre de télésurveillance.

17.6.2 État X-bus

1. Sélectionnez **État > Hardware > État X-bus**.

   La page ci-dessous où figure l'état des différents périphériques X-BUS s'affiche. Tous les transpondeurs détectés sont listés par défaut.

2. Sélectionnez l'un des onglets suivants :

   – Transpondeurs (pour programmer les transpondeurs, voir *Transpondeurs* page 237).

   – Claviers (pour programmer les claviers, voir *Claviers* page 243).

   – Contrôleurs de porte (pour programmer les contrôleurs de porte, voir *Contrôleurs de porte* page 247).

3. Cliquez sur l'un des paramètres identifiant un clavier/transporteur/porte de centrale (ID, libellé, type, numéro de série) pour afficher un rapport d'état détaillé.

17.6.2.1 Statut du transpondeur

1. Sélectionnez **État > Hardware > État X-bus**.
2. Sélectionnez l'onglet **Transpondeurs**.

   La liste des transpondeurs détectés et des chargeurs associés s'affiche.

ID Transpondeur	Ce numéro identifie le transpondeur.
Description	Texte descriptif du transpondeur. Ce texte est affiché dans le navigateur et sur le clavier.
Type	Le type de transpondeur détecté [E/S, module d'alimentation (PSU), clavier, etc.].
N° série	Le numéro de série du transpondeur.
Version	La version du firmware du transpondeur.
Comms.	L'état du transpondeur (en ligne ou hors ligne).
Etat	L'état du transpondeur (OK, défaut, OU autosurveillance).
Module d'alimentation	Le type de PSU affecté au transpondeur, le cas échéant. Cliquez sur le PSU pour afficher son état.

Actions exécutables

Rafraîchir	Cliquez sur ce bouton pour mettre à jour l'affichage de l'état du X-BUS.

Pour afficher plus d'informations d'état:

- Cliquez sur l'un des paramètres identifiant un transpondeur (ID, libellé, type, numéro de série) pour afficher un rapport d'état détaillé.

Nom	Description
Communication	L'état physique (OK, Défaut) et l'état programmé (OK, Isolé, Inhibé) de la connexion par câble du X-BUS au transpondeur.
Autosurveillance boîtier	L'état physique et l'état programmé de l'autosurveillance boîtier du transpondeur.
Défaut fusible	L'état physique et l'état programmé du fusible du transpondeur.
Défaut 230 V contrôleur	L'état physique et l'état programmé de l'alimentation secteur de la centrale.
Défaut batterie	L'état physique et l'état programmé de la batterie.
Défaut alim.	L'état physique et l'état programmé du chargeur.
OP autosurveillance	L'état physique et l'état programmé des sorties antisabotage sur le module d'alimentation.
Basse tension	Indication de l'état de faible tension de la batterie.

Actions exécutables

Nom	Description
Effacer les alertes	Cliquez sur ce bouton pour remettre à zéro toutes les alertes sur la centrale.
INHIBEE ⓘ	Cliquez sur ce bouton pour bloquer un défaut. La fonction Inhiber désactive le défaut ou la zone considérée pendant un cycle d'activation. Elle n'est pas disponible au niveau de sécurité EN 50131 Grade 3.
Isoler	Cliquez sur ce bouton pour isoler cette zone. Le fait d'isoler une zone la désactive jusqu'à ce que l'isolation soit annulée explicitement. L'isolation d'une zone impose d'être prudent puisque cette zone ne sera pas active quand le système est MIS EN SURVEILLANCE.

Voir également

Statut chargeur ci-dessous

17.6.2.2 Statut chargeur

La page **État du module d'alimentation** affiche des détails sur l'état actuel et sur ses sorties. Elle affiche aussi l'état de toute batterie connectée.

Les types suivants de modules d'alimentation sont pris en charge :

- Coffret chargeur SPCP332/333
- SPCP355.300 Smart PSU

Etat du coffret chargeur SPCP332/333

L'image suivante montre l'état du coffret chargeur :

Nom	Description
Type	Le type du module d'alimentation.
Version	La version du module d'alimentation.
Statut 230V	Affiche l'état de la connexion de l'alimentation secteur. Les valeurs possibles sont Défaut et OK.
Batterie lien	Affiche le type de batterie connecté.
État de la batterie	Affichage de la condition de la connexion de la batterie. Les valeurs possibles sont Défaut et OK.
Tension batterie	Affiche la lecture de la tension de la batterie.
Courant Batterie	Affiche le courant pris de la batterie.
Sorties	Affiche le courant sur les sorties, le courant soutiré par la sortie et l'état du fusible sur la sortie.

État du SPCP355.300 Smart PSU

L'image suivante montre l'état du SPCP355.300 Smart PSU.

Nom	Description
Type	Le type du module d'alimentation.
Version	La version du module d'alimentation.
Statut 230 V	Affiche l'état de la connexion de l'alimentation secteur. Les valeurs possibles sont Défaut et OK.
Température	Affiche la température du module d'alimentation.
Courant de charge	La tension du module d'alimentation
Courant de charge	Le courant soutiré par le bloc d'alimentation.
État de charge	Affiche le niveau de charge de la batterie.
Circuit primaire	Affiche l'état du circuit primaire fournissant l'électricité lorsque le secteur est branché.
Circuit de charge	Affiche l'état du circuit de charge des batteries lorsque le secteur est connecté.
Batterie	Affiche l'état, la tension et le courant de charge disponibles à partir des batteries.
Sorties	Affiche la tension, l'état du fusible et la condition d'autosurveillance des sorties du module d'alimentation.

17.6.2.3 Statut du clavier

1. Sélectionnez **État > Hardware > État X-bus**.
2. Sélectionnez l'onglet **Claviers**.

   La liste des claviers détectés s'affiche.

Nom	Description
ID Transpondeur	Ce numéro identifie de manière unique le clavier.
Description	Description textuelle du clavier (maxi 16 caractères).
Type	Le type de transpondeur détecté (= clavier).
N° série	Le numéro de série du clavier.
Version	La version du firmware du clavier.
Comms.	Le statut du clavier (en ligne ou hors ligne).
Etat	Le statut du clavier (OK, défaut).

Actions exécutables

Rafraîchir	Cliquez sur le bouton **Rafraîchir** pour mettre à jour la liste des claviers détectés et leur statut.

Pour afficher plus d'informations d'état:

- Cliquez sur l'un des paramètres identifiant un clavier (ID, libellé, type, numéro de série) pour afficher un rapport d'état détaillé.

Communication	L'état physique (OK, Anomalie) et l'état programmé (OK, Isolé, Inhibé) de la connexion par câble entre le clavier et le transporteur.
Autosurveillance boîtier	L'état physique et l'état programmé de l'autosurveillance boîtier du transpondeur.
PACE	S'applique uniquement aux claviers possédant un lecteur de tags PACE.
Panique	État de l'alarme de panique sur le clavier.
Feu	État de l'alarme d'incendie sur le clavier.
Médical	État de l'alarme médicale sur le clavier.
Code autosurveillance	État de l'alarme antisabotage du code sur le clavier

Actions exécutables

Effacer les alertes	Cliquez sur ce bouton pour remettre à zéro toutes les alertes sur la centrale.
INHIBEE ⓘ	Cliquez sur ce bouton pour bloquer un défaut. La fonction Inhiber désactive le défaut ou la zone considérée pendant un cycle d'activation. Elle n'est pas disponible au niveau de sécurité EN 50131 Grade 3.
Isoler	Cliquez sur ce bouton pour isoler cette zone. Le fait d'isoler une zone la désactive jusqu'à ce que l'isolation soit annulée explicitement. L'isolation d'une zone impose d'être prudent puisque cette zone ne sera pas active quand le système est MIS EN SURVEILLANCE.

17.6.2.4 Etat du contrôleur de porte

1. Sélectionnez **État > Hardware > État X-bus**.
2. Cliquez sur l'onglet **Contrôleurs Porte**.

   La liste des contrôleurs de porte détectés s'affiche.

ID Transpondeur	Ce numéro unique identifie le contrôleur de porte.
Description	Texte descriptif du contrôleur de porte (16 caractères maximum).
Type	Le type de transpondeur détecté (= contrôleur de porte)
N° série	Le numéro de série du contrôleur de porte.
Version	La version du firmware du contrôleur de porte.
Comms.	L'état du contrôleur de porte (en ligne ou hors ligne).
Etat	L'état du contrôleur de porte (OK, Défaut).
Module d'alimentation	Indique si le contrôleur de porte est équipé d'un module d'alimentation.

Actions exécutables

Rafraîchir	Cliquez sur le bouton **Rafraîchir** pour mettre à jour le statut des alertes du système.

Pour afficher plus d'informations d'état:

- Cliquez sur l'un des paramètres identifiant une porte de centrale (ID, libellé, type, numéro de série) pour afficher un rapport d'état détaillé.

Communication	L'état physique (OK, Anomalie) et l'état programmé (OK, Isolé, Inhibé) de la connexion par câble entre le clavier et le transporteur.
Autosurveillance boîtier	L'état physique et l'état programmé de l'autosurveillance boîtier du transpondeur.
Défaut fusible	L'état physique et l'état programmé du fusible du contrôleur de porte.
Code autosurveillance	État du code de l'utilisateur. Plusieurs tentatives infructueuses ont provoqué une alarme.

Actions exécutables

Effacer les alertes	Cliquez sur ce bouton pour remettre à zéro toutes les alertes sur la centrale.
INHIBEE ⓘ	Cliquez sur ce bouton pour bloquer un défaut. La fonction Inhiber désactive le défaut ou la zone considérée pendant un cycle d'activation. Elle n'est pas disponible au niveau de sécurité EN 50131 Grade 3.
Isoler	Cliquez sur ce bouton pour isoler cette zone. Le fait d'isoler une zone la désactive jusqu'à ce que l'isolation soit annulée explicitement. L'isolation d'une zone impose d'être prudent puisque cette zone ne sera pas active quand le système est MIS EN SURVEILLANCE.

17.6.3 Radio

La détection par capteur à radiofréquences (868 MHz) sur la centrale SPC est réalisée par des modules de réception radio installés en usine dans le clavier ou sur le contrôleur, ou en installant un transpondeur radio.

1. Sélectionnez **Configuration > Hardware > Sans fil > Sans fil**.

ID Détecteur	Type	Reçu	Etats	Récepteur	Signal	Enroller
58732159	Infrarouge	23/07/2014 11:56:31	Au repos	Centrale	Haut (9)	Enroller
60304133	Infrarouge	23/07/2014 11:55:57	Ouverte	Radio 4	Haut (9)	Enroller
58740535	Infrarouge	23/07/2014 11:55:57	Ouverte	Centrale	Haut (9)	Enroller
60304133	Infrarouge	23/07/2014 11:55:57	Ouverte	Centrale	Haut (9)	Enroller
58740535	Infrarouge	23/07/2014 11:55:56	Ouverte	Centrale	Haut (9)	Enroller
60304133	Infrarouge	23/07/2014 11:55:51	Ouverte	Radio 4	Haut (9)	Enroller
26663381	Contact magnétique	23/07/2014 11:55:21	Au repos	Centrale	Haut (9)	Enroller
60306493	Infrarouge	23/07/2014 11:54:58	AUTOSUR.	Radio 4	Haut (9)	Enroller
26424404	Contact magnétique	23/07/2014 11:54:53	Au repos	Radio 4	Haut (9)	Enroller
26220868	Contact magnétique	23/07/2014 11:54:48	Au repos	Radio 4	Haut (9)	Enroller
58906531	Infrarouge	23/07/2014 11:54:37	Au repos	Radio 4	Haut (9)	Enroller

2. Voir le tableau ci-dessous pour de plus amples informations.

Détecteur	Le numéro du détecteur programmé dans le système (1 = premier, 2 = deuxième, etc.).
ID	Le numéro d'identification unique du détecteur.
Type	Le type du détecteur radio détecté (contact magnétique, inertie/choc, etc.).
Zone	La zone sur laquelle le détecteur est enregistré.
Batterie	L'état de la batterie dans le détecteur (si elle est installée).
Supervision	Le statut de la supervision (OK = signal de supervision reçu, Non supervisé = pas de supervision).
Signal	L'intensité du signal reçu par le détecteur (01=basse, 09=haute). **Remarque :**bien qu'il ne soit pas possible d'enregistrer un appareil dont la force de signal est inférieure à 3, les appareils dont le signal passe au-dessous de cette valeur après leur enregistrement ne sont pas affectés.

Actions exécutables

Journal	Cliquez pour visualiser le journal du détecteur radio. *Journal – capteur sans fil X* à la page opposée.
Enroller	Cliquez sur ce bouton pour ouvrir la liste des périphériques radio dé-enregistrés.

1. Sélectionnez **État > Hardware > X-Shunt > WPA**.
2. Affiche l'identité et l'état de chaque WPA enregistré.

17.6.3.1 Journal – capteur sans fil X

Pour consulter un historique rapide des événements d'un détecteur radio :

1. Cliquez sur le bouton **Journal**.
2. Voir le tableau ci-dessous pour de plus amples informations.

Date/Heure	Date et heure de l'événement enregistré.
Récepteur	L'emplacement du récepteur sans fil, c'est-à-dire le module sans fil monté sur le clavier, le contrôleur ou le transpondeur sans fil.
Signal	L'intensité du signal reçu par le détecteur (01=basse, 09=haute).
Etat	L'état physique du détecteur.
Batterie	L'état de la batterie connectée au détecteur (OK, Défaut).

3. Pour créer un fichier de texte contenant les données du journal, cliquez sur **Fichier Texte.**

17.6.4 Zones

Pour la configuration, voir *Édition d'une zone* page 277.

1. Pour voir toutes les zones, sélectionnez **État > Entrées > Toutes les zones**. Pour voir seulement les zones X-BUS, sélectionnez l'onglet **Zones X-BUS**, et pour voir seulement les zones radio, sélectionnez l'onglet **Zones radio**.

2. Voir les tableaux ci-dessous pour de plus amples informations.

Rafraîchissement mode automatique	Cliquez sur ce bouton pour activer un rafraîchissement automatique de la synthèse de la zone. Cela ne peut être fait que pour toutes les zones, et non pour les zones de filtre.
Description de zone	Description textuelle de la zone (maxi 16 caractères).
Zone	Secteurs auxquels cette zone est affectée.
Type de zone	Le type de zone (Alarme, Entrée/Sortie, etc.).
Tolérance R.	Affiche la qualité de la résistance de fin de ligne pour la gamme de résistances indiquée. Les valeurs possibles sont : • Bon — valeur nominale +/- 25 % de la gamme définie. • OK — valeur nominale +/- 50 % de la gamme définie. • Pauvre — valeur nominale +/- 75 % de la gamme définie. • Insatisfaisant — toute autre valeur. • Bruyant — indique un problème de détection du signal. Le câblage peut se trouver très près d'un câble secteur ou de toute autre source d'interférence. Cette colonne n'est visible qu'en mode installateur. Pour plus d'informations sur les valeurs nominales de la résistance et leurs gammes définies, reportez-vous à Câblage des entrées de zone. *Câblage des entrées de zone* page 95
Entrée	L'état d'entrée de cette zone (Inconnue, Ouverte, Fermée, Déconnectée, Court-circuit, Impulsion, Brute, Masquée, Défaut, Hors limites, Zone instable en MES, Substitution DC, Bruyant). Substitution DC est une alerte antisabotage. Substitution DC vérifie périodiquement qu'aucun courant externe n'est appliqué au circuit. Instable : un état instable se produit lorsque la valeur de résistance d'entrée de zone n'est pas stable pendant une période d'échantillonnage définie. Bruyant : un état Bruyant se produit lorsqu'une interférence externe est induite dans le circuit d'entrée pendant une période d'échantillonnage définie. Hors limite : un état hors limite se produit lorsque la valeur de résistance d'entrée de zone ne se trouve pas dans les tolérances admises des valeurs actuelles de fin de ligne.

Etat	L'état programmé de cette zone. Une valeur d'état Normal signifie que la zone est programmée pour fonctionner normalement. Voici la liste complète des valeurs possibles : Isolé, Test, Inhibé, Changement état zone, Alarme, Issue de secours, Défaut avertissement, Défaut agression, Défaut détecteur, Défaut ligne, Panique, Agression, Technique, Médical, Verrouillé, Incendie, Anomalie, Détecteur masqué, Normal, Actionné, Autosurveillance, Post-alarme. Une zone se trouve en état de post-alarme si une alarme confirmée dépasse la durée limite fixée. La zone est alors rétablie et le système signale qu'une alarme s'est produite.

Actions exécutables

Rafraîchir	Met à jour les informations d'état affichées pour la centrale.
Journal	Cliquez sur le bouton **Journal** pour afficher un journal de l'état des entrées pour cette zone.
INHIBER (!)	Cliquez sur ce bouton pour bloquer un défaut ou une zone ouverte. La fonction Inhiber désactive le défaut ou la zone considérée pendant un cycle d'activation. Elle n'est pas disponible au niveau de sécurité EN 50131 Grade 3.
Restaurer	Cliquez sur ce bouton pour remettre à zéro toutes les conditions d'alarme sur la centrale.
Isoler	Zone : le fait d'isoler une zone la désactive jusqu'à ce que l'isolation soit annulée explicitement. L'isolation d'une zone impose d'être prudent puisque cette zone ne sera pas active quand le système est MIS EN SURVEILLANCE.
Test	Mettez une zone en surbrillance et cliquez sur ce bouton pour exécuter un test JDB sur cette zone.
TEST SISMIQUE	Cliquez sur ce bouton pour lancer un test du capteur sismique sélectionné. Pour plus d'informations sur les capteurs sismiques, reportez-vous à *Détecteurs sismiques* page 369.
Masquer entrées au repos	Cliquez sur ce bouton pour masquer toutes les entrées fermées.
Filtrer zones	Sélectionnez un type de zone dans la liste déroulante. Seule la synthèse de ce type de zone s'affiche.

17.6.5 sur les portes

1. Sélectionnez **Etat > Portes**.

2. Voir les tableaux ci-dessous pour de plus amples informations.

Contrôle	Ce numéro identifie de manière unique la porte.
Zone	Le numéro de zone auquel le détecteur de position de la porte est affecté (uniquement si l'entrée du détecteur de position de la porte est également utilisée comme zone d'intrusion).
Zone	Le secteur auquel l'entrée du détecteur de position de la porte et le lecteur de badge sont affectés.

Contact position porte (DPS)	Statut du détecteur de position de la porte.
Bouton libération porte (DRS)	Statut du bouton d'ouverture de la porte.
Etat	Le statut de la porte (OK, Défaut).
Mode Porte	Spécifie le mode de fonctionnement de la porte.

Actions exécutables

Rafraîchir	Met à jour la synthèse de portes.
Journal	Affiche un journal des événements pour la porte sélectionnée.
Verrouiller	Verrouille la porte sélectionnée.
Déverrouiller	Déverrouille la porte sélectionnée.
Normal	Remet la porte dans le contrôle de système normal.
Déverrouillage temporaire	Déverrouille la porte pendant un intervalle temporisé.

17.6.6 FlexC - État

Cette page affiche l'état de chaque système de transmission d'alarme (ATS) configuré sur votre système.

1. Pour voir l'état d'un ATS, allez sur l'écran **État > FlexC**.

2. Le tableau ci-dessous décrit les critères d'état disponibles pour chaque ATS.

ID d'enregistrement de l'ATS	Numéro ID unique sous lequel s'enregistre le système de transmission (ATS) sur le récepteur (RCT).
État ATS	État d'un système ATS, par exemple, en cours d'initialisation.

Temps écoulé depuis la dernière interrogation	Temps écoulé depuis l'envoi du dernier polling sur n'importe quel chemin de l'ATS.
Compteur File d'attente	Nombre d'événements en attente de transmission.
Compteur File d'attente	Nombre d'événements dans la file d'attente de transmission.
File d'attente Événement	Liste des événements actuellement dans la file d'attente. Le tableau répertorie les éléments suivants : • Séquence d'événement Nº • Horodatage Événement • Description Événement • Info Supplémentaire Événement • Heure de début • Durée de la Transmission
Journal des événements	Journal de bord de tous les événements traités par le système de transmission d'alarme (ATS). Le tableau répertorie les mêmes champs que pour les événements en attente ci-dessus ainsi que le champ additionnel suivant : • Séquence d'événement Nº • Horodatage Événement • Description Événement • Info Supplémentaire Événement • Résultat • Chemin transmis • Heure de début • ACK / Echec Horodatage • Durée de la Transmission
JDB réseau	JDB réseau pour un ATS montrant la périodicité fixée pour l'interrogation.
État des chemins de transmission dans l'ATS	Le tableau répertorie chaque chemin de l'ATS. Pour chaque ATP, le tableau montre le n° de séquence ATP, le nom de l'ATP, l'interface de communication, l'état de l'ATP, la dernière transmission réussie, le JDB réseau, le JDB chemin et le bouton d'appel test. **JDB réseau :** cliquez sur ce bouton pour afficher le JDB réseau. **JDB chemin :** affiche une liste des transmissions d'interrogations. Cliquez sur le bouton **Rafraîchir** pour mettre à jour le journal. Cliquez sur le bouton **Le plus récent en dernier** pour modifier l'ordre d'affichage. Par défaut, c'est l'événement le plus récent qui est affiché en haut de la liste. **Test manuel :** cliquez sur ce bouton pour effectuer un appel test. L'événement est ajouté aux événements en file d'attente.

17.6.7 Alertes système

1. Sélectionnez **Etat > Défauts système**.

2. Voir les tableaux ci-dessous pour de plus amples informations.

Système	Description de l'alerte système.
Entrée	L'état actuel de l'alerte qui a été détectée sur la centrale (OK, Défaut).
Etat	Le statut programmé de l'alerte système, c'est-à-dire si l'alerte a été isolée ou inhibée. La valeur de statut OK s'affiche si la condition d'alerte n'a pas été désactivée d'une manière ou d'une autre.

Actions exécutables

Rafraîchir	Cliquez sur ce bouton pour mettre à jour le statut des alertes du système.
Restaurer	Cliquez sur ce bouton pour réinitialiser une alerte sur la centrale.
INHIBEE	Cliquez sur ce bouton pour bloquer un défaut. La fonction Inhiber désactive le défaut ou la zone considérée pendant un cycle d'activation. La fonction Inhiber n'est pas disponible au niveau de sécurité EN 50131 Grade 3.
Isoler	Cliquez sur ce bouton pour isoler la zone. Le fait d'isoler une zone la désactive jusqu'à ce que l'isolation soit annulée explicitement. L'isolation d'une zone impose d'être prudent puisque cette zone ne sera pas active quand le système est MIS EN SURVEILLANCE.

17.7 Journaux de bord

Cette section recouvre :

17.7.1 JDB Système **208**
17.7.2 Journal des accès **209**
17.7.3 Journal WPA **210**
17.7.4 JOURNAL DES ALARMES **210**

17.7.1 JDB Système

Ce JDB affiche tous les événements du système SPC.

1. Sélectionner **JDB > JDB Système > JDB Système**.
2. Pour créer un fichier de texte contenant les données du journal, cliquez sur **Fichier Texte.**

3. La journalisation des changements d'état d'une zone est activée en sélectionnant l'attribut JDB (journal de bord) pour cette zone dans la page de configuration des attributs des zones.

Afin d'éviter que plusieurs événements ayant la même origine gonflent le journal, le système SPC limite la journalisation à 3 activations de la même zone pendant la période d'activation (en conformité avec les normes).

17.7.2 Journal des accès

Le journal de bord contient le suivi des événements du système SPC.

- Sélectionnez **Journal > Journal des accès**.

  La page suivante s'affiche :

JDB Système | JDB Accès | Modem 1 | Modem 2

JDB Accès

Heure	Evénement	Porte	Utilisateur
26/07/2012 16:01:17	Badge inconnu	1- DOOR 1	
26/07/2012 16:01:17	Entrée refusée - BADGE NON ENREGISTRE	1- DOOR 1	
26/07/2012 16:01:36	Badge inconnu	1- DOOR 1	
26/07/2012 16:01:36	Entrée refusée - BADGE NON ENREGISTRE	1- DOOR 1	
26/07/2012 16:02:07	Utilisateur 11 Badge ajouté par Utilisateur 1		1
26/07/2012 16:02:11	Entrée autorisée	1- DOOR 1	11
08/08/2012 12:43:17	Utilisateur 9 Badge ajouté par Utilisateur 1		1
08/08/2012 15:57:42	Badge inconnu	2- DOOR 2	
08/08/2012 15:57:42	Entrée refusée - BADGE NON ENREGISTRE	2- DOOR 2	
08/08/2012 15:57:46	Badge inconnu	1- DOOR 1	
08/08/2012 15:57:46	Entrée refusée - BADGE NON ENREGISTRE	1- DOOR 1	
08/08/2012 16:02:27	Utilisateur 7 Badge ajouté par Utilisateur 1		1
08/08/2012 16:02:55	Badge inconnu	1- DOOR 1	
08/08/2012 16:02:55	Entrée refusée - BADGE NON ENREGISTRE	1- DOOR 1	
08/08/2012 16:03:11	Utilisateur 8 Badge ajouté par Utilisateur 1		1
10/08/2012 12:37:29	Entrée autorisée	2- DOOR 2	11
10/08/2012 12:37:34	Entrée autorisée	2- DOOR 2	11
10/08/2012 12:37:37	Entrée autorisée	1- DOOR 1	11
10/08/2012 12:37:53	Entrée autorisée	1- DOOR 1	8
10/08/2012 12:37:55	Entrée autorisée	2- DOOR 2	8
17/08/2012 12:27:48	Entrée autorisée	2- DOOR 2	3
17/08/2012 12:27:56	Entrée autorisée	2- DOOR 2	3
17/08/2012 12:39:13	Entrée autorisée	2- DOOR 2	3
17/08/2012 12:39:18	Entrée autorisée	2- DOOR 2	3
17/08/2012 12:39:24	Entrée autorisée	2- DOOR 2	8
17/08/2012 12:39:29	Entrée autorisée	2- DOOR 2	11
17/08/2012 12:39:36	Entrée autorisée	2- DOOR 2	2
17/08/2012 12:40:11	Entrée autorisée	2- DOOR 2	11

- Pour créer un fichier de texte contenant les données du journal, cliquez sur le bouton **Fichier texte.**

17.7.3 Journal WPA

Ce JDB affiche tous les événements WPA du système.

- Sélectionner **JDB > JDB Système > JDB WPA**.

  La page suivante s'affiche :

JDB Système | JDB Accès | Modem 1 | Modem 2

JDB Système | JDB Alarme | JDB WPA

JDB WPA

17/06/2014 11:07:27 Alerte: WPA SUPERVISION 1 WPA 1
25/06/2014 09:34:02 Alerte: WPA SUPERVISION 1 WPA 1
07/07/2014 12:15:51 Alerte: WPA SUPERVISION 1 WPA 1
09/07/2014 16:05:23 Alerte: WPA SUPERVISION 1 WPA 1
09/07/2014 16:07:06 Alerte: WPA SUPERVISION 1 WPA 1
23/07/2014 10:18:18 Alerte: WPA SUPERVISION 1 WPA 1

17.7.4 JOURNAL DES ALARMES

Alarme JDB affiche une liste des événements d'alarme.

- Sélectionnez **JDB > JDB système > JDB alarme**.

Les types suivants sont affichés dans ce journal :

- Zones
  – Alarme
  – Panique

- Evénement système
  – Alarme confirmée
  – Contrainte Utilisateur
  – X-BUS Panique
  – Panique utilisateur
  – WPA Panique

17.8 Utilisateurs

Le tableau suivant montre le nombre maximal d'utilisateurs, de profils utilisateurs et de tags utilisateurs pour la centrale :

Nombre maximal	SPC4xxx	SPC5xxx	SPC6xxx
Utilisateurs	100	500	2500
Profils utilisateur	100	100	100
Profils par utilisateur	5	5	5
Modules TAG	32	250	250
ID SMS Utilisateur	32	50	100
Mots de passe Web	32	50	100
Télécommandes radio	32	50	100
Modules MDT	32	32	32

AVERTISSEMENT : si vous mettez à niveau à partir d'une version du micrologiciel précédant la version 3.3, prenez en compte les points suivants :
– Le mot de passe Web Installateur, s'il existe, est effacé et doit être saisi de nouveau après la mise à niveau.
– Tous les utilisateurs existants se voient attribuer un nouveau profil utilisateur correspondant à leur niveau d'accès autorisé. Si le nombre maximal de profils utilisateur est dépassé, aucun profil n'est affecté (voir *Ajouter/modifier des profils utilisateur* page 214). Veuillez vérifier l'ensemble de la configuration utilisateur après une mise à niveau du micrologiciel.
– L'ID Installateur par défaut est modifiée de 513 à 9999.

17.8.1 Ajouter/Éditer un utilisateur

1. Sélectionnez **Utilisateurs > Utilisateurs**.

   La liste des utilisateurs configurés s'affiche.

2. Cliquez sur le bouton **Ajouter utilisateur** ou sur le bouton **Éditer** correspondant à l'utilisateur requis.

   La page suivante apparaît :

3. Saisissez une **ID utilisateur** qui n'est pas déjà utilisée. Si une ID déjà utilisée est saisie, le message « ID non disponible » s'affiche.
4. Entrez un **Nom d'utilisateur** (16 caractères maximum, sensible à la casse).
5. Pour créer automatiquement un **Code PIN** pour un nouvel utilisateur, cliquez sur le bouton **Générer un code PIN**. Le cas échéant, changez le code. Entrez 0 si le code n'est pas demandé.

   Remarque : pour être en accord avec les approbations INCERT, le code PIN de l'utilisateur doit contenir plus de 4 chiffres.
6. Il est également possible de limiter l'accès au système de l'utilisateur en cochant la case **Date limite** et en saisissant les dates délimitant la période voulue.

   Alertes Utilisateur affiche l'état du code de l'utilisateur. Par exemple, cela affiche le nombre de jours restant avant que le code n'arrive à expiration, si les modifications périodiques sont activées dans la politique de code du système.
7. Vous pouvez activer l'option **Accès après alarme** pour accorder à cet utilisateur un accès au système limité à une durée spécifique.

   Les limites de temps pour cette option sont définies dans la page **Tempos système**. Allez sur **Configuration > Système > Tempos système** pour configurer cette option. Voir *Temporisations* page 269.

   En mode normal, aucun utilisateur ayant cet attribut sélectionné ne peut accéder au système.

8. Sélectionnez le profil d'utilisateur approprié (voir *Ajouter/modifier des profils utilisateur* page 214) pour cet utilisateur.
9. Le cas échéant, sélectionnez **Activer contrainte** pour cet utilisateur. Le nombre de codes utilisateur attribué par contrainte (PIN +1 ou PIN+2) est configurable dans Options système (voir *Options* page 257).

L'option **Contrainte** n'est disponible sur cette page que si l'option **Contrainte utilisateur** est activée pour le système dans **Options système**. Si l'option **Contrainte** est active pour cet utilisateur, les codes PIN consécutifs d'autres utilisateurs (par ex., 2906, 2907) ne peuvent pas être utilisés, puisqu'un événement « contrainte utilisateur » est déclenché quand l'utilisateur tape ce code sur le clavier.

Contrôle d'accès

Attribut	Description
Numéro badge	Saisissez le numéro de badge. Saisissez 0 pour désaffecter ce badge.
Badge inutilisé	Cocher pour désactiver temporairement ce badge
Extension de temps	Rallongement des temporisateurs de porte quand ce badge est utilisé. Cas des personnes à mobilité réduite.
Sans code	Permet d'accéder à une porte possédant un lecteur de code sans utiliser le code.
Prioritaire	Les badges prioritaires sont enregistrés localement sur les contrôleurs de porte. Ceci permet d'accéder à une zone même en cas de défaut technique si le contrôleur de porte ne peut communiquer avec la centrale. Le nombre maximal d'utilisateurs prioritaires est : • SPC4xxx – tous les utilisateurs • SPC5xxx – 512 • SPC6xxx – 512
Escorte	La fonction Escorte permet à des détenteurs de badge à accès privilégié d'escorter d'autres détenteurs de badge à travers certaines portes. Quand cette fonction est activée sur une porte, le badge avec le privilège « escorte » doit être présenté en premier, puis les autres détenteurs de badge ne possédant pas ce privilège présentent leur badge et peuvent ouvrir cette porte. Le délai entre la présentation du badge d'escorte et celle du badge normal est configuré pour chacune des portes.
Gardien	La fonction Gardien force un détenteur de badge avec privilège de gardien (le gardien) à accompagner dans une pièce (groupe de portes) des personnes n'ayant pas ce privilège. Le gardien doit pénétrer dans une pièce en premier. Les autres personnes sont autorisées à entrer dans la pièce uniquement si le gardien s'y trouve déjà. Le gardien n'est pas autorisé à quitter la pièce tant qu'il reste un porteur de badge non-gardien dans celle-ci. Identifie ce détenteur de badge en tant que gardien. L'utilisateur ayant l'attribut Gardien doit entrer dans une pièce (groupe de portes) avant les autres personnes et la quitter en dernier.

17.8.1.1 Appareils inconnus

Si un appareil inconnu, comme une télécommande, un Tag ou une carte a été scanné mais pas affecté à un utilisateur, un bouton est affiché dans la section correspondante de la page de l'utilisateur.

- Bouton **TÉLÉCOMMANDE – Télécommande inconnu** ou bien, si le périphérique est affecté à l'utilisateur, bouton **Supprimer télécommande**
- Bouton **Tag – Tag inconnu** ou bien, si le périphérique est affecté à l'utilisateur, bouton **Supprimer tag**
- Bouton **Contrôle d'accès – Badge inconnu**

Pour affecter une télécommande, un tag ou une carte à l'utilisateur :

1. Cliquez sur le bouton **Inconnu** pour le périphérique. La page Utilisateur affiche la liste des périphériques inconnus.
2. Cliquez sur **Ajouter** pour affecter le périphérique à l'utilisateur.

Remarque : pour affecter un badge à l'utilisateur, le profil d'utilisateur associé doit avoir le code site correct.

Pour supprimer l'affectation d'une télécommande ou d'un tag à un utilisateur :

1. Cliquez sur le bouton **Supprimer**.
   L'affectation du périphérique à l'utilisateur est supprimée et le périphérique est également supprimé du système.
2. Pour ajouter à nouveau le périphérique, vous devez le scanner une nouvelle fois.

Pour supprimer l'affectation d'une carte à un utilisateur :

1. Modifiez le numéro de la carte à zéro (0).
2. Cliquez sur **Enregistrer**.
   L'affectation du badge à l'utilisateur est supprimée et le badge est également supprimé du système.
3. Pour ajouter à nouveau la carte, vous devez la scannez une nouvelle fois.

17.8.2 Ajouter/modifier des profils utilisateur

REMARQUE : les profils d'utilisateurs généraux ne sont pas éditables par l'explorateur et doivent être édités sous SPC Manager.

1. Sélectionnez **Utilisateurs > Profils utilis.**

   La liste des profils configurés s'affiche avec le nombre d'utilisateurs attribués à chaque profil.

2. Cliquez sur **Ajouter Profil utilisateur** ou cliquez sur le bouton **Éditer** du profil souhaité.
   La page suivante s'affiche avec les options de configuration suivantes :

   – Paramètres généraux

   – Droits utilisateur/centrale

– Contrôle d'accès

Paramètres généraux

1. Saisissez une **ID utilisateur** qui n'est pas en cours d'utilisation. Si une ID déjà utilisée est saisie, le message « ID non disponible » s'affiche.
2. Entrez un **Nom Profil Utilisateur** (16 caractères maximum, sensible à la casse).
3. Sélectionnez tous les **Secteurs** allant être contrôlés par ce profil utilisateur.
4. Sélectionnez un **Calendrier** pour fixer les limitations horaires de ce profil dans le système.

Droits Utilisateur/Centrale

- Sélectionnez les droits d'utilisateur voulus à affecter à ce profil d'utilisateur.

Droits d'utilisateur

Droite	Type de profil d'utilisateur par défaut	Description
Droits utilis. – Intrusion		
MES totale	Limité Standard Gestionnaire	La fonction MES TOTALE active le système en surveillance totale et offre le niveau de protection maximal à un bâtiment (l'ouverture d'une zone d'alarme active l'alarme). Lorsque vous sélectionnez MES TOTALE, le buzzer retentit et l'afficheur du clavier décompte la temporisation de sortie. Vous devez quitter le bâtiment avant l'expiration de cette période. Lorsque la temporisation de sortie a expiré, le système est activé et l'ouverture des zones d'entrée/sortie lance la temporisation d'entrée. L'alarme est activée si le système n'est pas désactivé avant l'expiration de la temporisation d'entrée.
MES Partielle A	Standard Gestionnaire	Le mode MES PART. A active la protection du périmètre d'un immeuble, mais autorise le libre déplacement dans les zones d'accès. Les zones désignées comme EXCLUS A ne sont pas protégées dans ce mode. Par défaut, il n'y a pas de temporisation de sortie ; le système s'active instantanément lorsque ce mode est sélectionné. Une temporisation de sortie peut être appliquée à ce mode en activant la variable MES Partielle A temporisée.

Droite	Type de profil d'utilisateur par défaut	Description
MES Partielle B	Standard Gestionnaire	La option MES PARTIELLE B applique la protection à toutes les zones exceptées celles classifiées comme EXCLUS B. Par défaut, il n'y a pas de temporisation de sortie ; le système s'active instantanément lorsque ce mode est sélectionné. Une temporisation de sortie peut être appliquée à ce mode en activant la variable MES Partielle B temporisée.
MES Forcée	Standard Manager	L'option MES FORCÉE est présentée sur l'afficheur du clavier quand un utilisateur essaie d'activer le système alors qu'une zone d'alarme est ouverte ou en défaut (la ligne supérieure de l'afficheur indique la zone ouverte). La sélection de cette option active l'alarme et inhibe la zone pour la période choisie.
Mise hors surveillance	Limité Standard Gestionnaire	L'action MHS arrête l'alarme. Cette option est accessible sur le clavier uniquement après l'activation d'une zone Entrée/Sortie et la saisie d'un code d'utilisateur valable.
Retarder l'activation auto	Standard* Gestionnaire	L'utilisateur peut retarder ou annuler l'activation automatique.
Supprime le délai.	Standard Gestionnaire	L'utilisateur peut neutraliser automatiquement le retard à la MHS. Disponible uniquement pour les installations bancaires. Voir *Mise en / hors surveillance* page 284.
Restaurer	Standard Gestionnaire	La fonction RESTAURER remet à zéro une alerte du système et efface le message d'alerte associé à l'alerte. Une alerte ne peut être effacée que si l'état de fonctionnement normal des zones ayant déclenché l'alerte est rétabli, ou si le défaut est éliminé. L'utilisateur doit sélectionner l'option EFFACER ALERTES pour cette zone.
INHIBEE	Standard Gestionnaire	L'inhibition d'une zone désactive cette zone pendant une période d'armement. Ceci est la méthode à utiliser de préférence pour désactiver une zone en défaut ou ouverte lorsque le défaut ou l'ouverture est affichée sur le clavier chaque fois que le système est activé pour rappeler à l'utilisateur qu'il doit s'occuper de cette zone.
Isoler	Standard* Gestionnaire	Le fait d'isoler une zone la désactive jusqu'à ce que l'isolation soit annulée. Tous les types de zones du contrôleur peuvent être isolés. L'utilisation de cette fonction pour désactiver des zones en défaut ou ouvertes doit se faire avec précaution ; lorsqu'une zone est isolée, elle est ignorée par le système et susceptible de ne pas être prise en compte lors de l'activation ultérieure du système, ce qui pourrait compromettre la sécurité des bâtiments.
Droits utilis. – Système		
Accès Web	Standard* Gestionnaire	L'utilisateur peut accéder à la centrale via un navigateur Web.

Droite	Type de profil d'utilisateur par défaut	Description
Voir JDB	Standard Gestionnaire	Cette option du menu affiche l'événement le plus récent sur l'afficheur du clavier. Le journal de bord (voir *Journal des événements* page 175) fournit la date et l'heure de chaque événement enregistré dans le journal.
Utilisateurs	Gestionnaire	Un utilisateur peut créer et modifier d'autres utilisateurs de la centrale, à condition de disposer des droits supérieurs ou équivalents à ceux de l'utilisateur en question.
SMS	Standard* Gestionnaire	Cette fonction permet aux utilisateurs d'activer le service de messagerie par SMS si un modem est installé sur le système.
Réglage date	Standard Gestionnaire	Cette option du menu permet à l'utilisateur de programmer la date et l'heure du système (voir *Régler date/heure* page 183). Assurez-vous que l'heure et la date sont justes ; ces champs sont présentés dans le journal de bord lors du reporting des événements du système.
Changer le code PIN	Standard Gestionnaire	Cette option du menu permet à l'utilisateur de changer son code PIN (voir*Modifier code installateur* page 176). **Remarque :** pour être en accord avec les approbations INCERT, le code PIN de l'utilisateur doit contenir plus de 4 chiffres.
Voir vidéo / Vidéo dans le navigateur	Standard Gestionnaire	L'utilisateur peut voir des images vidéo directement sur le navigateur Web. **Remarque :** les droits d'accès à Internet doivent également être activés pour cette fonction.
Carillon	Standard Gestionnaire	Quand l'attribut CARILLON est actif pour une certaine zone, un court bip sonore est généré sur le buzzer du clavier quand on ouvre cette zone (pendant que le système est hors surveillance). Cette option du menu permet d'activer ou de désactiver le carillon sur toutes les zones.
Installateur	Gestionnaire	Cette option permet aux utilisateurs de donner l'accès à l'installateur pour effectuer une programmation. Avec les exigences CAT 1 et CAT 2 relatives à la Suisse, lorsque l'accès installateur est accordé, toutes les zones doivent être mises hors surveillance ; à défaut, l'installateur se verra refuser l'accès.
Mise à jour	Gestionnaire	L'utilisateur peut autoriser l'accès à la centrale pour permettre une mise à niveau du micrologiciel.
Droits utilis. – Pilotage		
Sorties	Standard Gestionnaire	L'utilisateur peut activer/désactiver les sorties configurées (interactions logiques). Voir *Éditer une sortie* page 228.
X-10	Standard Gestionnaire Contrôle d'accès	L'utilisateur peut activer/désactiver les tags X-10 configurés. **Remarque :** X-10 est en cours de maintenance. La fonction est conservée pour le produit, afin que la compatibilité soit maintenue en aval.

Droite	Type de profil d'utilisateur par défaut	Description
Contrôle de portes	Standard* Gestionnaire Contrôle d'accès	L'utilisateur peut verrouiller/déverrouiller les portes.
Contrôle RF	Standard Gestionnaire Contrôle d'accès	L'utilisateur peut piloter des sorties avec la télécommande radio
Droits utilis. – Tests		
Test sirène :	Standard Gestionnaire	L'utilisateur peut exécuter un test de sirène pour tester les sirènes externes, le flash, les sirènes internes et le buzzer afin de s'assurer de leur bon fonctionnement.
Test de déplacement	Standard Gestionnaire	L'utilisateur peut exécuter un test de déplacement pour vérifier le bon fonctionnement de tous les détecteurs du système.
Test WPA	Standard Gestionnaire	L'utilisateur peut effectuer un test WPA.
TEST SISMIQUE	Standard Gestionnaire	L'utilisateur peut tester le détecteur sismique.
Droits utilis. – Accès instal.		
Prog. Utilis. (Maître)		L'utilisateur possède les droits pour créer et modifier d'autres utilisateurs du système sans restriction.
Prog. Profil Utilis.		L'utilisateur peut créer et modifier des profils d'utilisateur du système.
Prog. Calendriers		L'utilisateur peut configurer des calendriers.
Prog. Portes		L'utilisateur peut modifier des portes.
Accès niveau Ingénieur		Permet à l'utilisateur d'effectuer des tâches de niveau Ingénieur. Cette fonction n'est disponible qu'en mode « Sans restriction » (la norme EN50131 impose que les opérations précédentes ne soient autorisées que par un utilisateur niveau Ingénieur pour un système de grade 3).
* Ces fonctions ne sont pas actives par défaut pour l'utilisateur considéré, mais peuvent être sélectionnées.		

Contrôle d'accès

1. Entrez un **Code site**, le cas échéant, pour tous les badges affectés à ce profil d'utilisateur. Voir *Lecteurs de cartes et de formats de badges pris en charge* page 409.
2. Sélectionnez les droits d'**Accès** pour ce profil d'utilisateur pour les portes configurées du système. Les options sont les suivantes :

   – Pas d'accès

   – Accès 24/24 (accès illimité)

   – Calendrier (si configuré)

Utilisateurs

La liste des utilisateurs affectés à ce profil s'affiche. Cliquez sur un utilisateur pour afficher ou modifier les données correspondantes.

Vous pouvez créer un nouveau profil d'utilisateur en vous basant sur un profil existant en cliquant sur **Retransmet**. Une nouvelle page de **Profil d'utilisateur** s'affiche.

Voir également

Ajouter/modifier des profils utilisateur page 214

Ajouter/Éditer un secteur page 278

17.8.3 Programmation SMS

Le système SPC offre une messagerie à distance (SMS) sur les systèmes ayant des modems installés.

Prérequis

- Un modem est installé et identifié par le système.
- La fonction **Authentification SMS** est activée. (Consultez *Options* page 257.)

1. Sélectionnez **Utilisateurs -> SMS Utilisateurs**.

   L'ID SMS Installateur et une liste d'ID SMS utilisateurs avec les détails SMS correspondants est affichée.

2. Cliquez sur le bouton **Test** pour tester un numéro de SMS.
3. Cliquez sur **Ajouter** pour ajouter une nouvelle ID SMS ou sur le bouton **Modifier** en regard de l'ID SMS correspondante.

4. Pour configurer les SMS, procédez comme suit :

ID SMS Utilisateur	ID générée par le système
N° SMS	Entrez le numéro de destination du SMS (avec l'indicatif du pays à trois chiffres). **Remarque :** le numéro SMS Installateur peut être supprimé en fixant la valeur à 0. Les numéros SMS Utilisateur ne peuvent pas être supprimés.
Utilisateur	Sélectionnez un nouvel utilisateur pour cette ID SMS Utilisateur, le cas échéant.
Événements SMS	Sélectionnez les événements centrale devant être envoyés par SMS à l'utilisateur ou à l'installateur.
Contrôle SMS	Sélectionnez les opérations pouvant être effectuées à distance sur la centrale par SMS. Voir *Commandes SMS* ci-dessous.

REMARQUE : les événements HOLD-UP ne sont pas transmis par SMS.

Si la ligne téléphonique est connectée au réseau RTC via un PBX, il est nécessaire d'insérer le chiffre approprié pour l'accès à la ligne avant le numéro du destinataire. Assurez-vous que le service **C**alling **L**ine **I**dentity (CLI) est actif sur la ligne choisie pour effectuer l'appel sur le réseau SMS. Pour les détails, consultez l'administrateur du PABX.

17.8.4 Commandes SMS

Les fonctions SMS peuvent être activées dès que le contrôle par SMS est configuré. En fonction de la configuration SMS, les commandes sont envoyées en utilisant un code ou l'ID de l'appelant. Le type de code dépend de la configuration de l'Authentification SMS.

Le tableau ci-dessous indique toutes les commandes SMS disponibles. Il décrit l'action déclenchée et la réponse.

Les commandes SMS sont envoyées sous forme de texte au numéro de téléphone de la carte SIM installée dans la centrale.

Pour écrire une commande avec un code, la syntaxe est la suivante :

****.commande ou **** commande

avec **** pour le code et « commande » pour la commande, c'est-à-dire que le code est suivi soit par une espace soit par un point. Par exemple, la commande « MSET » est saisie sous la forme : **** MSET ou ****.MSET. La version complète de la commande, si incluse dans une liste, peut également être utilisée. Par exemple, ****.MES TOTALE.

Si l'utilisateur ne dispose pas des droits suffisants pour exécuter une commande, le système renvoie la valeur ACCES REFUSE.

Si l'ID de l'appelant est désactivée et si le numéro de SMS de l'expéditeur est configuré, le préfixe du code n'est pas nécessaire.

COMMANDES (** = code)**

Avec le code	Avec l'ID de l'appelant	Action	Réponse
**** AIDE ****.AIDE	AIDE	Toutes les commandes disponibles sont affichées.	Toutes les commandes disponibles
**** MEST ****.MEST ****.MES TOTALE	MEST MARCHE TOTALE	Définit tous les secteurs auxquels l'utilisateur a accès.	Date/heure du système mis sous surveillance. Le cas échéant, la réponse est zones ouvertes / zones à MES forcée.
**** MESA ****.MESA		Autorise la MES Partielle A de l'alarme par SMS. Il est également possible de spécifier le nom personnalisé défini dans le champ de nouveau nom de MES Partielle de la page **Options**. Voir *Options* page 257.	Système activé
**** MESB ****.MESB		Autorise la MES Partielle B de l'alarme par SMS. Il est également possible de spécifier le nom personnalisé défini dans le champ de nouveau nom de MES Partielle de la page **Options**. Voir *Options* page 257. Par exemple : ****.MESA NUIT	Système activé
**** MHS ****.MHS ****.MHS	MHS MHS	Désactive tous les secteurs auxquels l'utilisateur a accès.	Système arrêté

Avec le code	Avec l'ID de l'appelant	Action	Réponse
**** ÉTAT ****.ETAT ****.ÉTAT	ETAT ÉTAT	Récupère l'état des secteurs.	État du système et des secteurs affectés • Pour un système contenant une zone unique, le système et le mode sont renvoyés, où le mode est l'état défini du système. • Pour un système multi-secteur, l'état de chacun est renvoyé.
**** XA1.ON ****.XA1.ON		Le périphérique X10 identifié comme A1 est activé.	État de A1
**** XA1.OFF ****.XA1.OFF		Le tag X10 identifié comme A1 est désactivé.	État de A1
**** LOG ****.LOG		Affichage de 10 événements récents au maximum.	Evénements récents
**** ENGA.ON ****.ENGA.ON	ENGA.ON	Activer l'accès Installateur.	Accès Installateur
**** ENGA.OFF ****.ENGA.OFF	ENGA.OFF	Désactiver l'accès Installateur.	Interdire Installateur
**** MANA.ON ****.MANA.ON		Activer l'accès Constructeur.	État de l'accès Constructeur
**** MANA.OFF ****.MANA.OFF		Désactiver l'accès Constructeur.	État de l'accès Constructeur
**** S5.ON **** S5.ON ****.SORTIE		Lorsque la sortie (interaction logique) est identifiée comme S5, elle est activée.	État de S5 Par exemple : • Sortie S5 active. • Sortie de chauffage activée (où le chauffage est le nom de la sortie).
**** S5.OFF **** O5.OFF		Lorsque la sortie (interaction logique) est identifiée comme S5, elle est désactivée.	État de S5 Par exemple : sortie S5 désactivée
****.RAZ ****.RESTAURER		Autorise l'effacement des alertes par SMS.	

Pour la confirmation du SMS, l'identification de la sortie (interaction logique) emploie le format SNNN, S étant la sortie, et NNN les caractères numériques (uniquement les chiffres significatifs). (Exemple : S5 pour sortie 5.)

