



SPC42xx/43xx/52xx/53xx/63xx **Centrale d'alarme intrusion**

3.6

Copyright

La disponibilité et les spécifications techniques peuvent être modifiées sans préavis.

© Copyright par Vanderbilt

Nous nous réservons tous les droits sur ce document et sur l'objet dont il traite. En acceptant le document, l'utilisateur reconnaît ces droits et accepte de ne pas publier le document ni de divulguer le sujet dont il traite en tout ou partie, de ne pas le remettre à une tierce partie quelle qu'elle soit sans notre accord au préalable écrit et de ne pas l'utiliser à d'autres fins que celles pour lesquelles il lui a été fourni.

Edition: 01.05.2016

ID document: A6V10316314

Table des matières

1	Signification des pictogrammes	11
2	Sécurité	12
2.1	Groupe cible	12
2.2	Consignes de sécurité générales	12
2.2.1	Informations générales	12
2.2.2	Transport.....	13
2.2.3	Réglages	13
2.2.4	Fonctionnement	13
2.2.5	Entretien et maintenance	14
2.3	Signification des avertissements écrits	14
2.4	Signification des panneaux de danger	14
3	Directives et normes	16
3.1	Directives de l'Union européenne	16
3.1.1	Vue d'ensemble de la conformité à la norme EN50131	16
3.1.2	Conformité aux agréments EN50131	21
3.1.3	Conformité aux agréments EN 50136-1:2012 and EN 50136-2:2014	23
3.1.4	Conformité aux agréments INCERT	23
3.1.5	Directives de conformité PD 6662:2010	25
3.1.5.1	Étendue du produit.....	25
3.1.5.2	Aperçu des normes.....	25
3.1.5.3	Méthodes d'obtention de l'activation et de la désactivation	26
3.1.5.4	Exigences en matière de configuration pour la conformité avec la PD 6662:2010	28
3.1.5.5	Exigences supplémentaires de mise en œuvre pour conformité à PD 6662:2010	30
3.1.5.6	Informations supplémentaires.....	30
3.1.6	Conformité avec les agréments VDS.....	31
3.1.7	Conformité avec les agréments NF et A2P	32
4	Caractéristiques techniques	34
4.1	SPC4000	34
4.2	SPC5000	36
4.3	SPC6000	38
5	Introduction	43
6	Installation du matériel	44
6.1	Montage d'un boîtier G2.....	44
6.2	Montage d'un boîtier G3.....	45
6.2.1	Montage du kit d'autosurveillance arrière	47
6.2.2	Installation de la batterie pour conformité EN50131	51
6.3	Montage d'un boîtier G5.....	52
6.3.1	Protection antisabotage	54
6.3.2	Montage du boîtier avec la protection antisabotage	54
6.3.2.1	Fonctionnement de l'antisabotage (autosurveillance)	56

6.3.3	Installation des batteries	57
6.4	Installation d'un clavier	58
6.5	Installation d'un transpondeur	58
7	Alimentation Auxiliaire Supervisée	59
7.1	SPCP355.300 Smart PSU.....	59
7.1.1	Sorties supervisées.....	61
7.1.2	Batteries	62
7.1.2.1	Installation des batteries	62
7.1.2.2	Test de la tension de la batterie.....	64
7.1.2.3	Protection contre la décharge profonde.....	64
7.1.2.4	Durée de veille de la batterie	64
7.1.3	Câblage de l'interface X-BUS	64
7.1.3.1	Câblage des entrées.....	65
7.1.3.2	Câblage des sorties	66
7.1.4	Témoin d'état du module d'alimentation	68
7.1.5	Restauration du système	69
8	Matériel de la centrale.....	70
8.1	Matériel de la centrale 42xx\43xx\53xx\63xx	70
8.2	Matériel de la centrale SPC5350 et 6350.....	73
9	Transpondeur de porte	76
10	Câblage du système.....	77
10.1	Câblage de l'interface X-BUS.....	77
10.1.1	Configuration en boucle	78
10.1.2	Configuration en branche.....	79
10.1.3	Configuration en étoile et multipoints.....	80
10.1.3.1	Exemples de câblage correct.....	84
10.1.3.2	Exemples de câblage incorrect.....	85
10.1.4	blindage.....	86
10.1.5	Plan câble	87
10.2	Câblage du transpondeur de branche.....	87
10.3	Mise à la terre du système	88
10.4	Câblage de la sortie de relais	88
10.5	Câblage des entrées de zone	89
10.6	Câblage d'une sirène extérieure SAB	92
10.7	Câblage d'un buzzer interne.....	93
10.8	Câblage du Bris de verre.....	93
10.9	Installation des modules d'extension.....	94
11	Mise sous tension de la centrale SPC.....	96
11.1	Mise sous tension avec seulement la batterie	96
12	Interface utilisateur du clavier	97
12.1	SPCK420/421	97
12.1.1	Introduction	97
12.1.2	Utilisation de l'interface du clavier LCD	99
12.1.3	Entrées de données sur le clavier LCD	102
12.2	SPCK620/623.....	103

	12.2.1	Introduction	103
	12.2.2	Description des témoins LED.....	106
	12.2.3	Description du mode d'affichage.....	107
	12.2.4	Touches de fonction au repos	108
13		Outils logiciels.....	109
14		Démarrage du système.....	110
14.1		Modes de programmation	110
	14.1.1	Codes Installateur	110
14.2		Outils de programmation	111
	14.2.1	Programmeur Rapide.....	111
14.3		Configuration des paramètres de démarrage	111
14.4		Créer les utilisateurs du système	113
14.5		Programmation d'un tag PACE	113
14.6		Programmation des tags sans fil.....	115
	14.6.1	Effacement d'alertes avec la télécommande	116
15		Programmation en mode Exploitation avec le clavier.....	117
16		Programmation en mode Paramétrage avec le clavier	118
16.1		ETAT DU SYSTEME.....	118
16.2		OPTIONS	119
16.3		TEMPORISATIONS	122
16.4		SECTEURS.....	125
16.5		GROUPE SECTEURS.....	126
16.6		Périph. X-BUS	126
	16.6.1	Adressage du X-BUS.....	126
	16.6.2	XBUS REFRESH	127
	16.6.3	RECONFIGURER.....	128
	16.6.4	CLAVIERS/TRANSPONDEURS/CONTROLEURS DE PORTE	128
	16.6.4.1	LOCALISER.....	129
	16.6.4.2	AFFICHER ETAT	129
	16.6.4.3	ÉDITION DES CLAVIERS	130
	16.6.4.4	ÉDITION DES TRANSPONDEURS	133
	16.6.4.5	ÉDITION DES CONTRÔLEURS DE PORTE.....	136
	16.6.5	MODE ADRESSAGE	138
	16.6.6	TYPE X-BUS.....	139
	16.6.7	RE-ESSAI BUS.....	139
	16.6.8	TEMPO DEF. COMMS	139
16.7		RADIO	139
	16.7.1	AJOUTER DES DETECTEURS	140
	16.7.2	MODIFIER DÉTECTEURS (AFFECTATION DE ZONE)	141
	16.7.3	AJOUTER WPA	141
	16.7.4	MODIFIER WPA	141
16.8		ZONES	142
16.9		PORTES.....	143
	16.9.1	PORTES	143
16.10		SORTIES.....	147

	16.10.1	Types et ports de sortie	147
16.11		COMMUNICATION	151
	16.11.1	PORTS SERIE	151
	16.11.2	PORTS ETHERNET	151
	16.11.3	MODEMS	152
	16.11.3.1	Supervision de l'interface réseau de transmission	152
	16.11.3.2	Pour configurer un modem	153
	16.11.4	CENTRE TELESURV.	154
	16.11.4.1	AJOUTER	154
	16.11.4.2	EDITER	155
	16.11.4.3	EFFACER	155
	16.11.4.4	FAIRE APPEL TEST	155
	16.11.5	TÉLÉMAINTENANCE	156
16.12		TEST.....	156
	16.12.1	TEST SIRENE.....	156
	16.12.2	TEST DEPLACEMENT	157
	16.12.3	TEST ZONE	157
	16.12.4	TEST SORTIE.....	158
	16.12.5	TEST JDB	158
	16.12.6	OPTIONS SONORES	159
	16.12.7	IND. VISUELS.....	159
	16.12.8	TEST WPA.....	159
	16.12.9	TEST SISMIQUE	160
16.13		UTILITAIRES	160
16.14		ISOLER	161
16.15		JOURNAL DE BORD	161
16.16		ACCES JDB	162
16.17		JOURNAL DES ALARMES	162
16.18		MODIFIER CODE INSTALLATEUR.....	162
16.19		GESTION UTILISAT.....	163
	16.19.1	AJOUTER	163
	16.19.2	EDITER	163
	16.19.2.1	CONTROLE D'ACCES	164
	16.19.3	EFFACER	166
16.20		PROFILS UTILISATEUR.....	166
	16.20.1	AJOUTER	166
	16.20.2	EDITER	167
	16.20.3	EFFACER	167
16.21		SMS.....	167
	16.21.1	AJOUTER	168
	16.21.2	EDITER	168
	16.21.3	EFFACER	169
16.22		X-10.....	169
16.23		MODIF DATE/HEURE	170
16.24		TEXTE INSTALLAT.....	170
16.25		CONTROLE PORTES.....	171

17	Programmation en mode Installateur avec le navigateur	172
17.1	Infos sur le système	172
17.2	Interface Ethernet	173
17.3	Connexion USB à la centrale	174
17.4	Connexion avec le navigateur	177
17.5	SPC Accueil.....	178
	17.5.1 Récapitulatif du système	178
	17.5.2 Vue générale des alarmes	178
	17.5.3 Affichage des vidéos	179
17.6	État de la centrale	180
	17.6.1 État.....	180
	17.6.2 État X-bus	181
	17.6.2.1 Statut du Transpondeur	181
	17.6.2.2 Etat de l'alimentation.....	183
	17.6.2.3 Statut du Clavier	185
	17.6.2.4 Etat du contrôleur de porte	187
	17.6.3 Radio.....	189
	17.6.3.1 Historique - Détecteur radio X	190
	17.6.4 Zones	190
	17.6.5 Portes.....	192
	17.6.6 FlexC - État.....	193
	17.6.7 Défauts système	194
17.7	Journaux de bord	195
	17.7.1 JDB Système	195
	17.7.2 JDB Accès	196
	17.7.3 Journal des événements WPA	196
	17.7.4 JOURNAL DES ALARMES.....	197
17.8	Utilisateur.....	197
	17.8.1 Ajouter/Éditer un utilisateur.....	197
	17.8.1.1 Appareils inconnus.....	199
	17.8.2 Ajouter/Modifier un profil utilisateur.	200
	17.8.3 Programmation SMS.....	204
	17.8.4 Commandes SMS.....	206
	17.8.5 Suppression des Mots de passe Web	208
	17.8.6 Paramètres de configuration Installateur	208
	17.8.6.1 Changement du code Ingénieur et du mot de passe d'accès installateur.....	210
17.9	Configuration	211
	17.9.1 Configurer les entrées et sorties de la centrale	211
	17.9.1.1 Éditer une entrée	211
	17.9.1.2 Éditer une sortie	212
	17.9.1.3 Configuration les systèmes de verrouillage et sorties de MES Auto	217
	17.9.1.4 Configuration de X-10.....	219
	17.9.2 Périph. X-BUS.....	220
	17.9.2.1 Transpondeurs	220
	17.9.2.2 Claviers	225