Pour la confirmation du SMS, l'appareil X-10 utilise le format : XYNN, où X signifie X-10, Y est la lettre alphabétique, et NN sont les caractères numériques disponibles. (Exemple : XA1)

Le service SMS fonctionne sur la base d'un protocole standard utilisé par les téléphones compatibles SMS. Veuillez noter que certains opérateurs du RTC ne proposent pas le service SMS via le RTC. Pour pouvoir envoyer des SMS par le RTC, les critères suivants sont requis :

- Le numéro de téléphone de l'appelant (ID appelant) doit être activé sur la ligne téléphonique.
- Ligne téléphonique directe, et non via un PABX ni d'autres équipements de télécommunications.
- Notez aussi que la plupart des opérateurs ne prennent pas en charge l'envoi de SMS à des abonnés de l'étranger. (En raison de problèmes de facturation.)

17.8.5 Suppression des Mots de passe Web

Cette page liste les mots de passe Installateur et Utilisateur créés pour l'accès à l'explorateur Web.

1. Sélectionnez **Utilisateurs > Mots de passe Web**

2. Cliquez sur le bouton **Supprimer** à côté du champ Installateur ou Utilisateur pour supprimer le mot de passe.

17.8.6 Paramètres de configuration Installateur

1. Sélectionnez **Utilisateurs > Installateur**.

2. Le cas échéant, modifier le **Nom d'utilisateur** pour l'accès installateur.
3. Cliquez sur le bouton **Changer le code PIN** pour modifier le code PIN installateur (voir *Changement du code Ingénieur et du mot de passe d'accès installateur* à la page suivante).

Remarque : pour être en accord avec les approbations INCERT, le code PIN de l'utilisateur doit contenir plus de 4 chiffres.

4. Sélectionnez la **langue** utilisée par l'installateur. (Affiché seulement si plusieurs langues sont disponibles) – *Mise à jour des langues* page 354.)

Contrôle d'accès

Attribut	Description
Numéro badge	Saisissez le numéro de badge. Saisissez 0 pour désaffecter ce badge.
Badge inutilisé	Cocher pour désactiver temporairement ce badge
Extension de temps	Rallongement des temporisateurs de porte quand ce badge est utilisé. Cas des personnes à mobilité réduite.
Sans code	Permet d'accéder à une porte possédant un lecteur de code sans utiliser le code.
Prioritaire	Les badges prioritaires sont enregistrés localement sur les contrôleurs de porte. Ceci permet d'accéder à une zone même en cas de défaut technique si le contrôleur de porte ne peut communiquer avec la centrale. Le nombre maximal d'utilisateurs prioritaires est : • SPC4xxx – tous les utilisateurs • SPC5xxx – 512 • SPC6xxx – 512
Escorte	La fonction Escorte permet à des détenteurs de badge à accès privilégié d'escorter d'autres détenteurs de badge à travers certaines portes. Quand cette fonction est activée sur une porte, le badge avec le privilège « escorte » doit être présenté en premier, puis les autres détenteurs de badge ne possédant pas ce privilège présentent leur badge et peuvent ouvrir cette porte. Le délai entre la présentation du badge d'escorte et celle du badge normal est configuré pour chacune des portes.
Gardien	La fonction Gardien force un détenteur de badge avec privilège de gardien (le gardien) à accompagner dans une pièce (groupe de portes) des personnes n'ayant pas ce privilège. Le gardien doit pénétrer dans une pièce en premier. Les autres personnes sont autorisées à entrer dans la pièce uniquement si le gardien s'y trouve déjà. Le gardien n'est pas autorisé à quitter la pièce tant qu'il reste un porteur de badge non-gardien dans celle-ci. Identifie ce détenteur de badge en tant que gardien. L'utilisateur ayant l'attribut Gardien doit entrer dans une pièce (groupe de portes) avant les autres personnes et la quitter en dernier.

17.8.6.1 Changement du code Ingénieur et du mot de passe d'accès installateur

Cette page permet de modifier le code d'accès au clavier ainsi que le mot de passe d'accès à l'explorateur Web, uniquement si l'on dispose des droits d'installateur.

1. Changer le code comme suit :

Ancien code	Saisissez le code Installateur existant. (chiffres seulement)
Nouveau code	Saisissez le nouveau code Installateur. (chiffres seulement)
Confirmer nouveau code	Resaisissez le nouveau code Installateur.

2. Cliquez sur le bouton **Modif. code perso** pour activer le nouveau code.

Le nombre minimal de caractères requis pour un code dépend du niveau de sécurité configuré pour le système, ou de la longueur du code configurée dans le champ **Tailles des codes** du menu **Paramètres centrale > Paramètres du système > Options**.

3. Changement du Mot de passe Web permettant d'accéder au navigateur Web.

Nouveau mot de passe	Entrez le nouveau mot de passe Web (lettres A-Z, chiffres 0-9).
Confirmez le nouveau mot de passe.	Veuillez répéter le nouveau mot de passe.

4. Cliquez sur le bouton **Changer mot de passe** pour activer le nouveau mot de passe.

Le mot de passe est sensible à la casse : assurez-vous de bien saisir les majuscules ou minuscules du nouveau mot de passe.

17.9 Configuration

Cette section recouvre :

17.9.1 Configuration des entrées/sorties du contrôleur **226**
17.9.2 Périph. X-BUS **236**
17.9.3 Radio **249**
17.9.4 Modification des paramètres du système **256**
17.9.5 Configuration des zones, des portes et des secteurs **277**
17.9.6 Calendriers **292**

17.9.7 Modification de son propre code PIN **296**

17.9.8 Configuration des paramètres avancés **296**

17.9.1 Configuration des entrées/sorties du contrôleur

Cette section recouvre :

17.9.1.1 Édition d'une entrée

1. Sélectionnez **Configuration > Hardware > Centrale**.

   La page suivante s'affiche.

2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Entrée	Le numéro est présenté à titre indicatif et ne peut pas être programmé.
Fin de ligne	Sélectionnez la résistance fin de ligne (EOL) de l'entrée de la zone (valeur par défaut : 4K7).
Analysé	Affiche si le détecteur est du type inertie/choc
Comptage d'impulsions	Comptage d'impulsions programmé sur la centrale qui déclenche une alarme à partir d'un détecteur de type inertie/choc.
Coup brutal	Le « Coup brutal » programmé sur la centrale qui déclenche une alarme à partir d'un détecteur de type inertie/choc
Zone	Nombre de zones sur la centrale
Description	Saisissez un texte pour décrire l'entrée (maxi 16 caractères). Ce texte est affiché dans le navigateur et sur le clavier.
Type	Le type de zone (voir *Types de zone* page 397).
Zone	Uniquement si l'option Secteurs (multiple) est activée dans le menu **Paramètres centrale > Paramètres système > Options**. Sélectionnez les secteurs auxquels cette zone a été affectée.
Attributs	Une icône dans ce champ indique que des attributs sont appliqués à cette zone (voir *Zones d'entrée : attributs* ci-dessous).

Zones d'entrée : attributs

Chaque zone sur le SPC peut se voir affecter un attribut qui détermine ses propriétés.

Pour appliquer un attribut à une zone :

1. Sélectionnez **Configuration > Hardware > Centrale > Attributs**.

   La page suivante s'affiche :

2. Cochez la case en dessous de l'attribut que vous choisissez.

Les attributs présentés sur cette page dépendent du type de zone sélectionnée. Pour connaître la liste des attributs affectables, consultez *Attributs applicables aux types de zones* page 408.

17.9.1.2 Éditer une sortie

1. Sélectionnez **Configuration > Hardware > Centrale**.

2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Type de sortie	• **Sortie système :** sélectionnez le type dans le menu déroulant. (Consultez *Types de sortie et ports de sortie* ci-dessous.) • **Sortie secteur :** Uniquement si l'option **Secteurs (multiples)** est activée dans le menu **Paramètres centrale > Paramètres Système > Options**. Sélectionnez un secteur et le type de sortie système pour ce secteur. (Consultez *Types de sortie et ports de sortie* ci-dessous.) • **Mappage de zone :** sélectionnez la zone qui doit être mappée. • **Interaction logique :** sélectionnez l'interaction logique qui doit être mappée. • **Sortie porte :** sélectionnez le numéro de porte et le type de sortie système pour la porte. (Consultez *Types de sortie et ports de sortie* ci-dessous.) • **Boîtier à clé :** sélectionnez l'ID du nœud pour le boîtier à clé requis et la position de clé requise pour relier à cette sortie.
Description	Saisissez un texte pour décrire la sortie (maxi 16 caractères). Ce texte est affiché dans le navigateur et sur le clavier.
Configuration des sorties	• **Mode :** sélectionnez le mode de fonctionnement. Continu : respecte le type de sortie. Intermittent : active et désactive lorsque le type de sortie est activé. Temporaire : génère une impulsion quand le type de sortie est activé. • **Redéclencher :** cochez la case pour redéclencher des sorties temporaires. • **Temps d'activation :** saisissez le Temps d'activation qui s'applique aux sorties temporaires et pulsées. • **Temps de repos :** saisissez le Temps de repos qui s'applique aux sorties pulsées. • **Inverser :** cochez cette case pour inverser la sortie physique. • **Enregistrer :** cochez cette case pour enregistrer les modifications d'état de la sortie dans le journal des événements. • **Calendrier :** sélectionnez si nécessaire le calendrier désiré. Voir *Calendriers* page 292.

Voir également

Calendriers page 292

Types de sortie et ports de sortie

Chaque type de sortie peut être attribué à un des 6 ports de sortie physiques sur le contrôleur SPC ou à une sortie de l'un des transpondeurs connectés. Les types de sortie qui ne sont pas attribués à des sorties physiques servent d'indicateurs d'événements sur le système et peuvent être enregistrés et/ou renvoyés vers des centres de télésurveillance éloignés si nécessaire.

Les ports de sortie des transpondeurs sont tous des sorties de type relais unipolaire (NO, COM, NC) ; par conséquent, les tags de sortie ont besoin d'une source d'alimentation externe s'ils sont reliés à des sorties de transporteur.

L'activation d'un certain type de sortie dépend du type de zone (voir *Types de zone* page 397) ou de l'alerte qui déclenche l'activation. Si plusieurs secteurs sont définis, les sorties du SPC sont groupées en sorties système et sorties secteur ; les sorties système sont activées pour indiquer un événement au niveau du système (par exemple une panne de courant) alors que les sorties secteur indiquent des événements détectés dans au moins un secteur. Chaque secteur dispose de son propre ensemble de

sorties secteur ; si le secteur est commun à d'autres secteurs, ces sorties indiqueront alors l'état de tous les secteurs avec lesquels il est commun, y compris son propre état. Par exemple, si le secteur 1 est commun avec les secteurs 2 et 3, et que la sirène ext. du secteur 2 est activée, alors la sirène ext. du secteur 1 sera aussi activée.

Certains types de sortie ne peuvent indiquer que des événements au niveau du système (aucun événement spécifique à un secteur). Voir le tableau ci-dessous pour de plus amples informations.

Type de sortie	Description
Sirène extérieure	Ce type de sortie est utilisé pour activer la sirène extérieure du système. La sortie est active quand une sirène extérieure du secteur est active. Par défaut, cette sortie est attribuée à la première sortie sur la carte de la centrale (EXT+, EXT-). **Remarque :** une sortie de sirène extérieure est activée automatiquement chaque fois qu'une zone programmée comme une zone d'alarme déclenche une alarme en mode MES Totale ou MES Partielle.
Flash sirène extérieure	Ce type de sortie est utilisé pour activer le flash sur la sirène extérieure du système. La sortie est active quand un flash du secteur est actif. Par défaut, cette sortie est attribuée à la sortie de relais de flash (sortie 3) sur la carte du contrôleur (NO, COM, NC). **Remarque :** une sortie de flash sirène extérieure est activée automatiquement chaque fois qu'une zone programmée comme une zone d'alarme déclenche une alarme en mode MES Totale ou MES Partielle. Le flash de la sirène extérieure est activé après un « Échec MES » si ce flash est sélectionné (case cochée) pour l'option « Échec MES » dans les options système.
Sirène intérieure	Ce type de sortie est utilisé pour activer la sirène intérieure du système. La sortie est active quand une sirène intérieure du secteur est active. Par défaut, cette sortie est attribuée à la deuxième sortie sur la carte de la centrale (INT+, INT-). **Remarque :** une sortie de sirène intérieure est activée automatiquement chaque fois qu'une zone programmée comme un type de zone d'alarme déclenche une alarme en mode MES Totale ou MES Partielle. La sirène intérieure est activée après un « Échec MES » si la sirène est sélectionnée (case cochée) pour l'option « Échec MES » dans les options système.
Alarme	Cette sortie est activée après qu'une zone d'alarme a été activée dans le système ou dans l'un des secteurs définis.
Alarme Confirmée	Cette sortie est activée en cas de confirmation d'une alarme. Une alarme est confirmée quand 2 zones indépendantes du système (ou faisant partie du même secteur) sont activées pendant un intervalle de temps défini.
Panique*	Cette sortie est activée après qu'une zone d'alarme de panique a été activée dans l'un des secteurs. Une alarme de panique est également déclenchée si un événement « Contrainte utilisateur » est déclenché ou si l'option Panique est activée sur le clavier.
Agression	Cette sortie est activée chaque fois qu'une zone programmée avec le type « Agression » déclenche une alarme dans un secteur.
Feu	Cette sortie est activée après qu'une zone d'incendie a été activée dans le système (ou toute autre zone).

Type de sortie	Description
Autosurveillance	Cette sortie est activée quand une condition de sabotage est détectée dans le système. Pour un système de niveau 3, si la communication avec un périphérique XBUS est perdue pendant plus de 100 s, une alarme pour sabotage est générée et les événements signalés par le SIA et le CIR enverront une alerte pour sabotage.
Médical	Cette sortie est activée si une zone médicale est activée.
Défaut	Cette sortie est activée quand une erreur technique est détectée.
Technique	Cette sortie surveille les activités dans une zone technique.
Défaut secteur*	Cette sortie est activée quand l'alimentation secteur tombe en panne.
Défaut batterie*	Cette sortie est activée en cas de défaut de la batterie de secours (secondaire). Elle est aussi activée dès que la tension passe sous le seuil des 11 V. L'option « Restaurer » pour ce genre de défaut est accessible uniquement si la tension remonte à au moins 11,8 V.
MES Partielle A	Cette sortie est activée si le système ou un secteur est en mode de surveillance partielle A.
MES Partielle B	Cette sortie est activée si le système ou un secteur est en mode de surveillance partielle B.
MES totale	Cette sortie est activée quand le système est en mode de surveillance totale.
Échec MES	Cette sortie est activée si le système ou un secteur n'a pas pu être mis en surveillance. Elle est libérée après la remise à zéro de l'alerte.
Entrée/sortie	Cette sortie est activée quand une zone de type Entrée/Sortie est activée, c'est-à-dire dès qu'un temporisateur d'entrée ou de sortie du système ou d'un secteur est exécuté.
Mémoire	La sortie est activée selon la configuration des sorties du système de gâches (voir *Configuration des sorties du système de gâches et de la MES automatique* page 234). Cette sortie peut être utilisée pour la remise à zéro des détecteurs verrouillés tels que les détecteurs de fumée ou d'inertie.
Issues de secours	Cette sortie est activée quand une issue de secours est activée.
Carillon	Cette sortie est activée brièvement quand une zone ayant l'attribut Carillon est ouverte.
Fumée	Cette sortie est activée brièvement (3 secondes) quand un utilisateur met le système hors surveillance. Elle peut être utilisée pour réinitialiser les détecteurs de fumée. La sortie sera également activée lorsque le secteur est restauré. Lorsque vous utilisez le secteur pour réinitialiser les détecteurs de fumées verrouillés, la première saisie du code ne désactivera pas la sortie de la fumée, mais rendra silencieuses les sirènes. Avec la saisie suivante du code, si le secteur de feu est encore en mode ouvert, la sortie destinée au feu sera activée momentanément. Ce processus peut être répété jusqu'à la fermeture du secteur de feu.
Test déplacement*	Cette sortie est activée brièvement quand un test de déplacement est effectué et qu'une zone est activée. Cette sortie peut être utilisée, par exemple, pour activer les tests fonctionnels des détecteurs branchés (si cette fonction est disponible).
Mise en service automatique	Cette sortie est activée quand la fonction de mise en service automatique est active.

Type de sortie	Description
Code contrainte	Cette sortie est activée si un état « Contrainte utilisateur » est déclenché (l'utilisateur tape le code + 1 sur le clavier).
Masquage détecteur	Cette sortie est activée en cas de présence d'une zone infrarouge masquée dans le système. Elle génère une sortie de panne sur la LED du clavier. Cette sortie est verrouillée de façon à rester active jusqu'à ce qu'elle soit rétablie par un utilisateur de niveau 2. Le masquage détecteur est enregistré par défaut dans le journal. Le nombre d'entrées de journal ne dépasse pas 8 entre les périodes d'armement.
Zone omise	Cette sortie est activée en cas de présence d'une zone désactivée, isolée, ou de déplacement dans le système.
Echec de communication	Cette sortie est activée en cas d'échec de la communication avec le centre de télésurveillance.
Test Homme Mort (PTI)	Cette sortie active un tag de détresse activé lors d'un test de cette fonction.
Mise hors surveillance	Cette sortie est activée quand le système est en mode MHS.
Annulation d'alarme	Cette sortie est activée en cas d'annulation d'alarme, par exemple par saisie d'un code valide par le clavier à la suite d'une alarme confirmée ou non. Elle est utilisée, par exemple, avec un composeur externe de numéros (SIA, CID, FF).
TEST SISMIQUE	Cette sortie sert à activer un test manuel ou automatique en zone sismique. Les détecteurs sismiques sont munis d'un petit capteur vibrant qui est fixé sur la même paroi que le détecteur et relié par câble à la centrale ou à l'un des transpondeurs. Au cours du test, la centrale attend 30 secondes l'ouverture de la zone sismique. Si celle-ci ne s'ouvre pas, le test aboutit à un échec. Si elle s'ouvre dans les 30 secondes, la centrale attend que la zone se referme dans le délai de 10 secondes. Si celle-ci ne se referme pas, le test aboutit à un échec. La centrale attend encore 2 secondes avant de transmettre le résultat du test. Que le test soit manuel ou automatique, le résultat est sauvegardé dans le JDB.
Alarme Locale	Cette sortie est activée en cas d'alarme d'intrusion locale.
Sortie Radio	Sortie activée quand on appuie sur un bouton de la télécommande ou du WPA.
Défaut ligne Modem 1	Cette sortie est activée en cas de défaut de ligne du modem principal.
Modem 1 en Panne	Cette sortie est activée en cas de défaut du modem principal.
Défaut ligne Modem 2	Cette sortie est activée en cas de défaut de ligne du modem secondaire.
Modem 2 en Panne	Cette sortie est activée en cas de défaut du modem secondaire.
Batterie faible	Cette sortie est activée en cas de bas niveau de charge de la batterie.
Comité d'accueil Vert	Cette entrée est activée si une procédure d'entrée « Tout va bien » est lancée et qu'aucune alarme n'est générée, par exemple, si le bouton « Tout va bien » est pressé dans le délai configuré après la saisie du code utilisateur.

Type de sortie	Description
Comité d'accueil Rouge	Cette entrée est activée si une procédure d'entrée « Tout va bien » est lancée et qu'une alarme discrète est générée, par exemple, si le bouton « Tout va bien » n'est pas pressé dans le délai configuré pour cela après la saisie du code utilisateur.
MES possible	Cette sortie devient active lorsqu'un secteur est prêt à être activé.
Acquis de MES	Cette sortie indique l'état de la configuration. La sortie commute pendant 3 secondes pour signaler que le paramétrage a échoué. La sortie reste pendant 3 secondes si le paramétrage est couronné de succès.
MES totale faite	Cette sortie est activée pendant 3 secondes pour signaler que le système a été complètement mis en service.
Blockschloss 1	Utilisé pour les appareils Blockschloss normaux. Lorsque toutes les zones du secteur sont fermées et qu'il n'y a aucun défaut en cours, la sortie « Bockschloss 1 » est activée. Si le verrou du Blockschloss est fermé, une entrée « Clé de MES » est activée, le secteur en question est activé et la sortie « Acquis de MES » est activée pendant 3 secondes pour indiquer que le paramétrage a réussi. « Blockschloss 1 » n'est pas désactivé. Si le Blockschloss est déverrouillé, l'appareil Blockschloss désactive l'entrée de la clé de mise en service (fermée) et le secteur est mis hors surveillance. « Blockschloss 1 » est alors désactivé.
Blockschloss 2	Utilisé pour le type d'appareil Blockschloss - Bosch Blockschloss, Sigmalock Plus, E4.03. Lorsque toutes les zones d'un secteur sont fermées et qu'aucun défaut n'est en cours, la sortie « Blockschloss 2 » est activée. Si le verrou du Blockschloss est fermé, une entrée « Clé de MES » est activée, le secteur en question est activé et la sortie « Acquis de MES » est activée pendant 3 secondes pour indiquer que le paramétrage a réussi. « Blockschloss 2 » est alors désactivé. Si le Blockschloss est déverrouillé, la zone de clé de mise en service est mise en position de désactivation (fermée) et le secteur est mis hors surveillance. « Blockschloss 2 » est activé (si le secteur est prêt à être mis en surveillance).
Elément de verrouillage	S'active si l'élément de verrouillage est en position « verrouillé ».
Élément de déverrouillage	S'active si l'élément de verrouillage est en position « déverrouillé ».
Code autosurveillance	S'active s'il existe un code anti-effraction dans le secteur. Disparaît lorsque l'état est réinitialisé.
Anomalie	S'active si une des zones a un état indiquant un problème.
Lien Ethernet	S'active s'il existe un problème sur le lien Ethernet.
Défaut réseau	S'active s'il existe un défaut de communication EDP.
RAZ Bris de vitre	Utilisé pour commander l'alimentation du détecteur de bris de vitre, ce qui permet de réinitialiser le détecteur en coupant son alimentation. La sortie est réinitialisée si l'utilisateur saisit son code, la zone n'est pas en état fermé et les sirènes sont désactivées.

Type de sortie	Description
Agression Confirmée	Active les scénarios suivants pour conformité avec PD6662 : • deux activations de zone d'agression à plus de deux minutes d'intervalle • l'activation d'une zone d'agression et d'une zone de panique à plus de deux minutes d'intervalle • Si l'activation d'une zone d'agression et d'une zone anti-sabotage ou d'une zone de panique et d'une zone anti-sabotage) survient dans le délai de deux minutes
Mode paramétrage	Activer si l'installateur est sur le site et que le système est en mode paramétrage.

Ce type de sortie ne peut indiquer que des événements au niveau du système (aucun événement spécifique à un secteur).

Voir également

Configuration des sorties du système de gâches et de la MES automatique ci-dessous

17.9.1.3 Configuration des sorties du système de gâches et de la MES automatique

1. Dans le menu **Règle**, cliquez sur le bouton **Éditer** pour l'option **Configuration des sorties** dans **Options système**.

   La page suivante apparaît :

2. Sélectionnez la condition sous laquelle la sortie du verrouillage est activée :

Tempo d'entrée	La sortie est activée à la fin de la tempo de sortie et désactivée au début de la tempo d'entrée.
Issues de secours	La sortie est activée si n'importe quelle zone Issue de secours est active.
Mise hors surveillance	La sortie est activée si un utilisateur met le système hors surveillance momentanément
Réinitialisation d'alarme	La sortie est activée lorsqu'une alarme est réinitialisée momentanément.
Effacement des alarmes	La sortie est activée pendant la phase de mise en surveillance si Bris de vitre / Détecteurs de fumée sont actifs et pas en alarme.
Sortie du mode Ingénieur	S'active lorsqu'un installateur sort momentanément du mode Ingénieur.
Code Clavier Valide	La sortie s'active lorsqu'un code utilisateur valable est saisi sur le clavier et que la zone d'incendie est active.

3. Sélectionnez le mode d'action de la sortie.

Actif	La sortie reste active pendant la phase de mise en service automatique.
Claviers	La sortie suit la signalisation du clavier.
Progressive	La sortie donne une signalisation progressive de la MES automatique.
Durée de l'impulsion	Sélectionnez la durée pendant laquelle la sortie de MES automatique reste active lorsqu'elle reçoit une impulsion.

17.9.1.4 Configuration – paramétrages X10

La page des paramètres X10 vous permet de configurer le fonctionnement du X10 sur la centrale.

1. Sélectionnez **Configuration > Sorties > X-10**.

   La page suivante s'affiche :

2. Cochez la case **Valider** pour activer la fonction X10 sur la centrale.
3. Cochez la case **JDB** pour activer la connexion de tous les événements X10 sur la centrale.
4. Cliquez sur **Enregistrer**.
5. Cliquez sur un onglet alphabétique (A-P) pour programmer les déclencheurs de l'appareil X10.

   Une liste des déclencheurs programmables de l'appareil (1–16) sera affichée pour ce caractère alphabétique :

Numéro de l'élément	C'est le numéro (1–16) qui est affecté à cet appareil.
Actif	Ce champ indique si l'appareil est activé ou pas.
Description	Ce champ contient un texte significatif servant à identifier le périphérique, par exemple : Lumière RdC (16 caractères maxi).
Touche de raccourci	Ce champ indique si l'activation de l'appareil X10 peut être commutée en saisissant un code sur le clavier.

Pour éditer un appareil X-10

1. Cliquez sur**Editer**.

   La page suivante s'affiche :

2. Pour de plus amples détails sur la programmation, consultez *Déclencheurs* page 298.

17.9.2 Périph. X-BUS

Cette section recouvre :

17.9.2.1 Transpondeurs

1. Sélectionnez **Configuration > Hardware > X-Bus > Transpondeurs**.

   La page suivante s'affiche :

Pour l'appellation et l'identification :

Dans la configuration de boucle, chaque transpondeur est numéroté consécutivement à partir du premier (transpondeur connecté au 1A 1B du contrôleur) jusqu'au dernier (transpondeur connecté au 2A 2B du contrôleur).

Exemple pour SPC63xx : les transpondeurs, lorsqu'ils sont numérotés de 1 à 63, sont des zones affectées (par groupements de 8) dans des identités consécutives allant de 1 à 512 (le plus grand numéro en identification de zone est 512). Ainsi, tout transporteur identifié par un numéro supérieur à 63 n'est attribué à aucune zone.

2. Cliquez sur les paramètres identifiant l'un des transpondeurs pour afficher la page **Configuration transpondeur**.

3. Configurez les champs suivants :

Description	Pour application sur les témoins LED des périphériques.
Volume limite	**Transpondeur audio seulement :** volume du haut-parleur pour le transpondeur audio et les satellites (WAC 11). Ils sont tous câblés en parallèle. À noter que le haut-parleur sur WAC 11 dispose d'un potentiomètre pour régler finement le volume. Le haut-parleur peut être réglé entre 0 et 7, ou être éteint.

Canal auxiliaire	**Transpondeur audio seulement :** cette option doit être activée si les satellites (WAC11) sont connectés à ce transpondeur. **Remarque :** cette option, lorsqu'elle est activée, met en route les microphones du satellite. Les haut-parleurs du satellite sont toujours activés, quel que soit le réglage.
Fin de ligne	Sélectionnez la fin de ligne correcte (par défaut : DEOL 4K7). Ce paramétrage doit toujours correspondre au câblage réel de l'entrée sur le contrôleur ou le transpondeur. Voir *Câblage du système* page 85.
(Zone) Description	Fournissez une description pour la zone affectée.
(Zone) Type	Choisissez le type de zone. Voir *Attributs zone* page 404.
Zone	Sélectionnez le secteur.
Attributs	Affectez les attributs selon vos souhaits. Voir *Types de zone* page 397.
Sorties / ALIM sorties (affiché SEULEMENT pour le SPCP355.300 Smart PSU)	
Sortie	La sortie numérotée. La valeur entre parenthèses correspond à la sortie physique sur la carte du module d'alimentation.
Description	Entrez un libellé pour la ligne de sortie.
Changer type	Au besoin, modifiez le type de la sortie.
Attributs	Affecte des attributs à la sortie.
Test	Testez la sortie.
Sortie supervisée	Sélectionnez quelles sorties doivent être surveillées. **Remarque :** la résistance parallèle, la diode et la charge requise doivent être appliquées avant d'activer cette option. Le SPCP355.300 doit exécuter un calibrage avant que la surveillance ne commence. Consultez *Sorties supervisées* page 66 pour plus d'informations.
Batterie principale seulement	Cochez cette case si aucune batterie secondaire n'est connectée au module d'alimentation.

Après avoir ajouté ou effacé des transpondeurs, allez sur **Configuration > Matériel > X-BUS > Plan de câblage et configuration**.

Cliquez sur **Reconfigurer** pour appliquer les modifications.

Lorsque vous cliquez sur **Reconfiguration**, la totalité du X-BUS est reconfigurée. Si un transpondeur est déconnecté et qu'un bouton de reconfiguration est pressé, le transpondeur disparaît sans informer les utilisateurs.

Reconfiguration du X-BUS

1. Sélectionnez **Configuration > Matériel > X-BUS > Plan de câblage et configuration**.
2. Cliquer sur **Reconfigurer**.

La page Plan de câblage X-BUS – Avertissement(s) s'affiche :

3. Cliquez sur **Reconfiguration**.

   Le X-BUS est reconfiguré.

   Si un transpondeur est déconnecté et qu'un bouton de reconfiguration est pressé, le transpondeur disparaît sans informer les utilisateurs.

Voir également

Câblage du système page 85

Attributs zone page 404

Types de zone page 397

Configuration d'un transpondeur d'indication

Il y a deux modes de configuration possibles pour le transpondeur d'indication :

- Mode lié
- Mode flexible

1. Sélectionnez **Configuration > Hardware > X-Bus > Transpondeurs**.
2. Cliquez sur l'un des paramètres d'identification de l'indicateur.

   La page suivante s'affiche pour la configuration **Mode lié**.

Mode lié

1. Entrez une description.
2. Sélectionnez si le module indicateur doit être limité par un code valide tapé sur un clavier.
3. Sélectionnez les secteurs qui doivent être contrôlés par les quatre touches de fonction.
4. Configurez l'entrée.

Mode flexible

1. Cliquez sur le bouton **Mode flexible**.
2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Touches de fonction	
Zone	Sélectionnez le secteur qui doit être contrôlé par la touche de fonction.
Fonction	Sélectionnez la fonction qui doit être exécutée par cette touche dans ce secteur.
Zone	Sélectionnez un secteur si le module indicateur est situé dans une zone protégée.
Indications visuelles	
Indicateur	Il y a 8 voyants/LED sur la droite et 8 voyants/LED sur la gauche.
Fonction	Fonction indiquée par cette LED.
Fonction Marche	Sélectionnez la couleur et l'état de chaque témoin lumineux quand la fonction sélectionnée est active.
Fonction Arrêt	Sélectionnez la couleur et l'état de chaque témoin lumineux quand la fonction sélectionnée est inactive.
Changer fonction	Cliquez sur ce bouton pour changer la fonction de ce voyant. La fonction peut être activée ou utilisée pour un système, un secteur, une zone ou un boîtier à clé.
Indications sonores	

Alarmes	Sélectionnez si les alarmes doivent être audibles.
Entrée/sortie	Sélectionnez si l'entrée et la sortie doivent être audibles.
Appui sur la touche	Choisissez si l'appui sur une touche doit être audible.
Désactivation	
Calendrier	Sélectionnez cette option si l'accès au transporteur d'indication doit être limité en fonction du calendrier.
Interaction logique	Sélectionnez si le module indicateur doit être limité par une interaction logique.
Boîtier à clé	Sélectionnez si le module indicateur doit être limité par un boîtier à clé.
Claviers	Sélectionnez si le module indicateur doit être limité par un code valide tapé sur un clavier. (Voir avertissement ci-dessus.)
Lecteur de badge	Sélectionnez si le module indicateur doit être activé jusqu'à ce qu'un badge/tag valide soit présenté sur le lecteur intégré.

3. Configurez l'entrée.

AVERTISSEMENT : votre système n'est pas conforme aux normes EN si vous permettez à une touche de fonction d'activer le système sans qu'un code PIN valable soit nécessaire.

Configuration d'un transpondeur de boîtier à clé

1. Sélectionnez **Paramètres > X-Bus > Transpondeurs**.
2. Cliquez sur l'un des paramètres d'identification du boîtier à clé.

   La boîte de dialogue suivante s'affiche.

3. Configurez les champs comme indiqué dans les tableaux ci-dessous.

Description	Saisissez une description du transpondeur du boîtier à clé.

Options Touche	
Mémoire	Sélectionnez si la position de la clé doit être verrouillée.
Tempo verrouillage	Entrez la durée du verrouillage en secondes (0 – 9 999, 0 indique que le verrou reste opérationnel jusqu'à ce que la clé soit tournée).
Secteurs	
Emplacement	Sélectionnez le secteur ou est placé le boîtier à clé.
Indications visuelles	
Voyant/LED	Il y a 1 voyant/LED sur la droite et 1 voyant/LED sur la gauche.
Fonction	Fonction pour ce voyant/LED.
Fonction Marche	Sélectionnez la couleur et l'état de chaque témoin lumineux quand la fonction sélectionnée est active.
Fonction Arrêt	Sélectionnez la couleur et l'état de chaque témoin lumineux quand la fonction sélectionnée est inactive.
Changer fonction	Cliquez sur ce bouton pour changer la fonction de ce voyant. La fonction peut être activée ou utilisée pour un système, un secteur, une zone ou un boîtier à clé.
Désactivation	
Calendrier	Sélectionnez si le module du boîtier à clé doit être limité par un calendrier.
Interaction logique	Sélectionnez si le module du boîtier à clé doit être limité par une interaction logique.
Sortie	
Sortie x	Configurez et saisissez un texte pour les sorties du boîtier à clé. Consultez *Éditer une sortie* page 228 pour plus d'informations.
Fonctions du boîtier à clé	

Positions au centre, à droite et à gauche	Sélectionnez la **Fonction** que cette position de boîtier à clé va exécuter et le **Secteur** concerné. Les fonctions du boîtier à clé sont : • Néant • Mise hors surveillance • MES Partielle A • MES Partielle B • MES totale • Bascule MHS / MES • Bascule MHS / MES Partielle A • Bascule MHS / MES Partielle B • All Okay • Autorisation avant MES/MHS • Shunt

AVERTISSEMENT : votre système n'est pas conforme aux normes EN si vous permettez à une fonction du boîtier à clé d'activer le système sans qu'un code PIN valable soit nécessaire.

17.9.2.2 Claviers

Éditer un clavier standard

1. Sélectionnez **Configuration > Hardware > X-Bus > Claviers**.
2. Cliquez sur l'un des paramètres d'identification du clavier standard.

3. Configurez les champs comme indiqué dans le tableau ci-dessous.

Description	Saisissez une description unique pour identifier le clavier.

Touches de fonction (état repos)	
Panique	Sélectionnez Activé, Désactivé ou Silencieux validé. Si elle est activée, l'alarme panique entre en fonction en appuyant simultanément sur les deux touches programmables.
Vérification	Si une zone de vérification a été assignée au clavier, en cas de déclenchement d'une alarme de panique, il suffit de deux touches simultanément ou de saisir un code de contrainte pour activer les événements audio et vidéo.
Indications visuelles	
Rétro-éclairage (Backlight)	Sélectionnez quand le rétroéclairage du clavier doit être actif. Les options sont les suivantes : Lorsqu'une touche est pressée ; Toujours En service ; Toujours Hors service.
Voyants	Activez ou désactivez les témoins sur le clavier.
Etat des MES	Sélectionnez si l'état de surveillance doit être indiqué au repos.
Indications sonores	
Avertisseur sonore	Activez ou désactivez le buzzer sur le clavier.
Buzzer avec MES partielle	Activez ou désactivez le buzzer pendant la temporisation de sortie de la MES partielle.
Appui sur une touche	Sélectionnez si le volume du haut-parleur doit être activé lors d'un appui sur une touche.
Désactivation	
Calendrier	Sélectionnez si le clavier doit être protégé par calendrier. Voir *Calendriers* page 292.
Interaction logique	Sélectionnez si le clavier doit être protégé par une interaction logique.
Boîtier à clé	Sélectionnez si le clavier doit être protégé par un boîtier à clé.
Entrée TAG	Cochez cette case pour désactiver les touches du clavier pendant la temporisation d'entrée lorsqu'un TAG est configuré sur le clavier.
Secteurs	
Emplacement	Sélectionnez le secteur sécurisé où est placé le clavier.
Secteurs	Sélectionnez depuis le clavier les secteurs à contrôler.
Options	
Tempo MEST	Sélectionnez pour configurer un décalage de l'activation sur tous les claviers. L'emplacement du clavier est ignoré et tous les secteurs exécutent un décompte complet de la temporisation de sortie.

REMARQUE : un secteur ne doit être affecté à un clavier que si celui-ci se trouve à l'intérieur du secteur affecté et si un chemin d'entrée/sortie est défini. Si un secteur est affecté, lorsque celui-ci est mis en ou hors surveillance, les temporisations d'entrée et de sortie sont utilisées (si elles sont configurées). Les autres fonctions liées aux chemins d'entrée/sortie deviennent également accessibles. Si aucun secteur n'est affecté, le secteur est mis en ou hors service immédiatement et les autres fonctions d'entrée/sortie ne sont plus accessibles.

Voir également

Calendriers page 292

Éditer un clavier confort

1. Sélectionnez **Configuration > Hardware > X-Bus > Claviers**.
2. Cliquez sur l'un des paramètres d'identification du clavier confort.

3. Configurez les champs comme indiqué dans le tableau ci-dessous.

Description	Saisissez une description unique pour identifier le clavier.
Touches de fonction (état repos)	
Panique	Sélectionnez Activé, Désactivé ou Silencieux validé. Si elle est activée, l'alarme panique entre en fonction en appuyant simultanément sur les deux touches programmables F1 et F2.
Feu	Activez pour permettre la mise en fonction de l'alarme incendie en appuyant simultanément sur les touches programmables F2 et F3.
Médical	Activez pour permettre la mise en fonction de l'alarme médicale en appuyant simultanément sur les touches programmables F3 et F4.
MES totale	Activez pour permettre la mise en fonction de la MES totale en appuyant deux fois sur la touche F2.
MES Partielle A	Activez pour permettre l'activation de la MES Partielle A en appuyant deux fois sur la touche F3.

MES Partielle B	Activez pour permettre l'activation de la MES Partielle B en appuyant deux fois sur F4.
Voyants indicateurs	
Rétro-éclairage (Backlight)	Sélectionnez quand le rétroéclairage du clavier doit être actif. Les options sont les suivantes : Lorsqu'une touche est pressée ; Toujours En service ; Toujours Hors service.
Intensité rétroéclairage	Sélectionnez l'intensité lumineuse du rétroéclairage. Plage 1 – 8 (élevé).
Voyants	Activez ou désactivez les témoins sur le clavier.
Etat des MES	Sélectionnez si l'état de surveillance doit être indiqué au repos. (LED)
Logo	Sélectionnez si le logo doit être visible au repos.
Montre analogique	Sélectionnez si la position de la montre doit être visible au repos. Les options sont : Aligné à gauche, Aligné au centre, Aligné à droite ou Désactivé.
Urgence	Activez si les touches de fonction Panique, Incendie et Médical doivent figurer sur l'afficheur LCD.
MES directe	Activez si les touches fonctions de MES Totale et Partielle doivent figurer sur l'afficheur LCD.
Icône « homme »	Activez si l'interaction logique doit être indiquée.
Indications sonores	
Alarmes	Sélectionnez le volume du haut-parleur pour les indications d'alarme.
Entrée/sortie	La plage est de 0 à 7 (volume maximal)
Carillon	Sélectionnez le volume du haut-parleur pour les indications d'entrée et sortie, ou désactivez le son.
Appui sur une touche	La plage est de 0 à 7 (volume maximal)
Annonce Vocale	Sélectionnez le volume du haut-parleur pour le carillon, ou désactivez le son.
Buzzer avec MES partielle	La plage est de 0 à 7 (volume maximal)
Mode silencieux	Activez ce paramètre pour désactiver le buzzer pendant les entrées et sorties lorsque le clavier est dans un secteur mis en surveillance. **REMARQUE :** le buzzer clavier est actif pour entrée/sortie/MES/MHS seulement si le secteur est le même que celui associé à l'emplacement du clavier, ou si le clavier est utilisé pour l'opération.
Désactivation	
Calendrier	Sélectionnez si le clavier doit être protégé par calendrier. Voir *Calendriers* page 292.

Interaction logique	Sélectionnez si le clavier doit être protégé par une interaction logique.
Boîtier à clé	Sélectionnez si le clavier doit être protégé par un boîtier à clé.
Entrée TAG	Cochez cette case pour désactiver les touches du clavier pendant la temporisation d'entrée lorsqu'un TAG est configuré sur le clavier.
Secteurs	
Emplacement	Sélectionnez le secteur sécurisé où est placé le clavier.
Secteurs	Sélectionnez depuis le clavier les secteurs à contrôler.
Options	
Tempo MEST	Sélectionnez pour configurer un décalage de l'activation sur tous les claviers. L'emplacement du clavier est ignoré et tous les secteurs exécutent un décompte complet de la temporisation de sortie.
Niveau d'accès clavier	Choisissez le niveau d'accès du clavier (1 à 3). Niveau 1 – Toutes fonctions Niveau 2 – Seulement MES, MHS, RAZ alarme Niveau 3 – Visualisation seulement

REMARQUE : un secteur ne doit être affecté à un clavier que si celui-ci se trouve à l'intérieur du secteur affecté et si un chemin d'entrée/sortie est défini. Si un secteur est affecté, lorsque celui-ci est mis en ou hors surveillance, les temporisations d'entrée et de sortie sont utilisées (si elles sont configurées). Les autres fonctions liées aux chemins d'entrée/sortie deviennent également accessibles. Si aucun secteur n'est affecté, le secteur est mis en ou hors service immédiatement et les autres fonctions d'entrée/sortie ne sont plus accessibles.

17.9.2.3 Contrôleurs de porte

Modification d'un contrôleur de porte

1. Sélectionnez **Configuration > Hardware > X-Bus > Contrôleurs de porte**.
2. Cliquez sur l'une des données marquées en bleu (p. ex., numéro de série).

3. Configurez les champs comme indiqué dans le tableau ci-dessous.

Pour l'appellation et l'identification :

Dans la configuration de boucle, chaque transpondeur est numéroté consécutivement à partir du premier (transpondeur connecté au 1A 1B du contrôleur) jusqu'au dernier (transpondeur connecté au 2A 2B du contrôleur).

Exemple pour SPC63xx : les transpondeurs, lorsqu'ils sont numérotés de 1 à 63, sont des zones affectées (par groupements de 8) dans des identités consécutives allant de 1 à 512 (le plus grand numéro en identification de zone est 512). Ainsi, tout transporteur identifié par un numéro supérieur à 63 n'est attribué à aucune zone.

ID Transpondeur	ID du contrôleur de porte définie avec les roues codeuses d'adressage.
Type	Type du contrôleur de porte.
N° série	Numéro de série du contrôleur de porte.
Description	Description du contrôleur de porte.
E/S de porte 1	• Si une porte est affectée aux E/S de porte, sélectionnez le numéro de la porte correspondante. Si les deux entrées et sorties sont configurables, sélectionnez **Zones/Sorties**. • Si un numéro de porte est sélectionné pour les E/S de porte, les paramètres de la porte peuvent être modifiés en cliquant sur le bouton Éditer. Vous pouvez également utiliser **Paramètres > Portes**. • Si **Zones/Options** est sélectionné, les deux zones et la sortie peuvent être configurées en cliquant sur le bouton Éditer.
E/S de la porte 2	
Profil 1	Pour les lecteurs ayant une LED verte/rouge.
Profil 2	Pour les lecteurs VANDERBILT ayant une LED jaune (AR618X).
Profil 3	Le profil 3 est utilisé avec les lecteurs HID qui envoient un code PIN à la centrale en tant que lecture de badge avec un code site prédéfini (0).
Profil 4	Le profil 4 est utilisé avec les lecteurs HID qui envoient un code PIN à la centrale en tant que lecture de badge avec un code site prédéfini (255).
Profil 5	Effectuez ce choix pour activer les lecteurs Sesam. Il est également recommandé de sélectionner l'option Forcer profil lecteur pour obtenir un retour d'informations durant la configuration.

Modification Zones/Sorties pour une E/S de porte

1. Sélectionnez une Zone/Sortie pour l'E/S de porte.
2. Cliquez sur le bouton **Modifier**.
3. Les deux entrées et la sortie appartenant à ces E/S de porte peuvent être configurées comme des entrées et sorties de porte normale. Voir *Éditer une porte* page 286.
4. Pour pouvoir utiliser les entrées, elles doivent être affectées à un numéro de zone.

17.9.2.4 Plan câble

Pour afficher la liste des transpondeurs/claviers dans l'ordre dans lequel ils sont configurés sur le système SPC :

- Sélectionnez **Configuration > Matériel > X-BUS > Plan de câblage et configuration**.

  La page suivante s'affiche :

Pour plus de détails sur l'interfaçage X-BUS, consultez *Câblage de l'interface X-BUS* page 85.

17.9.2.5 Configurations

Pour configurer les connexions X-BUS :

1. Sélectionnez **Configuration > Matériel > X-BUS > Paramétrage X-BUS**.

   La page suivante s'affiche.

2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Mode d'adressage	Choisissez si les transpondeurs/claviers sont adressés manuellement ou automatiquement sur le X-BUS.
Type X-BUS	Sélectionnez la configuration en boucle ou en branche.
Nouvelles tentatives	Nombre de tentatives de retransmission des données via l'interface X-BUS avant qu'une erreur de communication soit générée. (1 – 99 : la valeur par défaut 25)
Tempo communications	Le délai avant qu'un défaut de communication ne soit enregistré.

17.9.3 Radio

La détection par capteur à radiofréquences (868 MHz) sur la centrale SPC est réalisée par des modules de réception radio installés en usine dans le clavier ou sur le contrôleur, ou en installant un transpondeur radio.

1. Sélectionnez **Configuration > Hardware > Sans fil > Sans fil**.

ID Détecteur	Type	Reçu	Etats	Récepteur	Signal	Enroller
58732159	Infrarouge	23/07/2014 11:56:31	Au repos	Centrale	Haut (9)	Enroller
60304133	Infrarouge	23/07/2014 11:55:57	Ouverte	Radio 4	Haut (9)	Enroller
58740535	Infrarouge	23/07/2014 11:55:57	Ouverte	Centrale	Haut (9)	Enroller
60304133	Infrarouge	23/07/2014 11:55:57	Ouverte	Centrale	Haut (9)	Enroller
58740535	Infrarouge	23/07/2014 11:55:56	Ouverte	Centrale	Haut (9)	Enroller
60304133	Infrarouge	23/07/2014 11:55:51	Ouverte	Radio 4	Haut (9)	Enroller
26663381	Contact magnétique	23/07/2014 11:55:21	Au repos	Centrale	Haut (9)	Enroller
60306493	Infrarouge	23/07/2014 11:54:58	AUTOSUR.	Radio 4	Haut (9)	Enroller
26424404	Contact magnétique	23/07/2014 11:54:53	Au repos	Radio 4	Haut (9)	Enroller
26220868	Contact magnétique	23/07/2014 11:54:48	Au repos	Radio 4	Haut (9)	Enroller
58906531	Infrarouge	23/07/2014 11:54:37	Au repos	Radio 4	Haut (9)	Enroller

2. Voir le tableau ci-dessous pour de plus amples informations.

Détecteur	Le numéro du détecteur programmé dans le système (1 = premier, 2 = deuxième, etc.).
ID	Le numéro d'identification unique du détecteur.
Type	Le type du détecteur radio détecté (contact magnétique, inertie/choc, etc.).
Zone	La zone sur laquelle le détecteur est enregistré.
Batterie	L'état de la batterie dans le détecteur (si elle est installée).
Supervision	Le statut de la supervision (OK = signal de supervision reçu, Non supervisé = pas de supervision).
Signal	L'intensité du signal reçu par le détecteur (01=basse, 09=haute). **Remarque :**bien qu'il ne soit pas possible d'enregistrer un appareil dont la force de signal est inférieure à 3, les appareils dont le signal passe au-dessous de cette valeur après leur enregistrement ne sont pas affectés.

Actions exécutables

Journal	Cliquez pour visualiser le journal du détecteur radio. Voir *Journal – capteur sans fil X* à la page opposée.
Enroller	Cliquez sur ce bouton pour ouvrir la liste des périphériques radio dé-enregistrés.

1. Sélectionnez **État > Hardware > X-Shunt > WPA**.
2. Affiche l'identité et l'état de chaque WPA enregistré.

17.9.3.1 Journal – capteur sans fil X

Pour consulter un historique rapide des événements d'un détecteur radio :

1. Cliquez sur le bouton **Journal**.
2. Voir le tableau ci-dessous pour de plus amples informations.

Date/Heure	Date et heure de l'événement enregistré.
Récepteur	L'emplacement du récepteur sans fil, c'est-à-dire le module sans fil monté sur le clavier, le contrôleur ou le transpondeur sans fil.
Signal	L'intensité du signal reçu par le détecteur (01=basse, 09=haute).
Etat	L'état physique du détecteur.
Batterie	L'état de la batterie connectée au détecteur (OK, Défaut).

3. Pour créer un fichier de texte contenant les données du journal, cliquez sur **Fichier Texte.**

17.9.3.2 Configuration d'un WPA

AVERTISSEMENT : la configuration d'un WPA et la page de statut ne s'affichent que s'il y a un module radio installé sur la centrale ou sur l'un de ses transpondeurs et si la centrale dispose d'une licence pour le type de module installé.

Un WPA n'est pas affecté à un utilisateur. Généralement, un WPA est partagé entre plusieurs personnes, par exemple des gardes de sécurité qui travaillent en équipe ; il peut également être fixé de manière permanente sur une surface, par exemple sous un bureau ou derrière une caisse enregistreuse.

Un maximum de 128 WPA est autorisé pour chaque centrale.

Pour configurer un WPA à partir du navigateur :

- Sélectionnez le mode Paramétrage puis les options suivantes **Configuration > Hardware > Radio > WPA**.

Les éléments suivants peuvent être vérifiés ou configurés à partir de cette page :

- **État de la batterie**

  Le WPA envoie à la centrale l'état de la batterie dans chaque image. L'état de la batterie peut être OK ou Faible.

  La surveillance de la batterie nécessite d'avoir un WPA équipé d'une carte mère révision E-PC138612 ou ultérieure.

- **Statut de supervision**

  Le statut de supervision peut être l'un des suivants :

  – Défaut
  La centrale n'a pas reçu de message de supervision du WPA au cours de la période configurée à la page Paramètres radio.

  – Désactivé
  La supervision n'est pas configurée.

  – OK
  La supervision assure la transmission normalement.

- **Statut de test**

  Le statut de test peut être l'un des suivants :

  – Test non reçu
  Le WPA n'a pas été testé au cours de la période configurée dans la page des paramètres du module radio.

  – Désactivé
  La supervision n'est pas configurée.

  – OK
  Le test du WPA est OK.

1. Cliquez sur le bouton **Éditer** pour modifier la configuration WPA.
2. Cliquez sur le bouton **Supprimer** pour supprimer un WPA du système.

Ajouter un WPA

Pour ajouter un WPA dans le système :

1. Cliquez sur **Ajouter** sur la page principale de configuration et de statut WPA.

   La page **Configurer WPA** s'affiche pour le nouveau WPA.