17.9.2.3	Contrôleurs de porte	228
17.9.2.4	Plan câble	229
17.9.2.5	Paramètres.....	230
17.9.3	Radio.....	231
17.9.3.1	Historique - Détecteur radio X.....	232
17.9.3.2	Configuration d'un WPA.....	232
17.9.3.3	Modifier les paramètres radio	235
17.9.4	Modification des paramètres système	236
17.9.4.1	Options.....	236
17.9.4.2	Temporisations.....	245
17.9.4.3	Identification	248
17.9.4.4	Normes & Standards.....	249
17.9.4.5	Date & Heure	251
17.9.4.6	Langue	252
17.9.5	Configurer les zones, les portes et les secteurs	252
17.9.5.1	Éditer une zone	253
17.9.5.2	Ajouter / Éditer un secteur	253
17.9.5.3	Éditer une porte.....	262
17.9.5.4	Ajouter un groupe de secteurs.....	268
17.9.6	Calendriers.....	268
17.9.6.1	Ajouter / Éditer un calendrier	269
17.9.6.2	MES/MHS automatiques de secteurs	271
17.9.6.3	Autres actions des calendriers.....	271
17.9.7	Changer son code.....	272
17.9.8	Configuration des paramètres avancés	272
17.9.8.1	Déclencheurs	272
17.9.8.2	Interactions logiques	273
17.9.8.3	Vérification Audio/Vidéo.....	274
17.9.8.4	Mise à jour des licences SPC	278
17.10	Configurer les communications	278
17.10.1	Paramètres de communication	278
17.10.1.1	Configurer les services réseau de la centrale.....	279
17.10.1.2	Ethernet.....	280
17.10.1.3	Modems	280
17.10.1.4	Ports série	288
17.10.1.5	Enregistrement du portail SPC	289
17.10.2	FlexC®	289
17.10.2.1	Mode de fonctionnement	291
17.10.2.2	Configuration Démarrage Rapide ATP pour système de transmission conforme EN50136	291
17.10.2.3	Configurer un système de transmission ATS conforme EN50136-1 ou un ATS personnalisé.....	293
17.10.2.4	Exportation et importation d'un système ATS.....	302
17.10.2.5	Configuration de profils d'événement	303
17.10.2.6	Configuration de profils d'événement	307
17.10.3	Transmission.....	309
17.10.3.1	Centre de télésurveillance (CTS).....	309

	17.10.3.2 Configuration d'un EDP	313
	17.10.4 Outils PC	319
	17.10.4.1 SPC Pro / SPC Safe	319
	17.10.4.2 SPC Manager	320
	17.10.4.3 Télémaintenance	321
17.11	Opération sur les fichiers.....	322
	17.11.1 Mise à jour des fichiers	322
	17.11.1.1 Mise à jour du firmware.....	323
	17.11.1.2 Mise à jour des langues	325
	17.11.2 Utilisation du gestionnaire de fichiers	327
17.12	Utilisation de la clé de programmation rapide	328
	17.12.1 Connecter la clé de programmation à la centrale rapide	329
	17.12.2 Installation de la clé de programmation rapide sur un PC	329
	17.12.3 Gestion des fichiers de la clé de programmation rapide	330
	17.12.3.1 Configurez la clé de programmation rapide à l'aide du clavier	330
	17.12.3.2 Accès à la clé de programmation rapide à l'aide du navigateur	331
18	Accès à distance au serveur Web	332
18.1	Connexion RTC.....	332
18.2	Connexion GSM	334
19	Fonctions d'alarme anti-intrusion	337
19.1	Fonctionnement en mode Bancaire	337
19.2	Mode Evolué.....	337
19.3	Mode Simple.....	338
19.4	Alarmes totales et locales	338
20	Exemples de systèmes et scénarios	340
20.1	Utilisation d'un secteur commun	340
21	Détecteurs sismiques	342
21.1	Test du capteur sismique	343
	21.1.1 Procédure de test manuel et automatique.....	343
	21.1.2 Test automatique des détecteurs	344
	21.1.3 Test manuel des détecteurs	345
22	Utilisation du verrouillage de blocage	347
22.1	Verrouillage de blocage.....	347
22.2	Activation autorisée du verrouillage de blocage.....	348
22.3	Élément de verrouillage.....	349
23	Annexe.....	351
23.1	Connexions des câbles réseau	351
23.2	LED d'état de la centrale	351
23.3	Alimentation des transpondeurs avec les bornes d'alimentation secondaires.....	352
23.4	Calcul de la puissance nécessaire de la batterie	353
23.5	Paramètres par défaut des modes Simple, Evolué et Bancaire	355
23.6	Câblage de l'interface X-10	356
23.7	Codes SIA	356
23.8	Codes CID	361
23.9	Vue d'ensemble des types de claviers	362

23.10	Combinaisons de codes utilisateur.....	363
23.11	Codes Contrainte.....	364
23.12	Inhibitions automatiques.....	364
	23.12.1 Zones	364
	23.12.2 Codes PIN d'accès.....	364
	23.12.3 Accès Ingénieur	365
	23.12.4 Déconnexion de l'utilisateur clavier.....	365
23.13	Raccordement de la centrale au secteur.....	365
23.14	Maintenance de la centrale	365
23.15	Maintenance du chargeur (Smart PSU)	366
23.16	Type de zone	367
23.17	Attributs zone.....	370
23.18	Attributs applicables par types de zone.....	373
23.19	Niveaux ATS et spécifications d'atténuation	375
23.20	Lecteurs de cartes et de formats de badges pris en charge	375
23.21	Support SPC pour périphériques E-Bus.....	377
	23.21.1 Configuration et adressage des périphériques E-Bus	377
	23.21.1.1 Transpondeurs d'adressage pour SAP 8, SAP 14 et SAP 20	379
	23.21.1.2 Transpondeurs d'adressage pour l'ALIM SAP 25.....	380
23.22	Glossaire FlexC	380
23.23	FlexC - Commandes.....	382
23.24	Tempos des catégories d' ATS	383
23.25	Tempos des catégories de Chemin.....	384

1 Signification des pictogrammes

Les pictogrammes utilisés ont la signification suivante :

Symbole	Description
	Non disponible pour le SPC42xx, SPC43xx.
	Disponible seulement pour la centrale SPC avec une interface IP (SPC43xx/SPC53xx/SPC63xx).
	Non disponible pour l'installation de type « Simple » dans une résidence privée.
	Uniquement disponible en mode « Pas de restriction ».
	Chercher 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

2.1 Groupe cible

Les instructions fournies dans cette documentation sont destinées au groupe suivant :

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.	Assemble et installe les composants matériels sur 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
	<p>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 »).</p>

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 manque.
- 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

Endommagement de l'unité lors du transport

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

2.2.3 Réglages

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

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

Dommages résultant d'un emplacement de montage inapproprié

- Les conditions ambiantes recommandées par le fabricant doivent être respectées.
Voir les caractéristiques techniques.
- 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 déconnexion immédiatement accessible doit être fourni.
- Assurez-vous que le circuit sur lequel l'appareil est branché soit protégé par un fusible de 16 A (max.). Ne branchez aucun autre appareil de systèmes différents sur ce fusible.
- 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 que la tension de tous les câbles et conducteurs sortants soient suffisamment réduite.

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.

Risque d'explosion ou de brûlures si la batterie n'est pas installée correctement.

- Lorsque vous mettez de nouvelles batteries en place, vérifiez la polarité.
- N'utilisez que des batteries approuvées par le fabricant (type : cellule scellée régulée par soupapes).
- Ne court-circuitez pas les broches de la batterie.
- N'exposez pas la batterie au feu ou aux températures élevées.
- Ne démontez pas la batterie.
- Éliminez les batteries usagées en respectant la réglementation locale.
- Assurez-vous d'insérer la batterie correctement et de serrer l'attache ou le clip prévus pour immobiliser la batterie.

2.2.5 Entretien et maintenance

Risque d'électrocution lors de la maintenance

- Les travaux de maintenance doivent être effectués uniquement par des spécialistes formés.
- 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 panneaux de danger

	▲ AVERTISSEMENT
	Zone dangereuse

	 AVERTISSEMENT
	Tension électrique dangereuse

3 Directives et normes

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 télécommunications. La déclaration de conformité aux directives européennes est disponible pour les autorités compétentes auprès de <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/CE :

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
----------	------------

3.1.1 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 (agrément VDS A / C / EN / SES) S Cologne HRB 28788 Siège de la société : Amsterdamer Str. 174, 50735 Cologne Directeur général : Robert Reiner mann JörgWilms-Vahrenhorst (Substitut)

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
<ul style="list-style-type: none"> ● SPC6350.320 ● SPC6330.320 ● SPC5350.320 ● SPC5330.320 ● SPCP355.300 ● SPCP333.300 ● SPCE652.100 	EN50131 Grade 3

<ul style="list-style-type: none"> ● SPCK420.100 ● SPCK421.100 ● SPCE452.100 ● SPCE110.100 ● SPCE120.100 ● SPCA210.100 ● SPCK620.100 ● SPCK623.100 ● SPCN110.000 ● SPCN310.000 	
<ul style="list-style-type: none"> ● SPC5320.320 ● SPC4320.320 ● SPCP332.300 	EN50131 Grade 2

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

Exigence EN50131	SPC - Manuel d'installation et de configuration
Température de fonctionnement et plage d'humidité	Caractéristiques techniques du SPC4000 [→ 34] Caractéristiques techniques du SPC5000 [→ 36] Caractéristiques techniques du SPC6000 [→ 38]
Poids et dimensions	Caractéristiques techniques du SPC4000 [→ 34] Caractéristiques techniques du SPC5000 [→ 36] Caractéristiques techniques du SPC6000 [→ 38]
Montage	Installation du matériel [→ 44]
Installation, mise en service et maintenance, instructions, identifications de terminal	Installation du matériel [→ 44] Matériel de la centrale [→ 70]
Type d'interconnexions (voir 8.8) ;	Caractéristiques techniques du SPC4000 [→ 34] Caractéristiques techniques du SPC5000 [→ 36] Caractéristiques techniques du SPC6000 [→ 38] Câblage de l'interface X-Bus [→ 77]
Méthodes de MES et MHS (voir 11.7.1 à 11.7.3 et tableaux 23 à 26) ;	Programmation en mode Utilisateur avec le clavier Secteurs - Mise en / hors surveillance [→ 259] Configurer un transpondeur d'interrupteur à clé [→ 223] Configuration d'un tag (télécommande) radio [→ 115] Déclencheurs [→ 272]

Exigence EN50131	SPC - Manuel d'installation et de configuration
Pièces réparables par l'utilisateur	Caractéristiques techniques du SPC4000 [→ 34] Caractéristiques techniques du SPC5000 [→ 36] Caractéristiques techniques du SPC6000 [→ 38]
Alimentation requise sans bloc d'alimentation intégré	Voir les instructions d'installation des modules d'alimentation des unités SPCP33x et SPCP43x.
Bloc d'alimentation intégré, informations requises par EN 50131-6 :2008, Clause 6	Caractéristiques techniques du SPC4000 [→ 34] Caractéristiques techniques du SPC5000 [→ 36] Caractéristiques techniques du SPC6000 [→ 38]
Nombre maximal de chaque type de tag et de périphérique d'extension.	Câblage de l'interface X-Bus [→ 77] Caractéristiques techniques du SPC4000 [→ 34] Caractéristiques techniques du SPC5000 [→ 36] Caractéristiques techniques du SPC6000 [→ 38]
Consommation actuelle du CIE et de chaque type de tag et de périphérique d'extension, avec et sans alarme.	Voir les instructions d'installation correspondantes.
Courant nominal maximal de chaque sortie électrique	Caractéristiques techniques du SPC4000 [→ 34] Caractéristiques techniques du SPC5000 [→ 36] Caractéristiques techniques du SPC6000 [→ 38]
Fonctions programmables disponibles	Programmation en mode Paramétrage avec le clavier [→ 118] Programmation en mode Installateur avec le navigateur [→ 172]
Comment rendre les données inaccessibles aux utilisateurs du niveau 1 quand l'utilisateur de niveau 2, 3 ou 4 n'accède plus aux informations (voir 8.5.1)	Interface utilisateur du clavier [→ 97] Paramètres du clavier standard [→ 130] Paramètres du clavier confort [→ 131] Configurer un transpondeur d'indication [→ 222]

Exigence EN50131	SPC - Manuel d'installation et de configuration
<p>Masquage/réduction des signaux/messages traités comme événements « défaut » ou « masquage » (voir 8.4.1, 8.5.1 et Tableau 11) ;</p>	<p>Options système [→ 236] Câblage des entrées de zone [→ 89] Codes SIA [→ 356] Le masquage IRP (infrarouge passe) est toujours signalé en tant qu'événement de zone masquée (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 MHS - Aucun MES - Alarme Royaume-Uni, Europe, Suède, Suisse, Belgique MHS - Sabotage MES - Alarme</p>
<p>Priorité de traitement des signaux et des messages, et des indications (voir 8.4.1.2, 8.5.3) ;</p>	<p>Affichage du clavier standard [→ 99] Affichage du clavier confort [→ 103]</p>
<p>Nombre minimal de variations de codes PIN, touches logiques, touches biométriques et / ou touches mécaniques pour chaque utilisateur (voir 8.3) ;</p>	<p>Combinaisons de codes utilisateur [→ 363]</p>
<p>Méthode de WD interne à limitation de durée pour l'accès niveau 3 sans l'autorisation niveau 2 (voir 8.3.1) ;</p>	<p>Non pris en charge - L'installateur ne peut pas accéder au système sans permission.</p>
<p>Nombre et détails des codes PIN non admis (voir 8.3.2.2.1) ;</p>	<p>Inhibitions automatiques [→ 364]</p>
<p>Détails des méthodes biométriques d'autorisation (voir 8.3.2.2.3) ;</p>	<p>Sans objet</p>
<p>Méthode utilisée pour déterminer le nombre de combinaisons de codes PIN, touches logiques, touches biométriques et/ou touches mécaniques (voir 11.6) ;</p>	<p>Combinaisons de codes utilisateur [→ 363]</p>
<p>Nombre de tentatives de saisie du code invalides avant que l'interface utilisateur soit désactivée (voir 8.3.2.4) ;</p>	<p>Codes PIN d'accès [→ 364]</p>
<p>Détails de l'attribution d'une autorisation temporaire pour l'accès utilisateur (voir 8.3.2) ;</p>	<p>Menus utilisateur – Valider accès</p>
<p>Si la MES automatique à des heures présélectionnées est active, détails de l'indication précédant la MES et de tout contrôle automatique de l'inhibition de la MES (voir 8.3.3, 8.3.3.1) ;</p>	<p>Secteurs - Mise en / hors surveillance [→ 259]</p>
<p>Détails des conditions requises pour la MES (voir 8.3.3.4) ;</p>	<p>Activation et désactivation du système Configuration du clavier standard [→ 130] Configuration du clavier confort [→ 131] Sorties [→ 213] Types de zone [→ 367]</p>

Exigence EN50131	SPC - Manuel d'installation et de configuration
Notification des signaux de sortie ou des messages (voir 8.6) ;	Sorties [→ 213] Secteurs - Mise en / hors surveillance [→ 259] Droits d'utilisateur [→ 201]
Autres configurations de sortie vers l'interface avec des composants I&HAS (voir 8.2) ;	Sorties [→ 213] Types de zone [→ 367] Test [→ 156] Interface utilisateur du clavier [→ 97]
Critères de suppression automatique de l'attribut « test JDB » (voir 8.3.9) ;	Temporisations [→ 245]
Nombre d'événements aboutissant à une inhibition automatique	Inhibitions automatiques [→ 364]
Si le tag ACE est de type A ou B (voir 8.7) et s'il est portable ou mobile (voir 11.14) ;	Tous les périphériques sont câblés et alimentés par des modules d'alimentation système. Reportez-vous aux caractéristiques techniques correspondantes des modules d'alimentation.
Données de composant des mémoires non volatiles (voir le Tableau 30, étape 6) ;	Voir la documentation de l'utilisateur pour les claviers SPCK420/421 et SPCK620/623.
Durée de vie de la pile mémoire (voir 8.10.1) ;	N/D Enregistrement uniquement dans la mémoire non-volatile.
Fonctions en option disponibles (voir 4.1) ;	Programmation en mode Paramétrage avec le clavier Programmation en mode Installateur avec le navigateur [→ 172]
Fonctions supplémentaires disponibles (voir 4.2, 8.1.8) ;	Grade - Sans restriction Stratégies - Options système [→ 236]
Niveaux d'accès nécessaires pour accéder aux fonctions supplémentaires disponibles ;	Configuration de l'utilisateur (clavier) [→ 163] Configuration de l'utilisateur (explorateur) [→ 197]
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 Stratégies - Options système [→ 236] Conformité EN50131 [→ 21]

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
<ul style="list-style-type: none">● 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
<ul style="list-style-type: none">● SPC5320.320● SPC4320.320● SPCP332.300	EN50131-6

3.1.2 Conformité aux agréments EN50131

Configuration logicielle requise



Il n'est pas possible d'éditer le Pays ou le Grade dans SPC Pro. On ne peut modifier ces paramètres que dans le navigateur ou le clavier.

- 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.
- Les paramètres **Radio Superv.RF empêche MES** et **Détecteur RF perdu** doivent avoir une valeur autre que 0.
- Sélectionnez le **Temps de synchronisation avec la configuration Secteur** sous contrôle de l'**horloge** pour utiliser le secteur et l'horloge maître.

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

Hardware	Système	Entrées & Portes	Sorties	Portes	Secteurs	Calendriers	Changer son code	Avancé
Centrale	XBUS	Radio						
Transpondeurs	Claviers	Contrôleurs de porte	Plan câble	Paramètres X-Bus				
Configuration Clavier								
ID Clavier	2							
N° Série	559907							
Libellé	KEY 2	Entrer la description du clavier						
Réglage des touches de fonctions (état repos)								
Panique	Désactivé	Alarme Panique par l'appui simultané de deux touches						
Levée de doute								
Levée de doute	Non affecté	Une Vérification d'alarme sera faite sur le clavier où s'est produit une alerte ou une alarme contrainte						
Indications visuelles								
Rétro-éclairage	Lorsqu'une touche est appuyée	Sélectionner l'option rétro-éclairage écran du clavier						
Indicateurs	<input checked="" type="checkbox"/>	Active les voyants visibles						
Etat des MES	<input type="checkbox"/>	Sélectionner si l'état de surveillance doit être indiqué au repos						
Indications sonores								
Buzzer	<input checked="" type="checkbox"/>	Active le buzzer clavier						

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 radios 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).

	AVIS
	Les modules SPCN110 PSTN et SPCN130 GSM/GPRS sont testés sur les centrales approuvées de Grade 2 et 3 et peuvent être utilisés avec ces centrales approuvées.

3.1.3 Conformité aux agréments EN 50136-1:2012 and EN 50136-2:2014

Les produits SPC listés ont été testés conformément à la norme EN 50136-1:2012 and EN 50136-2:2014.

3.1.4 Conformité aux agréments INCERT

Configuration logicielle requise

La sélection de la Belgique (*) dans **Région** active l'application des lois locales ou nationales qui remplacent les exigences de la norme EN50131.

Hardware	Système	Entrées & Portes	Sorties	Portes	Secteurs	Calendriers	Changer son code	Avancé	
Options Système		Tempos Système		Identification		Normes & Standards		Date & Heure	Langue

Options de mise en conformité du système

Type d'installation

Simple

Evoluée

Bancaire

Spécificités Pays:

Sélectionner pour conformité au référentiel UK PD6662

Sélectionner pour conformité au référentiel Irish Standard

Sélectionner pour conformité au référentiel Suédois standard SSF 1014:3

Sélectionner pour conformité au référentiel Européen

(*) Sélectionner pour conformité au référentiel Suisse

(*) Sélectionner pour conformité au référentiel INCERT Standard

(*) Choisir pour être conforme aux exigences Espagnoles

(*) Sélectionner pour la conformité au référentiel Allemand VDS

(*) Sélectionner pour la conformité au référentiel Français NF&A2P

Grade

EN50131 Grade 2

EN50131 Grade 3

Pas de restriction

(*) La sélection de ce standard régional permet de remplacer les exigences EN50131 par celles du pays concerné.