Hardware
Système
Entrées & Portes
Sorties
Portes
Secteurs
Calendriers
Changer son code
Avancé
Centrale
XBUS
Radio
Radio
WPA
Paramétrage Radio
Configurer le Radio Personnel Alarme WPA
WPA Ajouté
WPA
2
Libellé
WPA 2
ID Transmetteur
Apprendre
Apuyez n'importe quel bouton su WPA, puis sélectionnez 'Apprendre'
Supervision
Cocher si le WPA doit être supervisé. (note: ceci implique que l'émission de supervision doit être activée dans le WPA.)
Test
Cocher si le WPA nécessite un test manuel corespondant à la plannification des tests.
Affectation de fonction aux boutons
Rouge
Aucun
Vert
Aucun
Jaune
Suspicion
Rouge + Vert
Agression
Rouge + Vert
Aucun
Jaune + Vert
Aucun

2. Configurez le WPA avec les informations suivantes :

Description/Nom	Saisissez une description ou un nom pour identifier de manière unique un WPA.
ID transmetteur	L'ID transmetteur est imprimée sur le boîtier du WPA et peut être saisie manuellement ici. L'ID peut également être identifiée à distance en appuyant sur l'un quelconque des boutons du WPA puis en cliquant sur **Apprendre**. La centrale saisit automatiquement cette ID dans ce champ sous réserve qu'aucun autre WPA n'y soit déjà défini.
Supervision	Le WPA peut être configuré pour envoyer des signaux de supervision périodique. La supervision est activée sur le WPA à l'aide d'un cavalier. La fonction de supervision doit également être activée sur la centrale pour le WPA concerné afin de permettre un fonctionnement correct de la supervision. Si la centrale ne reçoit pas de signal de supervision, elle déclenche une alarme qui s'affiche dans le clavier et est journalisée. Si la supervision n'est pas activée, le WPA envoie un message de supervision environ toutes les 24 heures pour indiquer l'état de la batterie du WPA à la centrale. Ce message est également randomisé pour limiter le risque de collision avec les autres WPA. Cochez la case **Supervision** si la supervision est activée pour un WPA particulier.
Test	Cochez la case **Test** si un test WPA périodique est requis. La fréquence du test périodique est configurée sur la page **Changer les paramètres radio** (voir page *Modification des paramètres radio* à la page opposée).
Affectation du bouton	Utilisez cette section pour assigner des fonctions à des associations de boutons. Les fonctions disponibles sont les suivantes : Panique, Panique silencieuse, Agression, Suspicion, Sortie RF utilisateur, Médical. Il est possible de sélectionner plusieurs combinaisons pour la même fonction. Pour une installation Financière, les valeurs par défaut sont : • Jaune – Suspicion • Rouge + Vert – Hold-up Pour les installations évoluée ou simple, les combinaisons sont les suivantes : • Rouge + Vert – Panique **Remarque :** si aucune fonction n'a été assignée à une combinaison de boutons, il est encore possible d'affecter cette combinaison à un déclencheur. Voir *Déclencheurs* page 298.

3. Cliquez sur le bouton Enregistrer (**Save**) pour enregistrer les paramètres.

Voir également

Modification des paramètres radio à la page opposée

Modification des paramètres radio à la page opposée

Déclencheurs page 298

Modifier un WPA

Pour modifier un WPA, cliquez sur le bouton **Éditer** sur la page principale de configuration et de statut WPA.

La page **Éditer** est similaire à la page **Ajouter**, mais elle n'affiche pas le bouton **Apprendre** permettant de saisir automatiquement l'ID du WPA.

17.9.3.3 Modification des paramètres radio

1. Sélectionnez **Configuration > Hardware > Radio > Paramètres radio**.

2. Voir le tableau ci-dessous pour de plus amples informations.

Antenne	Sélectionnez dans le menu déroulant le type d'antenne connectée au module sans fil (interne ou externe). Le type d'antenne requis pour le module sans fil dépend du type de module sans fil installé.
Supervision	Indiquez si un détecteur radio signalé comme manquant déclenche une alarme d'autosurveillance sur la centrale. Un détecteur radio est considéré manquant quand le détecteur ne renvoie pas le signal de supervision pendant une période prolongée supérieure au délai configuré dans **Détecteur RF perdu**. Voir *Temporisations* page 269.
Filtre	Cochez la case pour filtrer les signaux RF faibles.
Détecter brouillage radio	Cochez la case pour déclencher une alerte si un brouillage radio est détecté.
PANIQUE TELEC. RADIO	Sélectionnez les options de déclenchement des boutons panique de la télécommande radio : • Désactiver • Enable (Validation) • Validé (Silencieux) • Médical Utilisateur • Agression Utilisateur • Sortie Radio
Planification test WPA	Saisissez un délai maximal (en jours) entre deux tests WPA.
Supervision RF : MES impossible	Saisissez un temps en minutes au-delà duquel, si le détecteur n'envoie pas de signal, une activation est empêchée pour le secteur où se trouve la zone radio. Ce paramétrage s'applique uniquement aux zones d'intrusion : • Alarme • Entrée/sortie • Fin tempo de sortie • Panique • Holdup • Autosurveillance • Supervision Verrouillage • Sismique • Tout OK • Autorisation avant MES/MHS • Elément de verrouillage
Délai radio perdu	Saisissez un nombre de minutes au-delà duquel l'appareil sans fil (détecteur WPA) est signalé comme perdu.

17.9.4 Modification des paramètres du système

Cette section recouvre :

17.9.4.1 Options

1. Sélectionnez **Paramètres > Système > Système > Options**.
2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Options système

Les options affichées peuvent varier en fonction du niveau de sécurité du système.

Restriction	Options Système	Description
Paramètres généraux		
	Secteurs	Sélectionnez pour autoriser plusieurs secteurs sur le système. **Remarque :** cette option n'est affichée que pour les types d'installation Simple et Évolué.
	Code restauré	Grade 3 uniquement : un utilisateur qui ne possède pas les droits de remettre à zéro une alarme peut toutefois le faire si cette option est activée. Un code à 6 chiffres est affiché quand l'alarme est réinitialisée. L'utilisateur doit appeler l'installateur pour générer un code de restauration avec lequel l'utilisateur peut restaurer l'alarme.
	Autosurveillance Zone offline	Activez cette case si les zones de transpondeur hors ligne doivent générer une alarme d'anti-effraction de zone.
	RAZ Télécommande	Si activé, la télécommande radio peut restaurer des alertes si l'on appuie sur la touche Arrêt.
Web uniquement	LED des modules audio	Si coché, le transpondeur audio n'activera pas le voyant lorsque le microphone est actif.
	Transmission en mode paramétrage	Si activé, la centrale rapportera toujours des activations d'alarme et des alarmes de panique.
	Sorties en mode Paramétrage	Si sélectionné, les éléments suivants ne sont pas désactivés pour le Passage en mode paramétrage : • Sorties de centrale • Sorties de transpondeur • Témoins • Témoins de boîtier à clé
	Sirène Défaut Trans.	Si un échec de transmission apparaît, les sirènes extérieures seront activées.
	Contrainte redéclenchable	Si coché, l'alarme contrainte se déclenche de nouveau.
	Panique redéclenchable	Si coché, l'alarme de panique se déclenche de nouveau.

Restriction	Options Système	Description
	Pilotage des LED Lecteurs	Si activé, le comportement du voyant des lecteurs est contrôlé par la centrale.
	Silence pendant l'écoute	Si coché, les sirènes internes et externes (système et secteur), les buzzers du clavier, la synthèse vocale seront désactivés pendant la vérification audio.
	Mode sortie Watchdog	Active la sortie 6 sur la carte du contrôleur SPC pour utilisation à des fins de surveillance. Vous pouvez sélectionner les modes suivants de fonctionnement de la sortie Watchdog : • Désactivé — La sortie 6 est disponible comme une sortie d'utilisation générale. • Activé — La sortie 6 est normalement OFF, mais elle est activée lorsqu'un défaut de watchdog se produit. • Intermittent — La sortie 6 est INTERMITTENTE avec des intervalles de 100 ms. • Inversé validé — La sortie 6 est normalement ON, mais elle est désactivée si un défaut de watchdog se produit. Les options suivantes combinent l'option Validé avec le signalement d'une erreur matérielle, en cas de panne du microprocesseur principal. Si une telle panne se produit, un événement SIA est envoyé au CTS1. **Remarque :** la CTS doit être configurée pour utiliser SIA et SIA Étendu 1 ou 2. CID et FF ne sont pas pris en charge par cette méthode de transmission. • Reporting Validé + (10s) — L'événement d'échec est envoyé à la CTS1, 10 secondes après la détection du défaut. Cette option doit être utilisée pour la conformité à VdS 2252. • Reporting Validé + (60s) — L'événement d'échec est envoyé à la CTS1, 60 secondes après la détection du défaut. L'événement SIA rapporté est HF et l'extension SIA signale un **défaut matériel**. **Remarque :** les défauts matériels ne sont pas signalés si l'ingénieur est connecté au système. Pour plus d'informations sur les CTS, consultez le *Centres de télésurveillance (CTS)* page 336.
	SPCP355	Active l'alimentation VDS. Pour les installations VDS, cette option est automatiquement sélectionnée.
	Sirène si Echec de la MES	Permet d'activer la sirène intérieure en cas d'échec de la MES.
	Flash si Echec à la MES	Permet d'activer le flash en cas d'échec de la MES.
	Masquer Isolations	En cas d'activation, les messages d'isolation ne seront plus affichés sur le clavier.

Restriction	Options Système	Description
	Capacité de la batterie	Capacité totale des batteries en Ah, pour la centrale seule (3-100 Ah). Vous devez entrer les valeurs de Capacité de la batterie et **Courant maxi** pour voir s'afficher le temps de batterie restant sur le clavier, événement panne de secteur. Le temps s'affiche sous le menu ÉTAT < BATTERIE < TEMPS BATT.
	Courant Max	Courant total délivré par les batteries lors d'un défaut secteur (30-20 000 mA). Vous devez entrer les valeurs de **Capacité de la batterie** et de courant maximal pour voir s'afficher le temps de batterie restant sur le clavier en cas de panne de secteur. Le temps s'affiche sous le menu ÉTAT < BATTERIE < TEMPS BATT.
MES partielle		
	Nom MES Partielle A	Entrez un nouveau nom pour le mode MES PARTIELLE A (par exemple, mode Nocturne).
	Nom MES Partielle B	Entrez un nouveau nom pour le mode MES PARTIELLE B (par exemple, 1er étage seulement).
Alarme		
	Sirène immédiate	Permet d'activer les carillons/sirènes pertinents sans attendre la confirmation d'une alarme. Si cette case est désactivée, les carillons/sirènes pertinents sont activés seulement en cas d'alarme confirmée ou si le détecteur ayant causé l'alarme non confirmée se déclenche une deuxième fois.
	Sirène à chaque alarme	Permet de réactiver les carillons/sirènes quand une deuxième zone est activée (après l'extinction de la sirène). Si cette case n'est pas cochée, les sirènes extérieures sont activées une seule fois.
Web uniquement.	Interdira la MES avec une alerte	Si activé, un Utilisateur ne peut pas MES un secteur s'il existe une alerte secteur ou système. **Remarque :** cette option est disponible uniquement si **Standards > Spécificités pays** sélectionné est réglé sur la Suisse ou si le **niveau de sécurité** a pour valeur « Pas de restriction ».
	RAZ à MHS	Activez pour que les alertes soient remises à zéro automatiquement au bout de 30 secondes en mode MHS. **Remarque :** pour être conforme à PD6662, vous devez désactiver cette option.
	Antimasque en MES	Sélectionnez le type d'événement signalé à la suite d'une détection antimasque lorsque la centrale est MES. Les options sont les suivantes : Désactivé, Autosurv., Anomalie, Alarme. L'option ne peut être configurée qu'en mode Pas de restriction. Aux niveaux 2 ou 3, le type d'événement signalé est conforme aux normes de la région sélectionnée : • Irlande - Alarme • Autres régions - Alarme

Restriction	Options Système	Description
	Antimasque en MHS	Sélectionnez le type d'événement signalé à la suite d'une détection antimasque lorsque la centrale est MHS. Les options sont les suivantes : Désactivé, Autosurv., Anomalie, Alarme. L'option ne peut être configurée qu'en mode Pas de restriction. Aux niveaux 2 ou 3, le type d'événement signalé est conforme aux normes de la région sélectionnée : • Irlande - Désactivé • Autres régions - Autosurveillance
	Hors limites en MHS	Sélectionnez le type d'événement rapporté résultant d'une détection Résist. Hors limites lorsque la centrale est désactivée. Les options sont les suivantes : Désactivé, Autoprotection et Anomalie. L'option ne peut être configurée qu'en mode Pas de restriction. Aux niveaux 2 ou 3, le type d'événement signalé est conforme aux normes de la région sélectionnée : • Allemagne VDS – Autosurveillance • Tous les autres pays - problème
	Hors limites en MHS	Sélectionnez le type d'événement rapporté résultant d'une détection Résist. Hors limites lorsque la centrale est activée. Les options sont les suivantes : Désactivé, Autoprotection et Anomalie. L'option ne peut être configurée qu'en mode Pas de restriction. Aux niveaux 2 ou 3, le type d'événement signalé est conforme aux normes de la région sélectionnée : • Allemagne VDS – Autosurveillance • Tous les autres pays - problème
	Zone Instable MHS	Sélectionnez le type d'événement rapporté résultant d'une détection Zone instable lorsque la centrale est désactivée. Les options sont les suivantes : Désactivé, Autoprotection et Anomalie. Une zone est instable si un échantillon valable ne peut pas être obtenu en moins de 10 secondes. L'option ne peut être configurée qu'en mode Pas de restriction. Aux niveaux 2 ou 3, le type d'événement signalé est conforme aux normes de la région sélectionnée : • Allemagne VDS – Autosurveillance • Tous les autres pays - problème

Restriction	Options Système	Description
	Zone instable MES	Sélectionnez le type d'événement rapporté résultant d'une détection Zone instable lorsque la centrale est activée. Les options sont les suivantes : Désactivé, Autoprotection et Anomalie. Une zone est instable si un échantillon valable ne peut pas être obtenu en moins de 10 secondes. L'option ne peut être configurée qu'en mode Pas de restriction. Aux niveaux 2 ou 3, le type d'événement signalé est conforme aux normes de la région sélectionnée : • Allemagne VDS – Autosurveillance • Tous les autres pays - problème
	Fin de Ligne (RÉSIST. FIN LIGNE)	Sélectionnez la résistance fin de ligne à appliquer aux nouvelles zones créées dans le système. Une résistance peut aussi s'appliquer à toutes les zones. Sélectionnez une valeur pour activer la fonction appropriée. Pour appliquer un nouveau paramètre de résistance de fin de ligne à toutes les zones existantes, sélectionnez la case à cocher Mettre à jour toutes les zones. Si vous modifiez la valeur de fin de ligne, mais ne sélectionnez pas cette case à cocher, le nouveau réglage ne s'applique qu'aux zones ajoutées après la modification de la valeur.
	EOL Etendu EOL Wide	Si activé, les bandes larges de résistance de fin de ligne sont utilisées.
	Suspicion Audible	Si coché, l'alerte suspicion WPA activera les voyants et le buzzer clavier (mode Bancaire uniquement).
	Test sismique si MES manuelle	Si coché, tous les capteurs sismiques de tous les secteurs seront testés avant le paramétrage du secteur ou du système (mode Bancaire uniquement).
	RAZ alarme Auto	Activez cette option pour remettre à zéro les alertes automatiquement. Si la zone ouverte ayant déclenché une alarme est fermée, une remise à zéro manuelle avec le clavier/navigateur n'est pas nécessaire. Si cette option est inactive, l'utilisateur n'a plus besoin de remettre à zéro les alertes en réinitialisant l'entrée ayant déclenché l'alerte.
	Alarme en sortie	**Activé :** en cas d'activation d'une zone entrée interdite / sortie pendant la temporisation de sortie, une alarme locale se déclenche et les sirènes retentissent. **Désactivé :** en cas d'activation d'une zone entrée interdite / sortie pendant la temporisation de sortie, l'alarme ne se déclenche pas. **Remarque :** cette option n'est affichée que si le grade **Pas de restriction** est sélectionné comme activation non conforme à EN50131. Quand la **région** Suisse ou Belgique est sélectionnée, sous les **Options de mise en conformité du système**, cette option est automatiquement activée mais n'est pas visible sous **Options**.

Restriction	Options Système	Description
	Alarme activée Entrée	**Activé :** en cas d'activation d'une zone entrée interdite / sortie pendant la temporisation d'entrée, une alarme locale se déclenche et les sirènes retentissent. **Désactivé :** en cas d'activation d'une zone entrée interdite / sortie pendant la temporisation d'entrée, l'alarme ne se déclenche pas. **Remarque :** cette option n'est affichée que si le grade **Pas de restriction** est sélectionné comme activation non conforme à EN50131. Quand la **région** Suisse est sélectionnée, sous les **Options de mise en conformité du système**, cette option est automatiquement activée mais n'est pas visible sous **Options**.

Restriction	Options Système	Description
Confirmation		

Restriction	Options Système	Description
		L'option Confirmation détermine le moment à partir duquel une alarme est considérée comme étant confirmée. • BS8243 : ceci met en application les mises en conformité avec les exigences de la police du Royaume-Uni, et est également une contrainte spécifique pour les installations dans les entreprises au Royaume-Uni. Le texte stipule qu'une alarme n'est confirmée que si elle remplit les conditions suivantes : Après qu'une première alarme a été déclenchée dans une zone, une deuxième alarme est déclenchée dans cette zone avant l'expiration du délai de confirmation de l'alarme. Le délai de confirmation de l'alarme doit être compris entre 30 et 60 minutes. (Consultez *Temporisations* page 269.) Si la deuxième alarme dans la zone n'est pas activée avant la fin du délai de confirmation, la première est inhibée. La confirmation BS8243 est activée automatiquement dès que **Standards > Spécificités Pays** est réglé sur R-U. • Garda : ceci met en application les règles concernant les alarmes confirmées demandées par la police irlandaise. Les conditions requises sont les suivantes : une alarme est considérée comme confirmée dès qu'une deuxième alarme est activée dans la zone pendant le même cycle d'activation. L'option de confirmation Garda est activée automatiquement dès que **Standards > Spécificités Pays** est réglé sur Irlande.
	Confirmation	• EN-50131-9 Ceci met en application les mises en conformité avec la norme EN-50131-9 et avec le décret espagnol « INT/316/2011 du 1er février sur l'utilisation de systèmes d'alarme dans le cadre de la sécurité privée ». Le texte stipule qu'une alarme n'est confirmée que si elle remplit les conditions suivantes : – Activation de 3 zones en 30 minutes (par défaut), dont 2 peuvent provenir du même périphérique si les activations sont de type différent (par ex., alarme/sabotage). – 1 apparition d'alarme suivie d'une erreur ATS[1] dans un délai de 30 minutes (par défaut). – Erreur ATS suivie d'une condition d'alarme ou de sabotage dans un délai de 30 minutes (par défaut). Si la période de 30 minutes expire et que la zone est restaurée à son état physique normal, les alertes de zone doivent être supprimées par un utilisateur de niveau 2. Dans ce cas, la zone peut accepter une nouvelle alerte qui déclenchera une nouvelle activation. Alternativement, si la zone n'est pas rétablie à son état physique normal, alors cette zone sera inhibée si elle peut l'être. Si une alerte (ATS) intervient de nouveau après la fenêtre des 30 minutes (par défaut), la temporisation de 30 minutes redémarre. La confirmation EN50131-9 est activée automatiquement dès que **Standards > Spécificités Pays** est réglé sur Espagne. • VDS Ceci mettra en vigueur la conformité avec la norme VDS.

Restriction	Options Système	Description
Claviers		
ⓘ	Toujours afficher état (AFF. ÉTAT SURV.)	Si activé, l'état d'armement (MES / MES partielle / MHS) du système s'affiche en permanence en bas de l'afficheur clavier. Si cette case n'est PAS cochée, l'état d'armement est affiché sur l'afficheur du clavier pendant 7 secondes puis disparaît.
	Afficher les zones ouvertes	Si coché, les zones ouvertes seront affichées sur le clavier en mode MHS.
	Message si appel CTS	Si coché, un message s'affiche sur le clavier pendant 30 secondes après la MHS si une alarme confirmée a été transmise.
	CTS message ligne 1	Message CTS à afficher sur la 1ère ligne de l'afficheur (16 car.).
	CST message ligne 2	Message à afficher sur la 2e ligne de l'afficheur (16 car.).
	Affiche cámera offline	Si activé, les caméra hors ligne seront affichées sur les claviers en MHS.
	JDB Accès clavier	Activez cette option pour enregistrer au JDB les accès utilisateur via clavier (les tentatives bonnes et mauvaises).
	Langue au repos	Sélectionnez la langue affichée au repos. • Langue système : les textes sur les claviers, dans l'interface Web et dans le journal de bord sont affichés dans la langue sélectionnée. • Dernière utilisée : la dernière langue utilisée est affichée au repos.
	Utiliser Menu simplifié	Activez cette option pour utiliser des menus simplifiés pour les MES/MHS sur les claviers « Confort » et « Compact » (si un seul secteur configuré).
Code PIN		
	Taille des codes	Entrez le nombre de chiffres des codes utilisateur (8 chiffres maxi). L'augmentation du nombre de chiffres provoque l'ajout de zéros à gauche du code existant, par exemple le code utilisateur existant 2134 (quatre chiffres) devient 00002134 si vous sélectionnez 8 dans le champ Taille des codes. Si le nombre de caractères est diminué, les premiers caractères sont supprimés. Ainsi, le code 00002134 (8 caractères) devient 02134 si le nombre de caractères est fixé à 5. **Remarque :** Cette option ne peut être modifiée si un mode code SPC Manager est activé. Voir *SPC Manager* page 350. **Remarque :** pour être en accord avec les approbations INCERT, le code PIN de l'utilisateur doit contenir plus de 4 chiffres.
	Tag + Code	Si activé, les codes PACE et PIN sont requis.

Restriction	Options Système	Description
	Code contrainte	Sélectionnez l'une des fonctions Contrainte suivantes pour l'activer. • PIN+1 (le système bloque les valeurs précédente et suivante pour l'application de la contrainte). • PIN+2 (le système bloque les deux valeurs précédentes et suivantes pour l'application de la contrainte). La contrainte doit être activée pour les utilisateurs individuels. Voir la section se rapportant à Ajouter/Éditer un utilisateur.
	Règle Codes	Cliquez sur le bouton **Éditer** pour sélectionner les options d'utilisation du code. • Changement périodique requis – met en œuvre les changements prévus du code de l'utilisateur. La période est définie dans le champ **Validité Code** de **Temporisations**. Voir *Temporisations* page 269. • Avertir si changmt requis – génère une alarme utilisateur si le code de celui-ci est sur le point d'expirer ou a déjà expiré. La période d'avertissement est définie dans le champ **Avertissmt Code** de **Temporisations**. Voir *Temporisations* page 269. • L'Util. choisit le dernier digit – permet à l'utilisateur de choisir le dernier chiffre de son code. Les chiffres précédents sont générés par le système. • L'Util. choisit les 2 chiffres – permet à l'utilisateur de choisir les deux derniers chiffres de son code. Les chiffres précédents sont générés par le système. • Limite changmts – limite le nombre de changements possibles pendant la période de validité d'un code. Cette valeur est définie dans le champ **Limite Changmt Code** de **Temporisations**. Voir *Temporisations* page 269. • Sécuriser Code - si activé, le code sera automatiquement généré par la centrale.
Porte et Lecteur		
	Réinit Passback	Si activé, les états antipassback des badges sont effacés tous les jours à minuit.
	Ignorer le code site	En cas d'activation, le système d'accès ignore les codes site. En ignorant le code site, vous ajoutez seulement le numéro de badge et augmentez le nombre d'utilisateurs de badges sur le système de 100 à 2 500.
	Formats du badge	Cliquez sur le bouton **Éditer** pour sélectionner les formats de badge autorisés sur cette centrale. Consultez *Lecteurs de cartes et de formats de badges pris en charge* page 409 pour un complément d'information sur les lecteurs de badge et les formats de badge. **Remarque :** en sélectionnant **Wiegand**, vous activez tous les formats de badge Wiegand.

Restriction	Options Système	Description
Web uniquement.	Comportement Portes en MES	Sélectionnez le type d'identification d'utilisateur requis pour déverrouiller les portes lorsque le secteur est EN surveillance. Les options sont les suivantes : **Défaut**, **Badge et code**, **Badge ou code**.
Web uniquement.	Comportement Portes en MHS	Sélectionnez le type d'identification d'utilisateur requis pour déverrouiller les portes lorsque le secteur est HORS surveillance. Les options sont les suivantes : **Défaut**, **Badge et code**, **Badge ou code**.
	Pilotage des LED Lecteurs	Si coché, les LED du lecteur indiqueront la confirmation de MES/MHS pendant quelques secondes, et la demande de Badge + Code.
Installateur		
	RAZ Installateur	(Significatif uniquement si le Royaume-Uni est sélectionné dans les options Pays) : Si cette option est activée, les alarmes confirmées doivent être remises à zéro par l'installateur. Cette option est combinée à la fonction « Confirmation » .
	Sortie du mode Ingénieur	Si activé, l'installateur est autorisé à quitter le mode Paramétrage lorsqu'une alerte est active.
	Accès Installateur	Activez cette fonction si vous voulez que l'installateur ne puisse accéder au système que si l'utilisateur l'autorise. Si désactivé, l'option de menu ACTIVER LE PARAMÉTRAGE sur le clavier n'est pas disponible. **Remarque :** disponible uniquement si le **Niveau de sécurité** a pour valeur « Pas de restriction ». Pour les niveaux 2 et 3, le contrôle d'accès au système de l'installateur est toujours disponible.
	Accès Constructeur	Activez cette fonction si vous voulez que l'installateur ne puisse accéder au système que si l'utilisateur l'autorise. Si désactivé, l'option de menu ACTIVER L'INSTALLATEUR sur le clavier n'est pas disponible. **Remarque :** disponible uniquement si le **Niveau de sécurité** a pour valeur « Pas de restriction ». Pour les grades 2 et 3, le contrôle d'accès au système est toujours disponible si l'utilisateur est du type « Manager ».
SMS		
	Authentification SMS	Sélectionnez l'une des options suivantes : • Code PIN seulement : C'est un code utilisateur valable. • ID appelant uniquement : numéro de téléphone (avec l'indicateur du pays à trois chiffres) tel qu'il est configuré pour le contrôle par SMS par l'utilisateur. Le contrôle SMS ne peut être configuré par l'utilisateur que lorsque cette option est sélectionnée. • Code PIN et ID appelant • Code PIN SMS seul : code valable configuré pour l'utilisateur, différent du code de connexion de l'utilisateur. Les contrôles SMS ne peuvent être configurés par l'utilisateur que lorsque cette option est sélectionnée. • CODE PIN SMS et ID appelant

Restriction	Options Système	Description
Règles		
Web uniquement.	Règle comportement système	Configuration de l'accès Installateur et le comportement du rapport d'anti-effraction du système.
Web uniquement.	Règle sur les temporisations	Affiche les règles de temporisation du système.
Web uniquement.	Configuration des sorties	Cliquez sur le bouton **Éditer** pour configurer les paramètres de gâche et sortie MES automatique (voir*Configuration des sorties du système de gâches et de la MES automatique* page 234).
Web uniquement.	Comportement Alertes Système	Cette option permet de restreindre l'accès des utilisateurs et de l'installateur aux fonctions de RAZ, d'isolation et d'inhibition. La réaction du système aux alertes peut également être paramétrée.
Web uniquement.	Comportement Alarme Zone	Cette option permet d'indiquer si les utilisateurs et l'installateur peuvent remettre à zéro, inhiber ou isoler des alarmes de zones particulières.
Web uniquement.	Comportement Autosurv. Zone	Cette option permet d'indiquer si les utilisateurs et l'installateur peuvent remettre à zéro, inhiber ou isoler des effraction de zones spécifiques.
Web uniquement.	Règle d'affichage claviers	Sélectionnez les événements à afficher sur les claviers en mode MES et MHS.
Web uniquement.	Règle d'activation LEDs claviers	Sélectionnez les événements à afficher sur les claviers en mode MES et MHS.
Web uniquement.	Règles générales sur le système	Sélectionnez les options pour gérer l'activation de l'accès à distance du système et les paramètres de la sirène : - Pas d'alarme confirmée si activée de manière interne - Block RAZ à distance - Block Isolation à distance - Block Inhibition à distance - Pas de sirène extérieure si activée de manière interne - Retarde la transmission si la tempo d'entrée est lancée - Délai d'oubli de l'alarme confirmée

Restriction	Options Système	Description
Web uniquement.	Alertes syst. confirmant AI	Choisissez quelles alertes systèmes déclenchent des alarmes confirmées lorsqu'une alarme est déjà présente, et quelles alertes système mettent la centrale dans un état d'essai.
Données Agression		
Web uniquement.	Agression- mot clé 1	Saisissez le premier mot clé d'agression à envoyer au CMS (salle de contrôle) de la fausse monnaie dans un événement d'information d'agression (HD).
Web uniquement.	Agression- mot clé 2	Saisissez le deuxième mot clé d'agression à envoyer au CMS (salle de contrôle) en cas d'événement d'information d'agression (HD).
Web uniquement.	N° de téléphone 1	Saisissez le premier numéro de téléphone de site à envoyer au CMS (salle de contrôle) en cas d'événement d'information d'agression (HD).
Web uniquement.	N° de téléphone 2	Saisissez le deuxième numéro de téléphone de site à envoyer au CMS (salle de contrôle) en cas d'événement d'information d'agression (HD).

Voir également

Ajouter/Éditer un secteur page 278

17.9.4.2 Temporisations

Cette page indique les valeurs par défaut des temporisateurs et fournit leur description.

Ces paramètres qui varient en fonction du niveau de sécurité du système ne doivent être programmés que par un installateur autorisé. La modification des paramètres risque de compromettre la conformité du système SPC avec les normes de sécurité. Quand le niveau de sécurité est rétabli à EN 50131 Grade 2 ou EN 50131 Grade 3, les modifications effectuées dans cette page sont écrasées.

1. Sélectionnez **Configuration > Système > Temporisations du système**.

   La page **Temporisations du système** s'affiche.
2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Temporisations

Désignation des fonctions dans l'ordre suivant :

- 1re ligne : Web
- 2e ligne : clavier

Durée	Description	Défaut
Audible		
Sirènes intérieures DUREE SIRENE INT	Durée d'activation des sirènes intérieures lorsqu'une alarme est activée. (0 – 999 minutes ; 0 = jamais)	15min

Durée	Description	Défaut
Sirènes extérieures DUREE SIRENE EXT	Durée d'activation des sirènes extérieures lorsqu'une alarme est activée. (0 – 999 minutes ; 0 = jamais)	15min
Retard sirènes extérieures RETARD SIRÈNE EXT.	Cela provoque un décalage du déclenchement de la sirène extérieure. (0–999 secondes)	0 s
Carillon DUREE CARILLON	Durée d'activation en secondes de la sortie Carillon quand une zone avec l'attribut Carillon est déclenchée. (1-10 secondes)	2 s
Confirmation		
Confirmer TEMPS DE CONFIRM	**Remarque :** cette option n'est disponible que pour certaines combinaisons d'options de **Grade** et **Confirmation**. (Voir *Options* page 257 et *Normes* page 274.) Ce temporisateur s'applique à la fonction de confirmation d'alarme. Il définit la durée maximale entre les alarmes de deux zones différentes qui ne se chevauchent pas, avant qu'une alarme confirmée soit déclenchée. (0-60 minutes)	30 min
Agression confirmée	**Remarque :** cette option n'est disponible que pour certaines combinaisons d'options de **Grade** et **Confirmation**. (Voir *Options* page 257 et *Normes* page 274.) Ce temporisateur s'applique à la fonction de confirmation d'alarme. Il définit la durée maximale entre les alarmes de deux zones différentes qui ne se chevauchent pas, avant qu'une alarme confirmée soit déclenchée. (480-1200 minutes)	480 min
Délai de numérotation DÉLAI DE NUMÉROTATION	Lorsqu'il est programmé, le délai de numérotation provoque un temps d'attente prédéfini avant que le système n'appelle le Centre de télésurveillance (CTS). Ce décalage est destiné à limiter les interventions injustifiées du Centre de télésurveillance et de la police. En cas de déclenchement d'une deuxième zone, le délai de numérotation est ignoré et l'appel a lieu immédiatement. (0–999 secondes)	30 s
Annulation d'alarme ANNULATION D'ALARME	Temps après la transmission d'une alarme durant lequel un message d'annulation d'alarme peut être transmis. (0–999 secondes)	30 s
MES		
Autorisation MES AUTORISATION MES	Période de temps pendant laquelle l'autorisation MES est valide. (10-250 secondes)	20 s

Durée	Description	Défaut
Dernière issue DERNIÈRE ISSUE	La temporisation Dernière issue correspond au nombre de secondes pendant lequel l'armement est retardé après la fermeture d'une zone programmée avec l'attribut de dernière issue. (1-45 secondes)	7 s
Sirène si MES totale SIRÈNE SI MES TOTALE	Déclenche momentanément la sirène extérieure pour indiquer une condition de MES totale. (0-10 secondes)	0 s
Échec MES ÉCHEC MES	Nombre de secondes durant lequel le message Échec MES sera affiché sur le clavier (0 jusqu'à la saisie d'un code valide). (0–999 secondes)	10 s
Flash si MES totale FLASH SI MES TOTALE	Déclenche momentanément le flash de la sirène extérieure pour indiquer une condition de MES totale. (0-10 secondes)	0 s
Alarme		
Double déclenchement DOUBLE DÉCLENCH.	Délai maximal entre des activations de zones ayant l'attribut Double déclenchement pour déclencher une alarme. (1-99 secondes)	10 s
Test JOURS TEST JDB	Nombre de jours durant lequel une zone reste en test avant de revenir automatiquement en fonctionnement normal. (1–99 jours)	14 jours
Période de test sismique AUTOTEST SISMIQUE	Période moyenne entre les tests automatiques du détecteur sismique. (12–240 heures) **Remarque :** pour activer le test automatique, l'attribut **Test auto détecteur** doit être activé pour la zone sismique.	168 heures
Durée du test sismique DURÉE TEST SISM.	Temps maximum (secondes) d'attente du déclenchement du détecteur sismique lorsqu'il est sollicité par l'activation de la sortie Test sismique. (3-120 secondes)	30 s
Retard RAZ alarme auto	Délai avant une RAZ alarme auto lorsqu'un secteur est revenu à son état normal. (0-9999 secondes)	0 s
Verrouillage post-alarme VERROUILLAGE POST-ALARME	Le temps nécessaire pour que l'utilisateur puisse obtenir l'accès après une alarme. (1-120 minutes)	0min
Durée d'accès après alarme	Période pendant laquelle l'accès après alarme est autorisé pour un utilisateur après l'écoulement du temps de verrouillage d'accès. (10-240 minutes)	

Durée	Description	Défaut
Flash sirène extérieure DURÉE FLASH	Durée d'activation de la sortie flash lorsqu'une alarme est activée. (1 – 999 minutes ; 0 = indéfiniment)	15min
Alertes		
Tempo défaut 230 V DÉLAI DÉF. 230 V	Le temps de déclenchement d'une alerte par le système après qu'un défaut secteur a été détecté. (0-60 minutes)	0 min
Durée du brouillage radio	Le temps de déclenchement d'une alerte par le système après qu'un brouillage radio a été détecté. (0–999 secondes)	0 min
Installateur		
Accès Installateur ACCES INSTALLAT.	La temporisation d'Accès installateur démarre dès que l'utilisateur active l'Accès installateur. (0 – 999 minutes ; 0 indique que l'accès au système n'est pas limité dans le temps.)	0 min
Déconnexion installateur automatique DÉCONNECT. AUTO	La durée d'inactivité après laquelle l'installateur sera automatiquement déconnecté. (0–300 minutes)	0 min
Clavier		
Temps de saisie clavier TEMPS DE SAISIE CLAVIER	Le nombre de secondes pendant lequel un clavier attend une saisie avant de quitter le menu en cours. (10-300 secondes)	30 s
Langue clavier LANGUE CLAVIER	Temps d'attente en secondes avant qu'un clavier revienne à la langue par défaut. (0 – 9 999 secondes ; 0 = jamais)	10 s
Feu		
Pré-alarme incendie PRE-ALARME INCENDIE	Nombre de secondes d'attente avant l'envoi d'une alarme incendie pour les zones où l'attribut « Pré-alarme incendie » est activé. Consultez *Édition d'une zone* page 277. (1–999 secondes)	30 s
Confirmation incendie CONFIRMATION INCENDIE	Délai supplémentaire avant l'envoi du fichier d'alarme pour les zones où les attributs Pré-alarme incendie et Confirmation incendie sont activés. Consultez *Édition d'une zone* page 277. (1–999 secondes)	120 s
Code PIN		

Durée	Description	Défaut
Code PIN valide CODE PIN VALIDE	Période de temps pendant laquelle le code est valide (1-330 jours)	30 jours
Nbre maxi de changements de code NBRE MAXI DE CHANGEMENTS DE CODE	Nombre de changement du code dans la période de validité. (1–50)	5
Avertissement code AVERTISSMT. CODE	Temps avant que le code n'expire, démarrant la signalisation à l'utilisateur que son code va expirer (1-14 jours)	5 jours
Paramètres généraux		
Durée activation sortie RF SORTIE RADIO	Temps d'activation de la sortie RF dans le système. (0–999 secondes)	0 s
Limite de la Synchro d'heure LIMITE DE LA SYNCHRO D'HEURE	Durée limite pendant laquelle la synchronisation horaire n'a pas lieu. La synchronisation horaire n'a lieu que si l'heure et la date du système sont hors de cette limite. (0-300 secondes)	0 s
Tempo déf. liaison TEMPO DÉF. LIAISON	Temps avant l'apparition de Défaut liaison Ethernet (0–250 secondes ; 0 = Désactivé)	0 s
Camera Offline CAMERA OFFLINE	Délai avant info caméra Offline. (10-9999 secondes)	10 s
Fréquent FRÉQUENT (!)	Cet attribut ne s'applique qu'aux services à distance. Le nombre d'heures d'ouverture d'une zone si cette zone est programmée avec l'attribut **Fréquent**. (1-9999 heures)	336 h (2 semaines)
Contrainte silencieuse	Temps pendant lequel la contrainte reste silencieuse et non restaurable depuis le clavier. (0-999 minutes)	0 min
Agression/Panique silencieuse	Nombre de minutes pendant lequel une agression/panique reste silencieuse et non restaurable depuis le clavier. (0-999 minutes)	0 min

Les temps par défaut dépendent de la configuration Installateur. Les temps par défaut indiqués peuvent être admissibles ou pas et dépendent de la configuration effectuée par l'installateur.

Les paramétrages/plages valides peuvent dépendre du grade de sécurité spécifié sous **Configuration > Système > Standards**.

17.9.4.3 Identification

1. Sélectionnez **Configuration > Système > Identification**.

   La page suivante s'affiche.

2. Configurez les champs comme indiqué dans le tableau ci-dessous.

ID d'installation	Saisissez un numéro unique pour chaque installation ; ce numéro identifie l'installation (1 – 999999).
Nom du site	Saisissez le nom de l'installation. Le nom de l'installation doit être attribué avant l'enregistrement de celle-ci dans le système. L'installation peut être visualisée sur le clavier.
Date d'installation	Dans le menu déroulant, sélectionnez la date à laquelle l'installation a été terminée.
Nom de l'Installateur	Saisissez le nom de la personne qui a installé le système (pour un besoin d'assistance).
N° de téléphone Installateur	Saisissez le numéro de téléphone de la personne qui a installé le système (pour un besoin d'assistance).
Afficher Installateur	Cochez cette case pour afficher les détails de l'installation sur le clavier connecté à la centrale lorsque le système est au repos.
Verrouillage Installateur	Cochez cette case pour requérir l'utilisation du code verrouillage Installateur lors de la réinitialisation de la centrale aux valeurs usine.
Code verrouillage Installateur	Saisissez la valeur pour le code (4 chiffres).

17.9.4.4 Normes

Tous les systèmes d'alarme doivent répondre à des normes de sécurité données. Chaque norme a des exigences de sécurité spécifiques qui s'appliquent à la région de commercialisation / au pays dans lequel le système d'alarme est installé.

1. Sélectionnez **Configuration > Système > Normes**.

   La page suivante s'affiche.

2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Continent	Sélectionnez le continent correspondant à l'installation. Vous pouvez saisir Europe, Asie, Amérique du Nord, Amérique du Sud ou Océanie.
Type d'installation	Sélectionnez le type d'installation. Les options disponibles sont les suivantes : Simple, Évolué ou Bancaire.

Pays pour la conformité	Pour modifier le pays sur votre centrale, nous vous recommandons fortement de réinitialiser votre centrale aux valeurs par défaut et de sélectionner un nouveau pays avec l'assistant de démarrage. Sélectionnez le pays où le dispositif est installé et les exigences régionales que celui-ci doit respecter. Certaines sélections aboutissent au remplacement des exigences EN50131 par les réglementations locales ou nationales. Les options dans le champ **Grade** seront modifiées en fonction de votre sélection dans le champ **Pays pour la conformité**. Les options sont le Royaume-Uni, l'Irlande, l'Europe dans son ensemble (EN), l'Italie, la Suède, la Suisse, la Belgique, l'Espagne, l'Allemagne (VDS), la France, la Norvège, le Danemark, la Pologne, les Pays-Bas, la Finlande, le Portugal et la République tchèque.
Grade	Sélectionnez le niveau de sécurité applicable au site. Les options dans le champ **Grade** seront modifiées en fonction de votre sélection dans le champ **Pays pour la conformité**.

Grade sans restriction

Le niveau de sécurité **Pas de restriction** n'applique aucune restriction sécuritaire régionale à l'installation. En revanche, ce niveau permet à l'installateur de personnaliser l'installation en modifiant les options de sécurité et de configurer les options supplémentaires non conformes avec les normes de sécurité régionales.

Les options de configuration sans restriction sont indiquées dans le présent document par le symbole suivant : ⏻

Voir *Options système* page 257 pour des infos détaillées concernant les politiques de configuration du système.

17.9.4.5 Horloge

Cette page vous permet de régler la date et l'heure de la centrale. Le contrôleur comporte une horloge temps réel **R**eal-**T**ime **C**lock (RTC) secourue par une batterie pour conserver les informations d'heure et de date en cas de coupure de l'alimentation.

1. Sélectionnez **Configuration > Système > Horloge**.

   La page suivante s'affiche.

2. Sélectionnez l'**Heure** et la **Date** dans les menus déroulants.
3. Configurez les champs suivants :

Passage automatique heure d'été/hiver	Avec ce choix, le système bascule automatiquement sur l'heure d'été
Synchronisé sur le 50 Hz du secteur	Avec ce choix, le RTC se synchronise avec l'onde sinusoïdale de l'alimentation secteur.

L'heure et la date sélectionnées s'affichent sur le clavier, l'interface Web et le journal d'événements.

17.9.4.6 Langue

1. Sélectionnez **Configuration > Système > Langue**.

   La page suivante apparaît :

2. Pour l'option **Langue**, sélectionner la langue dans le menu déroulant.

   Cette option détermine la langue du système dans laquelle seront affichés les textes et menus sur les claviers, l'interface Web et le journal d'événements.

3. Pour l'option **Langue au repos**, choisissez entre « Utilise Langue Système » ou « Dernière langue utilisée ».

   La langue au repos détermine la langue qui s'affiche sur les claviers lorsque la centrale est au repos. Si l'option Dernière langue utilisée est sélectionnée, la langue affichée est celle associée au dernier utilisateur connecté.

La langue utilisée pour les claviers et les navigateurs dépend de la sélection effectuée pour chacun des utilisateurs. Par exemple, si la langue du système est le français mais que la langue individuelle de l'utilisateur est l'anglais, cette dernière langue est celle utilisée à la fois pour les claviers et le navigateur pour cet utilisateur, quelle que soit la langue spécifiée pour le système.

Voir également

Options page 130

17.9.5 Configuration des zones, des portes et des secteurs

Cette section recouvre :

17.9.5.1 Édition d'une zone

L'installateur et l'utilisateur peuvent consulter le JDB, isoler/restaurer une zone et tester / arrêter le test d'une zone conformément aux niveaux de sécurité EN 50131 Grade 2 et EN 50131 Grade 3.

1. Sélectionnez **Configuration > Entrées > Toutes zones**.

   La page suivante s'affiche.

Vous pouvez sélectionner **Configuration > Entrées > Zones X-Bus** pour configurer uniquement les zones câblées ou **Configuration > Entrées > Zones radio** pour configurer uniquement les zones radio.

2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Zone	Le numéro est présenté à titre indicatif et ne peut pas être programmé.
Description	Saisissez un texte (maxi 16 caractères) qui permet d'identifier la zone de manière unique.
Entrée	L'entrée physique est affichée en guise de référence et ne peut pas être programmée.
Type	Sélectionnez un type de zone dans la liste déroulante (voir *Types de zone* page 397).
Zone	Uniquement si l'option **Secteurs** (multiples) est activée. Sélectionnez dans la liste déroulante un secteur auquel la zone est affectée.
Calendrier	Sélectionnez si nécessaire le calendrier désiré (voir *Calendriers* page 292). Pour le grade de sécurité 2/3, un calendrier ne peut être associé qu'aux zones de type Tempo de sortie, Technique, Armement par clé, Shunt, et X-Shunt. Pour le grade de sécurité Pas de restriction, un calendrier peut être associé à toutes les zones indépendamment du type.
Attributs	Cochez la case voulue pour la zone. Seuls les attributs qui s'appliquent à ce type de zone seront présentés (voir *Attributs zone* page 404).

17.9.5.2 Ajouter/Éditer un secteur

Prérequis

- Uniquement si l'option **Secteurs** (multiples) est activée.

1. Sélectionnez **Configuration > Secteurs > Secteurs**.

   La page suivante s'affiche :

2. Cliquez sur **Éditer** pour éditer un secteur existant.
3. Cliquez sur **Ajouter** pour ajouter un nouveau secteur. Si l'installation est de type *Simple* ou *Évolué*, un secteur est automatiquement ajouté et la page **Éditer les paramètres de secteur** s'affiche.
   Veuillez noter que le nouveau secteur est automatiquement classé dans le type Standard.
   S'il s'agit d'une installation de type *Bancaire*, la fenêtre suivante s'affiche et le secteur doit être ajouté manuellement.

4. Saisissez une description pour le nouveau secteur et sélectionnez un type de secteur parmi l'un des suivants :

   – Standard – Convient à la plupart des secteurs.

   – DAB – Fournit les paramètres et les valeurs par défaut convenant aux DAB.

   – Chambre forte – Fournit les paramètres et les valeurs par défaut convenant aux chambres fortes.

   – Avancé – Permet le paramétrage de tous les secteurs (standard, DAB et chambre forte).
5. Cliquez sur le bouton **Ajouter** pour ajouter le secteur.

- Configurez les paramètres pour chaque type d'installation en fonction des sections suivantes.

Entrée/sortie

Configurez les paramètres d'Entrée/sortie suivants :

Tempo d'entrée	Le temps dont dispose l'utilisateur pour ARRÊTER l'alarme après avoir ouvert une zone d'entrée/sortie d'un système armé. Le temporisateur d'entrée s'applique à toutes les zones d'entrée / de sortie dans le secteur considéré (par défaut 45 secondes).

Tempo Sortie	Le temps (en secondes) accordé à l'utilisateur pour quitter un secteur protégé avant la MES complète. La temporisation de sortie sera décomptée sur le clavier, et l'avertisseur sonore va biper pour indiquer à l'utilisateur que le système va s'activer lorsque la temporisation sera à zéro. Le temporisateur de sortie s'applique à toutes les zones d'entrée / de sortie dans le secteur considéré (par défaut 45 secondes).
Désactiver temporisation de sortie	Sélectionnez si aucune temporisation de sortie n'est requise et que les paramètres sont activés sur la zone « Fin Tempo de sortie » ou sur la zone « Entrée/sortie » avec l'attribut « Tempo dernière issue ». Voir *Temporisations* page 269.
Saisie MHS par radio	La radio ne s'arrête qu'au cours de l'écoulement de la temporisation d'entrée. La valeur par défaut est activée.
Accès refusé si alarme	L'accès est temporairement refusé au secteur pour la durée spécifiée dans la temporisation du Blocage d'accès après alarme.
Empêche les MES	Si activé, la configuration est désactivée à partir du clavier
Empêche les MHS	Si activé, le changement de configuration est désactivé à partir du clavier.
Autorisation avant MES/MHS	Utilisé pour la configuration de verrouillage du blocage. Les options sont les suivantes : • Désactiver • ON • Mise hors surveillance • Mise en / hors surveillance Si l'option Désactiver est sélectionnée (valeur par défaut), le système sera activé et désactivé normalement, sans modification du fonctionnement. Si l'option Activer est sélectionnée, un signal d'« activation d'autorisation » est sélectionné pour configurer ce secteur. Elle peut être récupérée à partir des claviers ou d'une saisie de zone (voir le paramètre Autorisation du verrouillage de blocage). L'utilisateur ne peut pas activer le système à partir du clavier. Tout secteur nécessitant l'activation d'une autorisation apparaîtra comme bloqué sur le clavier de confort et n'apparaîtra pas sur le clavier standard lors de la configuration. Si l'option MHS est sélectionnée, l'utilisateur ne peut pas désactiver la zone à partir des claviers, mais peut utiliser le clavier pour générer le signal d'autorisation de l'activation. Pour les options d'activation et de désactivation, l'utilisateur ne pourra pas modifier le statut du secteur à partir du clavier, quel que soit le moment. Vous pouvez configurer un minuteur d'activation de l'autorisation. Voir *Temporisations* page 269.

Options MES/MHS Partielle

Configurez le fonctionnement de zones particulières pour les modes MES Partielle A et B comme indiqué ci-dessous :

MES Partielle valide	Activez la MES Partielle pour le fonctionnement A et B comme requis.

MES Part. temporisée :	Cliquez sur la case appropriée (MES Partielle A ou B) pour appliquer la temporisation de sortie sur le mode MES Partielle A ou B.
Attribut zones d'accès :	Cliquez sur la case appropriée pour modifier les zones d'accès dans les zones de type d'entrée / de sortie pour un fonctionnement MES Partielle A ou B. Cette fonction est utile pour une installation résidentielle lorsqu'un capteur infrarouge passif (PIR) est situé dans un couloir. Si l'utilisateur fait une mise en service partielle du système pendant la nuit et qu'il descend les escaliers à ce moment-là, il peut activer par inadvertance le capteur PIR du couloir et déclencher l'alarme. Si l'utilisateur paramètre l'option Attribut zones d'accès, l'avertisseur sonore retentit pendant la temporisation d'entrée lorsque le capteur PIR est activé, ce qui avertit l'utilisateur que l'alarme va s'activer si aucune action n'est engagée.
Zones type Entrée/Sortie :	Cliquez sur la case appropriée pour passer les zones d'entrée / de sortie en zones d'alarme durant un mode MES Partielle A ou B. Cette fonction est utile pour une installation résidentielle lorsque le système a été configuré en mode MES Partielle. A utiliser si le système est mis en surveillance partielle la nuit et si l'utilisateur souhaite le déclenchement immédiat de l'alarme dès que la porte principale ou la porte de derrière est ouverte en pleine nuit.
Attribut Zones locales :	cochez la case correspondante pour limiter la transmission des alarmes en mode MES Partielle au niveau local (pas de transmission à distance).
Pas de sirène	Si coché, aucune sirène ne sera activé pour une MES / MHS partielle de A ou B.