La sélection du **Grade 2** ou du **Grade 3** active la conformité avec EN50131 ainsi qu'avec certaines exigences INCERT :

- Uniquement un ingénieur peut remettre à zéro une alarme d'autoprotection. Pour INCERT, ceci s'applique à tous les grades. Normalement, cette contrainte s'applique uniquement au 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. Concernant toutes les autres variantes, 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 pile 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 la retient.
- Mettez le cavalier (J12) en place pour les batteries 17/10 Ah et retirez-le pour les batteries 7 Ah.
- La quantité de courant de la sortie Aux en utilisant une batterie de 10 Ah (SPC42xx/52xx) est :

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

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

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

3.1.5 Directives de conformité PD 6662:2010

Cette annexe 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 Standard.

3.1.5.1 Étendue du produit

Ce document a pour sujet les composants suivants du système SPC :

Contrôleur Grade 2 SPC4320.320-L1	Transpondeur SPCE652.100, 8 entrées / 2 sorties
Contrôleur Grade 2 SPC5320.320-L1	
Contrôleur Grade 3 SPC5330.320-L1	Transpondeur SPCP332.300 Smart PSU avec transpondeur E/S
Contrôleur Grade 3 SPC5350.320-L1	SPCP355.300 Smart PSU avec transpondeur 8 entrées / 2 sorties
Contrôleur Grade 3 SPC6330.320-L1	Smart PSU avec transpondeur E/S
Contrôleur Grade 3 SPC6350.320-L1	SPCP333.300
Clavier LCDSPCK420/421.100	Module RTC SPCN110.000
Transpondeur SPCE452.100, 8 sorties de relais	Module GSM SPCN310.000

3.1.5.2 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

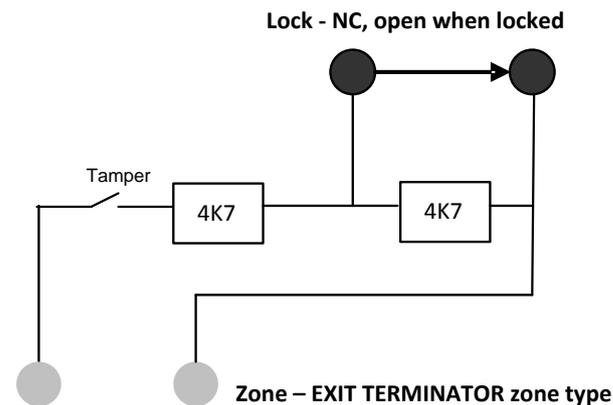
3.1.5.3 Méthodes d'obtention de l'activation et de la désactivation

3.1.5.3.1 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.
Reportez-vous à la section suivante de ce manuel :
Types de zone [→ 367]

b) Appuyez sur le bouton-poussoir monté à l'extérieur des locaux objets 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.
Reportez-vous à la section suivante de ce manuel :
Types de zone [→ 367]

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 ».
Reportez-vous à la section suivante de ce manuel :
Types de zone [→ 367]
Attributs zone [→ 370]

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

Reportez-vous à la section suivante de ce manuel :

OPTIONS [→ 119] (Clavier)

Options [→ 236] (Navigateur)

d) Clé numérique

N'est pas prise en charge par la SPC.

e) En conjonction 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.

3.1.5.3.2 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 audible que le système a été désactivé avec succès. Cette indication prend la forme d'une séquence de bips sonores 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 ARMEMENT PAR CLE 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 le 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 un lecteur TAG (par exemple, SPCK421) à côté de la porte d'entrée de locaux.

Reportez-vous aux sections suivantes de ce manuel :

- Types de zone [→ 367]
- Attributs zone [→ 370]



⚠ 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, quels que soit l'avancement 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 conjonction avec un centre de télésurveillance (CTS)

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

Reportez-vous aux sections suivantes de ce manuel :

Temporisations [→ 122]

3.1.5.4 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 econdes. Le délai du minuteur est lui aussi réglé sur 30 secondes.

Reportez-vous aux sections suivantes de ce manuel :

SECTEURS [→ 125]

Ajouter / Éditer un secteur [→ 253]

Temporisations [→ 122]

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 ».
Reportez-vous à la section suivante de ce manuel :
Ajout / Édition d'un CTS [→ 309]

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 ».
Reportez-vous aux sections suivantes de ce manuel :
SORTIES [→ 147] (Clavier)
Configurer les entrées et sorties de la centrale [→ 211] (Navigateur)
Ajout / Édition d'un CTS [→ 309]

Tentatives de retransmission

Les tentatives de retransmission (tentatives de numérotation) sont configurés dans ce manuel :
Ajout / Édition d'un CTS [→ 309]
Éditer les paramètres EDP [→ 318]
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 service

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.
Reportez-vous aux sections suivantes de ce manuel :
Temporisations [→ 122]
Attributs zone [→ 370]
SORTIES [→ 147] (Clavier)
Éditer une sortie [→ 212] (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,
- soit une zone d'agression et une activation 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.

Sécurité des communications pour le support à distance et les contrôles de système distant (DD 263:2010)

Veuillez vous assurer que SPC Pro est utilisé suivant les lignes directives spécifiées dans DD 263:2010.

3.1.5.5 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 à ceci doit être soulignée 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 être clairement notifiée à l'utilisateur final.
- Les méthodes de mise en œuvre de l'activation et de la désactivation devraient être clairement 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.

3.1.5.6 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 max.	M0 - M4
Temps de reporting	T3 comme max.
Disponibilité	Reportez-vous à la section suivante de ce manuel : Niveaux ATS et spécifications d'atténuation [→ 375]
Niveau de sécurité de l'émission de signal	Testé selon EN50136-1-1 et classé « S0 ».

3.1.6 Conformité avec les agréments VDS

Ce document d'installation comprend les informations d'installation du produit requis pour les certifications VdS.

Vanderbilt

N° de certification VdS. G 112104, G112124, et G112128.

Certificats VdS EN. EN-ST000142, EN-ST000143, EN-ST000055, EN-ST000056, EN-ST000057, EN-ST000058, EN-ST000061, EN-ST000062.

Siemens

N° de certification VdS. G116035.

Certificats VdS EN. 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.

Logiciels

Pour définir le système pour la conformité VDS, suivez la procédure ci-dessous :

1. connectez-vous à la centrale avec le navigateur.
2. Cliquez sur Mode paramétrage.
3. Cliquez sur Par.Centrale dans le menu.
4. Cliquez sur Normes & Standards.
5. Sélectionnez la France dans la liste de pays.
6. Sélectionnez le grade VDS requis par votre type d'installation.
 - Isolations distantes — il n'est pas possible d'ôter l'isolation de fautes isolées à l'aide du navigateur ou de SPCPro. Ceci ne peut se faire que sur les claviers.
 - Connexions distantes — il n'est pas possible d'utiliser le navigateur ou SPCPro pour se connecter à un système armé.
 - Alarmes confirmées — un système activé de manière interne ne peut pas créer une alarme confirmée.
 - Reporting erreur matérielle — dans les **Options**, vous devez sélectionner l'option du reporting **Validé + (10s)** de la liste déroulante du **Mode sortie Watchdog**.

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

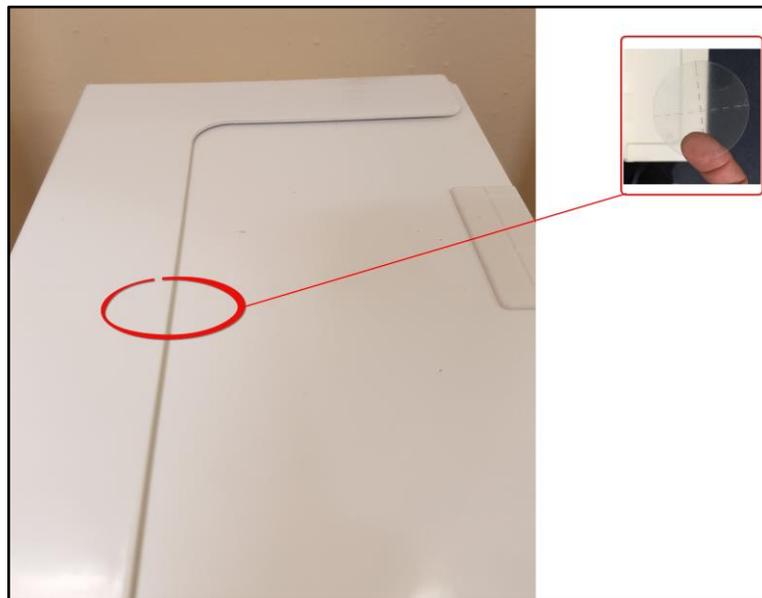
Matériel

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 pour X-Bus en configuration multipoints (en boucle)
- Les combinaisons suivantes de résistance de fin de ligne ne sont pas conformes aux normes VdS :
 - 1k, 470 ohm
 - 1k, 1k, 6k6 ohm

3.1.7 Conformité avec les agréments NF et A2P

Adresse de l'organisme certificateur	
CNPP Cert Pôle Européen de Sécurité - Vernon Route de la Chapelle Réanville CD 64 - 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





Pour être conforme au référentiel NF & A2P, le boîtier doit être plombé après fermeture au moyen de l'étiquette spéciale fournie.

Les produits SPC listés ont été testés conformément à la norme NF324 - H58, avec référence aux certifications EN, voir Conformité aux agréments EN50131 [→ 21] et aux spécifications RTC50131-6 et RTC50131-3.

Type de produit	Configuration	Standard	Logo
SPC6350.320 + SPCP355.300 (Cert. XXXXXXXXXXXX)	60h, non monitorisé	NF Grade 3, Class 1	
SPC5350.320 + SPCP355.300 (Cert. XXXXXXXXXXXX)	60h, non monitorisé		
SPC6350.320 (Cert. XXXXXXXXXXXX)	60h, non monitorisé		
SPC5350.320 (Cert. XXXXXXXXXXXX)	60h, 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		
SPCN110.000 SPCN310.000 SPCK420.100 SPCK620.100 SPCK623.100 SPCE652.100 SPCE452.100 SPCE110.100 SPCE120.100		NF Grade 2 et 3, Classe 1	

4 Caractéristiques techniques

4.1 SPC4000

Zones programmables	4
Nombre max. de codes utilisateur	100
Télécommandes	Jusqu'à 32
Alarme de panique radio	Jusqu'à 128
Mémoire d'événement	1 000 événements d'intrusion, 1 000 événements d'accès
Nombre de zones intégrées	8
Nombre max. de zones câblées	32
Nombre max. de zones radio	32 (retrancher les zones câblées)
Nombre max. 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 (30 V CC / courant d'interruption résistif de 1 A)
Nombre de collecteurs ouverts intégrés	2 sirènes internes / externes, 3 librement programmables (courant d'interruption résistif de 400 mA maxi, alimenté par la sortie auxiliaire)
Version	V3.x
Portes prises en charge	Max. 4 portes d'entrée ou 2 portes d'entrée/sortie
Nombre de lecteurs de badge	4 max.
Module radio	<ul style="list-style-type: none"> ● SPC4221 : récepteur SiWay RF intégré (868 MHz) ● SPC4320.220 : en option (SPCW111), ● SPC4320.320 : en option (SPCW110)
Vérification	4 zones de vérification avec 4 caméras IP et 4 périphériques audio max.
Vidéo	Jusqu'à 16 images pré-événement / 16 post-événement (avec une résolution JPEG 320 x 240, 1 image / seconde max.)
Audio	Jusqu'à 60 secondes d'enregistrement audio pré- / post-événement
Bus de terrain 1)	X-BUS sur RS-485 (307 ko/s)
Nombre de périphériques de terrain 2)	11 max. (4 claviers, 2 transpondeurs de porte, 5 transpondeurs d'entrée/sortie)
Périphériques de terrain connectables	<ul style="list-style-type: none"> ● Claviers : SPCK42x, SPCK62x ● Transpondeurs de porte : SPCA210, SPCP43x ● Transpondeurs avec E/S : SPCE65x, SPCE45x, SPCP33x, SPCE110, SPCE120, SPCV32x
Interfaces	<ul style="list-style-type: none"> ● X-BUS (1 branche) ● 1 RS232 ● USB (connexion PC) ● 1 clé de programmation rapide pour SPC ● SPC43xx : 1 Ethernet (RJ45) supplémentaire
Contact anti-effraction	Autosurveillance frontale intégrée à ressort, 2 entrées de contact d'autosurveillance auxiliaires
Alimentation	Type A (selon EN50131-1)
Tension secteur	230 V CA, + 10% / -15%, 50 Hz
Fusible d'alimentation secteur	250 mA T (pièce remplaçable sur le bornier)

	d'alimentation)
Consommation électrique	SPC42xx : 160 mA max. à 230 V CC SPC43xx : 200 mA max. à 230 V CC
Courant de service	Centrale SPC42xx : 160 mA max. à 12 V CA Centrale SPC43xx : 200 mA max. à 12 V CA
Courant de repos	Centrale SPC42xx : 140 mA max. à 12 V CC (165 mA avec RTC, 270 mA avec GSM, 295 mA avec RTC et GSM) Centrale SPC43xx : 170 mA max. à 12 V CC (195 mA avec RTC, 300 mA avec GSM, 325 mA avec RTC et GSM)
Tension en sortie	De 13 à 14 V CC en conditions normales (alimentation sur secteur et batterie entièrement chargée), 10,5 V CC min. en cas d'alimentation par un dispositif secondaire (avant désactivation du système pour la protection de la batterie contre la décharge profonde)
Déclencheur basse tension	7,5 VCC
Protection contre les surtensions	15,7 VCC
Ondulation crête à crête	5 % max. de la tension de sortie
Alimentation auxiliaire (nominale)	750 mA max. à 12 V CC
Type de batterie	SPC422x/4320 : YUASA de type NP7-12FR (7 Ah), batterie non fournie
Chargement de la batterie	SPC422x/4320 : 72 h max. 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 V CC +/- 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 réparables par l'utilisateur	Aucune pièce remplaçable par l'utilisateur
Température de fonctionnement	-10 ~ +50 °C
Humidité relative	90 % max. (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 en 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 recevoir jusqu'à	SPC422x/4320 : 1 transpondeur supplémentaire (taille 150 x 82 mm)
Indice IP	30

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

2) Davantage de transpondeurs E/S peuvent être adressés à la place d'un clavier ou d'un transpondeur de porte, mais le nombre d'entrées / sorties programmables ne doit pas dépasser le maximum défini pour le système.

4.2 SPC5000

Zones programmables	16
Nombre max. de codes utilisateur	500
Télécommandes	100 max.
Alarme de panique radio	Jusqu'à 128
Mémoire d'événement	10 000 événements d'intrusion, 10 000 événements d'accès
Nombre de zones intégrées	<ul style="list-style-type: none"> ● SPC5320\5330 — 8 ● SPC5350 — 16
Nombre max. de zones câblées	128
Nombre max. de zones radio	120 (retrancher les zones câblées)
Nombre max. 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	<ul style="list-style-type: none"> ● SPC5320\5330 — 1 flash (courant de commutation résistif 30 VCC /1A) ● SPC5350 — 4 (relais de commutation unipolaire, 30 VCC / courant de commutation résistif max. 1A)
Sorties électroniques	<ul style="list-style-type: none"> ● SPC5320\5330 — 5 sorties : <ul style="list-style-type: none"> – 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 <ul style="list-style-type: none"> – 5 sorties d'alimentation standards – 3 sorties surveillées
Version du Firmware	V3.x
Portes prises en charge	16 portes d'entrée ou 8 porte d'entrée/sortie max.
Nombre de lecteurs de badge	16 max.
Module radio	en option (SPCW110)
Vérification	16 zones de vérification avec 4 caméras IP et 16 périphériques audio max.
Vidéo	Jusqu'à 16 images pré-événement / 16 post-événement (avec une résolution JPEG 320 x 240, 1 image / seconde max.)
Audio	Jusqu'à 60 secondes d'enregistrement audio pré- / post-événement
Bus de terrain 1)	X-BUS sur RS-485 (307 ko/s)
Nombre de périphériques de terrain 2)	48 max. (16 claviers, 8 transpondeurs de porte, 16 transpondeurs d'entrée / sortie)
Périphériques de terrain pouvant être connectés	<ul style="list-style-type: none"> ● Claviers : SPCK42x, SPCK62x ● Transpondeurs de porte : SPCA210, SPCP43x ● Transpondeurs avec E/S : SPCE65x, SPCE45x, SPCP33x, SPCP35x, SPCE110, SPCE120, SPCV32x

Interfaces	<ul style="list-style-type: none"> ● 2 X-BUS (2 branches ou 1 boucle) ● 2 RS232 ● 1 USB (connexion PC), ● 1 clé de programmation rapide pour SPC, ● SPC53xx : 1 Ethernet (RJ45) supplémentaire
Contact anti-effraction	<ul style="list-style-type: none"> ● SPC5320/5330 : Autosurveillance frontale intégrée à ressort, 2 entrées de contact anti-effraction auxiliaires ● SPC5350 : Interrupteur d'autosurveillance avant / arrière
Alimentation	Type A (selon EN50131-1)
Tension secteur	230 V CA, + 10% / -15%, 50 Hz
Fusible d'alimentation secteur	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● SPC5320/5330 : 200 mA max. à 230 V CC ● SPC5350 : 500 mA max. à 230 V CA
Courant de service	<ul style="list-style-type: none"> ● SPC5320/5330 : Contrôleur : 200 mA max. à 12 V CA ● SPC5350 : 210 mA max. à 12 V CC
Courant de repos	Centrale SPC53xx : 170 mA max. à 12 V CC (195 mA avec RTC, 300 mA avec GSM, 325 mA avec RTC et GSM)
Tension en sortie	De 13 à 14 V CC en conditions normales (alimentation sur secteur et batterie entièrement chargée), 10,5 V CC min. en cas d'alimentation par un dispositif secondaire (avant désactivation du système pour la protection de la batterie contre la décharge profonde)
Déclencheur basse tension	11 VCC
Protection contre les surtensions	<ul style="list-style-type: none"> ● SPC5320/5330 : 15,7 VCC ● SPC5350 : 15 VCC nominal
Ondulation crête à crête	5 % max. de la tension de sortie
Alimentation auxiliaire (nominale)	<ul style="list-style-type: none"> ● SPC5320/5330 : 750 mA max. à 12 V CC ● SPC5350 : 2 200 mA max. à 12 V CC (8 sorties à fusibles séparés, 300 mA par sortie)
Type de batterie	<ul style="list-style-type: none"> ● SPC5320 : YUASA de type NP7-12FR (7 Ah), ● SPC5330 : YUASA de type NP17-12FR (17 Ah) ● SPC5350 : YUASA NP24-12 (12 V 24 Ah), Alarmcom AB1227-O (12 V 27 Ah) ● SPC5350: FIAMM FGV22703 (12V 27Ah) Batterie non fournie
Chargement de la batterie	<ul style="list-style-type: none"> ● SPC5320 : 72 h max., ● SPC5330/5350 : 24 h max. pour 80% de la capacité de la batterie
Protection de la batterie	<ul style="list-style-type: none"> ● SPC5320/5330 : Courant limité à 1 A (protection par fusible), protection contre la décharge profonde à 10,5 V CC +/- 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 réparables par l'utilisateur	<ul style="list-style-type: none"> ● SPC5320/5330 : Aucune pièce remplaçable par l'utilisateur ● SPC5350 : 8 fusibles à verre (400 mA AT) pour sorties 12 VCC
Température de fonctionnement	-10 ~ +50 °C
Humidité relative	90 % max. (sans condensation)
Couleur	RAL 9003 (blanc signal)
Poids	<ul style="list-style-type: none"> ● SPC5320 : 4 500 kg ● SPC5330 : 6 400 kg ● SPC5350 : 18 600 kg
Dimensions (l x h x p)	<ul style="list-style-type: none"> ● SPC5320 : 264 x 357 x 81 mm ● SPC5330 : 326 x 415 x 114 mm ● SPC5350 : 498 x 664 x 157 mm
Boîtier	<ul style="list-style-type: none"> ● SPC5320 : petit boîtier en métal (acier doux 1,2 mm) ● SPC5330 : boîtier métal articulé (acier doux 1,2 mm) ● SPC5350 : boîtier en métal (acier doux 1,5 mm)
Le boîtier peut recevoir jusqu'à	<ul style="list-style-type: none"> ● SPC5320 : 1 transpondeur supplémentaire, ● SPC5330 : 4 transpondeurs supplémentaires (taille 150 x 82 mm) ● SPC5350 : 4 transpondeurs supplémentaires (150 x 82 mm)
Indice IP / IK	30 / 06

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

2) Davantage de transpondeurs E/S peuvent être adressés à la place d'un clavier ou d'un transpondeur de porte, mais le nombre d'entrées / sorties programmables ne doit pas dépasser le maximum défini pour le système.