Secteurs liés

Cette section vous permet de lier des secteurs pour une mise en service ou une mise hors service :

MES totale	MES totale de ce secteur lorsque tous les secteurs liés sont en MES totale.
MES totale de tous	MES totale de tous les secteurs lorsque ce secteur est en MES totale.
Empêche la MES totale	Empêche la MES totale de ce secteur si tous les secteurs liés sont en MES totale.
Empêche la MES totale de tous	Empêche la MES totale des secteurs liés si ce secteur n'est pas en MES totale.
Mise hors surveillance	MHS de ce secteur quand tous les secteurs liés sont MHS.
MHS de tous	MHS de tous les secteurs quand ce secteur est MHS.
Empêche la MHS	Empêche la MHS de ce secteur si un des secteurs lié est en MES totale.
Empêche la MHS de tous	Empêche la MHS des secteurs liés si ce secteur est en MES totale.
Autorise les MES	Activer l'activation autorisée pour les zones liées. Reportez-vous à Autorise les MES pour le verrouillage de blocage.
Secteurs liés	Cliquez sur les secteurs que vous souhaitez lier à ce secteur.

Planifier

Configurez la planification avec les paramètres suivants :

Calendrier	Sélectionnez un calendrier pour contrôler la planification.

Mise hors surveillance	Sélectionnez si le secteur doit passer automatiquement MHS pour la durée indiquée dans le calendrier sélectionné.
MES totale	Sélectionnez cette option pour la MES totale du secteur pour la durée indiquée dans le calendrier sélectionné. Ce secteur sera également activé lorsque le temps de MHS ou la Durée du retard sera écoulé (voir *Mise en / hors surveillance* page 284). Si la durée de la MHS temporaire dépasse la durée planifiée, le secteur utilisera les paramètres du calendrier.
Verrouillage horaire	Sélectionnez cette option pour le verrouillage horaire du secteur selon le calendrier sélectionné. (Secteur de type chambre forte en mode Financier uniquement)
Accès avant verrouillage	Entrez le nombre de minutes (0 – 120) pour activer la temporisation à la fin de la période de MHS verrouillée. Si le secteur ne peut pas être mis hors surveillance lorsque cette temporisation expire, le secteur ne pourra pas être mis hors surveillance avant le démarrage de la nouvelle période de MHS verrouillée. (Secteur de type chambre forte en mode Financier uniquement)

Rapports

Les paramètres de configuration du Reporting sont applicables pour les secteurs standards dans les installations commerciales et bancaires uniquement et ne sont applicables que si un calendrier a été sélectionné. (Consultez *Planifier* à la page précédente .)

Ces paramètres permettent d'envoyer un rapport au Centre de contrôle ou à une personne désignée si la centrale est mise en ou hors service en dehors des périodes définies du calendrier.

MES trop tôt	Permet d'envoyer un rapport si la centrale passe manuellement en MES totale avant une MES planifiée et avant l'écoulement du temps en minutes saisi dans le champ Temporisation.
MES trop tard	Permet d'envoyer un rapport si la centrale passe manuellement en MES totale après une MES planifiée et après l'écoulement du temps en minutes saisi dans le champ Temporisation.
MHS trop tôt	Permet d'envoyer un rapport si la centrale passe manuellement en MHS avant une MHS planifiée et avant l'écoulement du temps en minutes saisi dans le champ Temporisation.
MHS trop tard	Permet d'envoyer un rapport si la centrale passe manuellement en MHS avant une MHS planifiée et avant l'écoulement du temps en minutes saisi dans le champ Temporisation.

Le reporting est effectué par SMS, ou au CTS par SIA et Contact ID. Un événement est également enregistré dans le journal système.

Seuls les événements configurés pour un reporting tardif ou précoce pour le secteur seront signalés.

Le reporting d'un événement doit également être activé pour un CTS ou un SMS, comme indiqué dans les sections suivantes.

Activation du reporting d'une MES/MHS inhabituelle pour un CTS

Pour configurer une transmission pour un CTS configuré pour communiquer par SIA ou par CID, sélectionnez **Communications > Transmission > CTS analogique > Éditer > Filtrer** pour afficher l'écran Filtres d'événements pour un CTS.

Le paramètre **Trop tôt/tard** est activé pour la transmission de toute MES/MHS se produisant hors plages.

Activation du reporting d'une MES/MHS inhabituelle pour SMS

Les événements SMS peuvent être configurés en utilisant les configurations Installateur et Utilisateur.

Pour la configuration Installateur, sélectionnez **Utilisateurs -> SMS Utilisateurs > SMS installateur > Éditer**.

Activez Trop tot/Trop tard pour signaler toutes les activations et désactivations qui ne sont pas incluses dans la planification.

Mise en / hors surveillance

Les paramètres suivants (à l'exception du paramètre Interverrouillage) ne sont pertinents que dans les cas suivants :

- Un calendrier est sélectionné (voir*Planifier* page 281), ou
- **Durée de la MHS** est activé (valeur supérieure à zéro), ou
- Les deux conditions ci-dessus sont réunies.

Présign. MES auto	Saisissez la durée en minutes de la présignalisation avant la MES automatique. (0-30) Notez que la centrale se met en service soit à l'heure planifiée, soit à l'heure définie par le paramètre MHS retardée. Le premier signal s'affiche pendant le délai configuré avant l'heure planifiée. D'autres signaux sont envoyés une minute avant l'heure de MES.
Arrêt MES auto	Permet à l'utilisateur d'annuler la MES auto en saisissant un code sur le clavier.
Dérog. MES auto	Permet à l'utilisateur de retarder la MES auto en saisissant un code sur le clavier.
Boîtier à clé	Autorise le décalage de la MES automatique à l'aide d'un transpondeur à boîtier à clé.
Durée du retard	Saisissez le nombre de minutes de décalage de la MES automatique. (1-300)
Nombre de dérogations	Saisissez le nombre de fois que la MES automatique peut être retardée. (0–99 : 0 = illimité)
MHS retardée	Saisissez le nombre de minutes de décalage de la MHS. (0 = pas de décalage)
Groupe Interverrouillage	Sélectionner un Groupe Interverrouillage à affecter à ce secteur. L'interverrouillage ne permet de mettre hors service à un instant donné qu'un seul secteur à la fois au sein du groupe. Fonction typiquement utilisée dans les secteurs DAB.
Durée de la MHS temporaire	Temps maxi que ce secteur restera en MHS avant qu'il ne repasse automatiquement en MES. (Plage 0–120 min : 0 = non activé).
Double code	Si cette option est activée, deux codes sont nécessaires pour mettre en ou hors service le secteur avec le clavier. Les deux codes doivent appartenir à des utilisateurs ayant les droits requis pour cette opération (mise en ou hors service). Si le deuxième code n'est pas saisi au bout de 30 secondes, ou s'il est erroné, le secteur ne peut alors pas être mis en ou hors service.
Mode MES forcée	Options de secteur pour une MES forcée (normale ou bloquée).
RAZ des alarmes à la MES Forcée	Cliquez sur cette option pour effacer les mémoires d'alarme lors de la mise en service forcée (pour les zones au repos). Si cette option est sélectionnée, lorsqu'une alerte est active ou qu'un secteur a besoin d'être restauré, il le sera automatiquement.

Fonctionnement avec travail en soirée

Un exemple d'utilisation des paramètres de mise en et hors service concerne les situations de travail en soirée où un calendrier est configuré pour une mise en service automatique à un moment particulier, mais les employés doivent occasionnellement travailler tard et le paramétrage automatique doit être retardé.

Chaque retard est défini par la valeur configurée dans le paramètre **Durée du retard**, et le paramètre **Nombre de dérogations** détermine le nombre de fois où la mise en service peut être retardée. Une valeur correcte doit figurer dans **Dérog. MES auto** pour que l'utilisateur puisse se servir de cette fonction.

Il existe trois façons de retarder la mise en service :

1. Saisie du code sur le clavier.
   RETARD est une option du menu sur le clavier standard. La fonction retard peut être utilisée à l'aide des boutons de la partie supérieure du clavier « Confort »
2. Utilisation du boîtier à clé.
   En tournant la clé vers la droite, on retarde la MES du système du délai configuré si le nombre maximal de fois où la MES peut être retardée (**Nombre de dérogations**) n'a pas été dépassé. En tournant la clé vers la gauche, on paramètre le retard à trois minutes (non configurable). Ceci peut être fait indépendamment du nombre de fois où la MES a été retardée.
3. Utilisation d'une télécommande, d'un WPA ou d'un bouton qui active le déclenchement de **Dérog. MES auto**.

MHS temporaire

Pour pouvoir mettre hors service temporairement un système lors d'une période spécifiée par un calendrier, les trois paramètres suivants doivent être configurés :

1. **Calendrier**
   Un calendrier doit être configuré et sélectionné pour ce secteur.
2. **Verrouillage horaire**
   Cette case doit être cochée pour que le secteur puisse être mis hors service uniquement lorsque c'est autorisé par le calendrier configuré.
3. **Durée de la MHS**
   Ce paramètre doit être supérieur à zéro pour définir une limite maximale de durée de mise hors service du secteur.

All Okay

« Tout va bien » requis	Si sélectionné, l'utilisateur doit confirmer que « Tout va bien », sinon une alarme discrète sera générée. Consultez *Édition d'une zone* page 277 pour plus de détails sur la configuration de l'entrée « Tout va bien ».
Tempo du TVB	Temps (seconde) pour activer l'entrée TVB avant qu'une alarme discrète ne soit générée. (Plage : 1–999 secondes)
Événement TVB	Sélectionnez le type d'événement à déclencher à l'expiration du délai de « Tout va bien ». Les options sont Panique (silencieuse), Panique et Contrainte.

Sortie Radio

Durée activation sortie RF	Saisissez le nombre de secondes pendant lesquelles la sortie RF sera activée. Une valeur de 0 seconde active / désactive la sortie.

Zones d'évacuation incendie

Zones d'évacuation incendie	Sélectionnez les portes qui s'ouvriront en cas d'incendie dans ce secteur. Cette option n'est pas affichée en mode simple.

Déclencheurs du secteur

La section Déclencheurs s'affiche si les déclencheurs ont été préalablement définis. (Consultez *Déclencheurs* page 298.)

Cliquez sur le bouton **Éditer** pour ajouter, éditer ou supprimer des conditions de déclenchement pour le secteur. La page suivante apparaît :

Configurez le déclencheur pour le secteur à l'aide des paramètres suivants :

Déclencheur	Sélectionnez un déclencheur dans la liste déroulante.
Front	Le déclencheur peut s'activer du côté positif ou négatif du signal d'activation.
Action	C'est l'action réalisée lorsque le déclencheur est activé. Les options sont les suivantes : • Mise hors surveillance • MES Partielle A • MES Partielle B • MES totale • Dérog. MES auto Cette action retarde la mise en service de l'alarme lorsque la temporisation de MES auto est opérationnelle. Le déclencheur n'ajoute du temps que si la Limite de retard n'a pas été dépassée ; chaque activation du déclencheur retarde la mise en service de la durée définie dans Durée du retard (voir *Mise en / hors surveillance* page 284). • RAZ des alarmes Cette action annule toutes les alarmes dans la zone configurée.

Remarque : les déclencheurs ne peuvent pas être configurés à partir d'un clavier.

Voir également

Déclencheurs page 298

17.9.5.3 Éditer une porte

1. Sélectionnez **Configuration > Portes**.

   La liste des portes configurées s'affiche.
2. Cliquez sur le bouton **Modifier**.
3. Configurez les champs comme indiqué dans les fenêtres ci-dessous.

Entrées de porte

Chaque porte dispose de deux entrées avec deux fonctionnalités prédéfinies. Ces deux entrées – le détecteur de position et le bouton d'ouverture de la porte – peuvent être configurées.

Nom	Description
Zone	L'entrée de détecteur de position de porte peut aussi être utilisée pour les fonctions « intrusion ». Si l'entrée de détecteur de position de porte est utilisée pour les fonctions « intrusion », sélectionnez le numéro de zone auquel l'entrée est attribuée. Si le détecteur de position de la porte est utilisé uniquement pour la partie accès, l'option « NON AFFECTÉE » doit être sélectionnée. Si le détecteur de position de la porte est affecté à une zone d'intrusion, il peut être configuré comme une zone normale, mais uniquement avec des fonctionnalités limitées (par exemple, tous les types de zones ne peuvent pas être sélectionnés). Si un secteur ou le système est activé avec le lecteur de badge, l'entrée du détecteur de position de la porte doit être affectée à un numéro de zone et au secteur/système qui doit être activé.
Description (Web uniquement)	Description de la zone à laquelle est affecté le détecteur de position de la porte.
Type de zone (Web uniquement)	Type de zone pour la zone à laquelle le détecteur de position de porte est affecté (tous les types de zones ne sont pas disponibles).
Attributs zone (Web uniquement)	Les attributs de la zone à laquelle est affecté le détecteur de position de porte peuvent être modifiés.
Zone (Web uniquement)	Le secteur auquel la zone et le lecteur de badge sont affectés. (Si le lecteur de badge est utilisé pour l'activation et la désactivation, ce secteur sera activé/désactivé.)
Position porte (web) Résistance fin de ligne DPS (claviers)	La résistance utilisée avec le détecteur de position de porte. Sélectionnez une résistance / une association de résistances.
DPS normalement ouvert	Indique si le bouton d'ouverture de porte est une entrée normalement ouverte ou non.
Libération porte (Web) DRS RES.FIN LIGN (claviers)	La résistance utilisée avec le bouton d'ouverture de porte. Sélectionnez une résistance / une association de résistances.
DRS normalement ouvert	Indique si le bouton d'ouverture de porte est une entrée normalement ouverte ou non.

Nom	Description
Pas de DRS (Web uniquement)	Sélectionnez pour ignorer le DRS. Si un DC2 est utilisé sur la porte, cette option DOIT être sélectionnée. Si elle n'est pas sélectionnée, la porte s'ouvrira.
Localisation du Lecteur (Entrée/Sortie) (Web uniquement)	Sélectionnez l'emplacement des lecteurs d'entrée et de sortie.
Formats de lecture (web) INFO LECTEUR (claviers)	Affiche le format du dernier badge lu avec chaque lecteur configuré.

Chaque numéro disponible peut être attribué à une zone, mais l'affectation n'est pas déterminée. Si le numéro 9 est affecté à une zone, celle-ci et un transpondeur d'entrée avec l'adresse 1 sont connectés au X-BUS (qui utilise les numéros de zones compris entre 9 et 16). La zone affectée à partir du contrôleur double porte est déplacée vers le prochain numéro disponible. La configuration est adaptée en conséquence.

Attributs de porte

Si aucun attribut n'est actif, on peut utiliser une carte en cours de validité.

Attribut	Description
Badge inutilisé	Le badge est bloqué provisoirement.
Groupe de portes	Utilisé lorsque plusieurs portes sont assignées au même secteur ou quand les fonctionnalités antipassback, gardien ou interverrouillage sont requises.
Badge et code	L'accès est possible seulement avec un badge et un code PIN.
Code seulement	Un code PIN est requis. Le badge n'est pas accepté.
Code PIN ou Badge	L'accès est possible seulement avec un badge ou un code PIN.
Code pour sortir	Code requis sur le lecteur de sortie. La porte doit posséder un lecteur d'entrée et un lecteur de sortie.
Code pour MES/MHS	Le code PIN est requis pour armer (MES) ou désarmer (MHS) le secteur lié. Le badge doit être présenté avant de saisir le code.

Attribut	Description
MHS à l'extérieur (navigateur)	Le secteur sera mis à l'arrêt lorsqu'un badge est présenté sur le lecteur d'entrée.
MHS à l'intérieur (navigateur)	Le secteur sera mis à l'arrêt lorsqu'un badge est présenté sur le lecteur de sortie.
Accès si MES	L'accès est autorisé si le secteur est en MES et que la porte est de type zone d'alarme ou zone d'entrée.
MES à l'extérieur (navigateur)	Le secteur sera mis en surveillance lorsqu'un badge est présenté deux fois sur le lecteur d'entrée.
MES sur lecteur de sortie	Le secteur sera mis en surveillance lorsqu'un badge est présenté deux fois sur le lecteur de sortie.
Forcer MES totale	Si l'utilisateur possède les droits correspondants, il peut forcer le réglage du lecteur d'entrée.
Urgence	La porte est déverrouillée automatiquement en cas de détection d'un incendie dans le secteur attribué.
Évacuat. globale	Un incendie dans un secteur quelconque déverrouille la porte.
Escorte	La fonction Escorte permet à des détenteurs de badge à accès privilégié d'escorter d'autres détenteurs de badge à travers certaines portes. Quand cette fonction est appliquée à une porte, un badge avec des « droits d'escorte » doit être présenté en premier, puis les autres détenteurs de badge ne possédant pas ce privilège peuvent ouvrir cette même porte. Le délai entre la présentation du badge d'escorte et celle du badge normal est configuré pour chacune des portes.
Anti-passback*	La fonction antipassback (protection physique) doit être activée sur la porte. Toutes les portes doivent posséder un lecteur d'entrée et un lecteur de sortie, et doivent faire partie d'un groupe de portes. Dans ce mode, les détenteurs de badge doivent utiliser leur badge pour entrer et sortir d'un espace défini par un groupe de portes. Si un détenteur de badge valide présente son badge pour entrer dans un espace mais qu'il ne le présente pas pour en sortir, il viole les règles d'antipassback. La prochaine fois qu'il tentera de pénétrer dans le même espace, une alarme d'antipassback réelle est déclenchée, l'empêchant ainsi d'entrer dans le groupe de portes.
Antipassback soft*	Les violations des règles d'antipassback sont seulement journalisées. Toutes les portes doivent posséder un lecteur d'entrée et un lecteur de sortie, et doivent faire partie d'un groupe de portes. Dans ce mode, les détenteurs de badge doivent utiliser leur badge pour entrer et sortir d'un espace défini par un groupe de portes. Si un détenteur de badge valide présente son badge pour entrer dans un espace mais qu'il ne le présente pas pour en sortir, il viole les règles d'antipassback. La prochaine fois qu'il tentera de pénétrer dans le même groupe de portes, une alarme d'antipassback logiciel est déclenchée. Cependant, le détenteur de badge pourra entrer dans ce groupe de portes.

Attribut	Description
Gardien*	La fonction Gardien permet à un détenteur de badge ayant le privilège de gardien (le gardien) d'accompagner dans une pièce d'autres détenteurs de badge n'ayant pas ce privilège. Le gardien doit pénétrer dans une pièce en premier. Les autres personnes ne sont autorisées à entrer dans la pièce que si le gardien s'y trouve déjà. Le gardien n'est pas autorisé à quitter la pièce tant qu'il reste un non-gardien.
Buzzer porte	Le buzzer monté sur la carte de circuit imprimé du contrôleur de porte retentit en cas d'alarme sur une porte.
Ignorer les portes forcées	L'ouverture forcée d'une porte est ignorée.
Group. Interver. * (navigateur)	Une seule porte d'un seul secteur peut être ouverte à la fois. Groupe Portes requis.
Préfixe de MES	Utilisation des touches (A, B, * ou #) en préfixe pour armer le système

* Groupe Portes requis.

Timers porte

Durée	Min.	Max.	Description
Accès autorisé	1 s	255 s	Durée pendant laquelle la porte reste ouverte après que l'accès est autorisé.
Accès refusé	1 s	255 s	Durée après laquelle le contrôleur sera de nouveau prêt, après un événement invalide.
Porte ouverte	1 s	255 s	Temps avant lequel la porte doit être fermée pour éviter une alarme « Porte ouverte trop longtemps ».
Porte restée ouverte	1 min	180 min	Temps avant lequel la porte doit être fermée pour éviter une alarme « Porte laissée ouverte ».
Extension de temps	1 s	255 s	Temps additionnel après avoir autorisé l'accès à un badge disposant d'un attribut d'extension de temps.
Escorte	1 s	30 s	Durée pendant laquelle, après avoir présenté un badge avec un attribut Escorte en accompagnement d'un utilisateur sans droit d'escorte, il est possible de franchir la porte.

Calendrier porte

Porte verrouillée	Sélectionnez un calendrier pour verrouiller la porte pendant la durée configurée. Aucun badge/code ne sera accepté pendant cette période.
Porte verrouillée	Sélectionnez un calendrier pour déverrouiller la porte. La porte sera déverrouillée pendant la durée configurée.

Déclencheurs de porte

Déclencheur	Description
Déclenchement qui déverrouillera momentanément la porte	Si le déclenchement affecté est activé, la porte se déverrouillera pendant une période définie avant de se verrouiller à nouveau.
Déclencheur qui verrouille la porte	Si le déclencheur affecté est activé, la porte est verrouillée. Aucun badge/code n'est accepté.
Déclencheur qui déverrouille la porte	Si le déclencheur affecté est activé, la porte est déverrouillée. Aucun badge/code n'est nécessaire pour ouvrir la porte.
Déclencheur qui affecte un mode normal à la porte	Si le déclencheur affecté est activé, la porte revient en fonctionnement normal. Cela permet d'annuler le verrouillage/déverrouillage de la porte. Un badge est nécessaire pour ouvrir la porte.

Interverrouillage de portes

La fonction Interverrouillage de portes empêche les autres portes d'un groupe d'interverrouillage de s'ouvrir si l'une quelconque des portes du groupe est ouverte.

Ci-dessous figure un exemple de la manière dont cette fonction est utilisée :

- Dans les systèmes d'entrée à double porte utilisés dans certains bâtiments et banques. Généralement, des boutons-poussoirs ou des lecteurs de badge sont utilisés pour obtenir l'accès, et des LED rouges et vertes indiquent si la porte peut être ouverte ou pas.
- Dans les zones techniques de DAB qui relient plusieurs portes de DAB. Typiquement, outre la porte qui donne accès à la zone, toutes les portes de DAB doivent être interverrouillées.

Pour créer un groupe de portes :

1. Créer un Groupe de portes. Voir *Éditer une porte* page 286.
2. Définissez l'attribut **Interverrouillage** pour les portes concernées dans le groupe. Voir *Éditer une porte* page 286.
3. Configurez une sortie de porte pour pouvoir utiliser l'interverrouillage de portes. Cette sortie s'active pour toutes les portes du groupe d'interverrouillage lorsqu'une porte appartenant au groupe est ouverte, y compris la porte ouverte elle-même.
   Cette sortie peut par exemple être connectée à un voyant ou une LED rouge pour signaler que la porte ne peut pas être ouverte et, dans le cas inverse, à un voyant ou une LED vert.

Pour configurer une sortie pour l'interverrouillage de portes.

1. En mode paramétrage, sélectionnez **Configuration > Hardware > X-Bus > Transpondeurs**.
2. Sur la page **Configuration transpondeur**, cliquez sur le bouton **Changer de type** pour la sortie requise.
3. Sélectionnez **Porte** comme type de sortie.
4. Sélectionnez la porte requise et **Interverrouillé** comme type de sortie.

17.9.5.4 ng to slaAjout d'un groupe de secteurs

Vous pouvez utiliser les groupes de secteurs pour configurer plusieurs secteurs. La configuration ne doit donc pas être faite pour chaque secteur individuel.

Prérequis

- Uniquement si l'option (multiples) Secteurs est activée.

1. Sélectionnez **Paramètre > Secteurs > Groupes Secteur**.

2. Cliquez sur le bouton **Ajouter**.
3. Entrez une description pour le groupe.
4. Sélectionnez les secteurs qui sont affectés à ce groupe.
5. Cliquez sur **Ajouter** .

REMARQUE : pour pouvoir gérer les groupes de secteurs avec le clavier Confort, activez tous les secteurs dans le champ **Secteurs** sous **Configuration > Matériel > X-BUS > Claviers > Type : clavier Confort**.

17.9.6 Calendriers

Les calendriers servent à planifier le contrôle horaire des opérations de plusieurs centrales, comme suit :

- MES et/ou MHS automatiques
- MES et/ou MHS automatiques des opérations d'une autre centrale, notamment déclencheurs, activation d'utilisateurs, de zones, de sorties physiques, etc.

Pour une heure donnée, toute planification dans un calendrier peut être active si les conditions horaires s'y référant sont respectées.

Chaque semaine de l'année se voit affecter un nombre ordinal. En fonction de la position des jours, il peut y avoir 52 ou 53 semaines dans une année. Le système de numération du calendrier SPC respecte la norme internationale ISO8601.

Configuration des calendriers

- Sélectionnez **Configuration > Calendriers**.

  Une liste des calendriers configurés s'affiche :

Actions exécutables

Ajouter	Ajouter un nouveau calendrier.
Exceptions	Configurez les horaires définis pour les circonstances exceptionnelles en dehors des horaires hebdomadaires normaux.
Éditer/Afficher	Edite ou affiche le calendrier sélectionné.
Effacer	Efface le calendrier sélectionné. Le calendrier ne peut pas être supprimé s'il est actuellement affecté à un élément de la configuration SPC, ç.-à-d. une zone, un secteur, un profil utilisateur, une sortie, un déclencheur, une porte ou un composant X-BUS. Un message s'affiche indiquant l'élément affecté.

Un calendrier général créé à l'aide de SPC Manager ne peut pas être supprimé, comme illustré sur le calendrier 3 ci-dessus.

17.9.6.1 Ajouter/Éditer un calendrier

1. Sélectionnez **Configuration > Calendriers > Ajouter**.

   La page suivante s'affiche :

Semaine No.	Jour Début - Jour Fin	Semaine type	Semaine No.	Jour Début - Jour Fin	Semaine type
Semaine 1:	02/01/2017 - 08/01/2017	Type 1	Semaine 28:	10/07/2017 - 16/07/2017	Type 1
Semaine 2:	09/01/2017 - 15/01/2017	Type 1	Semaine 29:	17/07/2017 - 23/07/2017	Type 1
Semaine 3:	16/01/2017 - 22/01/2017	Type 1	Semaine 30:	24/07/2017 - 30/07/2017	Type 1
Semaine 4:	23/01/2017 - 29/01/2017	Type 1	Semaine 31:	31/07/2017 - 06/08/2017	Type 1
Semaine 5:	30/01/2017 - 05/02/2017	Type 1	Semaine 32:	07/08/2017 - 13/08/2017	Type 1
Semaine 6:	06/02/2017 - 12/02/2017	Type 1	Semaine 33:	14/08/2017 - 20/08/2017	Type 1
Semaine 7:	13/02/2017 - 19/02/2017	Type 1	Semaine 34:	21/08/2017 - 27/08/2017	Type 1
Semaine 8:	20/02/2017 - 26/02/2017	Type 1	Semaine 35:	28/08/2017 - 03/09/2017	Type 1
Semaine 9:	27/02/2017 - 05/03/2017	Type 1	Semaine 36:	04/09/2017 - 10/09/2017	Type 1
Semaine 10:	06/03/2017 - 12/03/2017	Type 1	Semaine 37:	11/09/2017 - 17/09/2017	Type 1
Semaine 11:	13/03/2017 - 19/03/2017	Type 1	Semaine 38:	18/09/2017 - 24/09/2017	Type 1
Semaine 12:	20/03/2017 - 26/03/2017	Type 1	Semaine 39:	25/09/2017 - 01/10/2017	Type 1
Semaine 13:	27/03/2017 - 02/04/2017	Type 1	Semaine 40:	02/10/2017 - 08/10/2017	Type 1
Semaine 14:	03/04/2017 - 09/04/2017	Type 1	Semaine 41:	09/10/2017 - 15/10/2017	Type 1
Semaine 15:	10/04/2017 - 16/04/2017	Type 1	Semaine 42:	16/10/2017 - 22/10/2017	Type 1
Semaine 16:	17/04/2017 - 23/04/2017	Type 1	Semaine 43:	23/10/2017 - 29/10/2017	Type 1
Semaine 17:	24/04/2017 - 30/04/2017	Type 1	Semaine 44:	30/10/2017 - 05/11/2017	Type 1
Semaine 18:	01/05/2017 - 07/05/2017	Type 1	Semaine 45:	06/11/2017 - 12/11/2017	Type 1
Semaine 19:	08/05/2017 - 14/05/2017	Type 1	Semaine 46:	13/11/2017 - 19/11/2017	Type 1
Semaine 20:	15/05/2017 - 21/05/2017	Type 1	Semaine 47:	20/11/2017 - 26/11/2017	Type 1
Semaine 21:	22/05/2017 - 28/05/2017	Type 1	Semaine 48:	27/11/2017 - 03/12/2017	Type 1
Semaine 22:	29/05/2017 - 04/06/2017	Type 1	Semaine 49:	04/12/2017 - 10/12/2017	Type 1
Semaine 23:	05/06/2017 - 11/06/2017	Type 1	Semaine 50:	11/12/2017 - 17/12/2017	Type 1
Semaine 24:	12/06/2017 - 18/06/2017	Type 1	Semaine 51:	18/12/2017 - 24/12/2017	Type 1
Semaine 25:	19/06/2017 - 25/06/2017	Type 1	Semaine 52:	25/12/2017 - 31/12/2017	Type 1
Semaine 26:	26/06/2017 - 02/07/2017	Type 1	Semaine 53:	01/01/2018 - 07/01/2018	Type 1
Semaine 27:	03/07/2017 - 09/07/2017	Type 1			

2. Saisissez une **Description** pour le calendrier (16 caractères maxi).

Copie d'un calendrier

Pour faire une copie de cette structure de calendrier, cliquez sur le bouton **Dupliquer**.

Un nouveau calendrier est créé avec la même configuration que le calendrier d'origine. Vous pouvez fournir une nouvelle description du nouveau calendrier et éditer la configuration de celui-ci comme requis.

Type de semaine

Assignez un type de semaine à chaque semaine du calendrier pour le configurer. Trois semaines types peuvent être définies au maximum pour chaque calendrier. Toutefois, une semaine n'appartient pas obligatoirement à l'un des types (si aucun type n'est appliqué à la semaine, elle est du type « Aucun »). Il existe au maximum 64 configurations de calendrier dans le système.

Pour définir une semaine type

1. Cliquez sur **Prog des semaines types**.
2. Entrez l'heure souhaitée d'activation/désactivation ou de déclenchement. Utilisez les délais de MES/MHS automatique de secteurs (voir *MES/MHS automatiques de secteurs* page 296) ou de MES/MHS automatique pour d'autres opérations de centrale (voir *Autres actions des calendriers* page 296).

   On peut configurer trois programmes de semaine type au maximum.
3. Cliquez sur **Enregistrer**, puis sur **Retour**.

4. Sélectionnez la semaine type souhaitée dans le menu déroulant pour toutes les semaines planifiées du calendrier.
5. Cliquez sur **Enregistrer**.
6. Cliquez sur **Retour**.

Voir également

MES/MHS automatiques de secteurs à la page suivante

Autres actions des calendriers à la page suivante

Exceptions

Les exceptions et les jours exceptionnels servent à configurer les horaires définis automatiques en circonstances exceptionnelles, hors de la planification hebdomadaire normale définie dans les calendriers. Les exceptions sont définies par des dates de début et de fin de période (jour/mois/année), 4 périodes horaires d'activation/désactivation pouvant être fixées au maximum pour les différentes opérations de la centrale, y compris la MES/MHS de secteurs ou l'activation/désactivation de déclencheurs ou de sorties. 64 exceptions au maximum peuvent être configurées sur le système.

Les exceptions sont des entités génériques pouvant être affectées à un ou à plusieurs calendriers. Quand une exception est associée à un calendrier, les dates définies sont prioritaires par rapport aux autres configurations, les dates de début et de fin faisant toujours partie de l'exception.

Programmation des jours d'exception

1. Sélectionnez **Configuration > Calendriers > Jours d'exception > Ajouter**.

   La page suivante s'affiche.

2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Description	Entrez le nom de l'exception (16 caractères maximum).
Date de début/Date de fin	Sélectionnez la date de début et de fin.
Période activée/Période désactivée	Entrez l'heure souhaitée d'activation/désactivation ou de déclenchement. Utilisez les délais de MES/MHS automatique de secteurs (voir *MES/MHS automatiques de secteurs* ci-dessous) ou de MES/MHS automatique pour d'autres opérations de centrale (voir *Autres actions des calendriers* ci-dessous).
Calendriers	Sélectionnez le ou les calendriers désirés pour prise d'effet.

AVERTISSEMENT : les jours d'exception généraux créés à distance avec l'interface SPC Manager ne peuvent être effacés ni supprimés.

17.9.6.2 MES/MHS automatiques de secteurs

Un calendrier peut être configuré pour les MES ou MHS automatiques de secteur.

Pour un jour quelconque de la semaine, une configuration peut avoir un maximum de 4 temps de MES et 4 temps de MHS. Les temps configurés sont exprimés sur 24 h (hh:mm). Par exemple, si l'heure fixée est minuit, le format saisi doit être 24:00. Il est possible de définir une heure de MES sans la MHS correspondante, et vice-versa. Les temps configurés déclenchent la mise en ou hors service du secteur (sous réserve que toutes les conditions soient satisfaites). Les temps saisis ne correspondent pas des périodes, mais à des instants déterminés ou l'action précisée (MES/MHS) se produira. Si le contrôleur est mis sous tension ou réinitialisé, le statut MES/MHS est conservé et les déclenchements suivants de MES ou MHS se produisent en respectant la configuration.

17.9.6.3 Autres actions des calendriers

Les opérations de la centrale, y compris les déclencheurs, l'activation d'utilisateurs, de zones et de sorties physiques peuvent être automatiquement activées ou désactivées avec les configurations d'états On/Off, Vrai/Faux ou Actif/Inactif.

Les états On/Off, Vrai/Faux, Actif/Inactif peuvent être attribués à une sortie qui est réellement activée/désactivée et qui peut être configurée pour chaque jour de la semaine. Les configurations ont au maximum 4 heures d'activation et 4 heures de désactivation. Les temps configurés sont exprimés sur 24 h (hh:mm). Par exemple, si l'heure fixée est minuit, le format saisi doit être 24:00. Chaque configuration crée une paire de réglages pour un état On/Off, Vrai/Faux, Actif/Inactif. Toute configuration sans contrepartie est ignorée.

17.9.7 Modification de son propre code PIN

Pour modifier un code, consultez *Changement du code Ingénieur et du mot de passe d'accès installateur* page 224.

17.9.8 Configuration des paramètres avancés

Cette section recouvre :

17.9.8.1 Cause et effet

1. Sélectionnez **Configuration > Avancé > Cause et effet**.

   La page suivante s'affiche.

2. Cliquez sur le bouton Affectation pour exécuter l'une des actions suivantes :
   - **Sortie :** affectez une interaction logique (sortie virtuelle) pour déclencher une sortie physique. Sélectionnez cette option pour afficher la page **Interaction logique – Liste**. Pour plus d'informations, consultez *Interactions logiques* ci-dessous.
   - **Secteur :** affectez un déclencheur (entrée virtuelle) pour déclencher une action de secteur. Choisissez un **Secteur** dans la liste déroulante avant de cliquer sur le bouton **Affectation**. Pour plus d'informations, consultez *Déclencheurs* à la page suivante.
   - **Porte :** affectez un déclencheur (entrée virtuelle) pour déclencher une action de porte. Choisissez une **Porte** dans la liste déroulante avant de cliquer sur le bouton **Affectation**.

Pour afficher la liste des déclencheurs et actions configurés, sélectionnez **Configuration > Avancé > Cause et effet > Liste causes et effets**.

La page **Liste causes et effets** n'affiche que les causes et effets totalement fonctionnels. Par exemple, si une interaction logique n'est pas affectée à un déclencheur ou un raccourci clavier, elle ne s'affiche pas dans la liste.

AVERTISSEMENT : votre système n'est pas conforme aux normes EN si vous permettez à un déclencheur d'activer le système sans qu'un code PIN valable soit nécessaire.

17.9.8.2 Interactions logiques

Les déclencheurs sont utilisés avec les interactions logiques, qui sont des sorties virtuelles définies par l'utilisateur et pouvant être reliées à une sortie physique. Le système peut gérer 512 interactions logiques au maximum.

Pour une sortie continue, lorsque le déclencheur est un code utilisateur valide, les deux états doivent être les mêmes, soit négatifs, soit positifs.

1. Sélectionnez **Configuration > Avancé > Cause et effet > Interactions logiques**.

   La page suivante apparaît :

2. Entrez une **Description** pour l'interaction. C'est important car aucun numéro (la description seule de l'interaction logique) n'est affichée sur la page utilisateur **Sorties** pour activer et désactiver l'interaction.
3. Cochez la case **Local** si vous souhaitez ne pas autoriser les utilisateurs à activer et désactiver cette interaction, même s'ils possèdent les droits correspondants. Une interaction locale n'est pas visible à distance.
4. Sélectionnez la **Touche de raccourci** désirée.
   Un raccourci clavier est une combinaison [signe dièse (#) + chiffre] entrée sur le clavier. Si le raccourci est configuré et entré sur le clavier, l'utilisateur est invité à activer ou désactiver la sortie.

De nombreuses sorties peuvent être activées par un raccourci, que ce soit la fonction X-10 ou les interactions logiques.

5. Entrez une **Temporisation**pour l'interaction. L'unité de temps de base est le 1/10 de seconde.
6. Cliquez sur le bouton **Déclencheurs** pour configurer les déclencheurs afin qu'ils activent ou désactivent la sortie. Dans les deux cas, il faut définir un côté positif ou négatif pour le déclencheur. Voir *Déclencheurs* ci-dessous pour la configuration détaillée des déclencheurs.
7. Sélectionnez une sortie dans la liste déroulante.
8. Cliquez sur **Ajouter** pour ajouter une nouvelle interaction ou sur **Sauver** pour sauvegarder les nouveaux paramètres pour une interaction existante.

Voir également

Déclencheurs ci-dessous

17.9.8.3 Déclencheurs

Un déclencheur est un état du système [par exemple, fermeture de zone / heure / événement système (alarme), etc.] qui peut être utilisé en tant qu'entrée pour les Causes et effets. Les déclencheurs peuvent être affectés ensemble de manière logique à l'aide des opérateurs logiques ET/OU afin de créer des sorties utilisateur. Le système prend en charge 1 024 déclencheurs au maximum.

1. Sélectionnez **Configuration > Avancé > Déclencheurs**.

   La page suivante s'affiche.

2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Déclencheur	Le système a généré un numéro pour le nouveau déclencheur. Le déclencheur ne devient actif que si l'une des deux étapes optionnelles (calendrier / limitation de temps) est configurée
Description	Entrez une description textuelle du déclencheur.
Calendrier	Si nécessaire, sélectionnez un calendrier. Si vous en sélectionnez un, le déclencheur ne sera activé que pendant la période du calendrier. Voir *Calendriers* page 292.
Limitation horaire	Sélectionnez une période entre 00:00 et 24:00 pendant laquelle le déclencheur sera seul activé. L'heure de démarrage est inclusive, l'heure de fin est exclusive. **Remarque :** ce paramètre retarde seulement un passage de l'activation à la désactivation du déclencheur. Le passage de la désactivation à l'activation est immédiat.
Durée	Entrez la durée en secondes pendant laquelle les conditions du déclencheur doivent être vérifiées avant que le déclencheur soit activé.
Activation du déclencheur	• **Toutes** Toutes les conditions du déclencheur doivent être valides pour que le système puisse activer le déclencheur. • **Au moins une** Si au moins une condition du déclencheur est valide, le système peut activer le déclencheur.

Actions exécutables

Ajouter	Ajouter les conditions pour le déclencheur. Cliquez sur ce bouton pour ajouter une ou plusieurs conditions au déclencheur sélectionné. Voir *Conditions du déclencheur* à la page suivante.
Exceptions	Configurez les horaires définis pour les circonstances exceptionnelles en dehors des horaires hebdomadaires normaux.
Éditer/Afficher	Edite ou affiche le calendrier sélectionné.
Effacer	Efface le calendrier sélectionné. Le calendrier ne peut pas être supprimé s'il est en cours d'affectation à un élément de configuration SPC, ç.-à-d. une zone, un secteur, un profil utilisateur, une sortie, un déclencheur, une porte ou un composant X-BUS. Un message s'affiche indiquant l'élément affecté.

Conditions du déclencheur

Le tableau suivant liste les conditions du déclencheur et les États, Sorties, Événements ou Communications associés.

Condition du déclencheur	États, Sorties, Événements ou Communications
Zone	Le déclencheur est ACTIF quand les conditions suivantes sont satisfaites (ç.-à-d. lorsqu'une opération logique ET est exécutée) : le déclencheur est ACTIF si la zone configurée se trouve dans l'un des états suivants –**Ouvert**, **Fermé**, **Court-circuit**, ou **Déconnecté**.
Contrôle	Le déclencheur est ACTIF si l'une des options de porte suivantes est configurée : **Entrée acceptée**, **Entrée refusée**, **Sortie acceptée**, **Sortie refusée**, **Porte ouverte trop longtemps**, **Porte restée ouverte**, **Ouverture porte forcée**, **Porte normale**, **Porte verrouillée**, **Porte déverrouillée**.
Sortie	Le déclencheur est ACTIF si la sortie système est dans l'état configuré, qui peut être **On** ou **Off** : **Sortie système**, **Interaction logique**, **Sortie secteur**.
Système	Le déclencheur est actif pour l'événement système choisi et l'ID. Les ID sont : **Redémarrage système**, **Surconsommation**, **Accès installateur**, **Accès construct.,**, **Défaut câble XBUS**, **Défauts Xbus**. **Heure de déclenchement** – le déclencheur est activé à l'heure saisie dans la boîte prévue à cet effet au format hh : mm.
Utilisateur	**Tag radio** – cette condition peut être configurée pour un utilisateur particulier ou pour tous les utilisateurs. Si cette condition est sélectionnée, une impulsion OFF/ON/OFF instantanée est déclenchée quand l'utilisateur configuré (ou n'importe quel utilisateur) appuie sur le bouton '*' de la télécommande. Ceci s'applique uniquement aux boutons déclarés dans le système. **Bouton panique d'une télécommande radio** – cette condition peut être configurée pour un utilisateur particulier ou pour tous les utilisateurs. Si cette condition est sélectionnée, une impulsion OFF/ON/OFF instantanée est déclenchée quand l'utilisateur configuré (ou n'importe quel utilisateur) appuie sur le bouton Panique de la télécommande. Ceci s'applique uniquement aux boutons panique des télécommandes déclarées dans le système. **Code PIN clavier** – cette condition peut être configurée pour un utilisateur particulier ou pour tous les utilisateurs. Avec cette configuration, une impulsion OFF/ON/OFF instantanée est déclenchée quand l'utilisateur configuré (ou n'importe quel utilisateur) saisit un code PIN valide ou présente un TAG configuré. **Badge d'accès** – le déclencheur est activé lorsque l'utilisateur sélectionné se connecte à l'aide d'un badge d'accès. **Accès Web** – le déclencheur est activé lorsque l'utilisateur sélectionné se connecte avec le navigateur Web. **WPA** – le déclencheur est activé si un bouton ou plusieurs boutons sont enfoncés. Il est possible d'affecter une condition de déclencheur à tous les WPA ou à un seul WPA. Lorsqu'un déclencheur est défini avec une condition de déclencheur WPA, il peut être affecté à une interaction logique avec plusieurs objectifs, par exemple la mise en surveillance d'un système, la mise en route de l'éclairage ou l'ouverture d'une porte. **Accès clavier** – le déclencheur est activé lorsqu'un utilisateur quelconque se connecte avec le clavier sélectionné.

Condition du déclencheur	États, Sorties, Événements ou Communications
Profil	**Code PIN clavier** – si un utilisateur ayant un profil d'utilisateur configuré saisit un code PIN valide ou présente un TAG configuré, une impulsion OFF/ON/OFF instantanée est déclenchée. **Badge d'accès** – le déclencheur est activé lorsqu'un utilisateur ayant un profil d'utilisateur configuré se connecte à l'aide d'un badge d'accès. **Accès Web** – le déclencheur est activé lorsqu'un utilisateur ayant un profil d'utilisateur configuré se connecte à l'aide du navigateur Web.
Transpondeur	**Boîtier à clé**– le déclencheur peut être configuré pour une position spécifique de la clé dans le boîtier. **Indicateur** – le déclencheur peut être configuré pour une touche fonction spécifique.
Communication	**FlexC ATP** – le déclencheur est activé par la configuration ATS et ATP sélectionnée. **FlexC ATS** – le déclencheur est activé par la configuration ATS sélectionnée.

AVERTISSEMENT : votre système n'est pas conforme aux normes EN si vous permettez à un déclencheur d'activer le système sans qu'un code PIN valable soit nécessaire.

17.9.8.4 Vérification audio/vidéo

Pour paramétrer une vérification audio/vidéo sur un système SPC :

1. Installez et configurez le ou les transpondeurs audio.
2. Installez et configurez la ou les caméras vidéo.
3. Installez et configurez l'équipement audio.
4. Configurez la ou les zones de vérification.
5. Testez la lecture audio à partir des zones de vérification.
6. Affectez les zones de vérification aux zones physiques.
7. Configurez les paramètres de vérification.
8. Visualisez les images à partir des zones de vérification dans le navigateur Web.

REMARQUE : en fonction de la taille du fichier, les claviers et le contrôle d'accès peuvent être désactivés pendant plusieurs minutes lorsqu'un fichier audio est envoyé à la centrale.

Configuration de la vidéo

Vue d'ensemble

Les caméras sont utilisées pour la vérification vidéo. La centrale SPC peut accepter jusqu'à quatre caméras. Seules les caméras IP sont prises en charge et la centrale doit posséder un port Ethernet.

REMARQUE : les caméras ne sont pas partagées avec les autres applications CCTV.

Les caméras ne peuvent être configurées qu'avec le navigateur Web. La configuration avec le clavier n'est pas possible.

La centrale accepte deux résolutions de caméra :

- 320X240
  Ce réglage est recommandé si vous voulez regarder des images sur le navigateur
- 640X480 (avec quelques restrictions).

Les caméras suivantes sont prises en charge en complément d'autres caméras génériques :

- Vanderbilt CCIC1410 (caméra couleur 1/4" VGA IP)
- Vanderbilt CFMC1315 (caméra dôme d'intérieur couleur 1/3" 1.3 MP)

Une ligne de commande est disponible par défaut pour accéder directement aux détails de configuration des caméras ci-dessus. Les autres caméras IP génériques nécessitent une ligne de commande pour être saisies manuellement.

Ajout d'une caméra

1. Sélectionnez **Configuration > Avancé > Vérification > Vidéo**.

   Une liste de toutes les caméras préalablement configurées est affichée, de même que leur statut en ligne ou hors ligne. Une caméra est en ligne si une image a été obtenue de celle-ci dans les 10 secondes précédentes.

2. Cliquez sur le bouton **Ajouter** pour ajouter une nouvelle caméra ou sur **Éditer** pour modifier une caméra existante.

   La page suivante apparaît :

3. Configurez la caméra avec les paramètres suivants :

Camera ID (Identification de la caméra)	ID de caméra générée par le système.

Description	Saisissez une description pour identifier cette caméra.
Type	Sélectionnez l'un des types de caméra suivants : • Générique • Vanderbilt CCIC1410 • Vanderbilt CFMC1315
IP caméra	Entrez l'adresse IP de la caméra.
Port caméra	Saisissez le port TCP que la caméra écoute. La valeur par défaut est 80. **Remarque :** la caméra CCIC1410 peut seulement être utilisée avec le port 80.
Login	Caméras Vanderbilt CCIC1410 et CFMC1315 uniquement. Entrez un nom d'utilisateur de connexion pour la caméra qui sera ajoutée à la ligne de commande ci-dessous lorsque le bouton **Mise à jour ligne de commande** est activé.
Mot de passe	Caméras Vanderbilt CCIC1410 et CFMC1315 uniquement. Entrez un mot de passe de connexion pour la caméra qui sera ajoutée à la ligne de commande ci-dessous lorsque le bouton **Mise à jour ligne de commande** est activé.
Ligne de commande	Saisissez la ligne de commande à envoyer au serveur HTTP sur la caméra afin d'obtenir des images. Cette ligne doit inclure le nom d'utilisateur et le mot de passe pour la caméra. Consultez la documentation de la caméra pour connaître la ligne spécifique requise pour le type de caméra sélectionné. La ligne de commande par défaut pour une caméra Vanderbilt CCIC1410 ou CFMC1315 sans mot de passe est « /cgi-bin/stilljpeg ».
Images pré-événement	Saisissez le nombre d'images pré-événement à enregistrer (0 – 16). La valeur par défaut est 8.
Intervalle pré-événement	Saisissez l'intervalle, en secondes, entre les images pré-événement (1 – 10). La valeur par défaut est 1 seconde.
Images post-événement	Saisissez le nombre d'images post-événement à enregistrer (0 – 16). La valeur par défaut est 8.
Intervalle post-événement	Saisissez l'intervalle, en secondes, entre les images post-événement (1 – 10). La valeur par défaut est 1 seconde.

Configuration des zones de vérification

Pour créer une zone de vérification

1. Allez sur **Configuration > Avancé > Vérification > Zones de vérification**.

   Une liste de toutes les zones de vérification existantes s'affiche.

2. Cliquez sur le bouton **Ajouter**.
3. Entrez une **Description** pour la zone.

4. Sélectionnez un transpondeur **audio** dans la liste déroulante.
5. Sélectionnez une **vidéo** dans la liste déroulante.
6. Cliquez sur le bouton **Enregistrer**.
7. Affectez cette zone de vérification à une zone physique dans le système SPC. (Consultez *Édition d'une zone* page 277.)

Voir également

Édition d'une zone page 277

Configuration des paramètres de vérification

Remarque : les paramètres suivants s'appliquent à toutes les zones de vérification (voir *Configuration des zones de vérification* à la page précédente).

1. Sélectionnez **Configuration > Avancé > Vérification > Audio**.

   La page suivante apparaît :

2. Configurez les paramètres suivants.

Enregistrement avant alarme	Saisissez le temps requis, en seconde, pour l'enregistrement audio pré événement (0 – 120). La valeur par défaut est 10.
Enregistrement après alarme	Saisissez le temps requis, en secondes, pour l'enregistrement audio post-événement (0 – 120). La valeur par défaut est 30.

Affichage des images vidéo

Les images vidéo provenant des caméras configurées peuvent être regardées dans le navigateur Web en modes Paramétrage ou Exploitation. Cette fonctionnalité est également accessible aux utilisateurs qui disposent du droit Voir Vidéo dans leur profil. (Voir *Ajouter/Éditer un utilisateur* page 211.) Les droits d'accès à Internet doivent également être activés pour cette fonction.

Le droit Voir Vidéo peut également être paramétré sur le clavier (paramétrage « Vidéo dans le navigateur »).

Pour voir des images, rendez-vous sur **SPC Accueil > Vidéo**. Voir *Affichage des vidéos* page 192.