4.3 SPC6000

Zones programmables	60
Nombre max. de codes utilisateur	2 500
Télécommandes	100 max.
Alarme de panique radio	Jusqu'à 128
Mémoire d'événement	10 000 événements d'intrusion, 10 000 événements d'accès
Nombre de zones intégrées	<ul style="list-style-type: none"> ● SPC6320\6330 — 8 ● SPC6350 — 16
Nombre max. de zones câblées	512
Nombre max. de zones radio	120 (retrancher les zones câblées)
Nombre max. 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	<ul style="list-style-type: none"> ● SPC6320\6330 — 1 flash (courant de commutation résistif 30 VCC /1A) ● SPC5350 — 4 (relais de commutation unipolaire, 30 VCC / courant de commutation résistif max. 1A)
Sorties électroniques	<ul style="list-style-type: none"> ● SP6320\6330 — 5 sorties : <ul style="list-style-type: none"> – 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 <ul style="list-style-type: none"> – 5 sorties d'alimentation standards – 3 sorties surveillées
Version du Firmware	V3.x
Portes prises en charge	64 portes d'entrée ou 32 portes d'entrée/sortie max.
Nombre de lecteurs de badge	64 max.
Module radio	en option (SPCW110)
Vérification	32 zones de vérification avec au maximum 4 caméras IP et 32 périphériques audio.
Vidéo	Jusqu'à 16 images pré-événement / 16 post-événement (avec une résolution JPEG 320 x 240, 1 image / seconde max.)
Audio	Jusqu'à 60 secondes d'enregistrement audio pré- / post-événement
Bus de terrain 1)	X-BUS sur RS-485 (307 ko/s)
Nombre de périphériques de terrain 2)	128 max. (soit 32 claviers, 32 transpondeurs de porte, 64 transpondeurs d'entrée / sortie)
Périphériques de terrain pouvant être connectés	<ul style="list-style-type: none"> ● Claviers : SPCK42x, SPCK62x ● Transpondeurs de porte : SPCA210, SPCP43x ● Transpondeurs avec E/S : SPCE65x, SPCE45x, SPCP33x, SPCP35x, SPCE110, SPCE120, SPCV32x
Interfaces	<ul style="list-style-type: none"> ● 2 X-BUS (2 branches ou 1 boucle) ● 2 RS232 ● 1 USB (connexion PC), ● 1 clé de programmation rapide pour SPC, ● SPC63xx : 1 Ethernet (RJ45) supplémentaire
Contact anti-effraction	<ul style="list-style-type: none"> ● SPC6330 : Autosurveillance frontale intégrée à ressort, 2 entrées de contact anti-effraction 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	<ul style="list-style-type: none"> ● SPC6330 : 250 mA T (pièce remplaçable sur le bornier d'alimentation) ● SPC6350 : 800 mA T (pièce remplaçable sur le bornier d'alimentation)
Consommation électrique	<ul style="list-style-type: none"> ● SPC6330 : 200 mA max. à 230 V CA ● SPC6350 : 500 mA max. à 230 V CA
Courant de service	<ul style="list-style-type: none"> ● SPC6330 : 200 mA max. à 12 V CC ● SPC6350 : 210 mA max. à 12 V CC

Courant de repos	Centrale SPC63xx : 170 mA max. à 12 V CC (195 mA avec le RTC, 300 mA avec GSM, 325 mA avec le RTC et GSM)
Tension en sortie	<ul style="list-style-type: none"> ● SPC6330 : De 13 à 14 V CC en conditions normales (alimentation sur secteur et batterie entièrement chargée), min. 10,5 V CC en cas d'alimentation par un dispositif secondaire (avant désactivation du système pour la protection de la batterie contre la décharge profonde) ● SPC6350 : De 13 à 14 V CC en conditions normales (alimentation sur secteur et batterie entièrement chargée), min. 10,5 V CC en cas d'alimentation par un dispositif secondaire (avant désactivation du système pour la protection de la batterie contre la décharge profonde)
Déclencheur basse tension	11 V DC :
Protection contre les surtensions	<ul style="list-style-type: none"> ● SPC6330 : 15,7 V DC ● SPC6350 : 15 V CC nominal
Ondulation crête à crête	5 % max. de la tension de sortie
Alimentation auxiliaire (nominale)	<ul style="list-style-type: none"> ● SPC6330 : 750 mA max. à 12 V CC ● SPC6350 : 2 200 mA max. à 12 V CC (8 sorties à fusibles séparés, 300 mA par sortie)
Type de batterie	<ul style="list-style-type: none"> ● SPC6330 : YUASA de type NP17-12FR (17 Ah) ● SPC6350 : YUASA NP24-12 (12 V 24 Ah), Alarmcom AB1227-O (12 V 27 Ah) ● SPC6350: FIAMM FGV22703 (12V 27Ah) Batterie non fournie
Chargement de la batterie	SPC63xx : 24 h max. pour 80% de la capacité de la batterie
Protection de la batterie	<ul style="list-style-type: none"> ● SPC6330 : Courant limité à 1 A (protection par fusible), protection contre la décharge profonde à 10,5 V CC +/- 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 V CC
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 réparables par l'utilisateur	<ul style="list-style-type: none"> ● SPC6330 : Aucune pièce remplaçable par l'utilisateur ● SPC6350 : 8 fusibles en verre (400 mA AT) pour les sorties 12 V CC
Température de fonctionnement	-10 ~ +50 °C
Humidité relative	90 % max. (sans condensation)
Couleur	RAL 9003 (blanc signal)
Poids	<ul style="list-style-type: none"> ● SPC6330 : 6 400 kg ● SPC6350 : 18 600 kg
Dimensions (l x h x p)	<ul style="list-style-type: none"> ● SPC6330 : 326 x 415 x 114 mm ● SPC6350 : 498 x 664 x 157 mm
Boîtier	<ul style="list-style-type: none"> ● SPC6330 : boîtier métal articulé (acier doux 1,2 mm) ● SPC6350 : boîtier en métal (acier doux 1,5 mm)
Le boîtier peut recevoir jusqu'à	<ul style="list-style-type: none"> ● SPC6330 : 4 transpondeurs supplémentaires (taille 150 x 82 mm)

	<ul style="list-style-type: none"> ● SPC6350 : 6 transpondeurs supplémentaires (150 x 82 mm) ou 1 centrale supplémentaire + 4 transpondeurs
Indice IP / IK	30 / 06

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

2) Davantage de transpondeurs E/S peuvent être adressés à la place d'un clavier ou d'un transpondeur de porte, mais le nombre d'entrées / sorties programmables ne doit pas dépasser le maximum défini pour le système.

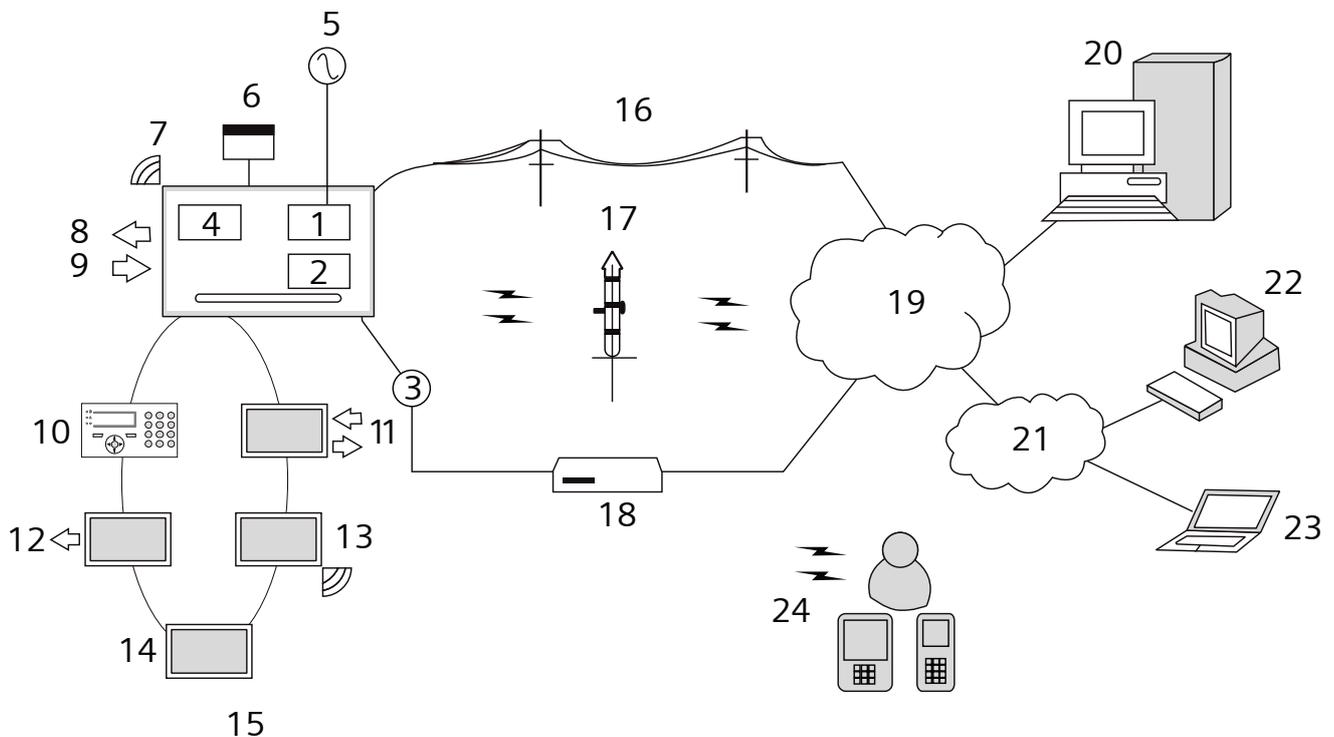
4.4 SPCP355.300

Nombre d'entrées intégrées	8
Résistance EOL	Double résistance 4K7 (par défaut), autres combinaisons de résistances sélectionnables
Sorties relais	3 (inverseur unipolaire, courant d'interruption résistif de 30 Vcc/1 A max.)
Sorties électroniques	3 supervisées (courant d'interruption résistif de 400 mA max. pour chaque sortie)
Interfaces	X-BUS (entrée, sortie, branche)
Informations délivrées à la centrale	Défaut secteur, défaut batterie, défaut fusible, défaut de charge batterie, tension et courant de charge batterie, tension et courant d'utilisation
Tension secteur	230 Vca, +10 à -15 %, 50 Hz
Courant de fonctionnement	245 mA max. à 12 Vcc (tous les relais activés)
Courant de repos	195 mA max. à 12 Vcc
Tension de sortie	13-14 Vcc dans des conditions normales (alimentation secteur et batterie entièrement chargée)
Alimentation auxiliaire (caractéristiques nominales)	2 360 mA max. à 12 Vcc (8 sorties avec fusibles indépendants, 300 mA max. par sortie)
Type de batterie	<ul style="list-style-type: none"> ● YUASA NP24-12 (12 V, 24 Ah) ● Alarmcom AB1227-0 (12 V, 27 Ah) ● FIAMM FGV22703 (12V 27Ah) Batterie non fournie
Contact autosurveillance	Contact d'autosurveillance à l'ouverture et à l'arrachement
Températures de fonctionnement	Entre 0° et +40 °C
Boîtier	Boîtier métallique (1,5 mm en acier doux)
Couleur	RAL 9003 (blanc)
Dimensions	498 x 664 x 157 mm
Poids (sans les batteries)	18,4 kg (boîtier avec couvercle) 11,3 kg (boîtier sans couvercle)
Indice IP / IK	30 / 06

5 Introduction

La centrale de la série SPC est une centrale 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 applications de communication (RTC/GSM/RF) pour en faire un système très polyvalent. Cette approche assure que les installateurs réalisent le montage rapidement avec un câblage réduit au minimum.