Voir également

Ajouter/Éditer un utilisateur page 211

Configuration de la vidéo page 301

17.9.8.5 Mise à jour des licences SPC

La fonction **Options licence** permet à l'utilisateur de mettre à jour ou d'ajouter des fonctionnalités au système SPC, par exemple pour les migrations, lorsque des périphériques installés et non autorisés pour SPC doivent être pris en charge par un contrôleur SPC.

1. Sélectionnez **Configuration > Avancé > Licence**.

2. Contactez l'assistance technique en précisant la fonctionnalité demandée et indiquez la clé de licence en cours telle qu'elle est affichée.

   Si la requête est approuvée, une nouvelle clé de licence est délivrée.

3. Entrez la nouvelle clé de licence dans le champ prévu à cet effet.

17.10 Configurer les communications

Cette section recouvre :

17.10.1 Paramètres de communication **305**
17.10.2 FlexC® **315**
17.10.3 Rapports **336**
17.10.4 Outils PC **349**

17.10.1 Paramètres de communication

Cette section recouvre :

17.10.1.1 Configuration des services de réseaux de la centrale

1. Sélectionnez **Communications > Communications > Services**.

   La page suivante s'affiche.

Services réseau

HTTP activé	☑	Cocher pour activer le serveur web
Port HTTP	443	Port d'écoute du Serveur web
TLS activé	☑	Cocher pour activer le HTTPS pour le Web server
Telnet activé	☐	Cocher pour valider le serveur Telnet
Port Telnet	23	Port d'écoute du Serveur Telnet
SNMP activé	☐	Cocher pour activer le protocole SNMP
Communauté SNMP	public	Id de Communauté du protocole SNMP
ENMP activé	☐	Cocher pour activer Enhanced Network Management Protocol (ENMP)
Port ENMP	1287	Port d'écoute du ENMP
Modif. du mot de passe ENMP	siemens	Mot de passe pour les modifications de congig. réseau via ENMP
Mise à jour ENMP activé	☑	Cocher pour autoriser les modifications de config. réseau via ENMP

2. Configurez les champs comme indiqué dans le tableau ci-dessous.

HTTP activé	Cochez cette case pour activer le serveur Web embarqué sur la centrale.
Port HTTP	Entrez le numéro de port balayé par le serveur Web. Par défaut, il est défini à 443.
TLS validé	Cochez cette case pour activer le chiffrage sur le serveur Web embarqué. Par défaut, il est activé. Lorsque le TLS est activé, on ne peut accéder aux pages Web qu'en tapant le préfixe « https:// » avant l'adresse IP.
Telnet activé	Cochez cette case pour activer le serveur Telnet. (Activé par défaut) **Remarque :** l'utilisation de Telnet sans une compréhension approfondie de celui-ci peut bouleverser la configuration du contrôleur ; l'utilisateur ne doit s'en servir que s'il en a une connaissance suffisante ou s'il est suivi par une personne qualifiée.
Port Telnet	Entrez le numéro du port Telnet.
SNMP activé	Cochez cette case pour activer SNMP (Simple Network Management Protocol). (Désactivé par défaut)
SNMP communauté	Entrez l'ID de communauté pour le protocole SNMP. (Public par défaut)
ENMP activé	Cochez cette case pour activer ENMP (Enhanced Network Management Protocol). (Par défaut : validé en mode Paramétrage)
Port ENMP	Entrez le numéro de port ENMP (par défaut : 1287).
Mot de passe ENMP	Entrez le mot de passe pour l'utilisation du protocole ENMP.
Changements ENMP activés	Cochez cette case pour activer les modifications de réseau à effectuer avec le protocole ENMP.

17.10.1.2 Ethernet

Le port Ethernet du contrôleur peut être configuré à partir de l'interface du navigateur ou de celle du clavier. Une connexion Ethernet avec le contrôleur SPC peut être établie en utilisant une liaison directe ou une liaison dans le réseau local.

1. Sélectionnez **Communications > Communications > Ethernet**.

   La page suivante s'affiche.

2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Adresse IP	Saisissez l'adresse IP de la centrale.
Réseau IP	Indiquez le masque de sous-réseau qui définit le type de structure d'adresse de réseau utilisé sur le LAN.
Adresse IP de la passerelle	Entrez l'adresse IP de la passerelle IP le cas échéant. Il s'agit de l'adresse à travers laquelle seront acheminés les paquets IP pendant l'accès à des adresses IP externes sur Internet.
Activer DHCP	Cliquez sur ce bouton pour activer l'affectation d'adresse dynamique sur la centrale.
Serveur DNS	entrez l'adresse IP du serveur DNS.

17.10.1.3 Configuration des modems

La centrale SPC dispose de deux connecteurs d'interface de modem intégrés (primaire et secours) qui vous permettent d'installer des modules GSM et/ou RTC sur le système.

Lorsqu'elle est en configuration usine, la centrale détecte, pendant la phase de réglage initial du système avec le clavier, si elle est équipée d'un modem primaire ou de secours, affiche dans ce cas le type de modem et l'active (ou les active) automatiquement avec la configuration par défaut. Aucune autre configuration de modem n'est autorisée à ce stade.

Pour programmer les modems :

Remarque : un modem doit être installé et identifié. (Voir section *Installation de modules de raccordement* page 100.)

1. Sélectionnez **Communications > Communications > Modems**.

2. Cliquez sur **Enable** (Activer).

3. Cliquez sur **Configurer**.
   - Si vous avez installé un modem GSM, la page des paramètres du modem GSM s'affiche. Pour plus d'informations, consultez *Modem GSM* à la page suivante.
   - Si vous avez installé un modem RTC, la page des paramètres du modem RTC s'affiche. Pour plus d'informations, consultez *Modem RTC* page 312.

La détection et la configuration SMS ne sont pas disponibles tant que les modems configurés ne sont pas activés.

Test SMS

Lorsque la fonction SIM est activée pour un modem, un test peut être réalisé vers le numéro de l'utilisateur désiré avec un message composé.

1. Saisissez le numéro du téléphone mobile (y compris les trois chiffres du préfixe du pays) dans le champ de numéro et un court message dans la boîte de dialogue.
2. Cliquez sur **Envoyer un SMS** et vérifiez que le message arrive sur le téléphone mobile.

Le test SMS sert uniquement à vérifier que la fonction SMS fonctionne correctement. Utilisez un message court avec des caractères alphabétiques (A-Z) pour tester la fonction.

Le service SMS fonctionne sur la base d'un protocole standard utilisé par les téléphones compatibles SMS. Veuillez noter que certains opérateurs du RTC ne proposent pas le service SMS via le RTC. Pour pouvoir envoyer des SMS dans le RTC, les critères suivants doivent être réalisés :

- Le numéro de téléphone de l'appelant (ID appelant) doit être activé sur la ligne téléphonique.
- Ligne téléphonique directe - ne fonctionne pas via une centrale téléphonique / auto-commutateur privé ni d'autres équipements de télécommunications.
- Notez aussi que la plupart des opérateurs ne prennent pas en charge l'envoi de SMS à des abonnés de l'étranger (pour des questions de facturation).

Fonction SMS

Le contrôleur SPC offre une messagerie à distance (SMS) sur les systèmes ayant des modems installés. Les opérations suivantes sont nécessaires pour configurer la fonction SMS lorsqu'un modem est installé :

- SMS – modem activé.
- Authentification SMS.
- Contrôle SMS installateur.
- Contrôle SMS utilisateur.

Suivant la configuration, les fonctions incluent les ressources suivantes :

- Notification d'évènements.
- Commandes à distance (certaines commandes à distance peuvent être affectées aux utilisateurs).

Options système SMS

Lorsqu'un modem est installé et que la fonction SMS est activée, pour que celle-ci puisse être utilisée, le système SPC doit appliquer l'Authentification SMS.

1. Sélectionnez **Paramètres > Système > Système > Options**.
2. Sélectionnez l'option souhaitée dans la liste déroulante **Authentification SMS** :
   - **Code PIN seulement :** code utilisateur valide. Voir *Création des utilisateurs système* page 123.
   - **ID appelant uniquement :** numéro de téléphone (avec l'indicateur du pays à trois chiffres) tel qu'il est configuré pour le contrôle par SMS par l'utilisateur. Le contrôle par SMS ne pourra être configuré par l'utilisateur que lorsque cette option aura été sélectionnée.
   - **Code PIN et ID appelant**
   - **Code PIN SMS seul :** code valable configuré pour l'utilisateur, différent du code de connexion de l'utilisateur. Le contrôle par SMS ne pourra être configuré par l'utilisateur que lorsque cette option aura été sélectionnée.
   - **CODE PIN SMS et ID appelant**

Commandes SMS

Consultez *Commandes SMS* page 220 pour plus d'informations.

Modem GSM

Prérequis

- Un GSM doit être installé et fonctionner correctement.

1. Sélectionnez **Communications > Communications > Modems**.
2. Cliquez sur **Configurer**.
3. Configurez les champs suivants.

Paramètres modem GSM

Pays	Sélectionnez le pays dans lequel le système SPC est installé.
Code PIN SIM	Entrez le code de la carte SIM installée dans le module GSM.
Technologie radio	**GSM seulement** Sélectionnez le type de signal que vous souhaitez utiliser sur le modem : • **2G uniquement** Cette option active uniquement la connexion sur les réseaux 2G. • **3G uniquement (par défaut)** Cette option active uniquement la connexion sur les réseaux 3G. • **Rechercher du 2G en premier** Cette option force le modem à se connecter aux réseaux 2G lorsqu'ils sont disponibles. Si le 2G n'est pas disponible, le modem se connecte au 3G. • **Rechercher du 3G en premier** Cette option force le modem à se connecter aux réseaux 3G lorsqu'ils sont disponibles. Si le 3G n'est pas disponible, le modem se connecte au 2G.

Analyse opérateur	**Multiréseaux SIM uniquement** Activez cette option pour que le modem recherche tous les réseaux disponibles et se connecte au signal le plus puissant.
Autoriser roaming	Sélectionnez pour activer l'itinérance GSM. **Avertissement :** si cette option est activée, le modem peut se connecter à un réseau dans un pays différent. **Remarque :** la modification de ce paramètre réinitialise le modem. **Remarque :** pris en charge par les modems GSM v3.08 ou supérieurs.
Code USSD	**Libre accès SIM uniquement** Saisissez le code que le modem peut utiliser pour demander au réseau le suivi de consommation de la carte SIM. Ce code dépend du réseau ; veuillez consulter votre fournisseur d'accès à cet effet.
Appels entrants	**Remarque :** Vanderbilt recommande de ne pas activer ces options pour les systèmes actuels. Le modem peut être programmé pour prendre les appels selon plusieurs modes différents : • **Pas de réponse aux appels entrants :** le modem ne répond jamais aux appels. • **Réponse aux appels entrants :** le modem répond aux appels. • **Réponse uniquement lorsque l'accès ingénieur est autorisé :** le modem ne répond aux appels que lorsque l'accès ingénieur est autorisé dans le système.
Surveillance ligne	• **Désactiver** • **Enable (Validation)** • **MES totale** Activez cette fonction pour surveiller le niveau de signal émis par le GSM branché sur le modem. L'option **MES totale** n'active cette fonction que si le système est en mode MES totale. **Remarque :** confirmation de la configuration EN 50131-9 Afin que la confirmation EN50131-9 fonctionne correctement, il faut que la surveillance de ligne soit activée. (Consultez *Options* page 257.)
Temporisateur de surveillance	Saisissez la durée en secondes pendant laquelle le niveau du signal doit passer sur Faible avant que le système SPC n'enregistre un défaut. Plage 0 – 9 999 secondes.
Délai Défaut Modem	Saisissez le délai en secondes avant que le système SPC n'envoie une alerte. Plage 0 – 9 999 secondes.
SMS Activation	Cliquez cette case pour activer la transmission et la réception de messages SMS et la commande de contrôle.
SMS automatisé	• **Désactiver** • **1 heure** • **24 heures** • **48 heures** • **7 jours** • **30 jours** Sélectionnez l'intervalle pour les messages SMS automatiques.

N° de SMS automatisé	Entrez le numéro SMS pour recevoir les messages SMS automatiques. Un seul appareil peut recevoir ces messages.
Date/heure de début	Saisissez la date/heure de début d'envoi de messages SMS automatiques par le système.
Configuration GPRS	
Point d'accès (APN)	Saisissez les détails du point d'accès pour activer les communications IP. Ces détails dépendent du fournisseur d'accès.
Point d'accès Nom d'utilisateur	Saisissez les détails du point d'accès pour activer les communications IP. Ces détails dépendent du fournisseur d'accès.
Mot de passe Point d'accès	Saisissez les détails du point d'accès pour activer les communications IP. Ces détails dépendent du fournisseur d'accès.
Configuration de la connexion Internet par modem	
Valider connexion Internet par modem	Sélectionnez cette option pour activer le modem et obtenir une connexion Internet
Téléphone	Saisissez le numéro de téléphone de la connexion par modem.
Login	Saisissez le nom d'utilisateur de la connexion par modem.
Mot de passe	Saisissez le mot de passe de la connexion par modem.

Cliquez sur **SMS test** pour envoyer un SMS pour tester le système.

Le test SMS sert uniquement à vérifier que la fonction SMS fonctionne correctement. Utilisez un message court avec des caractères alphabétiques (A-Z) pour tester la fonction.

Modem RTC

1. Sélectionnez **Communications > Communications > Modems**.
2. Cliquez sur **Configurer**.
3. Configurez les champs comme indiqué dans le tableau ci-dessous.

Paramètres modem RTC

Pays	Sélectionnez le pays dans lequel le système SPC est installé.

Appels entrants	Le modem peut être programmé pour prendre les appels selon plusieurs modes différents : • **Pas de réponse aux appels entrants :** le modem ne répond jamais aux appels. • **Réponse après x sonneries :** sélectionnez le nombre de sonneries (1 à 8) avant que le modem décroche. • **Réponse lorsque le correspondant appelle et raccroche après une sonnerie, puis renouvelle immédiatement l'appel** Si le correspondant appelle le modem, raccroche après une seule sonnerie puis rappelle immédiatement le modem. Le système SPC peut répondre à l'appel automatiquement après avoir été mis dans ce mode. • **Réponse uniquement lorsque l'accès ingénieur est autorisé :** le modem ne répond aux appels que lorsque l'accès ingénieur est autorisé dans le système.
Préfixe	Entrez le numéro requis pour accéder à une ligne (par ex. par connexion PBX).
Surveillance ligne	Activez cette fonction pour surveiller la tension de la ligne reliée au modem. Remarque : confirmation de la configuration EN 50131-9. Afin que la confirmation EN50131-9 fonctionne correctement, il faut que la surveillance de ligne soit activée. (Consultez *Options* page 257.)
Temporisateur de surveillance	Sélectionnez le délai en secondes pendant lequel la tension de la ligne doit être incorrecte avant que le SPC déclare que la ligne est défectueuse.
Délai Défaut Modem	Délai avant l'alerte système (0 – 9 999 secondes). 60 secondes par défaut.
SMS Activation	Cochez cette case pour activer la fonction SMS du système. **Remarque :** le service SMS fonctionne sur la base d'un protocole standard utilisé par les téléphones compatibles SMS. Veuillez noter que certains opérateurs du RTC ne proposent pas le service SMS via le RTC. Pour pouvoir envoyer des SMS dans le RTC, les critères suivants doivent être réalisés : Le numéro de téléphone de l'appelant (ID appelant) doit être activé sur la ligne téléphonique. Ligne téléphonique directe - ne fonctionne pas via une centrale téléphonique / auto-commutateur privé ni d'autres équipements de télécommunications. Notez aussi que la plupart des opérateurs ne prennent pas en charge l'envoi de SMS à des abonnés de l'étranger (pour des questions de facturation). **Remarque :** les SMS par RTC ne sont plus pris en charge. La fonctionnalité est conservée pour le produit, afin que la compatibilité en arrière soit maintenue.
SMS Serveur	Uniquement pour les modems filaires (RTC). Ce numéro affiche automatiquement le numéro par défaut pour le SMS dans le pays sélectionné. Saisissez un numéro de téléphone correct du fournisseur de service SMS avec couverture sur votre site.
SMS automatisé	Sélectionnez l'intervalle pour les messages SMS automatiques.
N° de SMS automatisé	Entrez le numéro SMS pour recevoir les messages SMS automatiques.
Configuration de la connexion Internet par modem	
Valider connexion Internet par modem	Sélectionnez cette option pour activer le modem et obtenir une connexion Internet.

Téléphone	Saisissez le numéro de téléphone de la connexion par modem.
Login	Saisissez le nom d'utilisateur de la connexion par modem.
Mot de passe	Saisissez le mot de passe de la connexion par modem.

Cliquez sur **SMS test** pour envoyer un SMS pour tester le système.

Le test SMS sert uniquement à vérifier que la fonction SMS fonctionne correctement. Utilisez un message court avec des caractères alphabétiques (A-Z) pour tester la fonction.

Si la fonction de message SMS est utilisée dans le réseau RTC, le numéro de téléphone du fournisseur de services SMS couvrant le secteur dans lequel le SPC est installé doit être programmé. Le système SPC compose automatiquement ce numéro pour contacter le serveur SMS lorsque la fonction SMS est activée. L'identité de la ligne appelante DOIT être activée sur le réseau RTC pour que cette fonction soit opérationnelle. Chaque pays aura son propre fournisseur de services SMS avec un numéro de téléphone unique.

Cette fonction n'est pas disponible dans tous les pays. Contactez votre prestataire local pour plus d'informations (prise en charge de la fonction, fournisseur d'accès recommandé).

17.10.1.4 Ports série

Le contrôleur SPC dispose de deux ports série (RS232) dont la fonction est la suivante :

- **X10 :** le port série 1 est une interface dédiée qui accepte le protocole X10. Ce protocole permet l'utilisation des câbles d'alimentation existants dans le bâtiment pour transmettre les informations de contrôle aux périphériques X10, permettant ainsi de déclencher et d'assurer le suivi de ces périphériques via l'interface de programmation du contrôleur SPC.
- **Journalisation des événements :** l'interface du port série 2 permet de relier la centrale au port série d'un PC ou d'une imprimante. Avec cette connexion, un programme terminal peut être configuré pour recevoir un JDB des événements système ou des événements d'accès provenant du contrôleur SPC.
- **Informations sur le système :** le port série 2 constitue également une interface permettant, via un programme terminal, d'exécuter des commandes afin d'interroger le contrôleur en vue d'obtenir des informations spécifiques sur le système. Cette fonction est disponible uniquement en tant qu'outil de débogage et d'information, et ne devrait être utilisée que par les installateurs expérimentés.

1	PC avec port série sur lequel est exécuté un hyperterminal
2	Contrôleur SPC
3	JP9
4	RS232

Pour configurer les ports série :

- Sélectionnez **Communications > Communications > Ports série**.

  La page suivante s'affiche :

Les paramètres affichés dépendent du type de connexion pour laquelle les ports sont utilisés. Les paramètres sont décrits dans la section suivante.

17.10.2 FlexC®

Le Protocole de communication de sécurité flexible de la centrale permet les communications pour un système de transmission d'alarme à chemin unique ou multiple (ATS) basé sur un protocole Internet

(IP). Un système de transmission d'alarme (ATS) est une voie de communication fiable entre un transmetteur supervisé (SPT, par ex. centrale SPC avec Ethernet intégré) et un frontal de réception (RCT, par ex. SPC Com XT ou serveur SPC Connect, www.spcconnect.com). Un ATS FlexC comporte un chemin de transmission d'alarmes principal (ATP) et au maximum neuf chemins de transmission d'alarmes de secours (ATP). Il active les fonctions suivantes :

- Le transfert de données bidirectionnel entre le SPT, par exemple la centrale SPC via Ethernet et RCT, par exemple, le serveur SPC Com XT ou le serveur SPC Connect, www.spcconnect.com.
- la supervision des communications d'un système de transmission complet et des chemins individuels.

Les centrales d'intrusion SPC prennent en charge FlexC sur IP avec l'une quelconque des interfaces suivantes :

- Ethernet
- Modem GSM avec GPRS activé.
- Modem RTC

Voir également

Configuration Démarrage Rapide ATP pour système de transmission conforme EN50136 à la page opposée

Configuration de profils d'événement page 331

Définition de l'exception d'événement. page 332

Configuration de profils d'événement page 335

FlexC - État page 206

Configurer un système de transmission ATS conforme EN50136-1 ou un ATS personnalisé. page 319

17.10.2.1 Mode de fonctionnement

Le système utilise la méthode d'acquittement après enregistrement lors de la transmission des événements.

La centrale d'alarme SPC envoie les événements vers le frontal SPC Com XT et demande un acquittement du frontal avant de déclarer que l'événement est correctement transmis. SPC Com XT acquitte l'événement seulement après qu'il a été enregistré dans la base de données SQL. SPC Com XT envoie ensuite l'événement au client SPC Com XT et aux interfaces Sur-Gard.

17.10.2.2 Configuration Démarrage Rapide ATP pour système de transmission conforme EN50136

FlexC fournit les fonctions suivantes du boîtier qui hissent FlexC en première position et lui permettent de fonctionner plus rapidement :

- Page de configuration Démarrage rapide pour un **ATS à chemin unique**, un **ATS à chemin double** et un **ATS double chemin-double récepteur** conformes EN50136.
- Profil Événements par défaut
- Profil Commandes par défaut (ne prend pas en charge la vérification vidéo audio)
- Le **Nom d'utilisateur de commande FlexC** par défaut (FlexC) et le **Mot de passe de commande** (FlexC) pour commander la centrale depuis le RTC (par ex., SPC Com XT)
- Cryptage automatique sans mot de passe

1. Pour configurer rapidement une connexion FlexC entre une centrale et un RCT (par ex., SPT Com XT), allez sur **Communications > FlexC > ATS FlexC**.
2. Sous **Ajouter un ATS conforme EN50136-1**, choisissez l'une des options suivantes pour afficher l'écran **Configuration ATP** :
   - **Ajouter ATS à chemin unique** - ATP principal seulement
   - **Ajouter ATS à chemin double** – ATP principal et secours
   - **Ajouter ATS double chemin-double récepteur** - ATP principal et secours

3. Complétez les champs de la page **Configuration ATP – ATS conforme EN50136** figurant dans le tableau ci-dessous. Au minimum, il faut compléter le champ **URL récepteur** ou **Adresse**

IP avant de sauvegarder. Si vous n'entrez pas de **Code Client-Identifiant**, vous pouvez charger la centrale avec l'**ID d'enregistrement de l'ATS** qui est automatiquement créée lors vous enregistrez. L'opérateur RCT doit entrer cette **ID d'enregistrement de l'ATS**, par exemple, dans SPC Com XT.

4. Cliquez sur **Enregistrer**. La page **Configuration système de transmission ATS** affiche l'**ID d'enregistrement de l'ATS** et l'ATP principal configuré ou les ATP principaux et de secours dans la **Table de séquence d'événement**.
5. Sur la page **Configuration de l'ATS**, cliquez sur **Enregistrer** pour valider le réglage par défaut, par exemple, le **Profil Événements par défaut**, le **Profil Commandes par défaut** (y compris le **Nom d'utilisateur de commande** FlexC et le **Mot de passe commande** FlexC), et le **Cryptage automatique** sans mot de passe. Pour modifier la configuration, consultez *Configurer un système de transmission ATS conforme EN50136-1 ou un ATS personnalisé.* à la page opposée.
6. Cliquez sur **Retour**. L'ATS est affiché dans la fenêtre **Système de transmission configuré**.

Identification de la centrale	
Nom de l'ATS	Saisissez le nom du système de transmission d'alarme (ATS). Si aucune valeur n'est entrée, les systèmes de transmission sont nommés par défaut ATS 1, ATS 2, etc.
Code client-Identifiant	Numéro unique qui identifie la centrale sur le RCT. Entrez 0 si vous n'avez pas de code Client-Identifiant. Dans ce cas, vous pouvez charger la centrale à l'aide de l'**ID d'enregistrement de l'ATS**. Pour un ATS conforme EN50136, l'**ID d'enregistrement de l'ATS** est automatiquement créée lorsque vous cliquez sur **Enregistrer**. Le récepteur peut envoyer le **Code Client-Identifiant** à la centrale dès qu'il est disponible.
Identification du récepteur RCT et identification du récepteur de secours (double chemin-double récepteur seulement)	
ID récepteur	Entrez l'**ID récepteur** unique qui identifie le récepteur RCT (par ex., SCP Com XT) dans la centrale. Cela doit coïncider avec la valeur entrée sur l'outil de gestion de configuration du Serveur SPC Com XT, dans le champ **ID serveur RTC** de l'onglet **Détails serveur**. Voir le *Manuel de configuration et d'installation du SPC Com XT*.
Adresse IP ou URL Récepteur	Entrez l'**URL récepteur** ou l'**Adresse IP** pour la localisation du serveur RCT (par ex., serveur SPC Com XT).
Port IP Récep.	Entrez le port TCP pour le récepteur (par ex., SPC Com XT). Cela doit être la même valeur que celle saisie dans le champ **Port récepteur FlexC** dans l'outil de gestion de configuration du récepteur SPC Com TX.
Interface du chemin	
Catégorie EN50136 Syst. transm.	Sélectionnez la catégorie ATS EN50136 (SP1-SP6, DP1-DP4). Pour une description des catégories, consultez *Tempos des catégories d' ATS* page 418.
Interface principale	Sélectionnez **Interface principale** pour appliquer le chemin de communication de l'élément suivant à l'interface principale : • Ethernet • GPRS : Modem 1 • GPRS : Modem 2 • Connexion Internet par modem : Modem 1 • Connexion Internet par modem : Modem 2

Interface de secours	Pour un **ATS Double Chemin**, sélectionnez l'**Interface de secours** à utiliser pour le chemin de communication de secours de l'élément suivant : • Ethernet • GPRS : Modem 1 • GPRS : Modem 2 • Connexion Internet par modem : Modem 1 • Connexion Internet par modem : Modem 2

17.10.2.3 Configurer un système de transmission ATS conforme EN50136-1 ou un ATS personnalisé.

Un système de transmission ATS est constitué d'une centrale d'alarme, de chemins réseau et d'un récepteur RCT (par ex. SPC Com XT). Il combine un ou plusieurs chemins de transmission entre une centrale SPC et un RCT. On peut ajouter au système de transmission un maximum de 10 chemins.

REMARQUE : pour un ATS conforme EN50136-1, le système de transmission programme le démarrage de séquence en configurant un chemin pour un système de transmission. Vous disposez ainsi d'un mode rapide de configuration. Voir *Configuration Démarrage Rapide ATP pour système de transmission conforme EN50136* page 317.

1. Pour configurer un système de transmission, allez sur **Communications > FlexC > FlexC ATS**.
2. Sélectionnez l'une des options suivantes :
   - Ajouter ATS à chemin unique
   - Ajouter ATS à double chemin
   - Ajouter ATS à double chemin – double récepteur
   - Ajouter un ATS personnalisé
3. Pour un ATS conforme EN50136, il faut commencer par régler les paramètres sur la page **Configuration ATP – EN50136**. Voir *Configuration Démarrage Rapide ATP pour système de transmission conforme EN50136* page 317.
4. La page **Configuration de l'ATS** s'affiche. L'ATS conforme EN50136-1 affiche un chemin principal ou un principal et un secours dans la **Table séquence des événements**.

5. Entrez le **Nom de l'ATS** pour identifier le système de transmission. Si aucune valeur n'est entrée, les systèmes de transmission sont nommés par défaut ATS 1, ATS 2, etc.
6. Pour ajouter 1 chemin principal et jusqu'à 9 chemins de secours à l'ATS, cliquez sur **Ajouter un chemin au récepteur FlexC** (voir *Ajouter Récepteur FlexC* à la page opposée) ou cliquez sur **Ajouter un chemin au CTS analogique**, (voir *Ajouter Récepteur Analogique* page 326).
7. Sélectionnez un **Profil événement** dans la liste déroulante. Pour personnaliser la manière dont les événements sont transmis par un système de transmission, voir *Configuration de profils d'événement* page 331.
8. Sélectionnez un **Profil Commande** dans la liste déroulante. Pour personnaliser les commandes activées pour qu'un récepteur contrôle une centrale, voir *Configuration de profils d'événement* page 335.
9. Complétez les champs **Défauts de l'ATS** comme indiqué dans la fenêtre ci-dessous.

Timeout Polling ATS	Le champ est calculé automatiquement en ajoutant des valeurs de la colonne **Timeout du polling en mode actif** dans la table de séquence d'événement, pour tous les chemins d'un système de transmission d'alarme (ATS). Vous pouvez saisir manuellement une autre valeur dans ce champ. Par exemple, Cat 2 [Modem] a un **Timeout du polling en mode actif** de 24 heures 10 minutes (87 000 secondes). Pour permettre un temps de réaction plus court, entrez une valeur inférieure.
Timeout événement ATS	Le temps s'écoulant à partir de l'apparition d'un événement non correctement transmis avant renoncement de l'ATS. 300 secondes par défaut.

Génère un Défaut de Transm.	Sélectionnez le résultat : le système peut créer un FTC ou un événement timeout de l'ATS.
Evénements gardés en attente	Sélectionnez cette option pour remettre les événements en file d'attente après un timeout ATS.
Délais de remise en file d'attente	Temps d'attente avant de remettre en file d'attente de transmission un événement qui avait échoué sur l'ATS par timeout. 300 secondes par défaut.
Temps max. de remise en file	Période de temps pendant laquelle un événement sera conservé dans la file d'attente avant d'être supprimé. 86 400 secondes par défaut.

10. Cliquez sur **Éditer détails d'installation** pour terminer les réglages permettant d'identifier la centrale et l'opérateur RCT. Voir *Éditer Détails Installation* page 328.
11. Cliquez sur **Enregistrer** et **Retour** pour revenir à la page **Configuration de l'ATS**. Le nouvel ATS est affiché dans la fenêtre **Syst. de transmission configuré**.
12. En présence de chemins multiples, on peut utiliser les flèches haut et bas dans la **Table de séquence d'événement** pour réordonner la séquence ATP.

REMARQUE : l'ID d'enregistrement de l'ATS est automatiquement créée pour un chemin. Il identifie la centrale sur le récepteur de manière unique. Si vous ne connaissez pas le Code Client-Identifiant, vous pouvez charger la centrale avec l'ID d'enregistrement de l'ATS. L'opérateur CMS doit aussi entrer cette ID d'enregistrement de l'ATS dans le RCT (par example, SPC Com XT). Voir le *Manuel de configuration et d'installation du SPC Com XT*.

Voir également

Tempos des catégories d' ATS page 418

Ajouter Récepteur FlexC

Ajouter un chemin au récepteur FlexC permet de configurer un chemin de transmission entre la centrale SPC et le récepteur (par ex. SPC Com XT). Il est possible de configurer jusqu'à 10 chemins pour chaque système ATS.

1. Cliquez sur **Ajouter Récepteur FlexC**.

2. Configurez les champs ATP décrits dans le tableau ci-dessous.

Identification de la centrale	
N° Séquence ATP	Ce champ affiche le numéro de séquence du chemin ATP dans la configuration du système de transmission ATS. 1 pour principal, 2 – 10 pour les secours.
ID Unique Chemin	Quand on enregistre un chemin ATP, le système assigne une ID unique au chemin. Le chemin est identifié par une ATP unique qui peut donc être reconnue par le récepteur.
Nom du Chemin	Nommez la connexion dans ce champ.
Code client-Identifiant	Entrez un numéro pour identifier uniquement la centrale sur le récepteur.
Identification du récepteur RCT	
ID récepteur	Entrez l'ID récepteur unique qui identifie le récepteur RCT (par ex. SCP Com XT) dans la centrale. Cela doit coïncider avec la valeur entrée dans l'outil de gestion de configuration du récepteur SPC Com XT, dans le champ **ID récepteur RTC**.
Adresse IP ou URL Récepteur	Entrez l'URL ou l'adresse IP du récepteur (par ex. SPC Com XT).
Port IP Récep.	Entrez le port TCP écouté par le récepteur (par ex. SPC Com XT). La valeur par défaut est 52 000. Elle doit coïncider avec la valeur figurant dans le champ **Port récepteur FlexC** de l'outil de gestion du récepteur. Voir le *Manuel de configuration et d'installation du SPC Com XT*.
Interface du chemin	
Interface de communication	Dans la liste déroulante, sélectionnez l'interface utilisée par ce chemin pour la communication. • Ethernet • GPRS : Modem 1 • GPRS : Modem 2 • Connexion Internet par modem : Modem 1 • Connexion Internet par modem : Modem 2
Catégories du Chemin	Sélectionnez la catégorie correspondant à ce chemin. Pour en savoir plus sur les catégories du chemin, voir *Tempos des catégories de Chemin* page 419.
Avancée	
Paramètres avancés du Chemin ATP	Il n'est pas recommandé de modifier les Paramètres avancés du Chemin ATP. La programmation avancée ne doit être utilisée que par des personnes expérimentées.

3. Le cas échéant, cliquez sur **Paramètres avancés du chemin ATP.** Si, par exemple, vous utilisez un cryptage automatique, vous pouvez remplir le champ **Mot de passe de cryptage**. Voir *Configurer les paramètres avancés du Chemin ATP* à la page opposée.
4. Cliquez sur **Enregistrer**.

Configurer les paramètres avancés du Chemin ATP

AVERTISSEMENT : il n'est pas recommandé de modifier les **Paramètres avancés du Chemin ATP**. La programmation avancée ne doit être utilisée que par des personnes expérimentées.

1. Cliquez sur **Paramètres avancés du Chemin ATP**.

2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Connexions du Chemin	
Chemin Actif	Choisir le mode de connexion ATP quand le chemin ATP fonctionne comme chemin de communication principal. • Permanent : connexion permanente • Temporaire : coupe après 1 seconde • Temporaire : coupe après 20 secondes • Temporaire : coupe après 80 secondes • Temporaire : coupe après 3 minutes • Temporaire : coupe après 10 minutes • Temporaire : coupe après 30 minutes

Connexion ATP inactive	Choisir le mode de connexion ATP quand le chemin ATP fonctionne comme chemin de communication de secours. • Permanent : connexion permanente • Temporaire : coupe après 1 seconde • Temporaire : coupe après 20 secondes • Temporaire : coupe après 80 secondes • Temporaire : coupe après 3 minutes • Temporaire : coupe après 10 minutes • Temporaire : coupe après 30 minutes
Test cyclique	
Mode d'appel de test (chemin inactif)	Sélectionnez la périodicité des tests cycliques lorsque le chemin est utilisé comme chemin inactif. • Désactivé • 10 minutes • 1 heure • 4 heures • 24 heures • 48 heures • 7 jours • 30 jours
Période Test Auto-Chemin Actif	Sélectionnez la périodicité des tests lorsque le chemin est utilisé comme chemin actif. • Désactivé • 10 minutes • 1 heure • 4 heures • 24 heures • 48 heures • 7 jours • 30 jours
Cryptage (256-bits AES avec CBC)	
Mode de la clé de cryptage	Choisissez le mode de mise à jour du cryptage. • Cryptage automatique • Cryptage automatique avec mises à jour • Cryptage Manuel **Remarque :** le cryptage automatique utilise la clé par défaut et la met à jour une fois. Le cryptage automatique avec mises à jour modifie la clé de cryptage tous les 50 000 messages ou bien une fois par semaine, selon l'événement se produisant en premier.

Mot de passe cryptage	Mot de passe optionnel utilisé pour renforcer la sécurité pendant la phase d'installation du chemin de transmission (ATP). Le mot de passe doit être renseigné indépendamment au niveau de la centrale et dans le récepteur d'alarme.
RAZ cryptage	RAZ de la clé de cryptage et du mot de passe avec les valeurs usine.
Profils des chemins	
Profil d'événement	Choisir le profil d'événement qui définit quels événements et comment ils seront transmis par ce système de transmission (ATS). • Utilise la programmation ATS • Profil Événements par défaut • Tous événements
Profile Commande	Choisir le profile de commande qui définira le jeu de commandes autorisées sur ce Système de Transmission (ATS). • Utilise la programmation ATS • Profil Commandes par défaut • Profil Commande personnalisée
Défauts Chemin	
Défaut Supervision du Chemin	Génère un défaut chemin si la supervision du chemin échoue ou si la transmission d'un événement échoue sur ce chemin.
Événement timeout	Délai pendant lequel le chemin (ATP) essaie de transmettre l'événement jusqu'à ce que l'événement passe en échec sur ce chemin et soit transféré au chemin suivant. • 30 secondes • 60 secondes • 90 secondes • 2 minutes • 3 minutes • 5 minutes • 10 minutes
Longueur minimale des messages	
Message de polling	Longueur minimum d'un message de polling. • 0 octet • 64 octets • 128 octets • 256 octets • 512 octets

Message Événement	Longueur minimale du message d'événement et de test automatique. • 0 octet • 64 octets • 128 octets • 256 octets • 512 octets
Autres messages	Longueur minimale du message de connexion, de mise à jour et des clés de cryptage. • 0 octet • 64 octets • 128 octets • 256 octets • 512 octets

3. Cliquez sur **Enregistrer**.

Ajouter Récepteur Analogique

Si une connexion entre la centrale SPC et le récepteur d'alarme (par ex. SPC Com XT) n'est plus établie, FlexC peut habiliter une connexion ATP entre la centrale SPC et un CTS analogique. Il est possible de configurer jusqu'à 10 chemins pour chaque système ATS.

1. Pour configurer un chemin de transmission entre une centrale et un récepteur analogique, cliquez sur **Ajouter Récepteur Analogique**.
2. Configurez les champs ATP décrits dans le tableau ci-dessous.

Identification de la centrale	
N° Séquence ATP	Ce champ affiche le numéro de séquence du chemin ATP dans la configuration du système de transmission ATS. 1 pour principal, 2 – 10 pour les secours
ID Unique Chemin	Cette ID identifie exclusivement le chemin sur le récepteur.
Nom du Chemin	Nommez la connexion dans ce champ.
Code client-Identifiant	Entrez un numéro pour identifier uniquement la centrale sur le récepteur (1 – 999999)
Connexion au CTS	
Numéro de téléphone 1	N° de téléphone 1
Numéro de téléphone 2	N° de téléphone 2
Choix du Modem	Sélectionnez le type de modem à utiliser. • Modem 1 • Modem 2

Test cyclique	
Mode d'appel de test (chemin inactif)	Sélectionnez la périodicité des tests lorsque le chemin est utilisé comme chemin inactif. 24 heures par défaut. • Appel test cyclique désactivé • 10 minutes • 1 heure • 24 heures • 48 heures • 7 jours • 30 jours.
Période Test Auto-Chemin Actif	Sélectionnez le mode d'émission des appels de test lorsque le chemin est utilisé comme chemin actif. 24 heures par défaut. • Appel test cyclique désactivé • 10 minutes • 1 heure • 24 heures • 48 heures • 7 jours • 30 jours.
Heure du premier test	Heure du premier Test après RAZ ou initialisation du système (ATS). • Envoyer immédiatement (par défaut) ou • Choisissez un intervalle d'une demi-heure entre 0:00 et 23:30.
Protocole pour l'événement	
Protocole	Protocole utilisé en communication. • SIA • SIA étendu 1 • SIA étendu 2 • Contact ID
Profil d'événement	Choisir le profil d'événement qui définit quels événements et comment ils seront transmis par ce système de transmission (ATS). • Utilise la programmation ATS • Profil Événements par défaut • Profile Événement par défaut pour le Portail • Tous événements • Profil d'événement personnalisé
Défauts Chemin	

Défaut Supervision du Chemin	Génère un défaut chemin si la supervision du chemin échoue ou si la transmission d'un événement échoue sur ce chemin.
Événement timeout	Délai pendant lequel le chemin (ATP) essaie de transmettre l'événement jusqu'à ce que l'événement passe en échec sur ce chemin et soit transféré au chemin suivant. 2 minutes par défaut. • 30 secondes • 60 secondes • 90 secondes • 2 minutes • 3 minutes • 5 minutes • 10 minutes

3. Cliquez sur **Enregistrer**.

Éditer Détails Installation

Les détails de l'installation ci-après sont transférés automatiquement au récepteur du CTS pour aider l'opérateur du CTS à enregistrer le site.

1. Cliquez sur le bouton **Éditer détails d'installation**.

2. Complétez les champs de la fenêtre ci-dessous.

ID Syst. de Transmission (ATS)	Numéro d'identification du système de transmission ATS (1–999999999).
ID Société	Pouur utilisation ultérieure.
Nom de Société	Nom de la société.
Adresse Installation ATS	L'adresse de l'installation du système ATS.
Coordonnées GPS	Le GPS coordonne l'installation.
Nom de l'installateur	Le nom de l'installateur du système de transmission (ATS).
N° de téléphone 1	Le numéro de téléphone de l'installateur du système de transmission (ATS).
N° de téléphone 2	Le numéro de téléphone de l'installateur du système de transmission (ATS).
Remarques	Toute autre information devant être transmise au récepteur.

3. Cliquez sur **Enregistrer**.

17.10.2.4 Configuration d'un système de transmission SPC Connect.

La fonction du système de transmission d'alarme **Ajouter SPC Connect** ouvre une voie de communication entre la centrale (SPT) et le serveur **SPC Connect** (RCT), www.spcconnect.com. Avec l'ID d'enregistrement du système de transmission SPC Connect, l'utilisateur d'une centrale peut ouvrir un compte utilisateur et enregistrer sa centrale sur le site Web de SPC Connect pour disposer d'un accès distant à son PC.

1. Pour configurer un système de transmission SPC Connect, allez sur **Communications > FlexC > FlexC ATS**.
2. Sur la page **Configuration ATS**, cliquez sur **Ajouter SPC Connect** pour ouvrir une voie de communication avec le serveur SPC Connect.

   Un système de transmission SPC Connect est ajouté au **Tableau de séquence des événements** avec les attributs suivants :

   - ID d'enregistrement de l'ATS SPC Connect
   - Chemin par défaut avec Ethernet. Pour en savoir plus sur les champs ATP, voir *Ajouter Récepteur FlexC* page 321.
   - Profil Événements par défaut pour SPC Connect
   - Profil Commandes par défaut pour SPC Connect
   - L'URL récepteur par défaut est www.spcconnect.com
   - Le code de compte SPT pour le chemin est affecté.
   - Notez l'**ID d'enregistrement** du système de transmission SPC Connect et transmettez-la au client avec le *Guide de l'utilisateur du système SPC Connect*.

17.10.2.5 Exportation et importation d'un système ATS

Les fichiers ATS se terminent par l'extension .cxml. Il faut créer l'ATS dans le navigateur SPC puis l'exporter avant de pouvoir l'importer dans un système.

1. Pour exporter un système de transmission ATS, allez sur **Communications > FlexC > FlexC ATS**.
2. Dans le tableau **Syst. de transmission configurés**, sélectionnez l'ATS à exporter puis cliquez sur le bouton **Exporter système de transmission (ATS)** (flèche verte).

3. Enregistrez le fichier sous le nom par défaut **export_flexc.cxml** ou renommez-le.
4. On peut ouvrir le fichier dans le Bloc-Notes.
5. Pour importer un ATS dans le système, allez sur **Communications > FlexC > FlexC ATS**.
6. Faites défiler vers le bas jusqu'à **Importer un Système de Transmission (ATS)**.
7. Cliquez sur **Parcourir** et sélectionnez un ATS à importer (fichier .cxml).

8. Cliquez sur **Importer un Système de Transmission (ATS)**.

   L'ATS est affiché dans la fenêtre **Système de transmission configuré** avec l'ID disponible suivante.

Lors de l'exportation d'un ATS, le Code Client-Identifiant passe à 0. Cela permet d'éviter qu'un ATS soit exporté puis réimporté en créant un double.

17.10.2.6 Configuration de profils d'événement

Le profil d'événement définit quels événements sont transmis par un système de transmission d'alarme (ATS), l'état de la transmission d'événements et les exceptions d'événement. L'exception d'événement permet de redéfinir les valeurs par défaut pour les personnaliser. Pour plus d'informations, consultez *Définition de l'exception d'événement.* à la page suivante.

Pour voir une liste de tous les événements, allez sur **Communications > FlexC > Profils d'événement**. Cliquez sur l'icône **Éditer** pour un profil d'événement. Allez jusqu'à la fin de la page et cliquez sur **Afficher le tableau complet des événements**.

Pour créer rapidement un nouveau profil d'événement, allez sur **Communications > FlexC > Profils d'événement**. Dans le tableau **Profils d'événement**, sélectionnez un profil d'événement et cliquez sur l'icône **Éditer**. Allez en bas de la page et cliquez sur **Dupliquer**. Vous pouvez maintenez procéder aux modifications requises.

1. Pour configurer pas à pas des profils d'événement FlexC, allez sur **Communications > FlexC > Profils d'événement**.
2. Cliquez sur **Ajouter**. La page **Profils d'événement** s'affiche.

3. Entrez un **Nom** permettant d'identifier l'événement.

4. Choisissez les groupes de filtre d'événement affectés à ce profil en cochant les cases **Transmet l'événement**.
5. Pour éviter la transmission de certains événements ou adresses contenus dans d'autres événements, il convient de choisir l'événement dans la liste déroulante **Ajouter Exception Événement**.
6. Cliquez sur **Ajouter** pour voir s'afficher la page **Définition de l'exception d'événement**. Voir *Définition de l'exception d'événement.* ci-dessous.
7. Cliquez sur **Retour** pour revenir à la page **Profils d'événement**.
8. Pour appliquer un profil d'événement à un secteur, choisissez le secteur dans **Filtre sur Secteur**.
9. Cliquez sur **Enregistrer** puis sur **Retour**. Le nouveau profil est affiché dans le tableau **Profils d'événement**.

Il est possible d'afficher la liste de toutes les exceptions d'événement pour un profil d'événement sous **Exceptions d'événement** dans la page**Profils d'événement**.

On ne peut pas supprimer le **Profil d'événement par défaut** et le **Profil d'événement par défaut pour le portail**, ni aucun profil d'événement affecté à un système de transmission d'alarme (ATS). Si vous tentez de supprimer un profil d'événement en cours d'utilisation, une erreur se produit.

Définition de l'exception d'événement.

L'option Exceptions d'événement permet de modifier les réglages suivants pour un intervalle d'adresses dans le cadre d'un événement :

- Transmet l'événement
- Code SIA
- Code CID
- Adresse de l'événement (par ex. ID de zone, ID du secteur, ID utilisateur)

Par exemple, dans le Groupe de filtre **Alarme Intrusion**, vous pouvez définir une exception sur événement pour un intervalle d'ID de zone dans l'événement Alarme Intrusion (BA), comme suit :

- Ne transmet pas les événements BA pour les ID de zone 1 – 9
- Redéfinit le code SIA de BA à YZ.
- Redéfinit le code CID de 130/1 à 230/1
- Redéfinit l'ID de zone 1 – 9 en ID de zone 101 – 109

1. Pour configurer une **Définition de l'exception sur événement**, renseignez les champs décrits dans la fenêtre ci-dessous.

Identification	
Nom	Entrez le nom de l'exception sur événement.
ID de l'événement	Numéro d'IDentification de l'événement dans le système. Affiché en lecture seule.
Description Événement	Description de l'événement. Affiché en lecture seule.
Event Filter (Filtre d'évènements)	
Transmet l'événement	Cochez la case pour transmettre l'événement. Cela prend le pas sur la valeur de transmission fixée pour le groupe de filtre d'événements. Par exemple, si le groupe de filtre **Alarme intrusion** est réglé sur transmission, il est possible d'exclure l'événement BA ou de désactiver ce paramètre.
Valider Filtre des Exceptions	Cochez la case correspondante pour exclure un intervalle d'adresses, par exemple ID de zone dans le réglage du champ **Transmet l'événement**.
si (0 ≤ *Zone ID* ≤ 9999) alors Transmet l'événement/Ne transmet pas l'événement	Renseignez un intervalle d'adresses à exclure du paramètre **Transmet l'événement**. Par exemple, si vous décidez de transmettre un événement type BA, vous pouvez décider de ne pas transmettre *Zone ID 1 – 9* pour cet événement. Inversement, si vous décidez de ne pas transmettre un événement type BA, vous pouvez décider de transmettre *l'identificateur de zone (Zone ID) 1 - 9* pour cet événement.
Format événement	

Code événement SIA	Code événement SIA par défaut qui est transmis pour représenter l'événement. Champ en lecture seule.
Code/qualificatif de l'événement Contact ID	Code/qualificatif de l'événement Contact ID par défaut transmis pour représenter l'événement. Champ en lecture seule.
Valider Redéfinition Exception	Cochez pour remplacer les Codes/qualificatifs CID et SIA et l'adresse d'événement par défaut par des valeurs personnalisées, par exemple pour redéfinir *Zone ID 1 – 9* en *Zone ID 101 –109*. Les champs ci-dessous sont affichés s'ils sont activés.
si (0 ≤ *Zone ID* ≤ 9999)	Renseignez l'intervalle d'adresses à redéfinir pour un événement ; pour redéfinir par exemple *Zone ID 1 – 9* en *Zone ID 101 –109*, saisissez *1* et *9*. Le nombre d'adresses de l'intervalle doit être égal à la quantité d'adresses définies dans le champ **Redéfinit adresse événement** ci-dessous.
redéfinit alors le code événement SIA vers BA	redéfinit le code SIA par défaut vers un code SIA personnalisé.
et redéfinit le Code/qualificatif de l'événement Contact ID en	Redéfinit le Code/qualificatif de l'événement Contact ID par défaut en un Code/qualificatif de l'événement Contact ID personnalisé.
et redéfinit adresse événement vers	Renseignez un nouvel intervalle d'adresses, si vous souhaitez par exemple redéfinir *Zone ID 1 – 9* en *Zone ID 101 – 109*, saisissez *101* et *109*.

2. Cliquez sur **Enregistrer**.
3. Cliquez sur **Retour** pour revenir à la page **Profils d'événement**.

   Le nom de chaque exception s'affiche dans le tableau **Exceptions sur événement** situé en bas de la page. La fenêtre présente les paramètres des champs **Transmet l'événement**, **Filtre des exceptions**, **Code événement (SIA/CID)** et **Redéfinition de l'exception** pour l'événement concerné.

4. Cliquez sur l'icône **Éditer** pour effectuer des changements ou sur **Supprimer** pour supprimer une **exception sur événement**.
5. Pour appliquer le profil d'événement à un secteur, cochez la case correspondant à ce secteur.
6. Cliquez sur **Sauver** pour sauver le profil d'événement.
7. Cliquez sur **Retour** pour voir le profil dans la fenêtre **Profils d'événement**.

17.10.2.7 Configuration de profils d'événement

Le profil de commande définit les commandes permises sur le système de transmission (ATS). Le profil détermine la manière dont un CMS contrôle une centrale. La commande par défaut ne prend pas en charge la vérification vidéo.

REMARQUE : pour créer rapidement un nouveau profil d'événement, allez sur **Communications > FlexC > Profils de commande**. Dans le tableau **Profils de commande**, sélectionnez un profil de commande et cliquez sur Éditer (crayon bleu) puis cliquez sur **Dupliquer** en bas de l'écran. Vous pouvez maintenez procéder aux modifications requises.

1. Pour ajouter un profil de commande pas à pas, allez sur **Communications > FlexC > Profils de commande**.

2. Cliquez sur **Ajouter** .

3. Entrez un **Nom** permettant d'identifier le profil de commande.
4. Sélectionnez un **Mode Authentification** (Utilisateur Commande ou Utilisateur SPC, Utilisateur pour les Commandes seulement ou N'importe quel utilisateur de la centrale) dans la liste déroulante.

REMARQUE : le **Nom d'utilisateur de commande** par défaut fournit un utilisateur prêt à l'emploi qui permet d'activer rapidement et facilement le contrôle de la centrale depuis le SPC Com XT. Une large gamme de commandes est ainsi disponible. Par exemple, l'utilisateur de commande par défaut peut définir tous les secteurs ou contrôler toutes les zones. Pour exercer un contrôle plus limité, par exemple pour ne permettre que la définition de certains secteurs, on peut définir un profil de commande personnalisé doté d'une série déterminée de droits. On ne peut pas supprimer le **Profil Commandes par défaut** et **Profil Commande par défaut pour le portail**, ni aucun profil de commande assigné à un système de transmission d'alarme (ATS).

5. Renseignez le nom d'utilisateur du profil de commande dans le champ **Nom d'utilisateur de commande**. Il doit correspondre au **Nom d'utilisateur d'authentification** du SPC Com XT.
6. Entrez le mot de passe de l'utilisateur du profil de commande dans le champ **Mot de passe commande**. Il doit correspondre au **PIN ou mot de passe utilisateur** d'authentification du SPC Com XT.
7. Sélectionnez le **Mode Audio temps réel** (Désactivé, Seulement après l'alarme, Toujours disponible, Système en MES totale) pour déterminer les options de confidentialité de transmission. L'option **Toujours disponible** crée le plus gros volume de données.
8. Sous **Filtre commande**, sélectionnez les commandes à activer. Pour obtenir la liste complète des commandes disponibles, voir *FlexC - Commandes* page 415.
9. Sélectionnez la commande à journaliser.
10. Cliquez sur **Enregistrer**.
11. Cliquez sur **Retour** pour voir le profil de commande dans le tableau **Profils de commande**.
12. Pour modifier un profil de commande, cliquez sur **Éditer** (icône de crayon), à côté d'un profil.

17.10.3 Rapports

Cette section recouvre :

17.10.3.1 Centres de télésurveillance (CTS)

La centrale SPC a la capacité de communiquer des informations à une station réceptrice éloignée lorsqu'une alarme spécifique se déclenche sur la centrale.

Ces Centres de télésurveillance doivent être configurés sur la centrale pour permettre cette communication à distance.

Ajouter/Éditer un CTS au moyen d'un SIA ou CID

Prérequis

- Un modem RTC ou GSM doit être installé et fonctionner correctement.

1. Sélectionnez **Communications > Transmission > CTS Analogique**.

   La page suivante s'affiche :

2. Cliquez sur le bouton **Modem1/2** pour faire un essai d'appel au CTS à partir du modem 1 ou du modem 2.
3. Cliquez sur le bouton **Journal** pour recevoir un fichier journal. Une page contenant tous les enregistrements d'essais d'appel, automatiques et manuels, s'affiche.
4. Pour ajouter ou éditer un CTS, cliquez sur **Ajouter**. – OU –
   Cliquez sur **Éditer**.

   La page suivante s'affiche.

5. Configurez les champs comme indiqué dans le tableau ci-dessous.

Description	Saisissez une description du Centre de télésurveillance éloigné.
Compte	Saisissez votre numéro de compte. Cette information doit être disponible sur la station réceptrice et est utilisée pour vous identifier à chaque fois que vous effectuez un appel vers le CTS. Un maximum de six caractères est autorisé pour un compte Contact ID.
Protocole	Saisissez le protocole de communication que vous souhaitez utiliser (SIA, SIA étendu, Contact ID, Fast Format). **Remarque** : SPC prend en charge le protocole SIA étendu. Sélectionnez ce protocole pour pouvoir ajouter des descriptions textuelles sur les événements SIA envoyés au Centre de télésurveillance.
Prioritaire	Sélectionnez une priorité pour le CTS en définissant le signalement principal et le signalement de secours.
Numéro de téléphone 1	Saisissez le premier numéro à appeler pour contacter le CTS. Ce système tentera toujours de contacter le CTS avec ce numéro avant d'en essayer un autre.
Numéro de téléphone 2	Saisissez le deuxième numéro à appeler pour contacter le CTS. Le système ne tentera de contacter le CTS avec ce numéro que si le premier numéro a conduit à un échec.
Nbre de tentatives de numérotation	Saisissez le nombre de fois où le système tentera de faire un appel vers le récepteur. (La valeur par défaut est 8.)
Délai de numérotation	Nombre de secondes d'attente après un échec de numérotation (0–999).
Interval num.	Saisissez le nombre de secondes d'attente après un échec de numérotation. (0-999)
Test cyclique	Activez les essais d'appel en choisissant un intervalle de temps. Cela générera un essai d'appel automatique du modem 1 vers le CTS principal.
Tester tout	Cochez cette case si vous souhaitez également déclencher un essai d'appel automatique du modem 2 vers le CTS de secours.

6. Cliquez sur le bouton **Ajouter** pour saisir ces informations sur le système.

   Une liste des comptes CTS configurés s'affiche dans le navigateur, ainsi que les informations du compte, une description, le protocole, l'état de numérotation, et l'heure et la date du dernier appel au CTS.

Éditer un filtre CTS au moyen d'un SIA ou CID

Pour configurer les événements du SPC qui déclenchent un appel au CTS :

1. Sélectionnez **Communications > Transmission > CTS Analogique > Éditer > Filtrer**.

   La page suivante s'affiche :

2. Configurez les champs suivants :

   Cochez l'une des cases suivantes si vous voulez déclencher un appel à distance vers le CTS pour l'informer de l'événement particulier.

Alarmes	Les alarmes sont activées.
Fin d'alarme	Les alarmes système sont réinitialisées.
Alarmes confirmées	Alarmes confirmées par d'autres zones
Annulation d'alarme	Annulations d'alarme. Les alarmes sont annulées par la saisie d'un code utilisateur valide sur le clavier à la suite d'une alarme confirmée ou non.
Défauts	Les défauts et l'antipiratage sont activés.
RAZ défauts	Les défauts et l'antipiratage sont réinitialisés.
Configurations	Le système est activé et désactivé.
Trop tôt / trop tard	Activation et désactivation du système non planifiées.
Inhibition	Des actions d'inhibition et d'isolation sont exécutées sur le système.

Evénements porte	Les événements porte sont activés. Ne fonctionne qu'avec le protocole SIA.
Autres	Tous les autres types d'événements sont détectés sur le système.
Réseau	Transmet les connexions/déconnexions du réseau IP (grâce à la scrutation).
Secteurs	Sélectionnez des secteurs spécifiques auxquels s'appliquent les événements ci-dessus.

En ajoutant un Centre de télésurveillance (CTS) séparé pour chaque secteur défini sur le système et en programmant chaque secteur pour qu'il transmette à son propre récepteur CTS séparé, le système s'apparentera à un ensemble multilocataire dans la mesure où un niveau élevé d'autonomie sera laissé à chaque secteur.

Éditer un filtre CTS au moyen de Scantronic.

Pour configurer les événements du SPC qui déclenchent un appel au CTS quand le protocole **Scantronic** est sélectionné :

1. Sélectionnez **Communications > Transmission > CTS Analogique > Éditer > Filtrer**.

   Une liste des huit canaux disponibles est affichée avec les conditions d'alarme programmables pour chaque canal.
2. Sélectionnez les conditions d'alarme voulues pour chaque canal. Pour une description de chaque condition, consultez *Types de sortie et ports de sortie* page 229.
3. Dans le menu déroulant **Champ**, sélectionnez **Système** ou un secteur particulier auquel appliquer les paramètres choisis.
4. Cliquez sur le bouton **Test** situé près du premier canal pour tester l'activation de l'alarme.

   L'icône de l'ampoule est activée.
5. Attendez 5 secondes environ puis cliquez de nouveau sur **Test** pour le même canal. Cela envoie une restauration de canal au CTS et désactive l'icône ampoule.
6. Continuer à tester les autres canaux.

17.10.3.2 Configuration EDP

IP

Le système a la capacité de communiquer à distance des informations au serveur SPC Com à l'aide du protocole propre de Vanderbilt, l'EDP (**E**nhanced **D**atagram **P**rotocol). En configurant correctement un récepteur EDP sur le système, il est possible de le programmer pour qu'il envoie automatiquement des données au serveur distant SPC Com lorsque surviennent des événements comme des activations d'alarme, des tentatives de sabotage ou des armements/désarmements. L'installateur peut configurer le système pour qu'il effectue des appels vers le serveur distant via les réseaux suivants :

- **RTC** (modem RTC requis)
- **GSM** (modem GSM requis)
- **Internet** (interface Ethernet)

Si vous utilisez un réseau RTC, assurez-vous que le modem RTC est bien installé et fonctionne correctement, et qu'une ligne RTC opérationnelle est connectée sur les bornes A et B du modem RTC.

Si vous utilisez le réseau GSM, assurez-vous que le modem GSM est bien installé et fonctionne correctement. Une connexion IP peut être réalisée par Internet sur un serveur avec une adresse IP publique fixe.

Si une connexion IP est requise, assurez-vous que l'interface Ethernet est correctement configurée (voir*Interface Ethernet* page 185) et que l'accès Internet est activé sur le routeur.

Ajout d'un récepteur EDP

1. Sélectionnez **Communications > Transmission > EDP**.

   La page suivante s'affiche :

Max. 8 récepteurs maxi peuvent être ajoutés au système SPC.

2. Cliquez sur le bouton **Ajouter**.

   La page suivante s'affiche.

3. Voir le tableau ci-dessous pour de plus amples informations.

Description	Entrez une description textuelle du récepteur.
Receiver ID (ID récepteur)	Saisissez un numéro unique qui sera utilisé par l'EDP pour identifier le récepteur.

Voir également

Édition des paramètres du récepteur EDP ci-dessous

Édition des paramètres du récepteur EDP

1. Sélectionnez **Communications > Transmission > EDP > Éditer**.

   La page suivante s'affiche.

Communications
FlexC
Transmission
Outils PC
CTS Analogique
EDP
CEI-ABI
Editer un récepteur
Libellé
EDP2
Description du récepteur
ID Récepteur
2
Identification numérique utilisée par l'EDP pour identifier le récepteur (1 - 999997)
Version de Protocole
Version 2
Sélectionner la version du protocole EDP à utiliser avec ce récepteur
Sécurité
Commandes activées
Cocher si les commandes externes sont autorisées depuis ce récepteur
Changer les codes Utilisateur
Cocher si le changement des codes Utilisateur est autorisé depuis ce récepteur EDP.
Clavier virtuel
Cocher pour autoriser l'accès d'un clavier virtuel depuis ce récepteur EDP.
Flux temps réel
Seulement après l'alarme
Sélectionner les paramètres de confidentialité pour les transmissions Audio/vidéo temps réeles vers ce récepteur.
Cryptage activé
Cocher si les données entrantes et sortantes du récepteur sont cryptées
Réseau
Réseau activé
Cocher si les évènements doivent être transmis via réseau Ethernet

2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Description	Éditez le nom du récepteur EDP. Le nom choisi peut comporter 16 caractères au maximum.
Receiver ID (ID récepteur)	Édition de l'ID récepteur de l'EDP. Intervalle de 1 à 999997 (999998 et 999999 sont réservés à des utilisations particulières)
Protocol Version (Version de protocole)	Sélectionnez la version de protocole EDP à utiliser avec ce récepteur EDP. Les options sont Version 1 ou Version 2. La Version 2 est recommandée si elle est prise en charge par le récepteur, car le protocole est plus sûr.
Compatibilité VdS 2471	(Norme Vds seulement) Si cette option est sélectionnée, le récepteur EDP mettra en œuvre les paramètres suivants pour ce récepteur : • 8s intervalle de test • Protocole TCP mis en œuvre • Nouveaux essais de TCP échouant avant 10s (9s approx.) • Le nombre de nouveaux essais d'événement EDP est fixé à 1, indépendamment du paramètre « Nombre de répétitions » dans « EDP - Télésurveillance IP ». • FTC sera généré dans les 20 s après une panne réseau.
Sécurité	
Commandes activées	Cochez cette case pour permettre aux commandes d'être accepté par le récepteur.
Changer les codes utilisateur	Cochez cette case pour permettre aux codes utilisateur d'être modifiés à partir d'un emplacement distant. Cette fonction ne s'applique que si les commandes sont activées à partir du récepteur.
Cryptage activé	Cochez cette case pour activer le cryptage sur les données vers et à partir du récepteur.
Clé de cryptage	Saisissez une clé hexadécimale (maxi 32 chiffres) qui sera utilisée pour crypter les données. **Remarque :** la même clé doit être utilisée sur le récepteur.
Clavier virtuel	Permet d'accéder à la centrale avec un clavier virtuel, c'est-à-dire un module logiciel de PC qui ressemble à un clavier SPC et qui agit comme lui. Il est disponible avec le client SPC Com.
Mode diffusion en continu	Signale qu'une diffusion en continu audio et vidéo est disponible. Les options sont Jamais, Toujours ou Uniquement après un événement d'alarme. La valeur par défaut est « Uniquement après un événement d'alarme ». **Remarque :** ce paramétrage touche clairement à la confidentialité et doit donc être activé uniquement lorsque c'est approprié et dans le respect des lois et réglementations locales.
Réseau (s'applique uniquement à la connexion Ethernet)	

Network Enable (Activer réseau)	Cochez cette case pour activer la transmission des événements dans le réseau.
Network Protocol (Protocole réseau)	Sélectionnez le type de protocole de réseau pour le récepteur. Les options sont UDP et TCP. TCP est recommandé s'il est accepté par le récepteur.
Adresse IP récepteur	Entrez l'adresse IP du récepteur.
Port IP récepteur	Saisissez le port IP que le récepteur EDP écoute.
Toujours connecté	Si activé, la centrale conserve une connexion permanente avec le récepteur. Si désactivé, la centrale ne se connecte au récepteur qu'après un événement d'alarme.
Centrale maître	Si activé, la centrale est le maître de la scrutation des messages. Applicable uniquement aux connexions UDP.
Intervalles des pollings	Entrez le délai en secondes entre deux scrutations.
Seuil Polling	Entrez le nombre de scrutations manquantes avant que l'échec de la connexion réseau soit signalé. Applicable uniquement aux connexions UDP.
Génère un défaut réseau	Si le test échoue, une alarme de défaut réseau est générée.
Numérotation (s'applique uniquement à la connexion par modem GPRS)	
Trans. par modem activée	Cochez cette case pour faire état d'événements au moyen d'une connexion par modem.
Type d'appel	Sélectionnez le type d'appel à utiliser quand la transmission par modem est activée. Sélectionnez GPRS.
Protocole GPRS	Sélectionnez le protocole de couche de transport utilisé sur la connexion GPRS. Les options sont UDP ou TCP. Applicable seulement si l'appel est du type GPRS.
Adresse GPRS	Sélectionnez l'adresse IP du récepteur EDP pour les connexions GPRS. Applicable seulement si l'appel est du type GPRS.
Port GPRS	Saisissez le port que le récepteur EDP écoute pour les connexions GPRS. Les options sont UDP ou TCP. Applicable seulement si l'appel est du type GPRS. La valeur par défaut est 50 000.
Tempo pour raccrocher GPRS	Saisissez le temps en secondes au bout duquel l'appel GPRS raccroche. (0 = rester connecté jusqu'à ce que la connexion IP soit disponible)
Autoconnexion GPRS	Cochez cette case pour déclencher automatiquement un appel GPRS vers le serveur si un défaut se produit sur le réseau IP.

Appel sur défaut réseau	Cochez cette case pour faire état de défauts sur le réseau lors d'un appel de test de numérotation.
Intervalle Numérotation 1*	Entrez le nombre de minutes entre deux tests de numérotation quand la liaison réseau est établie.
Intervalle Numérotation 2*	Entrez le nombre de minutes entre deux tests de numérotation quand la liaison réseau est tombée.
Adresse réseau*	Entrez l'adresse IP du récepteur. Cela n'est requis que si la connexion vers le récepteur EDP se déroule sur l'interface Ethernet. Si vous utilisez l'un des modems intégrés, laissez ce champ vide.
N° téléphone*	Saisissez le premier numéro de téléphone que le ou les modems vont composer pour contacter le récepteur.
N° téléphone 2*	Saisissez un deuxième numéro de téléphone que le ou les modems vont composer dans le cas où le premier numéro n'a pas permis d'établir la liaison.
Événements	
Récepteur principal	Cochez cette case pour indiquer qu'il s'agit du récepteur principal. Si la case n'est pas cochée, c'est qu'il s'agit d'un récepteur de secours.
Evénements gardés en attente	Cochez cette case si les événements qui n'ont pas pu être signalés doivent être réenvoyés au récepteur
Vérification	Cochez cette case si la vérification audio/vidéo doit être envoyée vers ce récepteur.
Event Filter (Filtre d'évènements)	Cliquez sur ce bouton pour éditer les filtres d'événements qui déclenchent un appel EDP. Voir *Éditer les paramètres du filtre d'événement* ci-dessous.

* L'appel EDP via RTC n'est pas pris en charge dans cette version.

Voir également

Programmation SMS page 219

Éditer les paramètres du filtre d'événement

1. Sélectionnez **Communications > Transmission > EDP > Éditer > Filtrer**.

   La page suivante s'affiche.

2. Configurez les champs comme indiqué dans le tableau ci-dessous.

   Cochez l'une des cases suivantes si vous voulez déclencher un appel à distance vers un récepteur EDP pour l'informer de l'événement particulier.

Alarmes	Les alarmes sont activées.
Fin d'alarme	Les alarmes système sont réinitialisées.
Alarmes confirmées	Alarmes confirmées par d'autres zones
Annulation d'alarme	Annulations d'alarme. Les alarmes sont annulées par la saisie d'un code utilisateur valide sur le clavier à la suite d'une alarme confirmée ou non.
Défauts	Les défauts et l'antipiratage sont activés.
RAZ défauts	Les défauts et l'antipiratage sont réinitialisés.
État de zone physique	Signalez toutes les modifications d'état d'entrée de zone.
Configurations	Le système est activé et désactivé.

Trop tôt / trop tard	Activation et désactivation du système non planifiées.
Inhibition	Des actions d'inhibition et d'isolation sont exécutées sur le système.
Evénements porte	Les événements porte sont activés. Ne fonctionne qu'avec le protocole SIA.
Autres	Tous les autres types d'événements sont détectés sur le système.
Autre (non standard)	Codes SIA utilisés avec SPC COM XT non pris en charge, notamment les événements Camera Online/Offline.
Réseau	Transmet les connexions/déconnexions du réseau IP (grâce à la scrutation).
Secteurs	Sélectionnez des secteurs spécifiques auxquels s'appliquent les événements ci-dessus.

Éditer les paramètres EDP

1. Sélectionnez **Communications > Transmission > EDP > Paramètres**.

   La page suivante s'affiche.

2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Enable (Validation)	Cochez cette case pour activer l'EDP sur le système.
ID EDP centrale	Saisissez un identifiant numérique utilisé par le récepteur EDP pour identifier uniquement la centrale.
Panel Port (Port de la centrale)	Sélectionnez le port IP pour recevoir les paquets IP. La valeur par défaut est 50 000.
Limite paquet	Saisissez le nombre maximum d'octets d'un paquet EDP pour la transmission.
Événement timeout	Saisissez le délai d'attente (en secondes) entre les retransmissions d'événements non acquittés.
Compteur d'essais	Saisissez le nombre maximal de retransmissions d'événement autorisé par le système.
Nbre de tentatives de numérotation	Saisissez le nombre maximal de tentatives de numérotation infructueuses qui sont acceptées par le système avant que le modem ne soit verrouillé (les appels suivants ne seront plus autorisés). La durée de suspension est définie dans l'option Suspension numérotation.
Délai de numérotation	Saisissez la durée d'attente (en secondes) avant que le système ne renouvelle l'appel après un échec.
Suspension numérotation	Saisissez la durée (en secondes) pendant laquelle le système va suspendre la numérotation lorsque le nombre maximal de tentatives infructueuses de numérotation a été atteint. Saisissez « 0 » pour autoriser une numérotation continue.

Options d'enregistrement d'événements au JDB

État des communications	Enregistrement dans le JDB de toutes les communications disponibles.
Commandes EDP	Enregistrement dans le JDB de toutes les commandes executées via EDP.
Événements A/V	Enregistrement dans le JDB lorsque les événements de vérification audio/vidéo sont envoyés au récepteur.
Diffusion en continu A/V	Enregistrement dans le JDB lorsque la diffusion en continu audio/vidéo commence.
Clavier utilisé	Enregistrement dans le JDB lorsque le clavier distant est activé.

17.10.3.3 Paramètres protocole CEI-ABI

1. Sélectionnez **Communications > Transmission > CEI-ABI**.

   La page suivante s'affiche :

2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Enable (Validation)	Cochez cette case pour activer le support CEI-ABI.
Mode de connexion	• Sélectionnez **Client** pour connecter la centrale au récepteur CEI-ABI. • Sélectionnez **Serveur** pour permettre à la centrale d'attendre les connexions.
IP Serveur	Si vous sélectionnez **Client** pour **Mode de connexion**, saisissez l'adresse TCP/IP du récepteur CEI-ABI.
Port serveur	Entrez le port IP du serveur.
Adresse physique	Saisissez une adresse physique pour le CEI-ABI sur la centrale.
Adresse logique	Saisissez une adresse logique pour le CEI-ABI sur la centrale.

17.10.4 Outils PC

Cette section recouvre :

17.10.4.1 SPC Connect PRO

SPC Connect PRO est une application de bureau destinée à l'installation et la maintenance des systèmes SPC. Grâce à SPC Connect PRO, vous pouvez créer et configurer des installations avant d'arriver sur un site. Cet outil peut également être utilisé en association avec le service de cloud SPC Connect pour se connecter à distance aux sites des clients et leur apporter une assistance technique.

1. Sélectionnez **Communications > Outils PC > SPC Connect PRO**.
2. Configurez les champs comme indiqué dans le tableau ci-dessous et cliquez sur **Enregistrer**.

SPC Connect PRO	Cochez cette case pour autoriser SPC Connect PRO à se connecter à la centrale.
Ethernet	Cochez cette case pour autoriser SPC Connect PRO à se connecter par Ethernet.
Port TCP	Saisissez le port TCP sur duquel la centrale reçoit les connexions entrantes en provenance de SPC Connect PRO.
USB	Cochez cette case pour autoriser SPC Connect PRO à se connecter par USB.
Série 1 (X10)	Cochez cette case pour autoriser SPC Connect PRO à se connecter par Série 1 (X10).
Modem 1	Cochez cette case pour autoriser SPC Connect PRO à se connecter par le modem 1.

17.10.4.2 SPC Manager

La configuration en mode SPC Manager détermine le nombre de caractères du code utilisateur et, par conséquent, le nombre de codes disponibles globalement dans le système sous contrôle de SPC Manager.

Mode41 : les codes PIN à 4 caractères activent un total de 1 000 utilisateurs

Mode51 : les codes PIN à 5 caractères activent un total de 10 000 utilisateurs

Mode61 : les codes PIN à 6 caractères activent un total de 100 000 utilisateurs

Mode71 : les codes PIN à 7 caractères activent un total de 1 000 000 utilisateurs

Mode81 : les codes PIN à 8 caractères activent un total de 10 000 000 utilisateurs

En mode SPC Manager, des zéros sont ajoutés devant les codes PIN d'utilisateur à 4 ou 5 caractères. Ceux-ci modifient le PIN pour une utilisation globale. Par exemple, si **Mode71 : codes à 7 chiffres** est sélectionné, 3 zéros sont ajoutés au code à 4 caractères existant. Ainsi, 2222 devient 0002222.

Pour activer le mode SPC Manager :

1. Sélectionnez **Communications > Outils PC > SPC Manager**.

2. Sélectionnez l'utilisateur général du SPC Manager dans le menu déroulant.
3. Cliquez sur le bouton **Enregistrer**.

   Le mode ne peut pas être activé si un conflit existe entre un code utilisateur local existant et un autre code du système général. L'erreur « Code invalide » s'affiche.
4. Cliquez sur le bouton approprié pour supprimer le code et enregistrer le nouveau mode ou pour accepter le nouveau code aléatoire affiché et enregistrer le nouveau mode.

REMARQUE : les modes SPC Manager ne peuvent pas être changés s'il existe des utilisateurs généraux dans le système.

17.11 Gestion des fichiers

Pour travailler avec les fichiers et la configuration de la centrale :

- Sélectionner **Fichier**.

  La fenêtre suivante s'affiche :

Mise à jour	Options de mise à niveau du contrôleur, du micrologiciel du périphérique et de la langue de la centrale. Voir *Mise à jour des fichiers* ci-dessous.
Gestionnaire de Fichiers	Options de gestion du fichier de configuration du système et de téléchargement entrant et sortant des données utilisateurs vers et de la centrale. Voir *Utilisation du gestionnaire de fichiers* page 356.
Audio	Télécharger un fichier audio sur le SPC. Cliquez sur **Naviguer** puis cliquez sur **Télécharger** pour ajouter le fichier audio sur le SPC. Après le téléchargement, cliquez sur le bouton **Test** pour valider le fichier audio.
Défaut	Rétablit la configuration usine par défaut du système SPC. **REMARQUE ! L'adresse IP est conservée pour se connecter à l'interface Web après un retour à la configuration usine à partir de la page Web.**
Réinitialisation	Redémarre la centrale.
Règles pour les textes	Cet onglet résume la configuration de votre produit SPC, pour les paramètres **sélectionnés Pays**, **Grade** et **Type** .

17.11.1 Mise à jour des fichiers

Pour la mise à niveau du firmware et des langues du système :

- Sélectionnez **Fichier > Mise à jour** .

  La page suivante apparaît :

Voir également

Options page 257

17.11.1.1 Mise à niveau du micrologiciel

REMARQUE : l'accès du fabricant est requis pour effectuer la mise à niveau. Il doit être valide à la fois pour la mise à niveau du micrologiciel de la centrale et de celui des périphériques. Voir *Options* page 257.

Le micrologiciel du SPC se trouve dans deux fichiers séparés :

- Fichier micrologiciel du contrôleur
  Contient uniquement le micrologiciel pour l'UC du contrôleur. Le nom de fichier a l'extension *.fw.
- Fichier micrologiciel du périphérique
  Contient le micrologiciel pour les nœuds X-BUS, ainsi que pour les modems RTC et GSM. Le nom de fichier a l'extension *.pfw.

Les deux fichiers sont mis à niveau séparément.

REMARQUE : il est recommandé de mettre à niveau tous les micrologiciels de périphérique après chaque nouvelle mise à niveau du micrologiciel du contrôleur.

Remarque : le micrologiciel peut également être mis à niveau à partir du clavier.

Firmware Centrale

Pour mettre à jour le firmware de la centrale :

1. Sélectionnez l'option **Opérations de mise à jour de la centrale** de la page **Fichier**.

   La page suivante apparaît :

2. Localisez le fichier firmware à mettre à jour en cliquant sur le bouton **Browse** (Rechercher) de l'option souhaitée puis cliquez sur **Mise à jour**.

   Une page de confirmation s'affiche.

3. Cliquez sur le bouton **Confirmer** pour confirmer la mise à niveau de la nouvelle version du micrologiciel du contrôleur.

   Lorsque le micrologiciel du contrôleur est mis à niveau, le système affiche un message pour indiquer que le système est en cours de réinitialisation. Vous devez vous reconnecter au système pour poursuivre votre tâche.

AVERTISSEMENT : si vous revenez à une version antérieure du micrologiciel du contrôleur (par exemple en installant une version moins récente), le système rétablira tous les paramètres par défaut. Par ailleurs, si vous revenez à une version antérieure du micrologiciel, il est important de faire de même avec le micrologiciel du périphérique correspondant. Dans le cas contraire, des zones peuvent apparaître déconnectées, ouvertes ou fermées.

AVERTISSEMENT : si vous mettez à niveau à partir d'une version du micrologiciel précédant la version 3.3, prenez en compte les points suivants :
– Le mot de passe Web Installateur, s'il existe, est effacé et doit être saisi de nouveau après la mise à niveau.
– Tous les utilisateurs existants se voient attribuer un nouveau profil utilisateur correspondant à leur niveau d'accès autorisé. Si le nombre maximal de profils utilisateur est dépassé, aucun profil n'est affecté (voir *Ajouter/modifier des profils utilisateur* page 214). Veuillez vérifier l'ensemble de la configuration utilisateur après une mise à niveau du micrologiciel.
– L'ID Installateur par défaut est modifiée de 513 à 9999.

Mise à jour des Firmware de Tags

Le firmware des périphériques est mis à jour en suivant la même procédure que pour le firmware de la centrale.

Le fichier du micrologiciel de périphérique n'est enregistré que temporairement parmi les fichiers système. Lorsqu'un nouveau fichier de micrologiciel de périphérique est téléchargé, la version actuelle et la nouvelle version du micrologiciel de chaque périphérique et modem sont affichées comme suit :

- Cliquez sur le bouton **Mise à niveau** pour les périphériques nécessitant une mise à niveau ou cliquez sur **Mise à jour complète** pour mettre à niveau tous les périphériques.

  Si le firmware d'un périphérique correspondant au ficher .pfw est plus ancien que la version actuelle, le bouton **Downgrade** s'active.

Au cours de la mise à jour, la centrale vérifie que le firmware du fichier admet la version du hardware installé sur les tags installés et rejette les mises à jour des tags qui ne sont pas pris en charge.

Si la version du fichier .pfw diffère de la version du contrôleur, un message d'avertissement s'affiche.

Si le numéro le plus élevé de version de firmware disponible est différent du numéro le plus élevé existant pour un tag, un message d'avertissement est également affiché.

Mise à niveau du micrologiciel du SPCP355.300 Smart PSU

Pour mettre à niveau le SPCP355.300 Smart PSU, vous devez vous assurer des éléments suivants :

- L'alimentation secteur doit être connectée.

Le micrologiciel du SPCP355.300 Smart PSU ne peut être mis à niveau que via le navigateur.

Cette procédure de mise à niveau peut prendre jusqu'à 2 minutes. N'effectuez aucune action sur le navigateur et ne redémarrez pas ou ne fermez pas le système avant la fin de la mise à niveau. Un message sera affiché une fois le processus terminé.

Voir également

Ajouter/modifier des profils utilisateur page 214

17.11.1.2 Mise à jour des langues

Vous pouvez télécharger un fichier de langue personnalisé (*.clng) sur la centrale.

REMARQUE : la centrale doit être autorisée pour la langue personnalisée et pour les autres langues.

Pour mettre à jour les langues du système :

1. Sélectionnez **Fichier > Mise à jour** .

   La page **Opérations de mise à jour de la centrale** est affichée :

2. Localisez le fichier firmware à mettre à jour en cliquant sur le bouton **Browse** (Rechercher) de l'option **Mise à jour des fichiers langues**, sélectionnez le fichier requis puis cliquez sur **Mise à jour**.

   La liste des langues disponibles dans ce fichier s'affiche.

3. Cochez la case en regard de la langue à installer.

4 langues au maximum peuvent être installées.

4. Cliquez sur le bouton **Mise à jour éléments sélectionnés**.

   La fenêtre **Confirmer MàJ langue** montre les langues en cours d'installation.

5. Cliquez sur le bouton **Confirmer**.

Un message est affiché pour indiquer si l'actualisation de la langue a été réussie ou a échoué.

Suppression des langues

Pour supprimer des langues du fichier langues :

1. Localisez le fichier firmware à mettre à jour en cliquant sur le bouton **Browse** (Rechercher) de l'option **Mise à jour des fichiers langues**, sélectionnez le fichier requis puis cliquez sur **Mise à jour**.

   La liste des langues disponibles dans ce fichier s'affiche.

2. Décochez les cases des langues à supprimer.
3. Cliquez sur le bouton **Mise à jour éléments sélectionnés**.

   La page **Confirmer MàJ langue** s'affiche. Pour supprimer une langue, la centrale désinstalle d'abord toutes les langues puis réinstalle les langues choisies.

4. Cliquez sur le bouton **Confirmer** pour confirmer les langues à supprimer.

Voir *Langue* page 277 pour un complément d'information concernant la sélection des langues « Système » et « Au repos » dans le navigateur.

Voir *Options* page 130 pour un complément d'information concernant la sélection des langues « Système » et « Au repos » avec le clavier.

Voir également

Langue page 277

17.11.2 Utilisation du gestionnaire de fichiers

- Sélectionnez **Fichier > Gestionnaire de fichiers**.

  Une page affiche les détails de la configuration du système, de la langue et des fichiers de suivi.

Fichier de configuration du système

Les options suivantes sont disponibles pour la gestion du fichier de configuration système :

Télécharger	Télécharge un fichier de configuration à partir du contrôleur. **Remarque :** si un message d'erreur apparaît après avoir cliqué sur le bouton de téléchargement, procédez comme suit : 1. Sélectionnez **Options Internet** dans le menu **Outils**. 2. Sélectionnez l'onglet **Avancé**. 3. Cochez la case **Ne pas enregistrer les pages cryptées sur le disque**. 4. Cliquez sur **Appliquer**. 5. Cliquez sur **OK**. 6. Cliquez à nouveau sur **Télécharger**. Lors du téléchargement sortant d'un fichier de configuration, les paramètres de configuration sont stockés dans un fichier **.cfg**. Ce fichier peut alors être téléchargé vers d'autres contrôleurs pour éviter des procédures de programmation longues.
Télécharger	Télécharge un fichier de configuration vers le contrôleur.
Secours	Enregistre une copie de secours de la configuration actuelle dans une mémoire flash.
Restaurer	Restaure une copie de secours de la configuration actuelle à partir de la mémoire flash.

Données utilisateur

Les options suivantes sont disponibles pour la gestion des données utilisateur :

Télécharger	Cliquez sur le bouton pour **Télécharger** les données utilisateur à partir de la centrale. Une boîte de dialogue demande si vous voulez enregistrer le fichier **user.csv**.
Télécharger	Cliquez sur le bouton **Parcourir** pour **Télécharger** les données utilisateur sur la centrale. Elles doivent se trouver dans un fichier au format .csv.

18 Accès à distance au serveur Web

Ce chapitre recouvre :

18.1 Connexion RTC **357**
18.2 Connexion GSM **359**

18.1 Connexion RTC

Connexion RTC

1	PC distant avec navigateur
2	Modem RTC
3	Réseau RTC
4	Ligne de téléphone
5	Modem RTC
6	Contrôleur SPC
7	JP9 ~~SPC4xxx~~

Il est possible d'accéder au serveur Web sur le contrôleur via une connexion distante sur une ligne téléphonique RTC. Un module RTC et une ligne RTC doivent être connectés sur le contrôleur comme indiqué ci-dessus pour permettre l'accès à distance au contrôleur.

À l'extrémité distante de la connexion, l'utilisateur doit disposer d'un modem RTC installé sur un PC ayant accès à une ligne RTC.

Pour accéder à distance à la centrale :

1. Installez un modem RTC sur le contrôleur (voir l'instruction d'installation correspondante).
2. Connectez la ligne téléphonique sur les bornes à vis A/B du connecteur sur le dessus du modem.

3. Utilisez le mode programmation Installateur à partir du clavier et configurez le modem (principal ou secours) pour répondre à un appel entrant.
4. Sur le clavier, allez sur **Paramétrage > Mode > Comms > Modems**.
5. Sélectionnez les réglages suivants :

   – **Valider modem :** activez le modem

   – **Type :** affiche le type de modem (RTC)

   – **Code pays :** sélectionnez le code pays adapté (Irlande, Royaume-Uni, Europe)

   – **Mode réponse :** sélectionnez le nombre de sonneries pour indiquer au modem d'attendre un certain nombre de sonneries avant de répondre à l'appel entrant

   – **Sonneries modem :** sélectionnez le nombre de sonneries avant de répondre à l'appel (maximum 8 sonneries)
6. Créez une connexion par modem sur le PC distant en utilisant le numéro de téléphone de la ligne connectée au module RTC du contrôleur. La configuration de la connexion d'accès à distance sous Windows XP est décrite ci-dessous.

Sous Windows XP :

1. Ouvrez l'Assistant nouvelle connexion en allant sur **Centrale > Connexions réseau > Créer de nouvelles connexions** (dans la page **Tâches du réseau**).
2. Sur la page **Type de connexion réseau**, sélectionnez **Établir une connexion à Internet**.
3. Sur la page **En cours de préparation**, choisissez **Configurer ma connexion manuellement**.
4. Sur la page **Connexion Internet**, choisissez **Se connecter en utilisant un modem d'accès à distance**.
5. Sur la page **Nom de la connexion**, saisissez le nom de la connexion, par exemple Connexion à distance SPC.
6. Sur la page **Numéro de téléphone à composer**, saisissez le numéro de téléphone de la ligne RTC connectée au modem RTC.
7. Sur la page **Disponibilité de la connexion**, indiquez si cette connexion est disponible pour tous les utilisateurs.
8. Sur la page **Informations de compte Internet**, entrez les données suivantes :

   – Nom d'utilisateur : SPC

   – Mot de passe : password (par défaut)

   – Confirmez le mot de passe : password

   La page **Fin d'exécution de l'assistant nouvelle connexion** s'affiche.
9. Cliquez sur **Terminer** pour enregistrer la connexion par modem sur le PC.

Le code par défaut doit être modifié et soigneusement conservé, car Vanderbilt ne sera pas en mesure de retrouver ce nouveau code. En cas d'oubli du code, il faudra revenir au code usine par défaut du système, ce qui effacera la programmation réalisée. La programmation peut être rétablie si une sauvegarde est disponible.

Pour activer la connexion d'accès à distance :

- Cliquez sur l'icône située sur la page **Centrale > Connexions réseau**.

  Le PC effectue un appel de données sur la ligne RTC connectée au module SPC RTC.

  Le module SPC RTC répond à l'appel de données après le nombre défini de sonneries et établit une liaison IP avec l'ordinateur distant.

  Le système SPC affecte automatiquement une adresse IP au PC distant.

Pour certains systèmes d'exploitation Windows, une boîte de dialogue relative à la certification Windows est affichée. Vanderbilt considère qu'il est possible de continuer. Pour toute question, adressez-vous à l'administrateur réseau ou à un technicien Vanderbilt.

Pour obtenir cette adresse IP :

1. Faites un clic droit sur l'icône de numérotation.
2. Cliquez sur l'onglet **Détails**.

   L'adresse IP s'affiche en tant qu'adresse IP du serveur.
3. Saisissez cette adresse IP dans la barre d'adresse du navigateur et cliquez.
4. Lorsque l'icône de connexion par modem s'affiche sur la barre des tâches du PC, ouvrez le navigateur et saisissez l'adresse IP du SPC.

   La page de connexion du navigateur s'affiche.

Pour établir une connexion par modem sur un autre système d'exploitation, consultez le menu d'aide du système d'exploitation concerné.

18.2 Connexion GSM

Connexion GSM

1	PC distant avec navigateur
2	Modem GSM
3	Modem RTC
4	Réseau GSM
5	Réseau RTC
6	Antenne externe
7	Modem GSM
8	Contrôleur SPC

Il est possible d'accéder au serveur Web sur le contrôleur via une connexion distante sur le réseau GSM. Un module GSM (avec une carte SIM) doit être connecté sur le contrôleur comme indiqué ci-dessus pour permettre l'accès à distance au SPC. L'option de transmission de données doit être activée sur la carte SIM et le numéro de donnée doit être utilisé.

Sur le côté distant de la connexion, l'utilisateur doit avoir un modem RTC ou GSM installé sur un PC équipé d'un navigateur. Si un modem RTC est installé, il doit être connecté à une ligne RTC fonctionnelle.

Pour accéder à distance à la centrale :

1. Installez un modem GSM sur le contrôleur (voir l'instruction d'installation correspondante).
2. Utilisez le mode de programmation Paramétrage à partir du clavier et configurez le modem (principal ou secours) pour répondre à un appel entrant.
3. Sur le clavier, allez sur le menu suivant : PARAMÉTRAGE > COMMUNICATION > MODEMS, et sélectionnez les paramètres listés :

Valider modem	Activez l'option MODEM VALIDE.
Type	Affiche le type de modem (GSM).
Code pays	Sélectionnez le code pays adapté.
Mode réponse	Sélectionnez le nombre de sonneries pour indiquer au modem d'attendre un certain nombre de sonneries avant de répondre à l'appel entrant.
Sonneries modem	Sélectionnez le nombre de sonneries avant de répondre à l'appel (maximum 8 sonneries).

Sous Windows XP :

1. Ouvrez l'**Assistant nouvelle connexion** en allant sur **Centrale > Connexions réseau > Créer de nouvelles connexions** (dans la fenêtre **Tâches du réseau**).
2. Dans la fenêtre **Type de connexion réseau**, sélectionnez **Établir une connexion à Internet**.
3. Dans la fenêtre **En cours de préparation**, choisissez **Configurer ma connexion manuellement**.
4. Dans la fenêtre **Connexion Internet**, choisissez **Se connecter en utilisant un modem d'accès à distance**.
5. Dans la fenêtre **Nom de la connexion**, saisissez le nom de la connexion, par exemple Connexion à distance SPC.
6. Dans la fenêtre **Numéro de téléphone à composer**, saisissez le numéro de téléphone de la ligne GSM connectée au modem GSM.
7. Dans la fenêtre **Disponibilité de la connexion**, indiquez si cette connexion est disponible pour tous les utilisateurs.
8. Dans la fenêtre **Information de compte Internet**, entrez les données suivantes :

   – Nom d'utilisateur : SPC

   – Mot de passe : password

   – Confirmez le mot de passe : password

   La page **Fin d'exécution de l'assistant nouvelle connexion** s'affiche.
9. Cliquez sur **Terminer** pour enregistrer la connexion par modem sur le PC.

Pour activer la connexion d'accès à distance :

- Cliquez sur l'icône située sur la page **Centrale > Connexions réseau**.

  Le PC effectue un appel de données sur la ligne GSM connectée au module SPC GSM.

Le module SPC GSM répond à l'appel de données après le nombre défini de sonneries et établit une liaison IP avec l'ordinateur distant.

Le système SPC affecte automatiquement une adresse IP au PC distant.

Pour certains systèmes d'exploitation Windows, une boîte de dialogue relative à la certification Windows est affichée. Vanderbilt considère qu'il est possible de continuer. Pour toute question, adressez-vous à l'administrateur réseau ou à un technicien Vanderbilt.

Pour obtenir cette adresse IP :

1. Faites un clic droit sur l'icône de numérotation.
2. Cliquez sur l'onglet **Détails**.

   L'adresse IP s'affiche en tant qu'adresse IP du serveur.
3. Saisissez cette adresse IP dans la barre d'adresse du navigateur et cliquez.
4. Lorsque l'icône de connexion par modem s'affiche sur la barre des tâches du PC, ouvrez le navigateur et saisissez l'adresse IP du SPC.

   La page de connexion du navigateur s'affiche.

Pour établir une connexion par modem sur un autre système d'exploitation, consultez le menu d'aide du système d'exploitation concerné.

19 Fonction alarme anti-intrusion

Le système SPC peut fonctionner selon trois modes différents (Bancaire, Évolué et Simple), chacun prenant en charge plusieurs secteurs.

Chaque secteur peut fonctionner selon quatre modes d'alarme différents. Les modes Évolué et Bancaire disposent de plus de types d'alarme programmables que le mode Simple. Les noms et les types de zones par défaut pour chaque mode sont indiqués dans *Paramètres par défaut des modes Simple, Évolué et Bancaire* page 384.

19.1 Fonctionnement mode Bancaire

Le mode Bancaire convient à des établissements bancaires ou financiers qui possèdent des zones sécurisées, comme les chambres fortes et les DAB.

Chaque secteur défini sur le système dispose des modes d'alarme listés ci-dessous.

Mode d'alarme	Description
MHS	Le secteur est désactivé, seules les zones d'alarme classées 24 HEURES activent l'alarme.
MES PART. A	Ce mode assure la protection du périmètre d'un immeuble, tout en autorisant le libre déplacement dans les zones d'entrée et d'accès. Les zones désignées comme EXCLUS A ne sont pas protégées dans ce mode. Par défaut, il n'y a pas de temporisation de sortie (le système s'active instantanément lorsque ce mode est sélectionné). Une temporisation de sortie peut être appliquée à ce mode en activant la variable MES Partielle A temporisée.
MES PART. B	L'option MES PARTIELLE B applique la protection à toutes les zones sauf aux zones exclues à l'aide de l'attribut de zone EXCLUS B. Par défaut, il n'y a pas de temporisation de sortie (le système s'active instantanément lorsque ce mode est sélectionné). Une temporisation de sortie peut être appliquée à ce mode en activant la variable MES Partielle B temporisée.
MES TOTALE	La mise en surveillance totale du secteur est sans restriction, l'ouverture d'une zone d'entrée / de sortie lance la temporisation d'entrée. L'alarme est activée si elle n'est pas arrêtée avant l'expiration de la temporisation.

19.2 Fonctionnement mode Évolué

Le mode Évolué est adapté aux entreprises ayant plusieurs secteurs et de nombreuses zones d'alarme. Chaque secteur défini sur le système dispose des modes d'alarme listés ci-dessous.

Mode d'alarme	Description
MHS	Le secteur est désactivé, seules les zones d'alarme classées 24 HEURES activent l'alarme.

Mode d'alarme	Description
MES PART. A	Ce mode assure la protection du périmètre d'un immeuble, tout en autorisant le libre déplacement dans les zones d'entrée et d'accès. Les zones désignées comme EXCLUS A ne sont pas protégées dans ce mode. Par défaut, il n'y a pas de temporisation de sortie (le système s'active instantanément lorsque ce mode est sélectionné). Une temporisation de sortie peut être appliquée à ce mode en activant la variable MES Partielle A temporisée.
MES PART. B	La option MES PARTIELLE B applique la protection à toutes les zones sauf aux zones exclues à l'aide de l'attribut de zone EXCLUS B. Par défaut, il n'y a pas de temporisation de sortie (le système s'active instantanément lorsque ce mode est sélectionné). Une temporisation de sortie peut être appliquée à ce mode en activant la variable MES Partielle B temporisée.
MES TOTALE	La mise en surveillance totale du secteur est sans restriction, l'ouverture d'une zone d'entrée / de sortie lance la temporisation d'entrée. L'alarme est activée si elle n'est pas arrêtée avant l'expiration de la temporisation.

19.3 Fonctionnement mode Simple

Le mode Simple est adapté aux installations résidentielles ayant un ou plusieurs secteurs et un nombre faible ou limité de zones d'alarme. Chaque secteur défini sur le système dispose des modes d'alarme listés ci-dessous.

Mode d'alarme	Description
MHS	Le secteur est désactivé, seules les zones d'alarme classées 24 HEURES activent l'alarme.
MES PART. A	Ce mode assure la protection du périmètre d'un bâtiment tout en autorisant le libre déplacement dans les zones d'entrée et d'accès (par exemple la porte principale et le hall d'entrée) Les zones désignées comme EXCLUS A ne sont pas protégées dans ce mode. Il n'y a pas de temporisation de sortie associée à ce mode et la protection est appliquée instantanément dès que ce mode est choisi.
MES PART. B	L'option MES PARTIELLE B applique la protection à toutes les zones sauf aux zones exclues à l'aide de l'attribut de zone EXCLUS B. Par défaut, il n'y a pas de temporisation de sortie ; le système s'active instantanément lorsque ce mode est sélectionné. Une temporisation de sortie peut être appliquée à ce mode en activant la variable MES Partielle B temporisée.
MES TOTALE	La mise en surveillance totale du secteur est sans restriction, l'ouverture d'une zone d'entrée / de sortie lance la temporisation d'entrée. L'alarme est activée si elle n'est pas arrêtée avant l'expiration de la temporisation d'entrée.

19.4 Alarmes totales et locales

Le type d'alarmes généré par le système SPC peut varier en fonction du type de zone qui a déclenché l'alarme. La très grande majorité des alarmes nécessitent une indication visuelle (flash) et sonore (sirène) en cas d'intrusion dans des locaux ou un bâtiment.

Par défaut, les trois premières sorties physiques du contrôleur SPC sont affectées à une sirène extérieure, une sirène intérieure et un flash sirène extérieure. Lorsqu'elles sont activées, ces trois sorties combinées

sont suffisantes pour informer d'une condition d'alarme les personnes situées à l'intérieur ou dans l'environnement immédiat du bâtiment ou des locaux où s'est déroulée l'intrusion.

Les alarmes totales et locales sur le SPC activent les sorties physiques suivantes :

- Sortie de contrôleur 1 : sirène extérieure
- Sortie de contrôleur 2 : sirène intérieure
- Sortie de contrôleur 3 : flash

Pour plus de détails sur le mode de câblage des sirènes et du flash, consultez *Câblage du système* page 85.

Une activation **Alarme totale** reporte l'alarme au centre de télésurveillance (CTS) si celui-ci a été configuré sur le système.

Une activation **Alarme locale** ne déclenche pas d'appel vers le CTS, même si celui-ci a déjà été configuré.

Une **Alarme silencieuse** n'active pas les sorties 1 – 3 (pas de signal visuel ou sonore de l'alarme). L'événement d'alarme est transmis au CTS. Les alarmes silencieuses sont générées uniquement si une zone ayant l'attribut Silencieux est ouverte pendant que le système est mis en surveillance.

20 Exemples de systèmes et scénarios

Ce chapitre recouvre :

20.1 Comment utiliser un secteur commun **367**

20.1 Comment utiliser un secteur commun

Les secteurs communs offrent un moyen simple de paramétrer plusieurs secteurs dans une seule installation. Un utilisateur affecté à un secteur commun a la possibilité de METTRE EN SURVEILLANCE les secteurs de ce secteur commun (même ceux qui ne lui ont pas été affectés). Cependant, tout utilisateur ne peut METTRE HORS SURVEILLANCE que les secteurs qui lui ont été affectés.

Les secteurs communs ne doivent être utilisés que lorsqu'un seul clavier est installé à l'emplacement d'accès principal et partagé par tous les utilisateurs du bâtiment (il n'est pas recommandé de définir un secteur commun sur un système avec plusieurs claviers dans différents secteurs).

Scénario : deux services d'une entreprise (Comptabilité et Ventes) partagent un point d'accès commun (porte principale)

Dans ce cas, créez trois secteurs sur le système (Secteur commun, Comptabilité et Ventes). Le Secteur commun doit inclure le point d'accès principal (porte principale). Attribuez les zones de la Comptabilité au Secteur 2, et les zones des Ventes au Secteur 3. Installez un clavier à la porte principale et attribuez-le aux trois secteurs. Définissez deux utilisateurs (minimum) sur le système, un pour chaque service, et affectez les utilisateurs à leur secteur respectif et au secteur commun.

Fonctionnement : mise en service du système

Le responsable de la Comptabilité quitte le bureau à 17 heures. Quand il tape son code sur le clavier, le menu MES TOTALE propose les 3 options suivantes :

- TOUS SECTEURS : active tous les secteurs attribués au secteur commun (Secteur commun, Comptabilité, Ventes) et tous les autres secteurs attribués au responsable (dans cet exemple, pas d'autres secteurs). La temporisation de sortie sur la porte principale informe l'utilisateur qu'il doit quitter le bâtiment.
- COMMUN : active tous les secteurs attribués au secteur commun (Secteur commun, Comptabilité, Vente) et lance le temporisateur de sortie pour la porte principale.
- COMPTABILITÉ : active uniquement le secteur Comptabilité. Le secteur Vente n'est pas mis en surveillance et l'accès par la porte principale est toujours possible.