Synthèse

1	RTC	13	Transpondeur radio
2	GSM	14	Module d'alimentation
3	Ethernet	15	Configuration en boucle
4	Récepteur radio	16	Réseau RTC
5	Alimentation secteur	17	Réseau GSM
6	Batterie 12 V	18	Routeur à large bande
7	RF	19	Réseau
8	Sorties câblées (6)	20	Serveur
9	Entrées câblées (8)	21	LAN/WLAN
10	Claviers	22	Centre de services
11	Transpondeur E/S	23	Utilisateur distant
12	Sortie transpondeur	24	Interfaces mobiles

6 Installation du matériel

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.

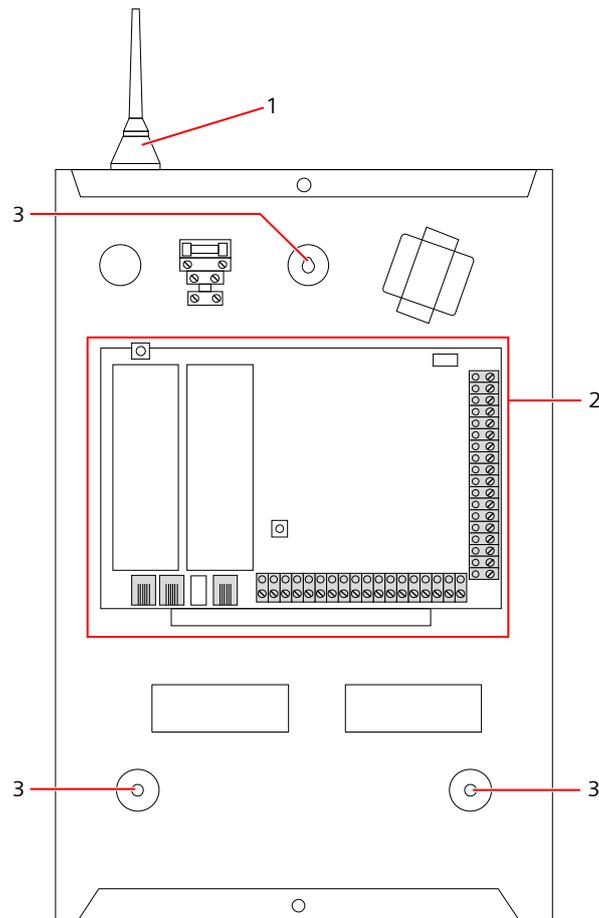
Pour ouvrir le boîtier, enlevez les deux vis en vous servant d'un tournevis adéquat et enlevez le couvercle directement de l'embase.

Le boîtier G2 contient la carte de circuit imprimé de la centrale montée sur 4 picots. Un module d'entrée / sortie en option peut être installé directement sous la carte de la centrale. Une batterie d'une capacité de 7 Ah max. peut être installée sous la centrale.

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 firmware.

Le boîtier G2 SPC dispose de trois trous de vis pour la fixation murale.

Pour fixer le boîtier au 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 du 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 deux trous de vis inférieurs à l'aide d'un crayon après avoir pris soin d'aligner le boîtier à la verticale.



Boîtier standard

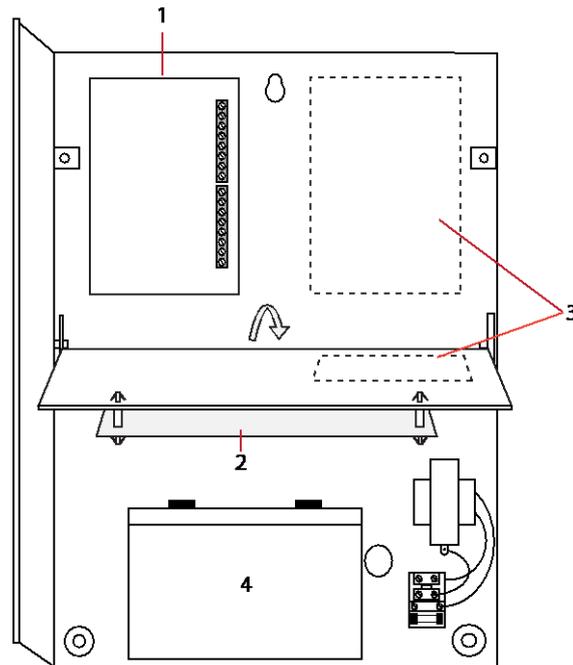
1	Antenne radio
2	SPC E/S Centrale
3	Trous de vis pour la fixation murale

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.

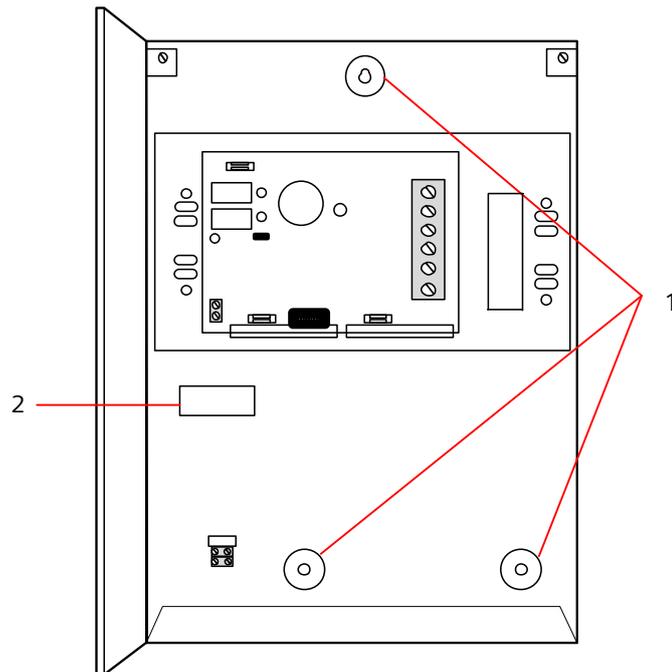
Le boîtier G3 contient la carte-mère de la centrale montée sur un support de fixation articulé. Les transpondeurs et les modules d'alimentation peuvent être montés sur la face inférieure du support de fixation articulé et également sur la paroi arrière du boîtier sous le support de fixation.



- 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 firmware.

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



Pour fixer le boîtier au mur :

1. Enlevez le couvercle et localisez le premier trou de la vis de fixation 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'autosurveillance arrière

Un interrupteur d'autosurveillance arrière peut être requis pour obtenir l'agrément local.

L'interrupteur d'autosurveillance 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 du kit d'autosurveillance arrière

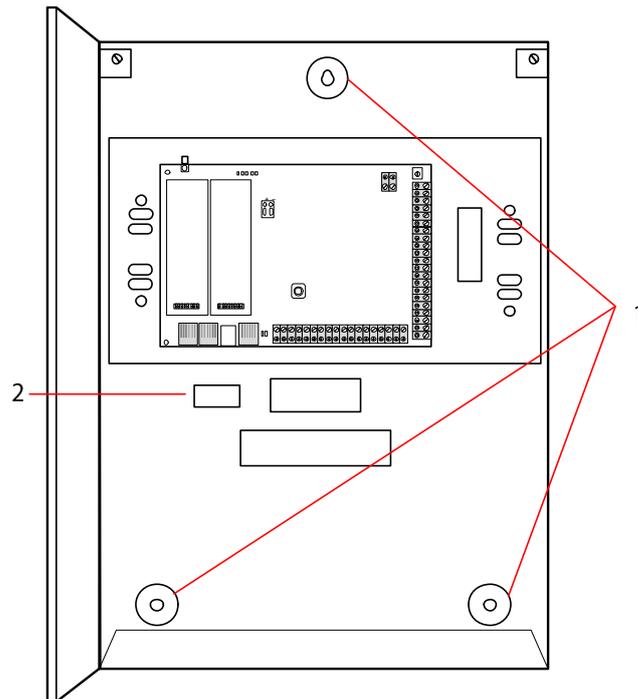
Le kit d'autosurveillance arrière dote les centrales SPC d'un dispositif d'autosurveillance à l'avant et à l'arrière.

Le kit d'autosurveillance arrière inclut les éléments suivants :

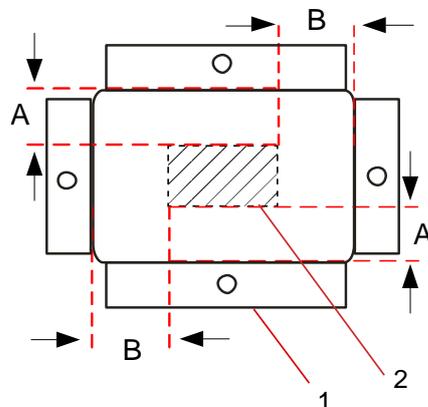
- Interrupteur d'autosurveillance
- câbles de connexion de l'interrupteur d'autosurveillance à la centrale
- plaque de fixation murale

Montage du support mural

1. Montez le boîtier du SPC en position adéquate sur le mur à l'aide des trois éléments de fixation (voir la réf. 1 ci-dessous).