Lorsque le dernier employé du service Ventes quitte le bâtiment, il ferme toutes les portes et fenêtres du SECTEUR 3 et saisit son code sur le clavier. Le menu MES TOTALE propose les 3 options suivantes :

- TOUS SECTEURS : active tous les secteurs attribués au secteur commun (Secteur commun, Comptabilité, Ventes) et tous les autres secteurs attribués à l'employé du service Ventes (dans cet exemple, pas d'autres secteurs). La temporisation de sortie sur la porte principale informe l'utilisateur qu'il doit quitter le bâtiment.
- COMMUN : active tous les secteurs attribués au secteur commun (Secteur commun, Comptabilité, Vente) et lance le temporisateur de sortie pour la porte principale.
- VENTE : active TOUS les secteurs attribués au secteur commun (Secteur commun, Comptabilité, Vente) parce qu'il n'y a plus aucun autre secteur hors surveillance dans le système.

Fonctionnement : mise hors surveillance du système

Quand le responsable du service Comptabilité retourne au bureau le jour suivant, il tape son code sur le clavier et le menu MISE A L'ARRET propose les 3 options suivantes :

- TOUS SECTEURS : désactive tous les secteurs attribués à la Comptabilité (Secteur commun, Comptabilité) et les autres secteurs attribués au responsable. Dans ce cas, il n'y a pas de secteur supplémentaire.

  Remarque : un employé de la Comptabilité ne peut pas METTRE HORS SURVEILLANCE le secteur Ventes.
- COMMUN : désactive UNIQUEMENT le secteur commun (Réception). Cela laisse la possibilité de désactiver uniquement le secteur Réception tout en laissant la Comptabilité et les Ventes sous surveillance.
- COMPTABILITÉ : désactive le secteur Comptabilité et le secteur commun (Réception). Dans ce cas, le secteur Ventes reste sous surveillance tandis que l'accès par la porte principale est toujours possible.

Utilisation des secteurs communs :

- Zone clé de MES

  Si le chemin d'entrée/sortie dans le secteur commun est programmé en tant que zone clé de MES, tous les secteurs du secteur commun sont MIS EN SURVEILLANCE lorsqu'il est activé. La désactivation de la zone clé de MES MET HORS SURVEILLANCE tous les secteurs dans les secteurs communs.
- Claviers multiples

  Si des secteurs affectés au secteur commun disposent de leur propre clavier pour l'entrée et la sortie, il est important que les durées de sortie associées à ces secteurs laissent suffisamment de temps à l'utilisateur pour qu'il puisse atteindre la sortie du secteur commun. Cela pour le cas où le secteur en cours d'activation est le dernier secteur désactivé du système, ce qui aboutit donc à l'activation de la totalité du secteur commun.

En guise de règle, nous recommandons d'utiliser les secteurs communs dans les installations qui n'ont qu'un seul clavier situé au point d'accès commun, c'est-à-dire la porte d'accès principale à la totalité du bâtiment.

21 Détecteurs sismiques

Les détecteurs de vibration, également appelés détecteurs sismiques, sont utilisés pour détecter une intrusion effectuée à l'aide de moyens mécaniques tels que le perçage des parois et des coffres.

La prise en charge des détecteurs sismiques est possible uniquement si le type d'installation pour la centrale est « Bancaire ».

Il existe plusieurs moyens pour tester les détecteurs sismiques. Le moyen le plus simple pour tester les détecteurs sismiques est de taper fortement sur un mur ou un coffre au cours d'un test de déplacement et de vérifier que la zone s'ouvre bien. Cette méthode de test convient à tous les détecteurs sismiques.

Si le détecteur sismique est équipé d'un émetteur de contrôle, les options de test suivantes sont possibles :

- test manuel lancé au clavier (non pris en charge par le navigateur) ;
- test automatique périodique ou lorsque la centrale est mise en service à l'aide du clavier.

L'émetteur de contrôle est un vibrateur haute fréquence fixé à faible distance du détecteur sur le même mur. L'émetteur de contrôle est câblé sur une sortie de la centrale ou d'un transpondeur.

Configuration des détecteurs sismiques dans la centrale

1. Configurer une zone sismique. Les détecteurs sismiques doivent être affectés à une zone. (Consultez *Édition d'une zone* page 277.)

2. Déterminez les attributs pour la zone.

3. Activez le test automatique du détecteur avec l'attribut **Test sismique**.
4. Sélectionnez un calendrier de contrôle de la zone sismique, le cas échéant.
5. Affectez cette zone à une zone de vérification si une vérification audio/vidéo est requise.
6. Configurez les temporisations pour définir la fréquence de test des zones sismiques (la valeur par défaut est 7 jours) et la durée des tests. (L'attribut de zone Test sismique automatique doit être activé). (Consultez *Temporisations* page 269.)

7. Configurez une sortie pour tester une zone sismique. (Consultez *Types de sortie et ports de sortie* page 161.)
   Si la centrale est configurée pour utiliser des secteurs (comme c'est habituellement le cas dans les environnements bancaires), la sortie peut être affectée soit au système, soit au secteur. La sortie ne doit être affectée au système que si la centrale n'utilise pas de secteurs.

Utilisation du clavier

1. Sélectionnez **PARAMÉTRAGE > ZONES > (sélectionner zone) > TYPE DE ZONE > SISMIQUE**.
2. Sélectionnez **PARAMÉTRAGE > ZONES > (sélectionner zone) > ATTRIBUTS > AUTOTEST SISMIQUE**.

Voir également

Temporisations page 269

Types de sortie et ports de sortie page 161

Édition d'une zone page 277

21.1 Test des détecteurs sismiques

Les zones sismiques doivent être configurées pour que les tests manuels et automatiques puissent se dérouler. Que le test soit manuel ou automatique, le résultat est sauvegardé dans le JDB.

Au cours d'un test sismique, une ou plusieurs zones sismiques sont testées. Lorsqu'une zone est testée, toutes les autres zones du même secteur sont temporairement désactivées car il n'y a qu'un seul résultat de test sismique par secteur.

21.1.1 Procédures de tests manuel et automatique

Un test manuel ou automatique se déroule de la manière suivante :

1. La centrale active la sortie Test sismique pour le ou les secteurs auxquels appartiennent la ou les zones à tester.
2. La centrale attend que toutes les zones à tester s'ouvrent puis vérifie que tous les capteurs sismiques du secteur passent en état d'alarme dans le délai configuré pour la **Durée du test sismique**. Toute zone ne s'étant pas ouverte dans le délai fixé est considérée comme n'ayant pas réussi le test.
3. Lorsque toutes les zones sismiques du secteur sont ouvertes ou que le délai maximal de test sismique est atteint (premier événement à se produire), la centrale efface la sortie du test sismique pour ce secteur.

4. La centrale attend le délai fixé pour que tous les capteurs sismiques du secteur se ferment. Toute zone ne s'étant pas fermée est considérée comme n'ayant pas réussi le test.
5. La centrale attend encore un délai fixé avant de transmettre le résultat du test. Que le test soit manuel ou automatique, le résultat est sauvegardé dans le JDB.

La sortie sismique est normalement haute ; elle baisse au cours du test (ç.-à-d., lorsqu'elle est active). Si le signal n'est pas adapté à un détecteur donné, alors la sortie physique peut être configurée de manière à être inversée.

21.1.2 Test automatique des détecteurs

Les détecteurs sismiques sont testés soit périodiquement, soit après que le système a été mis en surveillance à l'aide du clavier.

Test automatique périodique

Les tests automatiques périodiques sont réalisés sur toutes les zones sismiques pour lesquelles les tests automatiques sont activés.

Les tests automatiques sont randomisés pendant la période de test configurée et sont effectués de manière indépendante pour chaque secteur.

Toutes les zones sismiques d'un même secteur (pour lequel les tests automatiques sont activés) sont testées simultanément.

L'option de configuration **Période de test sismique** dans le menu **Temporisations du système** (voir *Temporisations* page 269) détermine la périodicité moyenne pour les tests automatiques des détecteurs sismiques. La valeur par défaut est fixée à 168 heures (soit 7 jours) ; des valeurs comprises dans l'intervalle 12 – 240 heures sont admises.

La durée du test est choisie de manière aléatoire dans la plage spécifiée +/- 15 %. Par exemple si un test est prévu toutes les 24 heures, il peut être réalisé entre 20,4 et 27,6 heures après le dernier test.

Un test sismique est réalisé après chaque réinitialisation, sous réserve que les tests automatiques soient validés. Si la centrale était en mode Paramétrage avant une réinitialisation, le test n'est alors réalisé que lorsque la centrale a quitté le mode Paramétrage après la réinitialisation.

Si le test sismique échoue, un événement Anomalie est signalé (SIA code « BT »). Un événement Restauration lui est également associé (SIA code « BJ »).

Test automatique lors de la MES

L'option **Test sismique si MES** est configurable dans le menu **Options** (voir *Options* page 257). Si elle est activée, toutes les zones sismiques dans l'ensemble des secteurs devant être mis en surveillance sont testées avant la séquence de mise en surveillance normale. Ceci ne s'applique qu'en mode clavier.

Lorsque le test est en cours d'exécution, « AUTOTEST SISMIQUE » s'affiche sur le clavier. Si le test sismique réussit, la mise en surveillance se déroule normalement.

Si tous les secteurs, un groupe de secteurs ou un seul secteur sont sélectionnés pour être mis en surveillance et si un test sismique échoue, alors le message « ÉCHEC DU TEST SISMIQUE » s'affiche. En cliquant sur **Retour**, vous affichez une liste des zones en défaut que vous pouvez consulter à l'aide des touches de flèche vers le haut et vers le bas.

En fonction des paramètres **Inhiber** définis pour les zones sismiques en défaut et pour votre profil utilisateur, les événements suivants peuvent se passer :

- Si toutes les zones sismiques ayant échoué au test ont l'attribut **Inhiber** et que votre profil d'utilisateur est configuré avec le droit **Inhiber** :

1. Appuyez sur **Retour** sur l'une quelconque des zones en défaut.

   Le message « TOUT FORCER ? » s'affiche.
2. Appuyez à nouveau sur **Retour** pour inhiber toutes les zones sismiques qui ont échoué au test.

(Vous pouvez également revenir au menu précédent.)

La mise en surveillance se poursuit normalement.

- Si certaines des zones sismiques ayant échoué au test n'ont pas l'attribut **Inhiber** ou que votre profil d'utilisateur ne dispose pas du droit **Inhiber**, appuyez sur **Retour**.

  Le message « ÉCHEC MES » s'affiche et aucun secteur n'est mis en surveillance.

Il n'y a pas de test sismique automatique pour les secteurs qui se mettent automatiquement en surveillance pour quelque raison que ce soit (par exemple, des secteurs activés par un calendrier ou un déclencheur). De même, il n'y a pas de test sismique automatique lorsque le système est mis en surveillance avec SPC Com ou le navigateur. Néanmoins, un test sismique automatique est réalisé lorsqu'un clavier virtuel est utilisé avec SPC Com.

Aucun événement n'est signalé si le test sismique échoue lors de la mise en surveillance.

Après la mise en surveillance, la temporisation de test automatique du système se réinitialise après chaque exécution de test.

21.1.3 Test manuel des détecteurs

Pour tester manuellement les détecteurs, sélectionnez l'option TEST > TEST SISMIQUE dans le menu TEST sur le clavier.

Un test sismique manuel peut être réalisé au clavier par l'installateur en mode Paramétrage ou par un utilisateur du type Manager ou Standard :

- Un installateur est autorisé à tester tous les détecteurs dans tous les secteurs configurés du système à l'aide de n'importe quel clavier.
- Un utilisateur est autorisé à tester uniquement les détecteurs des secteurs qui sont affectés à lui-même et au clavier particulier qu'il utilise.

Pour effectuer un test sismique en mode Paramétrage, sélectionnez PARAMÉTRAGE > TEST > TEST SISMIQUE.

Pour effectuer un test sismique en mode Utilisateur, sélectionnez MENUS > TEST > TEST SISMIQUE.

Remarque : les instructions suivantes s'appliquent aux modes Installateur et Utilisateur, mais il convient de noter que seule une partie des options est accessible à un utilisateur.

Les options suivantes sont accessibles dans le menu TEST SISMIQUE :

- TESTER TOUS LES SECTEURS
  Permet de tester les zones sismiques dans tous les secteurs disponibles, lorsqu'il y a au moins deux secteurs qui contiennent des zones sismiques.
- *« NOM DU SECTEUR »*
  Les noms des secteurs contenant des zones sismiques sont listés individuellement. Si un secteur spécifique est sélectionné, les options suivantes sont possibles :

  – TESTER TOUTES LES ZONES
  Permet de tester toutes les zones sismiques de ce secteur, lorsqu'il y a au moins deux zones sismiques.

  – *« NOM DE LA ZONE »*
  Les noms de toutes les zones sismiques sont listés et peuvent être sélectionnés pour être testés individuellement.

Le message « TEST SISMIQUE » s'affiche sur le clavier en cours de test.

Si le test échoue, le message « ÉCHEC DU TEST SISMIQUE » s'affiche. Si la touche « i » ou VOIR est pressée, vous verrez s'afficher une liste de toutes les zones en défaut que vous pourrez balayer.

Si le test réussit, le message « TEST SISMIQUE OK » s'affiche.

Les informations sont enregistrées dans le journal des événements avec les détails suivants :

- utilisateur à l’origine du test
- résultat (OK ou ÉCHEC)
- numéros et noms du secteur et de la zone.

Les événements ne sont pas rapportés pour les tests manuels.

22 Utilisation du verrouillage de blocage

L'utilisation du verrouillage de blocage et celle d'activation autorisée d'un blocage de verrouillage sont prises en charge par la centrale SPC.

22.1 Verrouillage de blocage

Un verrouillage de blocage est un verrouillage mécanique mis en place dans une porte en plus du verrou normal. Il est utilisé pour activer et désactiver le système d'intrusion. SPC prend en charge les appareils à verrouillage de blocage normaux (Blockschloss 1), tout comme les appareils Bosch Blockschloss, Sigmalock Plus et E4.03 (Blockschloss 2).

En fonction du type de verrouillage de blocage, il faut un signal pour activer le verrouillage et le déverrouillage du verrou. Cela signifie que le verrouillage de blocage ne peut être verrouillé et le système activé que si le signal « MES possible » est affiché sur la centrale. Cela est contrôlé par un commutateur magnétique.

Un verrouillage de blocage s'utilise de la manière suivante :

1. si aucune zone n'est ouverte, en attente d'alarme ou en attente d'alarme dans le secteur, le secteur est prêt à être activé et le signal MES Possible est envoyé par la centrale.
2. Si l'appareil a verrouillage de blocage est alors verrouillé, la sortie Blockschloss 1/2 est activée.
3. Suite au changement correspondant sur le type d'entrée de clef de mise en service, le secteur respectif est défini.
4. La sortie Acquis de MES est activée pendant 3 secondes pour signaler une activation réussie du secteur. La sortie Blockschloss 1 est désactivée lorsque le système est activé. Blockschloss 2 reste activée une fois le système activé.
5. Si le verrouillage de blocage est déverrouillé, l'entrée de clé de mise en service passe en état non activé (fermé).
6. Après la modification du type d'entrée de la clé de MES, le secteur est désactivé. Blockschloss 1 est désactivée si le secteur est prêt à l'activation, tandis que Blockschloss 2 est activée dans la même configuration.

Les exigences en matière de configuration pour un verrouillage de blocage sont les suivantes :

- Sorties :
  – MES possible
  – Acquis de MES
  – MES totale faite
  – Blockschloss 1/2
- Entrées
  – Armement par clé

22.2 Activation autorisée du verrouillage de blocage

La fonctionnalité d'autorisation d'activation étend la procédure d'activation et de désactivation pour un verrouillage de blocage avec un deuxième niveau de sécurité. Avant de pouvoir activer ou désactiver le système, il faut qu'un code soit saisi sur un appareil externe, tel qu'un lecteur de badge ou de code équipé d'un contrôleur distinct. Ce contrôleur peut être connecté à tout système d'intrusion à l'aide des sorties et des entrées.

Il fonctionne de la manière suivante :

1. la centrale signale à l'appareil externe d'activation lorsqu'il est possible d'activer à l'aide d'une sortie MES possible.
2. Une fois le code entré, l'entrée d'autorisation d'activation est définie et le Blockschloss 1/2 est activé.
3. Le verrouillage de blocage ouvre une entrée de la centrale (clef de MES) qui démarre la procédure d'activation de la centrale.
4. L'appareil externe d'activation attend jusqu'à 8 secondes que le signal MES totale faite soit activé à partir de la centrale.
5. Si ce signal n'est pas reçu, l'activation échoue et l'appareil d'activation externe désactive à nouveau le système.

Les exigences de configuration de l'autorisation d'activation sont les suivantes :

- Attributs de secteur :

  – Autorisation MES

  ON

  MES et MHS (nécessaire pour VdS)

  Mise hors surveillance

- Sorties :

  – MES possible

  – Acquis de MES

  – MES totale faite

- Entrées

  – Armement par clé

22.3 Élément de verrouillage

Pour VdS, il est obligatoire d'empêcher l'entrée dans un secteur activé. Cela est possible à l'aide d'un élément de verrouillage monté dans le cadre de la porte. Il consiste en un petit boulon en plastique qui bloque la porte dans l'état MES. La position du boulon est signalée par les sorties **Élément de verrouillage – Verrouiller** ou **Élément de verrouillage – Déverrouiller**. Ce signal est contrôlé pendant le processus d'activation. Si l'information « verrouillé » n'est pas reçue, l'activation échoue.

Si un élément de verrouillage se trouve dans un secteur, la temporisation de sortie sera au moins égale à quatre secondes pour que l'élément de verrouillage puisse être activé. Au bout de quatre secondes, l'élément de verrouillage sera activé pendant trois secondes. Une fois cette durée atteinte, l'entrée **Élément de verrouillage** doit être en état fermé. Le système sera alors activé.

Si un élément de verrouillage est ouvert pendant une période d'activation, il sera traité comme une zone d'alarme.

Si un élément de verrouillage est fermé pendant un processus de désactivation, il sera alors considéré comme cible d'un essai de sabotage et émettra une alarme antisabotage sur le secteur.

Si l'élément de verrouillage n'arrive pas à s'ouvrir une fois le signal de déverrouillage envoyé à l'appareil, un avis de problème sera émis dans cette zone pour signaler qu'un problème mécanique s'est produit.

Si l'entrée **Élément de verrouillage** (si elle est configurée) ne se trouve pas en état fermé lorsque la temporisation arrive à expiration, le système ne sera pas activé et un signal Echec MES sera émis. La sortie **Élément de verrouillage – Déverrouiller** sera désactivée.

Les exigences de configuration pour l'élément de verrouillage sont les suivantes :

- Sorties :
  - Élément de verrouillage – Bloquer
  - Élément de verrouillage – Débloquer
- Entrées
  - Élément de verrouillage

23 Annexe

Cette annexe recouvre :

23.1 Connexions du câble réseau **379**
23.2 LED d'état du contrôleur **380**
23.3 Alimentation des transpondeurs à partir des bornes auxiliaires **381**
23.4 Calcul de la puissance nécessaire pour la batterie **382**
23.5 Paramètres par défaut des modes Simple, Évolué et Bancaire **384**
23.6 Câblage de l'interface X10 ..... **385**
23.7 Codes SIA **386**
23.8 Codes CID **391**
23.9 Vue d'ensemble des types de clavier **393**
23.10 Combinaisons de codes utilisateur **394**
23.11 Codes utilisateur de contrainte **394**
23.12 Inhibitions automatiques **394**
23.13 Raccordement du câble secteur sur le contrôleur **395**
23.14 Contrôleur de maintenance **395**
23.15 Maintenance Smart PSU **396**
23.16 Types de zone **397**
23.17 Attributs zone **404**
23.18 Attributs applicables aux types de zones **408**
23.19 Niveaux ATS et spécifications d'atténuation **409**
23.20 Lecteurs de cartes et de formats de badges pris en charge **409**
23.21 Support SPC pour périphériques E-Bus **411**
23.22 Glossaire FlexC **414**
23.23 FlexC - Commandes **415**
23.24 Tempos des catégories d' ATS **418**
23.25 Tempos des catégories de Chemin **419**

23.1 Connexions du câble réseau

IP

Un PC peut être connecté directement sur l'interface Ethernet du contrôleur SPC ou via une connexion LAN. Les tableaux ci-dessous montrent les deux configurations de connexion possibles.

- Si le SPC est raccordé à un réseau existant via un concentrateur, connectez un câble traversant droit à partir du concentrateur sur le SPC et un autre à partir du concentrateur sur le PC.
- Si le contrôleur n'est pas raccordé à un réseau (c'est-à-dire qu'un concentrateur ou un interrupteur n'est pas utilisé), un câble null modem doit être connecté entre le contrôleur SPC et le PC.

Pour connecter le contrôleur SPC à un PC via un concentrateur, utilisez un câble traversant droit.

BROCHE RJ45	BROCHE RJ45
1 (RX +)	1 (TX +)
2 (RX -)	2 (TX-)
3 (TX+)	3 (RX+)
6 (TX-)	6 (RX -)

Pour connecter la centrale SPC directement à un PC, utilisez un câble null modem.

BROCHE RJ45	BROCHE RJ45
1 (RX +)	3 (TX+)
2 (RX -)	6 (TX-)
3 (TX+)	1 (RX +)
6 (TX-)	2 (RX -)

23.2 LED d'état du contrôleur

TÉMOIN	Fonction
Témoin 1	Données sans fil CLIGNOTEMENT : les données sans fil sont en cours de réception par le module radio ÉTEINTE : aucune donnée sans fil n'est en cours de réception
Témoin 2	État de la batterie ALLUMÉE : la tension de la batterie a chuté en dessous du niveau de décharge profonde (10,9 V) ÉTEINTE : état de la batterie OK
Témoin 3	Alimentation secteur ALLUMÉE : défaut alimentation 230 V ÉTEINTE : alimentation 230 V OK
Témoin 4	État X-BUS ALLUMÉE : la configuration du X-BUS est une configuration en boucle ÉTEINTE : la configuration du X-BUS est une configuration en branche CLIGNOTEMENT : détection de transpondeurs fin de ligne ou rupture d'un câble.
Témoin 5	Défaut système ALLUMÉE : un défaut matériel a été détecté sur la carte ÉTEINTE : aucun défaut matériel n'a été détecté

TÉMOIN	Fonction
Témoin 6	Écriture sur la mémoire flash ALLUMÉE : le système est en train d'écrire sur la mémoire flash ÉTEINTE : le système n'est pas en train d'écrire sur la mémoire flash
Témoin 7	Pulsation CLIGNOTEMENT : le système fonctionne normalement

ALLUMÉE	ÉTEINTE	CLIGNOTEMENT

23.3 Alimentation des transpondeurs à partir des bornes auxiliaires

Pour calculer le nombre de transpondeurs/claviers pouvant être alimentés sans problème par les terminaux d'alimentation auxiliaires 12 VCC, ajoutez le courant maximum total tiré par tous les transpondeurs/claviers à alimenter et déterminez si ce total est inférieur à la puissance auxiliaire 12 VCC.

Consultez les spécifications techniques pour le courant auxiliaire spécifique et la fiche de données ou d'instruction d'installation des modules, claviers et transpondeurs pour la consommation courante.

Courant du transpondeur 1 (mA) + courant du transpondeur 2 (mA) + ….. < puissance auxiliaire

Si les sorties électroniques ou de relais alimentent déjà des appareils externes, l'alimentation fournie à ces appareils doit être soustraite de l'alimentation électrique auxiliaire 12 VCC pour déterminer la quantité de courant disponible à partir des terminaux de courant auxiliaires (0 V 12 V).

Si le courant maximal total soutiré par les transpondeurs dépasse le courant auxiliaire, un transpondeur à module d'alimentation doit être utilisé pour fournir du courant supplémentaire.

Alimentation des transpondeurs à partir des bornes auxiliaires

1	Contrôleur SPC
2	Batterie
3	Bornes d'alimentation auxiliaire 12 V
4	Claviers
5	Claviers
6	Transpondeur E/S

23.4 Calcul de la puissance nécessaire pour la batterie

Il est important qu'une source d'énergie de secours soit disponible pour alimenter tous les appareils en cas de défaut sur l'alimentation secteur. Pour que cette condition soit réalisée, connectez toujours la batterie et le chargeur appropriés.

Les tableaux ci-dessous fournissent une valeur approximative du courant de charge maximal que chaque type de batterie peut fournir pendant les périodes de disponibilité indiquées.

Les valeurs approximatives ci-dessous supposent que la carte de circuit imprimé du contrôleur SPC utilise sa charge maximale (toutes les entrées connectées ont une résistance fin de ligne) et que la puissance de sortie utile de la batterie est égale à 85 % de sa capacité maximale.

$$\frac{0{,}85 \times \text{capacité de la batterie (Ah)}}{\text{Temps (heures)}} - (\text{Icont} + \text{Isirène}) = \text{Imax}$$

Taille de la batterie = capacité en Ah, en fonction du boîtier SPC choisi

Temps = temps de fonctionnement de secours en heures, en fonction du grade de sécurité

Icont = courant de repos (en A) pour le contrôleur SPC

Isirène = courant de repos (en A) pour les sirènes extérieures et intérieures raccordées

Imax = le courant maximal pouvant être soutiré à la sortie de courant auxiliaire

Quantité de courant de la sortie Aux en utilisant une batterie de 7 Ah (SPC422x/522x)

COMMS / Durée de veille	AUCUN (mA)	RTC (mA)	GSM (mA)	RTC + GSM (mA)
12 h	356	331	226	201
30 h	58	33	Indisponible	Indisponible

Quantité de courant de la sortie Aux en utilisant une batterie de 17 Ah (SPC523x)

COMMS / Durée de veille	AUCUN (mA)	RTC (mA)	GSM (mA)	RTC + GSM (mA)
12 h	750	750	750	750
30 h	342	317	212	187

Quantité de courant de la sortie Aux en utilisant une batterie de 7 Ah (SPC432x/532x)

COMMS / Durée de veille	AUCUN (mA)	RTC (mA)	GSM (mA)	RTC + GSM (mA)
12 h	326	301	196	171
30 h	28	Indisponible	Indisponible	Indisponible

Quantité de courant de la sortie Aux en utilisant une batterie de 17 Ah (SPC533x/633x)

COMMS / Durée de veille	AUCUN (mA)	RTC (mA)	GSM (mA)	RTC + GSM (mA)
12 h	750	750	750	750
30 h	312	287	182	157

Quantité de courant de la sortie Aux en utilisant une batterie de 24 Ah (SPC535x/635x)

COMMS / Durée de veille	AUCUN (mA)	RTC (mA)	GSM (mA)	RTC + GSM (mA)
12 h	1650	1625	1610	1585
24h	650	625	610	585
30 h	450	425	410	385
60h	50	25	10	Indisponible

Quantité de courant de la sortie Aux en utilisant deux batteries de 24 Ah (SPC535x/635x)

COMMS / Durée de veille	AUCUN (mA)	RTC (mA)	GSM (mA)	RTC + GSM (mA)
12 h	2205	2180	2165	2140
24h	1650	1625	1610	1585
30 h	1250	1225	1210	1185
60h	450	425	410	385

Quantité de courant de la sortie Aux en utilisant une batterie de 27 Ah (SPC535x/635x)

COMMS / Durée de veille	AUCUN (mA)	RTC (mA)	GSM (mA)	RTC + GSM (mA)
12 h	1900	1875	1860	1835
24h	775	750	735	710
30 h	550	525	510	485
60h	100	75	60	35

Quantité de courant de la sortie Aux en utilisant deux batteries de 27 Ah (SPC535x/635x)

COMMS / Durée de veille	AUCUN (mA)	RTC (mA)	GSM (mA)	RTC + GSM (mA)
12 h	2205	2180	2165	2140
24h	1900	1875	1860	1835
30 h	1450	1425	1410	1385
60h	550	525	510	485

L'indication N/A signifie que la batterie sélectionnée n'a pas la capacité nécessaire pour alimenter uniquement la charge minimale du contrôleur SPC pendant la durée de veille indiquée. Voir *Calcul de la puissance nécessaire pour la batterie* page 382 pour connaître la charge maximale des périphériques et des modules.

N'utiliser que des batteries à cellule scellée régulée par soupapes.

Une conformité EN implique que la batterie puisse délivrer le courant pendant la durée de secours définie.

23.5 Paramètres par défaut des modes Simple, Évolué et Bancaire

Ce tableau indique les noms et types de zones par défaut sur le contrôleur pour chaque mode opératoire. Toutes les zones sur les transpondeurs connectés doivent être classées comme non utilisées jusqu'à ce qu'elles aient été explicitement configurées par l'Installateur.

Caractéristique	Mode Simple	Mode Évolué	Mode Bancaire
Noms des zones			
Contrôleur – Zone 1	Porte d'entrée	Porte d'entrée	Porte d'entrée
Centrale - Zone 2	Salon	Fenêtre 1	Fenêtre 1
Centrale - Zone 3	Cuisine	Fenêtre 2	Fenêtre 2
Centrale - Zone 4	Escalier avant	INFRAROUGE 1	INFRAROUGE 1
Centrale - Zone 5	Escalier arrière	Infrarouge 2	Infrarouge 2
Centrale - Zone 6	Couloir PIR	Issue de secours	Issue de secours
Centrale - Zone 7	Infrar. réception	Alarme incendie	Alarme incendie
Centrale - Zone 8	Bouton d'urgence	Bouton d'urgence	Bouton d'urgence
Types de zone			
Contrôleur – Zone 1	ENTRÉE/SORTIE	ENTRÉE/SORTIE	ENTRÉE/SORTIE
Centrale - Zone 2	ALARME	ALARME	ALARME
Centrale - Zone 3	ALARME	ALARME	ALARME
Centrale - Zone 4	ALARME	ALARME	ALARME
Centrale - Zone 5	ALARME	ALARME	ALARME
Centrale - Zone 6	ALARME	ISSUE SECOURS	ALARME
Centrale - Zone 7	ALARME	FEU	ALARME
Centrale - Zone 8	PANIQUE	PANIQUE	ALARME

23.6 Câblage de l'interface X10

Câblage du X10 au contrôleur

Code PIN	RJ45	RJ11
TX	8	4
TERRE	5	1
RX	1	2

23.7 Codes SIA

LIBELLÉ	CODE
FIN D'ANOMALIE 230 V	AR
ANOMALIE 230 V	AT
ALARME INTRUSION	BA
COMMUTATION INTRUSION	BB
ANNULATION D'ALARME INTRUSION	BC
ANOMALIE SWINGER	BD
FIN D'ANOMALIE SWINGER	BE
FIN D'ANOMALIE INTRUSION	BJ
FIN D'ALARME INTRUSION	BR
ANOMALIE INTRUSION	BT
INTRUSION DÉCOMMUTÉ	BU
INTRUSION VÉRIFIÉ	BV
TEST ALARME INTRUSION	BX
PROBLÈME LORS DE LA MES	CD
MES FORCÉE	CF
MES	CG
ÉCHEC FERMETURE	CI
MES TROP TÔT	CK
MES TRANSMISE	FE
MES AUTOMATIQUE	CP
MES À DISTANCE	CQ
MES PAR BOÎTIER A CLÉ	CS
MHS TROP TARD	CT
ACCÈS FERMÉ	DC
ACCÈS REFUSÉ	DD
PORTE FORCÉE	DF
ACCÈS AUTORISÉ	DG
ACCES REFUSE : ANTIPASSBACK	DI
PORTE RESTÉE OUV.	DN
ACCÈS OUVERT	DO

LIBELLÉ	CODE
FIN D'ALARME PORTE	DR
DEMANDE DE SORTIE	DX
ALARME DE SORTIE	EA
FIN D'AUTOSURVEILLANCE PÉRIPH. X-BUS	EJ
PÉRIPH. X-BUS MANQUANT	EM
PÉRIPH. X-BUS RETROUVÉ	FR
FIN D'ALARME PÉRIPH. X-BUS	ER
AUTOSURV. PÉRIPH. X-BUS	ES
ANOMALIE PÉRIPH. X-BUS	ET
ALARME INCENDIE	DF
INCENDIE COMMUTÉ	FB
ALARME INCENDIE ANNULÉE	FC
FIN D'ANOMALIE INCENDIE	FJ
FIN D'ALARME INCENDIE	FR
ANOMALIE INCENDIE	FT
INCENDIE DÉCOMMUTÉ	FU
ALARME AGRESSION	HA
AGRESSION COMMUTÉ	HB
FIN D'ANOMALIE AGRESSION	HJ
FIN D'ALARME AGRESSION	HR
ANOMALIE AGRESSION	HT
AGRESSION DÉCOMMUTÉ	HU
AGRESSION CONFIRMÉE	HV
AP FAUX CODES UTILISATEUR ¦WEB ou ¦XBUS	JA
TIME CHANGED	JT
LOCAL PROGRAMMING	LB
MODEM RESTORAL ¦ 1 ou 2	LR
MODEM TROUBLE ¦ 1 ou 2	LT
FIN PROG. LOCALE	LX
ALARME MÉDICAL	MA
MÉDICAL COMMUTÉ	MB

LIBELLÉ	CODE
FIN D'ANOMALIE MÉDICAL	MJ
FIN D'ALARME MÉDICAL	MR
ANOMALIE MÉDICAL	MT
MÉDICAL DÉCOMMUTÉ	MU
PÉRIMÈTRE ARMÉ	NL
FIN D'ALARME IP LIAISON RÉSEAU	RB (NR)
FIN D'ALARME GPRS LIAISON RÉSEAU	RB (NR)
DÉFAUT IP LIAISON RÉSEAU	NT
DÉFAUT GPRS LIAISON RÉSEAU	NT
MHS AUTOMATIQUE	OA
MHS SECTEUR	OG
MHS TROP TÔT	OK
TRANSMISSION MHS	OU
MHS PAR BOÎTIER A CLÉ	OS
MES TROP TARD	OT
MHS À DISTANCE	OQ
MHS DUE À ALARME	OR
PANIQUE	PA
PANIQUE COMMUTÉ	PB
FIN D'ANOMALIE PANIQUE	PJ
FIN D'ALARME PANIQUE	PR
ANOMALIE PANIQUE	PT
PANIQUE DÉCOMMUTÉ	PU
RELAIS FERMÉ	RC
RÉINITIALISATION À DISTANCE	RN
RELAIS OUVERT	RO
TEST CYCLIQUE	RP
MISE SOUS TENSION	RR
SUCCÈS PROGRAMMATION DISTANTE	RS
DONNÉES PERDUES	RT
TEST MANUEL	RX

LIBELLÉ	CODE
AUTOSURVEILLANCE	TA
AUTOSURV. COMMUTÉ	TB
FIN AUTOSURVEILLANCE	TR
AUTOSURV. DÉCOMMUTÉ	TU
APPEL TEST CYCLIQUE	TX
ALARME GÉNÉRIQUE	UA
GÉNÉRIQUE COMMUTÉ	UB
FIN D'ANOMALIE GÉNÉRIQUE	UJ
FIN D'ALARME GÉNÉRIQUE	UR
ANOMALIE GÉNÉRIQUE	UT
GÉNÉRIQUE DÉCOMMUTÉ	UU
DÉFAUT SIRÈNE	YA
FIN BROUILLAGE RF	XH
FIN AUTOSURVEILLANCE RF	XJ
LECTEUR VERROUILLÉ	RL
LECTEUR DÉVERROUILLÉ	RG
CLAVIER DÉVERROUILLÉ	KG
DÉFAUT BROUILLAGE RF	XQ
AUTOSURVEILLANCE RF	XS
ÉCHEC TRANSMISSION	YC
DÉFAUT CHECKSUM	YF
FIN D'ANOMALIE SIRÈNE	YH
TRANSMISSION RÉTABLIE	YK
BATTERIE ABSENTE	YM
ANOMALIE ALIM.	YP
ALIM. NORMALE	YQ
FIN D'ANOMALIE BATTERIE	YR
ANOMALIE COMMUNICATION	YS
ANOMALIE BATTERIE	YT
RÉINITIALISATION WATCHDOG	YW
SERVICE DEMANDÉ	YX

LIBELLÉ	CODE
SERVICE ACHEVÉ	YZ
ÉVÉNEMENTS SIA SPÉCIAUX	
CONTRAINTE UTILISATEUR	HA
FIN DE CONTRAINTE UTILISATEUR	HR
ALARME PANIQUE ENET	PA
FIN D'ALARME PANIQUE ENET	PR
ALARME PANIQUE UTILISATEUR	PA
ALARME INCENDIE ENET	DF
FIN D'ALARME INCENDIE ENET	FR
ALARME MÉDICAL ENET	MA
FIN D'ALARME MÉDICAL ENET	MR
PTI PANIQUE	PA
PTI TILT	MA
PTI CLIP CEINTURE	HA
FIN D'ANOMALIE PANIQUE PTI	PR
FIN D'ANOMALIE PTI TILT	MR
FIN D'ANOMALIE PTI CLIP CEINTURE	HR
RPA PANIQUE	PA
FIN D'ANOMALIE RPA PANIQUE	PR
RPA AGRESSION	HA
FIN D'ANOMALIE RPA AGRESSION	HR
CHANGER CODE UTILISATEUR	JV
CODE EFFACÉ	
CODES SIA NON STANDARDS POUR RAPPORT D'ÉTAT DE ZONE	
ZONE OUVERTE	ZO
ZONE FERMÉE	ZC
ZONE COURT-CIRCUIT	ZX
ZONE DÉCONNECTÉE	ZD
ZONE MASQUÉE	ZM
ZONE DE MARCHE	TP
DÉBUT TEST DE MARCHE	ZK

LIBELLÉ	CODE
FIN TEST DE MARCHE	TC
ZONE BATT FAIBLE	XT
ZONE FIN DÉFAUT BATT FAIBLE	XR
AUTRES CODES SIA NON STANDARDS	
CAMERA ONLINE	CU
CAMERA OFFLINE	CV
ALERTE FERMÉE	SD
ALERTE ROUVERTE	DI
X-BUS ALERTE FERMÉE	NB
XBUS ALERTE RÉOUVERTE	NO
BADGE INCONNU	AU
ACCÈS UTILISATEUR	JP
FIN D'ACCÈS UTILISATEUR	ZG
BASSE TENSION	XD
RESTORAL BASSE TENSION	XG
CHARGE PROFONDE	XK
VERROUILLÉ	WW

23.8 Codes CID

CODE	ÉVÉN. CID	LIBELLÉ
100	MEDICAL	Alarme et réinitialisation Médical et Homme mort.
110	FEU	
120	PANIQUE	
121	CONTRAINTE	
129	AGRESSION CONFIRMÉE	Voir *Exigences en matière de configuration pour la conformité avec la PD 6662:2010* page 29.
130	INTRUSION	
134	ENTRÉE/SORTIE	
137	AUTOSURVEILLANCE	Défaut et réinitialisation Autosurv. coffret et auxiliaire.
139	VÉRIFIÉ	Alarme confirmée.
144	AUTOSURVEILLANCE DÉTECTEUR	Défaut et réinitialisation Autosurveillance de zone.

CODE	ÉVÉN. CID	LIBELLÉ
150	NON-INTRUSION	
300	ANOMALIE SYSTÈME	Défaut et réinitialisation PSU.
301	PERTE ALIMENTATION SECTEUR	Défaut et réinitialisation alimentation secteur PSU.
302	BATTERIE FAIBLE	
305	RESET	Réinitialisation système.
311	DÉFAUT BATTERIE	Défaut et réinitialisation batterie PSU.
312	SURCHARGE ALIM.	Défaut et réinitialisation fusibles interne, externe et auxiliaire du PSU.
320	BUZZER	Défaut et réinitialisation Autosurveillance sirène.
330	ANOMALIE PÉRIPHÉRIQUE SYSTÈME	Défaut et réinitialisation PSU.
333	DÉFAUT TRP	Défaut et réinitialisation câble et communication nœud X-BUS.
338	BATT. TRP	Défaut et réinitialisation batterie nœud X-BUS.
341	AUTOSURVEILLANCE TRP	Alarme et réinitialisation autosurveillance X-BUS et autosurveillance antenne RF.
342	ALIM. SECTEUR TRP	Défaut et réinitialisation alimentation nœud X-BUS.
344	BROUILLAGE RF	Défaut et réinitialisation brouillage RF.
351	TELCO 1	Défaut et réinitialisation modem principal.
352	TELCO 2	Défaut et réinitialisation modem secondaire.
376	ANOMALIE AGRESSION	
380	ANOMALIE DÉTECTEUR	
401	OUVRIRFERMER	Mise hors service, post-alarme et mise en service totale.
406	ANNULATION D’ALARME	Annulation de l’alarme.
451	OUVRIRFERMER TROP TÔT	
452	OUVRIRFERMER TROP TARD	
453	ÉCHEC OUVERTURE	MHS trop tard.
454	ÉCHEC FERMETURE	MES trop tard.
456	ÉVÉNEMENT MES PARTIELLE	MES partielle A et B.
461	CODE AUTOSURVEILLANCE	Code autosurveillance de l’utilisateur.
466	SERVICE	Mode Installateur activé et désactivé.
570	COMMUTATION	Zone inhibée et désinhibée, zone isolée et non isolée.

CODE	ÉVÉN. CID	LIBELLÉ
601	TEST MANUEL	Test manuel du modem.
602	TEST AUTOMATIQUE	Test automatique du modem.
607	TEST DE DÉPLACEMENT	
613	ZONE DE MARCHE	
614	ZONE INCENDIE DÉPLACEMENT	
615	ZONE PANIQUE DÉPLACEMENT	
625	REMISE À L'HEURE	Remise à l'heure.

23.9 Vue d'ensemble des types de clavier

Type de clavier	N° de modèle	Fonctionnalités de base	Détection de proximité	Audio
Clavier standard	SPCK420	✓	-	-
Clavier avec PACE	SPCK421	✓	✓	-
Clavier Confort	SPCK620	✓	-	-
Clavier Confort avec audio/CR	SPCK623	✓	✓	✓

Fiche signalétique du clavier SPCK420/421

1	Étiquette à l'intérieur du clavier
2	Fiche signalétique déroulante contenant les données de contact de l'installateur. Inscrivez toutes les informations de contact utiles à la fin de l'installation.

23.10 Combinaisons de codes utilisateur

Le système accepte 4, 5, 6, 7 ou 8 caractères numériques pour le code de chaque utilisateur (code Utilisateur ou Installateur). Le nombre maximal de combinaisons/variations logiques pour chaque nombre de caractères numériques du code est indiqué dans le tableau ci-dessous.

Nombre de caractères numériques	Nombre de variations	Derniers codes utilisateur valides
4	10 000	9999
5	100 000	99999
6	1 000 000	999999
7	10 000 000	9999999
8	100 000 000	99999999

Le nombre maximal de combinaisons/variations logiques est calculé comme suit :

$10^{\text{Nombre de caractères numériques}}$ = Nombre de variations (incluant le code Utilisateur ou Installateur)

Remarque : pour être en accord avec les approbations INCERT, le code PIN de l'utilisateur doit contenir plus de 4 chiffres.

Le code par défaut de l'installateur est 1111. Consultez *Codes PIN installateur* page 121 pour plus d'informations.

23.11 Codes utilisateur de contrainte

Si le code comporte une contrainte, il ne peut pas être configuré pour la dernière valeur de l'intervalle déterminé par le nombre de caractères de ce code. La contrainte PIN+1 ou PIN+2 impose que 1 ou 2 codes supplémentaires soient disponibles après un code donné. Par exemple, pour une attribution de 4 caractères, le nombre total de codes disponibles est de 10 000 (de 0 à 9999). Dans ce cas, avec la contrainte PIN+1, le dernier code pouvant être attribué est 9998. Si la contrainte PIN+2 est utilisée, la dernière valeur de code possible est 9997.

Si la fonction Contrainte est active, les codes utilisateur consécutifs (par ex. 2906, 2907) ne peuvent pas être utilisés, puisqu'un événement « contrainte utilisateur » est déclenché lorsque ce code est tapé sur le clavier.

Lorsque le système a été configuré pour PIN+1 ou PIN+2 dans **Options Système** (voir *Options* page 257) et que les utilisateurs ont été activés pour la contrainte (voir *Utilisateurs* page 211), aucune modification n'est possible sauf si tous les utilisateurs sont supprimés et que les codes sont réaffectés.

23.12 Inhibitions automatiques

Le système accepte les inhibitions automatiques dans les conditions suivantes.

23.12.1 Zones

Lorsque les options Royaume-Uni et Évolué sont sélectionnées (voir *Normes* page 274), le système propose la fonctionnalité DD243. Dans cet exemple, le système inhibe les zones répondant aux conditions suivantes :

- La zone d'entrée n'envoie pas de signal d'alarme au centre de télésurveillance et ne peut pas faire partie d'une alarme confirmée ; elle sera donc inhibée comme le demande la norme DD243.

- Si une alarme est déclenchée dans une zone donnée mais pas dans une deuxième zone au cours de la temporisation de confirmation (30 minutes par défaut), la première zone est inhibée automatiquement et aucune alarme supplémentaire n'est déclenchée dans cette zone pendant la période de mise en surveillance.

23.12.2 Codes PIN d'accès

Pour les systèmes Grade 2 : après 10 tentatives infructueuses de saisie d'un code erroné, le clavier ou le navigateur est bloqué pendant 90 secondes. Après 10 tentatives supplémentaires, le clavier est de nouveau bloqué pendant 90 secondes. Quand l'utilisateur entre un code correct, le compteur est remis à zéro, permettant ainsi une saisie erronée de 10 codes avant de se bloquer.

Pour les systèmes Grade 3 : après 10 tentatives infructueuses de saisie d'un code erroné, le clavier ou le navigateur est bloqué pendant 90 secondes. Après chaque tentative supplémentaire, le clavier est de nouveau bloqué pendant 90 secondes. Quand l'utilisateur entre un code correct, le compteur est remis à zéro, permettant ainsi une saisie erronée de 10 codes avant de se bloquer.

23.12.3 Accès Installateur

Un Installateur ne peut accéder au système que s'il y est autorisé par un type d'utilisateur « Manager » (voir attribut « Installateur » dans *Droits d'utilisateur* page 215) et uniquement pour une durée prédéfinie (voir « Accès Installateur » dans *Temporisations* page 269).

23.12.4 Déconnexion clavier de l'utilisateur

Si aucune touche du clavier n'est pressée pendant une période déterminée (voir « Temps de saisi clavier » dans *Temporisations* page 269», l'utilisateur est automatiquement déconnecté.

23.13 Raccordement du câble secteur sur le contrôleur

Exigences :

Un dispositif de coupure approuvé et facilement accessible doit être intégré dans la configuration de câblage du bâtiment. Il doit pouvoir couper les deux phases en même temps. Il peut s'agir d'interrupteurs, de disjoncteurs ou de dispositifs du même type

- Le dispositif de coupure doit avoir une distance minimale de 3 mm entre les contacts
- La taille minimale du conducteur utilisé pour le raccordement au secteur est 1,5 mm au carré
- Les disjoncteurs doivent avoir un pouvoir de coupure maximal de 16 A

Le câble secteur est fixé à l'aide d'une attache sur la pièce métallique en V de la plaque inférieure, la pièce en V devant être située entre le câble et l'attache. Assurez-vous que l'attache est fixée sur la partie isolante externe du câble secteur, c'est-à-dire la gaine PVC. L'attache doit être extrêmement bien serrée pour que le câble soit être parfaitement immobilisé en cas de traction sur celui-ci.

Le conducteur de protection doit être fixé sur le bornier d'alimentation de telle manière que si le câble secteur devait glisser de sa fixation et exercer une contrainte sur les conducteurs, le conducteur de protection serait le dernier à subir cette contrainte.

Le câble secteur doit être d'un type approuvé et être repéré HO5 VV-F ou HO5 VVH2-F2.

L'attache en plastique doit avoir une classification d'inflammabilité V-1.

23.14 Contrôleur de maintenance

Le système doit être entretenu conformément au calendrier de maintenance en vigueur. Les seules pièces remplaçables sur le contrôleur sont le fusible d'alimentation secteur, la batterie de secours et la pile de l'horloge (montée sur la carte de circuit imprimé).

Il est recommandé de vérifier les points suivants pour un contrôle de maintenance :

- Le Journal des événements pour vérifier si des tests ont mis en évidence un défaut sur la batterie de secours depuis le dernier entretien ; dans ce cas, la batterie de secours doit être vérifiée.
- La batterie de secours doit être remplacée conformément au calendrier de maintenance pour s'assurer qu'elle est toujours capable d'alimenter le système pendant la durée prévue pour celui-ci. Contrôler l'état physique de la batterie : si elle est endommagée ou en cas de fuite de l'électrolyte, remplacez la batterie immédiatement par une batterie neuve.

REMARQUE : la nouvelle batterie doit avoir au moins la même capacité que la précédente (dans la limite acceptée par le système).

- Si le fusible d'alimentation secteur grille, le système doit être vérifié pour en rechercher la raison. Le fusible doit être remplacé par un fusible de même calibre. Le calibre est indiqué sur l'étiquette du système à l'arrière du boîtier.
- La pile au lithium de l'horloge intégrée sur la carte de circuit imprimé n'est mise à contribution que lorsque le système n'est pas alimenté ; dans cette situation, la pile a une durée de vie d'environ cinq ans. L'alimentation étant totalement coupée du système, la pile doit être contrôlée visuellement tous les ans afin de s'assurer que celui-ci conserve la date et l'heure. Si le système ne conserve pas la date et l'heure, la pile doit être remplacée par une nouvelle pile au lithium de type CR1216.
- Toutes les connexions électriques doivent être vérifiées pour s'assurer que l'isolation est correcte et qu'il n'y a pas de risque de court-circuit ou de déconnexion.
- Nous vous recommandons également de vérifier toutes les notes sur les nouvelles versions de micrologiciel afin d'améliorer la sécurité du système.
- Vérifiez le bon état de tous les assemblages physiques. Tout assemblage détérioré doit être remplacé par des pièces identiques.

23.15 Maintenance Smart PSU

Le système doit être entretenu conformément au calendrier de maintenance en vigueur. Les seules pièces remplaçables sur le Smart PSU sont le fusible d'alimentation secteur et la batterie de secours.

Il est recommandé de vérifier les points suivants pour un contrôle de maintenance :

- Le Journal des événements du contrôleur pour vérifier si des tests ont mis en évidence un défaut sur la batterie de secours depuis le dernier entretien ; dans ce cas, la batterie de secours doit être vérifiée.
- La batterie de secours doit être remplacée conformément au calendrier de maintenance pour s'assurer qu'elle est toujours capable d'alimenter le système pendant la durée prévue pour celui-ci. Contrôler l'état physique de la batterie : si elle est endommagée ou en cas de fuite de l'électrolyte, remplacez la batterie immédiatement par une batterie neuve.

REMARQUE : la nouvelle batterie doit avoir au moins la même capacité que la précédente (dans la limite acceptée par le système).

- Vérifiez que les LED du pupitre de commande du PSU sont dans l'état prévu. Consultez la documentation du Smart PSU pour des détails sur les LED.
- Si le fusible d'alimentation secteur grille, le système doit être vérifié pour en rechercher la raison. Le fusible doit être remplacé par un fusible de même calibre. Le calibre est indiqué sur l'étiquette du système à l'arrière du boîtier.
- Toutes les connexions électriques doivent être vérifiées pour s'assurer que l'isolation est correcte et qu'il n'y a pas de risque de court-circuit ou de déconnexion.

- Nous vous recommandons également de vérifier toutes les notes sur les nouvelles versions de micrologiciel afin d'améliorer la sécurité du système.
- Vérifiez le bon état de tous les assemblages physiques. Tout assemblage détérioré doit être remplacé par des pièces identiques.

23.16 Types de zone

Les types de zones du système SPC sont programmables à l'aide du clavier et du navigateur. Le tableau ci-dessous fournit une description rapide de chaque type de zone pouvant être géré par le système SPC. Chaque type de zone active son propre type de sortie unique (un drapeau ou un indicateur interne) qui peut ensuite être attribué à une sortie physique pour activer un périphérique spécifique.

Type de zone	Gestion de la catégorie	Description
ALARME	Intrusion	Ce type de zone est attribué par défaut. Il est le plus utilisé pour les installations standards. Un activation Ouvert, Déconnecté ou Autosurveillance dans n'importe quel mode (sauf MES) entraîne une alarme totale immédiate. En mode MHS, les conditions d'autosurveillance sont entrées dans un journal, ce qui provoque l'émission du message d'alarme AUTOSURVEILLANCE ZONE et déclenche une alarme locale. En mode MES partielle A, MES partielle B, MES totale, toutes les activités sont journalisées.
ENTRÉE/SORTIE	Intrusion	Ce type de zone devrait être attribué à toutes les zones se trouvant sur un chemin d'entrée ou de sortie (par exemple, la porte principale ou les autres accès à l'immeuble). Ce type de zone inclut un délai d'entrée et de sortie. Le temporisateur d'entrée contrôle ce délai. Quand le système est en MES totale, ce type de zone inclut un délai de sortie permettant de quitter un secteur sans déclencher d'alerte. Le temporisateur de sortie contrôle ce délai. Ce type de zone est inactif en mode MES partielle A.
TEMPORISATION DE SORTIE	Intrusion	Ce type de zone est utilisé en combinaison avec un bouton poussoir sur un chemin de sortie. Il a la fonction d'une terminaison de sortie, c'est-à-dire qu'il représente un délai de sortie infini pendant lequel le système ne peut pas être activé tant qu'on n'appuie pas sur le bouton.
FEU	Agression	Les zones de type Incendie surveillent la déclaration d'un incendie 24 heures sur 24. Leur réponse est indépendante du mode de fonctionnement de la centrale. Quand on ouvre une zone de type Incendie, une alarme totale est générée et le type de sortie INCENDIE est activé. Si l'attribut « Transmission seule » est actif, l'activation est transmise au centre de télésurveillance sans qu'une alarme totale soit générée.

Type de zone	Gestion de la catégorie	Description
ISSUE SECOURS	Agression	Il s'agit d'un type spécial de zone 24/24, utilisée pour les issues de secours incendie qui ne devraient jamais être ouvertes. Quand le système est hors surveillance, une activation de cette zone déclenche la sortie Issue de secours, ce qui déclenche à son tour des messages d'alerte.
LIGNE	Défaut	Entrée de surveillance de la ligne de télémesure. Elle est normalement utilisée en combinaison avec une sortie d'état de la ligne téléphonique d'un numéroteur digital externe ou d'un système de communication directe. Quand ce type de zone est activé, une alarme locale est déclenchée en mode hors surveillance, et une alarme totale dans tous les autres modes.
PANIQUE	Agression	Ce type de zone est actif 24 heures sur 24. Il est activé par un bouton Panique. Quand une zone de type Panique est activée, un événement de Panique est transmis indépendamment du mode de surveillance de la centrale. Toutes les activations sont journalisées et transmises si l'attribut JDB (journal de bord) est appliqué à la zone. Si l'attribut SILENCIEUX est actif, l'alarme est silencieuse (l'activation est transmise au CTS), sinon une alarme totale est déclenchée.
ALARME AGRESSION	Agression	Ce type de zone est actif 24 heures sur 24. Il est activé par un bouton. Quand une zone de type Agression est activée, l'événement correspondant est transmis indépendamment du mode de surveillance de la centrale. L'attribut SILENCIEUX est défini par défaut et l'alarme sera donc silencieuse. En cas de désactivation, elle générera une alarme totale. Toutes les activations sont journalisées et transmises si l'attribut JDB (journal de bord) est appliqué à la zone.
AUTOSURVEILLANCE	Autosurveillance	En cas d'ouverture en mode hors surveillance, une alarme locale est générée, mais aucune alarme externe ne sera activée. Si le système est en MES totale, une alarme totale est générée. Si le niveau de sécurité actif du système est Grade 3, une alarme ne peut être remise à zéro qu'en entrant un code d'installateur.
TECHNIQUE	Intrusion	Une zone technique contrôle une sortie de zone technique dédiée. Après un changement d'état d'une zone technique, l'état de la sortie de zone technique change également. Ceci est le cas : • au moment de l'ouverture de la zone technique, la sortie de zone technique est activée • au moment de la fermeture de la zone technique, la sortie de zone technique est désactivée Si plus d'une zone technique est attribuée, la sortie de zone technique reste active jusqu'à ce que toutes les zones techniques soient fermées.

Type de zone	Gestion de la catégorie	Description
MEDICAL	Agression	Ce type de zone est utilisé en combinaison avec des interrupteurs médicaux radio ou filaires. Quand ce type de zone est activé indépendamment du mode : • la sortie de communication numérique médicale est activée (sauf si l'attribut Local est appliqué) • le buzzer de la centrale est activé (sauf si l'attribut Silencieux est appliqué) • le message ALARME MEDICALE est affiché.

Type de zone	Gestion de la catégorie	Description
ARMEMENT PAR CLE	Intrusion	Ce type de zone est normalement utilisé en combinaison avec un mécanisme de verrouillage par clé. Une clé de MES peut être configurée pour exécuter les **Options de paramétrage** suivantes : • **MES totale** • **MES Partielle A** • **MES Partielle B** Une zone d'armement par clé ACTIVE le système / le secteur / les secteurs communs en fonction de l'**Option de paramétrage** quand elle est OUVERTE, et DÉSACTIVE le système / le secteur / les secteurs communs en fonction de l'**Option de paramétrage** quand elle est FERMÉE. • Si la zone du type ARMEMENT PAR CLE est attribuée dans un système sans secteurs, l'action « armement par clé » ACTIVE/DESACTIVE le système. • Si la zone du type ARMEMENT PAR CLE est attribuée à un secteur, l'action « armement par clé » ACTIVE/DESACTIVE le secteur. • Si la zone du type ARMEMENT PAR CLE est attribuée à un secteur commun, l'action « armement par clé » ACTIVE/DESACTIVE tous les secteurs du secteur commun. • Si l'attribut SEULEMENT OUVERT est appliqué, l'état d'armement du système / du secteur / des secteurs communs alterne à chaque ouverture du verrou. (En d'autres termes : ouvrir une fois pour ACTIVER le système, fermer et rouvrir pour DÉSACTIVER.) • Si l'attribut MISE EN SURVEILLANCE POSSIBLE est appliqué, l'activation de la zone met le système en surveillance totale. • Si l'attribut MISE HORS SURVEILLANCE POSSIBLE est appliqué, l'activation de la zone met le système hors surveillance. L'armement par clé provoque la MES forcée du système/du secteur et inhibe automatiquement toutes les zones ouvertes ou les zones en défaut. **Remarque : votre système ne sera pas conforme aux normes EN si vous activez ce type de zone pour mettre en surveillance le système sans saisir tout d'abord un code PIN valable sur un périphérique externe.**

Type de zone	Gestion de la catégorie	Description
SHUNT	Intrusion	Ce type de zone n'est disponible que si le type d'installation est Evolué. Le type de zone Shunt peut être attribué quand le type d'installation est Simple, mais il sera sans effet. Quand une zone de ce type est ouverte, toutes les zones auxquelles l'attribut SHUNT est appliqué sont inhibées. Ceci s'applique au système quand il est mis en surveillance et hors surveillance. Dès que la zone de type Shunt est fermée, l'inhibition des zones ayant l'attribut SHUNT est annulée.
X-SHUNT	Intrusion	Ce type de zone n'est disponible que si le type d'installation est Evolué. L'ouverture d'une zone du type X-shunt inhibe la zone suivante installée dans le système. Ceci s'applique au système quand il est mis en surveillance et hors surveillance. Dès que la zone de type X-shunt est refermée, l'inhibition de la zone suivante est annulée.
DEFAUT DETECTEUR	Défaut	Les zones de panne de détecteur sont des zones 24/24 utilisées pour un périphérique de détection, comme un détecteur PIR. Le type Zone de panne déclenche une sortie de défaut. Lorsque le système est armé, une sortie de défaut est déclenchée. La LED du clavier et le buzzer sont activés s'il n'est pas armé.
SUPERV.VERROUIL.	Intrusion	Uniquement disponible en mode Évolué. Utilisé pour surveiller un verrou de porte. Le système peut être programmé pour ne pas être activé sauf si la porte est verrouillée.
SISMIQUE	Intrusion	Uniquement disponible si la centrale est en mode Bancaire. Les détecteurs de vibration, également appelés détecteurs sismiques, sont utilisés pour détecter une intrusion effectuée à l'aide de moyens mécaniques tels que le perçage des parois et des coffres.
TOUT VA BIEN	Intrusion	Ce type de zone permet d'utiliser une procédure d'entrée spéciale à lancer avec un code d'utilisateur et une entrée TVB. Une alarme discrète est générée si le bouton TVB n'est pas activé dans un délai configurable après la saisie d'un code utilisateur. (Voir *Ajouter/Éditer un secteur* page 278 pour des informations détaillées sur la configuration TVB) TVB utilise deux sorties, État d'entrée (voyant vert) et État avertissement (voyant rouge) afin d'indiquer l'état d'entrée au moyen des voyants du clavier.
INUTILISEE	Intrusion	Permet à une zone d'être désactivée sans qu'il soit nécessaire d'installer une résistance fin de ligne pour chaque zone. Une activation de la zone est ignorée.

Type de zone	Gestion de la catégorie	Description
DEFAUT HOLDUP	Défaut	Les zones Défaut agression sont des zones 24/24, utilisées pour un périphérique de signalisation d'agression, comme un WPA. Le type Zone de panne déclenche une sortie de défaut. Lorsque le système est armé, une sortie de défaut est déclenchée. La LED du clavier et le buzzer sont activés s'il n'est pas armé. Ce type de zone signalera les messages SIA, HT (Holdup Trouble) et HJ (Holdup Trouble Restore) et, pour le CID, un événement de problème de capteur (380) est produit.
DEFAUT WARNING	Défaut	Les zones Défaut avertissement sont des zones 24/24 utilisées pour un périphérique de signalisation d'avertissement, comme une alarme interne ou externe. Le type Zone de panne déclenche une sortie de défaut. Lorsque le système est armé, une sortie de défaut est déclenchée. La LED du clavier et le buzzer sont activés s'il n'est pas armé. Ce type de zone signalera les messages SIA, YA (Défaut sirène) et YH (Fin alarme) et, pour le CID, un événement de problème de capteur (380) est produit. **Remarque :** sur un système de niveau 2, une panne de câble déclenchera une panne et pas une alarme.
VALIDATION MES/MHS	Intrusion	Applicable à l'utilisation de Blockschloss. Ce type de zone est utilisé pour envoyer un signal d'autorisation de MES à la centrale pour indiquer que le Blockschloss est prêt à être activé. L'option d'activation doit être sélectionnée pour l'attribut « Autorisation avant MES/MHS » pour le secteur.
ELEMENT DE VERROUILLAGE	Intrusion	En cas d'utilisation d'un élément de verrouillage (boulon) avec un Blockschloss, ce type de zone signale la position de l'élément de verrouillage à la centrale (verrouillé ou déverrouillé). Cet écrou verrouille la porte en état activé. Ce signal est contrôlé pendant le processus d'activation. Si l'information « verrouillé » n'est pas reçue, l'activation échoue.

Type de zone	Gestion de la catégorie	Description
BRIS DE VITRE	Intrusion	La zone est connectée à une interface de bris de vitre RI S 10 D-RS-LED combinée à des détecteurs de bris de vitre GB2001. • Ce type de zone est disponible sur les contrôleurs et les transpondeurs. Il n'est pas disponible comme sans fil ou comme type de zone de porte si le DC2 est configuré comme porte. • Le type de zone effectue son rapport de la même manière via SIA et ID de contact. • Les droits de restauration / inhibition / isolation d'un bris de vitre sont identiques à ceux du type de zone d'alarme. • Condition de mise sous tension — Comme le courant est fourni par la centrale, tout changement d'état pendant les 10 premières secondes n'est pas pris en compte pour permettre à l'appareil d'atteindre un état de fonctionnement normal. • Condition de réinitialisation — Les signaux ne sont pas pris en compte par l'interface de bris de vitre pendant les 3 secondes suivant la réinitialisation du périphérique. • Sortie du mode Paramétrage — La sortie de bris de vitre peut être commutée en cas de sortie du mode Paramétrage. Dans ce cas, les signaux provenant de ce capteur ne seront temporairement pas pris en compte pendant 3 secondes.
EAU		Ce type de zone réagit de la même façon qu'un type de zone Technique.
CHALEUR		Ce type de zone réagit de la même façon qu'un type de zone Technique.
FRIGO/CONGÉL.		Ce type de zone réagit de la même façon qu'un type de zone Technique.
GAZ		Ce type de zone réagit de la même façon qu'un type de zone Technique.
SPRINKLER		Ce type de zone réagit de la même façon qu'un type de zone Technique.
CO		Ce type de zone réagit de la même façon qu'un type de zone Technique.
ENTRÉE/SORTIE 2		Ce type de zone réagit de la même façon qu'un type de zone d'Entrée/Sortie avec une temporisation d'entrée séparée. Il peut y avoir deux temporisations d'entrée dans le building à différents endroits.

23.17 Attributs zone

Dans le système SPC, les attributs de zone déterminent la manière dont les types de zones programmés fonctionnent.

Attribut zone	Description
Accès	Lorsque l'attribut Accès d'une zone est défini, à l'ouverture de cette zone, une alarme ne sera pas générée si la temporisation d'entrée ou de sortie est en cours. Si le système est en MES totale, l'attribut Accès n'est pas actif et l'ouverture de la zone ne génère pas une alarme totale. L'attribut Accès est le plus souvent utilisé pour les détecteurs PIR situés à proximité d'une zone d'entrée/sortie. Il permet une libre circulation à l'utilisateur dans la zone d'accès pendant que la temporisation d'entrée ou de sortie décompte. L'attribut Accès n'est valide que pour les types de zones Alarme. Tous les périphériques connectés (sirènes intérieures et extérieures, buzzers, flash) sont activés. **Remarque :** une zone d'alarme avec attribut Accès peut être automatiquement modifiée en une zone d'entrée/sortie en mode MES partielle si l'option Accès MES partielle est validée.
Exclus A	Si l'attribut Exclus A est défini pour une zone, alors aucune alarme ne sera générée par l'ouverture de cette zone lorsque la centrale est en mode MES partielle A. L'attribut Exclus A est valide uniquement pour un type de zone Alarme et des zones d'entrée/sortie. Une alarme TOTALE est générée si une zone ayant l'attribut EXCLUS A s'ouvre tandis que le système est en mode MES TOTALE ou MES PARTIELLE B (sirènes intérieures et extérieures, flash).
Exclus B	Si l'attribut Exclus B est défini, l'ouverture de la zone ne déclenchera pas d'alarme lorsque la centrale est en mode MES partielle B. L'attribut Exclus B est valide uniquement pour un type de zone Alarme et des zones d'entrée/sortie. Une alarme TOTALE est générée si une zone ayant l'attribut EXCLUS B s'ouvre tandis que le système est en mode MES TOTALE ou MES PARTIELLE A (sirènes intérieures et extérieures, flash).
24 heures	Si une zone reçoit un attribut 24 heures, elle est active à tout moment et provoque une alarme totale lorsqu'elle est ouverte, quel que soit le mode. Cet attribut ne peut être affecté qu'à un type de zone ALARME. Génère une alarme TOTALE en modes MHS, MES et MES PARTIELLE. **Remarque :** l'attribut 24 heures prend le pas sur les paramètres de tous les autres attributs pour une zone d'alarme particulière.
Locale	Quand l'attribut Local est défini, une alarme générée par l'ouverture d'une porte ne provoque pas un reporting externe de l'événement. L'attribut Local est valide pour les types de zones Alarme, Entrée/Sortie, Incendie, Issue de secours et Médical.
MHS locale	Lorsque cet attribut est défini, une alarme générée par l'ouverture de la zone lorsque le secteur est en surveillance totale ou partielle sera consignée de la manière habituelle. Cependant, si le secteur est hors surveillance, il n'y aura qu'une alarme locale, ç.-à-d. un buzzer au clavier, un clignotement de la LED et un affichage dans la zone. Cet attribut n'est applicable que sur les zones Alarme, Incendie et Sismique.

Attribut zone	Description
Double déclenchement	Utilisez cet attribut pour des détecteurs problématiques. Certains détecteurs peuvent générer par exemple des signaux d'activation parasites, déclenchant ainsi de fausses alarmes dans le système. Une zone avec l'attribut Double déclenchement déclenche une alarme si elle est activée deux fois pendant le délai de double déclenchement. Le délai de double déclenchement est fixé en secondes (voir *Temporisations* page 269). Deux actions d'ouverture au cours de cette période génèrent une alarme. Toutes les zones ouvertes ayant l'attribut Double déclenchement sont journalisées lorsque le système est armé.
Carillon	Lorsque l'attribut Carillon est défini pour une zone, toute ouverture de la zone en mode MHS provoque le déclenchement des buzzers internes pendant un court moment (environ 2 secondes). L'attribut Carillon est valide pour les types de zones Alarme, Entrée/Sortie et Technique.
INHIBEE	Lorsque l'attribut Inhibée est défini, un utilisateur peut inhiber cette zone. L'inhibition désactive le défaut ou la zone considérée pendant un seul cycle d'activation.
Normalement ouvert	Lorsque l'attribut Normalement ouvert est appliqué, le système s'attend à ce qu'un capteur/détecteur connecté soit un périphérique normalement ouvert. Par exemple, un capteur est censé être activé si les contacts sont fermés sur le périphérique.
Silencieux	Si l'attribut Silencieux est défini, il n'y a pas d'indication audio ou visuelle de l'alarme. L'activation de l'alarme est envoyée au centre de télésurveillance. Si le système est hors surveillance, un message d'avertissement s'affiche sur l'écran.
Journal	Si cet attribut est défini, tous les changements d'état de la zone sont journalisés.
Ouverte en sortie	Si cet attribut est défini, la zone sera signalée si elle est ouverte au moment de la MES.
Fréquent	Cet attribut ne s'applique qu'aux services à distance*. Si cet attribut est défini pour une zone, elle doit s'ouvrir pour permettre des services à distance en fonction de ce même attribut.
Fin de ligne	L'attribut Fin de ligne (EOL) fournit un nombre de configurations de câblage de zone d'entrée au système.
Analysé	L'attribut Analysé doit être défini pour une zone si cette zone est câblée avec un détecteur inertiel. Les valeurs Comptage d'impulsion et Coup brutal doivent être programmées pour chaque détecteur inertiel du système après un étalonnage simple de l'appareil.
Comptage d'impulsion	Niveau comptage d'impulsion pour détecteurs intertiels.
Coup brutal	Niveau déclenchement de coup brutal pour détecteurs intertiels.
Dernière issue	L'attribut Dernière issue ne peut être affecté qu'à un type de zone d'entrée/sortie. Utilisez cet attribut pour déroger à la procédure standard de décompte de la temporisation de sortie lorsque le système est en surveillance totale. Lorsque tous les autres chemins d'entrée/sortie des locaux sont fermés, mettez le système en surveillance totale et fermez la zone finale d'entrée/sortie. Dès que la porte est fermée, la temporisation Dernière issue commence à décompter pour mettre en surveillance le système.
Shunt	Une zone dont l'attribut Shunt est défini sera inhibée lorsqu'une zone de type Shunt est ouverte. Cela offre un moyen pour grouper l'inhibition des zones avec l'ouverture du type de zone Shunt.

Attribut zone	Description
Transmission seule	Cet attribut ne s'applique qu'à un type de zone INCENDIE. Si cet attribut est défini, alors l'activation de la zone Incendie ne sera signalée qu'au centre de télésurveillance. Aucune alarme ne sera générée sur le site.
Seulement ouvert	Cet attribut ne s'applique qu'à un type de zone CLÉ DE MES. S'il est défini, l'état de surveillance du bâtiment ne s'activera qu'au moment des ouvertures.
Mise en surveillance possible	Cet attribut ne s'applique qu'à un type de zone CLÉ DE MES. Si cet attribut est appliqué, l'activation de la zone met le système/secteur en surveillance totale. Utilisez cet attribut lorsque vous voulez que l'utilisateur ait uniquement la possibilité de METTRE TOTALEMENT EN SURVEILLANCE le système à partir d'une zone Clé de MES.
Mise hors surveillance possible	Cet attribut ne s'applique qu'à un type de zone CLÉ DE MES. Si cet attribut est défini, l'activation de la zone met le système/secteur hors surveillance. Utilisez cet attribut lorsque vous voulez que l'utilisateur ait uniquement la possibilité de METTRE TOTALEMENT HORS SURVEILLANCE le système à partir d'une zone Clé de MES.
Rapport Zone technique	Permet à une zone, lorsqu'elle est ouverte, d'envoyer, quel que soit le mode, une alarme au CTS dans FF, CID, SIA et SIA étendu. Lorsque des secteurs sont sélectionnés, l'alarme n'est envoyée qu'au CTS auquel le secteur a été affecté. Il s'agirait d'une UA – Alarme inconnue – suivie par le numéro de zone et un texte si SIA étendu est sélectionné. Elle envoie également un SMS à l'utilisateur final et à l'installateur si cette option est choisie lorsque le filtre d'alarme non confirmée est sélectionné.
Affichage Zone technique	Permet à une zone d'ouverture de s'afficher sur le clavier du système. La LED d'alerte doit également s'allumer. Lorsque des secteurs sont sélectionnés, elle ne s'affiche que sur le clavier affecté au secteur dans lequel la zone a été sélectionnée. L'alerte ne peut s'afficher que sur le clavier lorsque le secteur est en mode hors surveillance et pas dans les modes Partielle A, Partielle B et en surveillance.
Zone technique Audible	Permet d'activer le buzzer dans une zone activée. Le principe de fonctionnement est le même que pour Affichage zone technique dans les différents modes de surveillance et sur des systèmes avec des secteurs.
Délai zone technique	Permet à la zone d'avoir un délai programmable. Le délai peut varier de 0 à 9 999 secondes et s'applique à toutes les zones techniques. Le principe de fonctionnement est le même que pour le temporisateur Tempo défaut 230 V : si la zone est fermée pendant le délai, une alarme n'est pas envoyée au CTS, un SMS n'est pas envoyé à l'utilisateur, et la sortie technique ne déclenche pas. **Remarque :** la sortie Technique ne s'enclenchera pas tant que la temporisation de retard n'aura pas expiré.
Rapport en mode armé uniquement	Les ouvertures ne sont signalées qu'en mode armé.
Pré-alarme incendie	Si activé et qu'une alarme incendie se produit, une temporisation de pré-alarme incendie démarre et les sirènes internes et les buzzers se déclenchent. (Voir *Temporisations* page 269.) Si l'alarme n'est pas annulée pendant la durée de la temporisation, une alarme incendie est confirmée, les sirènes internes et externes se déclenchent et un événement est envoyé au CTS.
Confirmation incendie	Si activé, une temporisation Confirmation feu est enclenchée qui ajoute un temps supplémentaire à la temporisation de pré-alarme incendie jusqu'à ce qu'une alarme incendie soit signalée pour la zone. Voir *Temporisations* page 269.

Attribut zone	Description
Test sismique / Test automatique du détecteur	Un type de zone sismique peut être testé manuellement ou automatiquement. Cet attribut permet d'activer le test automatique. Consultez *Temporisations* page 269 pour obtenir des informations détaillées sur comment configurer la temporisation qui détermine la fréquence à laquelle la centrale teste toutes les zones sismiques possédant cet attribut. La valeur par défaut pour la temporisation est de 7 jours.
Temporisée	L'attribut Temporisée est utilisé pour les zones Clé de MES afin de retarder la mise en surveillance d'un secteur. La durée correspond à la temporisation de sortie du secteur pour lequel la clé de MES est associée.
Vérification	Sélectionnez la zone de vérification configurée pour affecter à cette zone l'action de vérification du déclenchement audio/vidéo.
MES FORCEE	Si activé, le périphérique à armement par clé peut activer le système, inhibant automatiquement toutes les zones ouvertes.

23.18 Attributs applicables aux types de zones

Le tableau ci-dessous indique les attributs applicables par type de zone :

Zone Type / **Attribute**	Alarm	Entry/Exit	Exit Term	Fire	Fire Exit	Line	Panic	Holdup	Tamper	Tech	Medical	Keyarm	Unused	Shunt	X-Shunt	Detector Fault	Lock Supervision	Seismic **	All Okay	Hold-up Fault	Warning Fault	Setting Authorisation	Lock Element	Glass Break
Access	√																							√
Exclude A	√	√																					√	√
Exclude B	√	√																					√	√
24 Hour	√																	√						√
Local	√	√		√	√						√					√				√	√		√	√
Unset Local	√			√														√						√
Double Knock	√																							√
Chime	√	√								√												√		√
Inhibit	√	√	√	√	√	√	√	√	√	√	√	√		√	√	√	√	√	√	√	√		√	√
Normal Open	√	√	√	√	√	√	√	√	√	√	√	√		√	√	√	√		√	√	√	√	√	√
Silent	√						√	√																√
Log	√	√	√	√	√	√	√	√	√	√	√	√		√	√	√	√	√	√	√	√	√	√	√
Shunt	√	√			√																			√
Frequent *	√	√	√							√		√		√	√									√
Analyzed	√	√			√																			
Pulse Count	√	√			√																			
Gross attack	√	√			√																			
Calendar	√	√	√	√	√	√	√	√	√	√	√	√		√	√	√	√	√	√	√	√	√	√	√
Verification	√	√		√	√		√	√		√	√							√						√
Exit Open		√																						
Seismic Test																		√						
Timed												√												
Report Only				√																				
Open Only												√										√		
Final Exit		√																					√	
Fullset enable												√												
Unset enable												√												
Shunt	√	√			√																			√
Report (Tech)										√														
Display(Tech)										√														
Audible (Tech)										√														
Delay (Tech)										√														
Report When Set										√														
Fire Pre-alarm				√	√																			
Fire Recognition				√	√																			
Force set												√												

Uniquement disponible en mode Évolué.

** Uniquement en association avec des services à distance.*

*** Uniquement disponible en mode Bancaire.*

23.19 Niveaux ATS et spécifications d'atténuation

Niveaux d'ATS (Alarm Transmission System, Système de transmission d'alarme)

Le tableau suivant récapitule les niveaux d'ATS nécessaire pour la centrale, en cas de communication :

- GSM vers un centre de télésurveillance (CTS)
- RTC vers un centre de télésurveillance (CTS)
- Ethernet vers un logiciel de réception SPC Comm
- GPRS vers un logiciel de réception SPC Comm

	GSM CTS	RTC CTS	Ethernet	GPRS
Niveau ATS	ATS 2	ATS 2	ATS 6	ATS 5

Atténuation de RTC

Pour un numéroteur RTC, il est recommandé d'utiliser un câble de télécommunication interne CW1308 ou équivalent pour connecter le modem à la ligne téléphonique. La longueur du câble doit être comprise entre 0,5 m et 100 m.

Atténuation d'Ethernet

Pour Ethernet, nous recommandons l'utilisation d'un câble de catégorie 5 d'une longueur comprise entre 0,5 m et 100 m.

Atténuation de GSM

La force du champ du signal GSM doit être d'au moins -95 dB. En deçà de ce niveau, le modem signalera une erreur de signal faible à la centrale. Cette erreur sera traitée comme les autres erreurs du système.

Surveillance du RTC (SPCN110) et du GSM (SPCN320)

Une panne de l'interface entre le modem RTC et la centrale sera détectée après 30 secondes, au bout desquelles une erreur ATS sera signalée.

Une panne de l'interface entre le modem RTC et la centrale sera détectée après 30 secondes, au bout desquelles une erreur ATS sera signalée.

23.20 Lecteurs de cartes et de formats de badges pris en charge

Les lecteurs et formats suivants sont pris en charge par le système SPC :

Lecteur	Format du badge
HD500-EM PR500-EM SP500-EM PM500-EM	IB41-EM IB42-EM IB44-EM IB45-EM ABR5100-BL ABR5100-TG ABR5100-PR

Lecteur	Format du badge
AR6181-RX AR6182-RX	IB41-EM IB42-EM IB44-EM IB45-EM ABR5100-BL ABR5100-TG ABR5100-PR
HD500-Cotag PR500-Cotag SP500-Cotag PM500-Cotag HF500-Cotag	IB928 IB911 IB968 IB961 IB958M
PP500-Cotag	IB928 IB911 IB968 IB961 IB958M
PP500-EM	IB41-EM IB42-EM IB44-EM IB45-EM ABR5100-BL ABR5100-TG ABR5100-PR
AR6181-MX AR6182-MX	ABP5100-BL MIFARE Classique 1K ABP5100-BL MIFARE Classique 4K
iClass R10 iClass R15 iClass R30 iClass R40 iClassRK40	ABP5100-BL Seulement MIFARE 32 bit par défaut

Lecteur	Format du badge
MultiClass RP40 MultiClass RP15 MultiClass RPK40	ABP5100-BL Seulement MIFARE 32 bit par défaut IB41-EM IB42-EM IB44-EM IB45-EM ABR5100-BL ABR5100-TG ABR5100-PR
HID Prox Pro	26 bit Wiegand EPX 36 bit Wiegand

Codes et restrictions du site

Format Lecteur	Code du site disponible	Restrictions
EM4102	Non	N° maxi de badge 9999999999
COTAG	Non	N° maxi de badge 9999999999
Wiegand 26 bits	Oui	Code site maxi 255 N° maxi de badge 65535
Wiegand 36 bits	Oui	Code site maxi 32767 N° maxi de badge 524287
HID Corporate 1000	Oui	Code site maxi 4095 N° maxi de badge 1048575
HID 37	Non	N° maxi de badge 34359738370
HID 37F	Oui	Code site maxi 65535 N° maxi de badge 5242875
HID 37BCD	Non	N° maxi de badge 99999999
HID ICLASS MIFARE	Non	N° maxi de badge 4294967295
HID ICLASS DESFIRE	Non	Numéro de badge chiffré. N° maxi de badge 72 x 10^{16}. Ce numéro doit être reconnu par la centrale
AR618 WIE BCD 52 BIT	Non	N° maxi de badge 4294967295
AR618 OMRON 80 BIT	Non	N° maxi de badge 9999999999999

23.21 Support SPC pour périphériques E-Bus

La passerelle E-Bus SPC (SPCG310) est un transpondeur X-BUS permettant la communication entre un contrôleur SPC et des périphériques E-Bus Sintony. L'adressage de l'E-BUS Sintony permet des adresses doubles de transpondeur sur différentes sections de l'E-BUS. Les périphériques X-BUS n'ont besoin que d'adresses uniques. Pour prendre cela en compte, il peut s'avérer nécessaire d'effectuer un réadressage du périphérique E-BUS. Pour plus d'informations, consultez *Mode adressage* page 151.

REMARQUE : Vanderbilt vous recommande de lire le document **Sintony System Migration (Migration du système Sintony)** avant de configurer les périphériques E-Bus.

23.21.1 Configuration et adressage des périphériques E-Bus

Il est possible de configurer et d'adresser les périphériques E-Bus Sintony suivants, pour communiquer avec le contrôleur SPC :

- Claviers Sintony SAK41/SMK41, SAK51/SMK51 et SAK53/SMK53
- Transpondeurs d'entrée Sintony
- Transpondeurs de sortie Sintony
- PSU Sintony : SAP 8, SAP 14, SAP 20 et SAP 25

1. Dans le navigateur, allez sur **Paramètres > X-BUS > Transpondeurs**.

   La liste des **Transpondeurs configurés** s'affiche.
2. Sélectionner un **SPC E-Bus Gateway**.
3. Sur la page **Configuration transpondeur**, saisissez une **Description** pour le **Gateway E-BUS pour SPC**. Pour un complément d'information sur la configuration des transpondeurs, voir *Transpondeurs* page 237.

4. Pour adresser un périphérique E-Bus, sélectionnez une adresse dans la liste déroulante décrite dans le tableau ci-dessous. Si l'ID est marquée par une astérisque (*), cela indique qu'elle est déjà utilisée. Cette adresse ne peut pas être sélectionnée.
5. Cliquer sur le bouton **Sélectionner**.

   Le message `Adressage en cours... Une reconfiguration du Xbus va être requise` s'affiche en haut de la page.

   La Gateway E-BUS pour SPC émet un bip sonore répété.
6. En fonction du périphérique E-Bus concerné, appuyer et maintenir enfoncé le bouton d'adressage comme décrit dans la colonne **Adressage** du tableau ci-dessous.

   Le Gateway E-BUS pour SPC émet un bip continu pour indiquer que l'adresse est maintenant associée au périphérique E-Bus.
7. Allez sur **Paramètres > X-BUS > Transpondeurs**.
8. Cliquer sur le bouton **Reconfigurer**.

`Reconfiguration terminée` s'affiche en haut de la page. Les entrées et sorties E-Bus sont affichées dans la liste des **Transpondeurs configurés**. Si un transpondeur d'entrée est associé à une ALIM, le type d'ALIM est affiché dans la colonne **ALIM**. Les claviers sont affichés dans la liste des **Claviers configurés**.

9. Pour terminer la procédure d'adressage et ajouter les périphériques ALIM SAP 8, SAP 14 et SAP 20 à la liste des **Transpondeurs configurés**, consultez *Transpondeurs d'adressage pour SAP 8, SAP 14 et SAP 20* ci-dessous.
10. Si le X-BUS a des conflits d'adressage, le message d'avertissement `ID Invalide ou déjà utilisée comme IDx Transpondeur` s'affiche. Répétez les étapes précédentes jusqu'à l'élimination des conflits d'adressage.

Périphérique E-Bus : menu déroulant	Description	Format d'adresse	Adressage
Claviers	ID à assigner aux claviers Sintony.	E-BUS ID (X-BUS ID)	Maintenir simultanément enfoncées les touches 1 et 3 jusqu'à ce que le Gateway E-BUS pour SPC émette un bip continu.
Entrée	ID à assigner aux transpondeurs d'entrée Sintony	E-BUS ID (X-BUS ID)	Maintenir enfoncé le bouton d'adressage pendant 5 secondes et le relâcher pour entendre le bip continu.
Sortie	ID à assigner aux transpondeurs de sortie Sintony	E-BUS ID (X-BUS ID)	Maintenir enfoncé le bouton d'adressage pendant 5 secondes et le relâcher pour entendre le Gateway E-BUS pour SPC émettre un bip continu.
Module d'alimentation	ID assignables aux périphériques ALIM Syntony SAP 8, SAP 14, SAP 20 et SAP 25	E-BUS ID (X-BUS ID des transpondeurs associés)	Maintenez enfoncé le bouton d'adressage jusqu'à entendre le Gateway E-BUS pour SPC émettre un bip continu.

Voir également

Mode adressage page 151

23.21.1.1 Transpondeurs d'adressage pour SAP 8, SAP 14 et SAP 20

Après avoir assigné une adresse ALIM à un SAP 8, SAP 14 ou SAP 20 (voir *Configuration et adressage des périphériques E-Bus* à la page précédente), vous devez assigner un transpondeur d'entrée à l'ALIM. Cela simule une communication avec la centrale SPC via un transpondeur.

1. Sur la liste **Transpondeurs configurés**, sélectionner le **Gateway E-BUS pour SPC**.

   La page **Configuration du transpondeur** s'affiche.
2. Consulter la nouvelle adresse ALIM dans la liste déroulante.

   Un point d'exclamation (!) précède l'adresse ALIM que vous avez assignée au périphérique. Cela indique qu'un transpondeur d'entrée est disponible pour être assigné à l'ALIM.
3. Notez le numéro indiqué entre crochets à côté de l'adresse ALIM. Ce nombre est l'adresse à assigner au transpondeur d'entrée. Par exemple, si l'adresse ALIM est **ID 14 (27)**, il faut sélectionner manuellement un transpondeur avec l'**ID 27** dans la liste déroulante **Entrée**.
4. Dans la liste déroulante **Entrée**, sélectionner l'adresse transpondeur entre parenthèses à côté de l'adresse ALIM.
5. Cliquer sur le bouton **Sélectionner**.
6. Allez sur **Paramètres > X-BUS > Transpondeurs**.

7. Cliquer sur **Reconfigurer**.

   Le périphérique ALIM est affiché dans la liste des **Transpondeurs configurés**.

23.21.1.2 Transpondeurs d'adressage pour l'ALIM SAP 25.

L'ALIM SAP 25 Sintony est dotée de deux transpondeurs internes. Une adresse doit être assignée à chaque transpondeur. Ces deux adresses sont assignées automatiquement dès la fin de la procédure d'adressage décrite dans *Configuration et adressage des périphériques E-Bus* page 412. La formule `2n - 1` est applicable lorsque `n` est une valeur de l'adresse ALIM. Par exemple, si l'ID 10 est assignée au SAP 25, chaque transpondeur se verra assigner les ID E-Bus 19 et 20.

REMARQUE : dans la liste déroulante ALIM, le symbole dièse (#) précède l'adresse d'un SAP 25 pour indiquer que l'adressage automatique des transpondeurs va provoquer un conflit avec les transpondeurs d'entrée existants. Pour résoudre un tel conflit, il faut réadresser l'un des périphériques en conflit.

23.22 Glossaire FlexC

Acronyme	Description EN50136-1	Exemple FlexC
AE	**Système de gestion des alarmes** Équipement situé au CTS pour sécuriser et afficher les états d'alarme ou les changements d'état d'alarme en réponse à la réception des alarmes entrantes avant l'envoi d'une confirmation. L'AE ne fait pas partie de l'ATS.	Client SPC Com XT
CTS	**Centre de télésurveillance** Centre géré en permanence vers lequel sont envoyés les informations d'un ou plusieurs systèmes d'alarme (AS).	Le SPC Com XT doit être installé dans un CTS.
AS	**Système d'alarme** Installation électrique qui répond à la détection manuelle ou automatique de la présence d'un risque. Le système d'alarme (AS) ne fait pas partie du système de transmission (ATS).	Centrale SPC
ATE	**Équipement de transmission d'alarme** Terme collectif désignant l'ATE, le MCT (Monitoring Centre Transceiver) et le frontal de réception des alarmes.	-
ATP	**Chemin de transmission d'alarme** Chemin qu'un message d'alarme traverse entre un Système d'Alarme (AS) et son équipement d'Alarme associé (AE). Le chemin de transmission (ATP) commence à l'interface entre un système d'alarme (AS) et le transmetteur (SPT) et finit à l'interface entre le récepteur (RCT) et le système de gestion des alarmes (AE). Pour les fonctions de notification et de supervision, le sens inverse peut aussi être utilisé.	Un chemin prédéfini entre la centrale SPC et le récepteur SPC ComXT. Par exemple, un système utilisant Ethernet comme chemin principal et GPRS comme chemin de secours aura deux ATP différents au sein de l'ATS.

Acronyme	Description EN50136-1	Exemple FlexC
ATS	**Système de transmission d'alarme** Ensemble constitué de l'équipement de transmission d'alarme (ATE) et de réseaux de communication, utilisés pour transmettre l'état d'un ou plusieurs systèmes d'alarme (AS) d'un établissement surveillé vers un ou plusieurs systèmes de gestion des alarmes (AE) d'un ou plusieurs CTS. Un système ATS peut comprendre plus d'un chemin ATP.	Un système de transmission d'alarme combinant un ou plusieurs chemins de transmission entre une centrale SPC et un le SPC Com XT.
RCT	**Frontal de réception** Équipement de transmission d'alarme (ATE) dans le CTS, relié à un ou plusieurs systèmes de gestion des alarmes (AE) et un ou plusieurs réseaux de transmission, qui constitue au moins un chemin de transmission d'alarme (ATP). Dans certains systèmes, cet équipement d'émission et de réception peut être capable d'indiquer les changements d'état du système d'alarme et de gérer un JDB. Cela peut être nécessaire en cas de défaillance de l'informatique de gestion des alarmes du centre.	Récepteur SPC Com XT
SPT	**Transmetteur supervisé** Équipement de transmission d'alarme (ATE) - au niveau du site surveillé - incluant : l'interface au système d'alarme (AS) et l'interface à un ou plusieurs réseaux de transmission - qui constitue au moins un chemin de transmission d'alarme (ATP).	Intégré à la centrale SPC avec Ethernet, GPRS, PPP sur RTC.

FlexC utilise divers acronymes (repris de la norme EN50136-1).

Acronyme	Description
ASP	**Protocole de sécurité analogique (ASP)** Les protocoles de transmission d'alarme sont généralement utilisés pour la transmission d'alarme sur le réseau téléphonique, par ex. SIA ou Contact ID.

23.23 FlexC - Commandes

La fenêtre ci-dessous liste les commandes disponibles pour un profil de commande. Le profil de commande assigné à un système de transmission ATS définit le mode de contrôle d'une centrale depuis le SPC Com XT.

Filtre commande	Commandes
Commandes système	Lit Résumé Centrale
	Définit la date et l'heure du système
	Accès Installateur autorisé
	Accès Constructeur autorisé

Filtre commande	Commandes
Commandes intrusion	Lit l'état des secteurs
	Lit le changement d'état d'un secteur
	Change le mode d'un secteur (MES/MHS)
	Lit l'état des alertes de la centrale
	Réalise des actions sur alerte
	Arrête les sirènes
	Lit l'état d'une zone
	Contrôle une zone
	Lit le JDB du système
	Lit le JDB d'une zone
	Lit le JDB radio
Commandes de sorties	Lit l'état d'une sortie interaction logique
	Contrôle une sortie interaction logique
Commandes utilisateur	Vérifie un utilisateur dans la centrale
	Lit la configuration d'un utilisateur
	Ajouter utilisateur
	Édite un utilisateur
	Supprimer un utilisateur
	Lit la configuration d'un profil utilisateur
	Ajout d'un profil utilisateur
	Édite un profil utilisateur
	Supprime un profil utilisateur
	Change le code PIN d'utilisateur
Commandes sur Calendrier	Lit la configuration d'un calendrier
	Ajouter un calendrier
	Édite un calendrier
	Édite une semaine du calendrier
	Supprime un calendrier
	Ajouter un jour exceptionnel
	Édite un jour exceptionnel
	Supprime un jour exceptionnel

Filtre commande	Commandes
Commandes de communication	Lit l'état de l'Ethernet
	Lit l'état d'un modem
	Lit le JDB d'un modem
	Lit le JDB d'un récepteur CTS
FlexC - Commandes	Lit l'état d'un ATS FlexC
	Lit le JDB réseau d'un ATS FlexC
	Lit le JDB événement d'un ATS FlexC
	Lit le JDB d'un ATS FlexC
	Lit le JDB réseau d'un Chemin FlexC
	Exporte le fichier de configuration d'un ATS FlexC
	Importe le fichier de configuration d'un ATS FlexC
	Supprime un ATS FlexC
	Supprime un Chemin FlexC
	Supprime un Profile Événement FlexC
	Supprime un Profile de Commande FlexC
	Active un TestAuto sur un Chemin FlexC
Commandes de contrôle d'accès	Lit la configuration d'une porte
	Lit l'état d'une porte
	Pilote une porte
	Lit le JDB d'accès
Commandes de vérification	Lit une image de caméra
	Lit l'état d'une zone de vérification
	Lit les données d'une zone de vérification
	Envoi des données à une zone de vérification
Clavier virtuel	Pilote un clavier

Filtre commande	Commandes
Fichier de Commandes	Met à jour le firmware de la centrale
	Met à jour le firmware des périphériques
	Télécharger le firmware des périphériques
	Mettre à jour la progression PFW
	Upload un fichier de configuration
	Download un fichier de configuration
	Enregistre la configuration de la centrale
	Redémarre la centrale
Commandes maintenance	Lit les infos de la centrale
	Lit les états de la centrale
	Lit l'en-tête des fichiers configuration
	Lit la configuration de langue
	Lit la configuration intrusion
	Lit l'état des périphériques X-BUS
	Lit la configuration d'un secteur

23.24 Tempos des catégories d' ATS

Ce tableau décrit les tempos des catégories d'ATS définies dans la norme EN50136-1 et précise comment FlexC respecte ces dispositions au titre des catégories SP1-SP6, DP1-DP4.

		Tempos requis par EN50136-1				FlexC - Implémentation des tempos pour les différentes catégories d'ATS			
Catégories d'ATS	Interfaces par défaut	Événement timeout	Timeout Polling Chemin Principal	Timeout polling Chemin de secours (principal OK)	Timeout polling Chemin de secours (principal NOK)	Événement timeout	Timeout Polling Chemin Principal	Timeout polling Chemin de secours (principal OK)	Timeout polling Chemin de secours (principal NOK)
SP1	Cat 1 [Ethernet]	8 mn	32 jours	-	-	2 mn	30 Jours	-	-
SP2	Cat 2 [Ethernet]	2 mn	25 h	-	-	2 mn	24 h	-	-
SP3	Cat 3 [Ethernet]	60 s	30 mn	-	-	60 s	30 mn	-	-
SP4	Cat 4 [Ethernet]	60 s	3 mn	-	-	60 s	3 mn	-	-
SP5	Cat 5 [Ethernet]	30 s	90 s	-	-	30 s	90 s	-	-
SP6	Cat 6 [Ethernet]	30 s	20 s	-	-	30 s	20 s	-	-

		Tempos requis par EN50136-1				FlexC - Implémentation des tempos pour les différentes catégories d'ATS			
Catégories d'ATS	**Interfaces par défaut**	**Événement timeout**	**Timeout Polling Chemin Principal**	**Timeout polling Chemin de secours (principal OK)**	**Timeout polling Chemin de secours (principal NOK)**	**Événement timeout**	**Timeout Polling Chemin Principal**	**Timeout polling Chemin de secours (principal OK)**	**Timeout polling Chemin de secours (principal NOK)**
DP1	Cat 2 [Ethernet] Cat 2 [Modem]	2 mn	25 h	50 h	25 h	2 mn	24 h	24 h 30	24 h 10
DP2	Cat 3 [Ethernet] Cat 3 [Modem]	60 s	30 mn	25 h	30 mn	60 s	30 mn	24 h 30	30 mn
DP3	Cat 4 [Ethernet] Cat 4 [Modem]	60 s	3 mn	25 h	3 mn	60 s	3 mn	24 h 30	3 mn
DP4	Cat 5 [Ethernet] Cat 5 [Modem]	30 s	90 s	5 h	90 s	30 s	90 s	4 h 10	90 s

23.25 Tempos des catégories de Chemin

La fenêtre suivante présente les paramètres appliqués aux événements d'expiration du délai d'attente, aux intervalles de polling (actifs et inactifs) et aux timeouts du polling (actifs et inactifs) pour chaque catégorie de chemin. Pour l'Ethernet, l'intervalle de polling et l'intervalle de tentative sont identiques. Pour réduire les coûts liés aux appels GPRS, l'intervalle et l'intervalle de tentative des chemins GPRS sont différents ; par exemple, les interrogations Cat 3 [Modem] interviennent toutes les 25 min, puis toutes les 60 s pendant 5 min pendant un maximum de 30 min. Pour une vue d'ensemble de l'intervalle de polling configuré, allez sur **État > FlexC > JDB réseau**.

Si un chemin est actif puis devient inactif, il reste dans le taux actif de polling pendant deux cycles supplémentaires avant de passer à un intervalle de polling **Chemin tombé**.

Catégories de chemin Ethernet		Polling quand le chemin est actif			Polling quand le Chemin est inactif			Polling quand le Chemin est tombé	
Catégories du Chemin	**Événement timeout**	**Intervalles des pollings**	**Intervalle de tentative**	**Timeout Test**	**Intervalles des pollings**	**Intervalle de tentative**	**Timeout Test**	**Intervalles des pollings**	**Délai**
Cat 6 [Ethernet]	30 s	8 s	30 s	20 s	8 s	30 s	20 s	30 s	30 s
Cat 5 [Ethernet]	30 s	10 s	30 s	90 s	10 s	30 s	90 s	30 s	30 s
Cat 4 [Ethernet]	60 s	30 s	30 s	3 mn	30 s	30 s	3 mn	30 s	30 s

Catégories de chemin Ethernet		Polling quand le chemin est actif			Polling quand le Chemin est inactif			Polling quand le Chemin est tombé	
Catégories du Chemin	**Événement timeout**	**Intervalles des pollings**	**Intervalle de tentative**	**Timeout Test**	**Intervalles des pollings**	**Intervalle de tentative**	**Timeout Test**	**Intervalles des pollings**	**Délai**
Cat 3 [Ethernet]	60 s	60 s	60 s	30 mn	60 s	60 s	30 mn	60 s	30 s
Cat 2A [Ethernet]	2 mn	2 mn	2 mn	4 h	2 mn	2 mn	4 h	2 mn	30 s
Cat 2 [Ethernet]	2 mn	2 mn	2 mn	24 h	2 mn	2 mn	24 h	2 mn	30 s
Cat 1 [Ethernet]	2 mn	2 mn	2 mn	30 Jours	2 mn	2 mn	30 Jours	2 mn	30 s
Catégories de chemin modem									
Cat 5 [Modem]	30 s	10 s	30 s	90 s	4 h	2 mn	4 h 10	10 min	90 s
Cat 4A [Modem]	60 s	60 s	60 s	3 mn	4 h	2 mn	4 h 10	30 mn	90 s
Cat 4 [Modem]	60 s	60 s	60 s	3 mn	24 h	2 mn	24 h 30	1 h	90 s
Cat 3 [Modem]	60 s	25 mn	60 s	30 mn	24 h	2 mn	24 h 30	4 h	90 s
Cat 2A [Modem]	2 mn	4 h	2 mn	4 h 10	24 h	2 mn	24 h 30	4 h	90 s
Cat 2 [Modem]	2 mn	24 h	2 mn	24 h 10	24 h	2 mn	24 h 30	24 h	90 s
Cat 1 [Modem]	2 mn	24 h	10 min	25 h	30 Jours	10 min	30 jours 1 h	7 jours	90 s

24 Remarques

Publié par Vanderbilt International (IRL) Ltd.
Clonshaugh Business and Technology Park
Clonshaugh
Dublin 17
D17 KV 84
Ireland

www.vanderbiltindustries.com

© Vanderbilt 2018

Les données et la conception peuvent être modifiées sans préavis. La fourniture du produit dépend de sa disponibilité.

ID document : A6V10276959-c
Version du document : X.X
Date d'édition : 11.2018