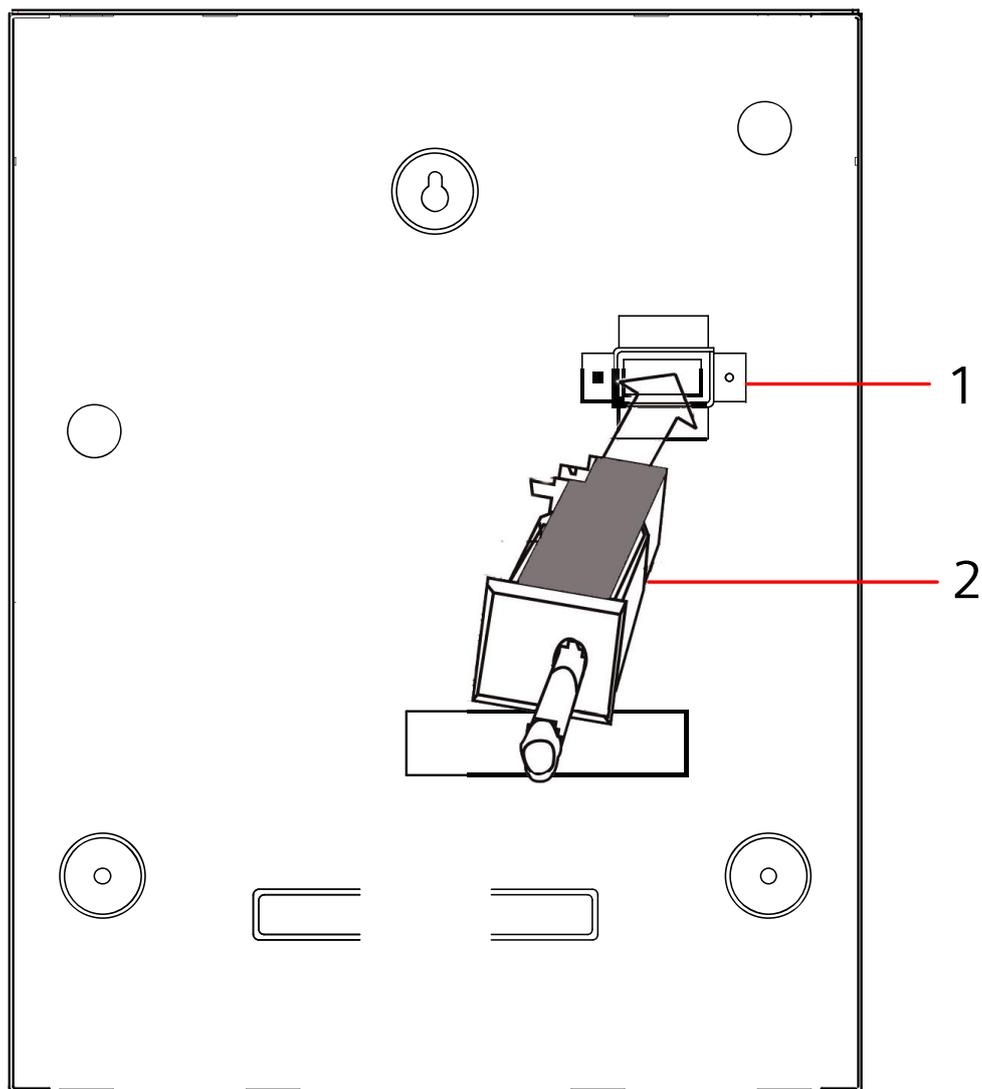
2. Tracez une ligne autour de l'intérieur de la découpe du dispositif d'autosurveillance (voir la réf. 2 ci-dessus). Ces lignes serviront de repère pour la plaque murale. Retirez le boîtier du mur.
3. Placez la plaque murale (voir la réf. 1 ci-dessous) sur le mur en la centrant précisément autour du rectangle que vous avez préalablement tracé (voir la réf. 2 ci-dessus).



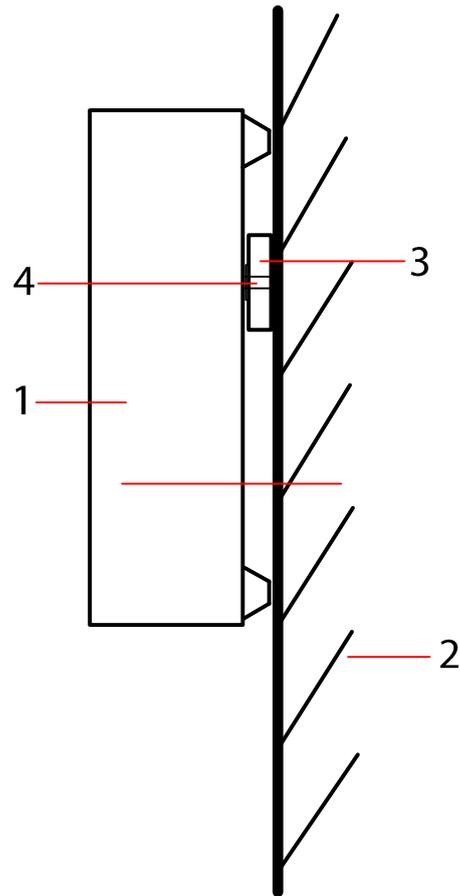
4. Vérifiez que les quatre brides de la plaque murale affleurent avec le mur.
5. Marquez les quatre fixations sur la plaque murale.
6. Percez les trous et utilisez des vis (4 mm maxi) adaptées au matériau du mur.
7. Montez la plaque murale sur le mur.

Mise en place de l'interrupteur d'autosurveillance arrière

1. Insérez l'interrupteur d'autosurveillance (voir la réf. 2 ci-dessous) à l'arrière du boîtier de façon que le bouton-poussoir soit tourné vers l'extérieur (voir la réf. 1 ci-dessous).



2. Remplacez le boîtier sur le mur à l'aide des trois fixations que vous avez précédemment retirées (voir la réf. 2 ci-dessous). Vérifiez visuellement que la plaque murale et la partie métallique du boîtier affleurent.



1 Boîtier

2 Mur

3 Plaque de fixation murale

4 Interrupteur d'autosurveillance



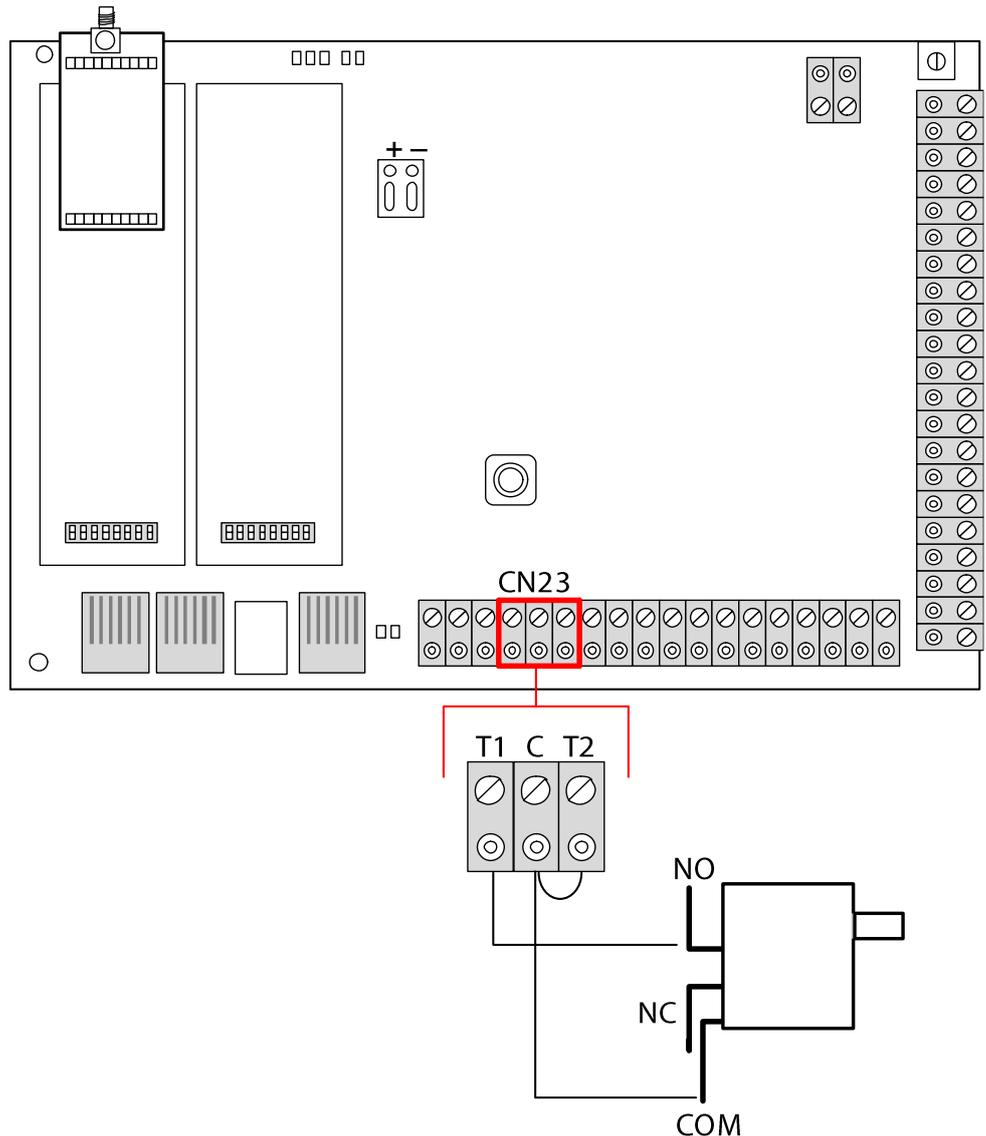
⚠ AVERTISSEMENT

Si cet alignement est incorrect, le boîtier ne s'enclenchera pas sur ses fixations.

Câblage de l'interrupteur d'autosurveillance à la centrale

Toutes les centrales installées disposent d'entrées supplémentaires configurées comme entrées d'autosurveillance. Elles sont destinées à recevoir le câblage du dispositif d'autosurveillance et n'ont pas besoin d'être programmées.

Le système fait référence à cet interrupteur d'autosurveillance comme « Autosurveillance Aux. 1 ».



1. Connectez les contacts NO sur l'interrupteur d'autosurveillance T1 de la centrale.
2. Connectez les contacts COM sur le commutateur d'autosurveillance C du contrôleur. Assurez-vous que le cavalier T2 n'est pas retiré.
3. Après avoir câblé l'interrupteur d'autosurveillance, vous pouvez mettre la centrale en service normalement.

6.2.2 Installation de la batterie pour conformité EN50131

Pour assurer la conformité aux normes EN50131, la batterie doit être immobilisée dans le boîtier. À cet effet, repliez les pattes à l'arrière du boîtier articulé de manière que la batterie soit bien fixée.

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

Si vous utilisez une batterie de 17 Ah, la batterie est tournée vers la droite et la patte du milieu la retient.



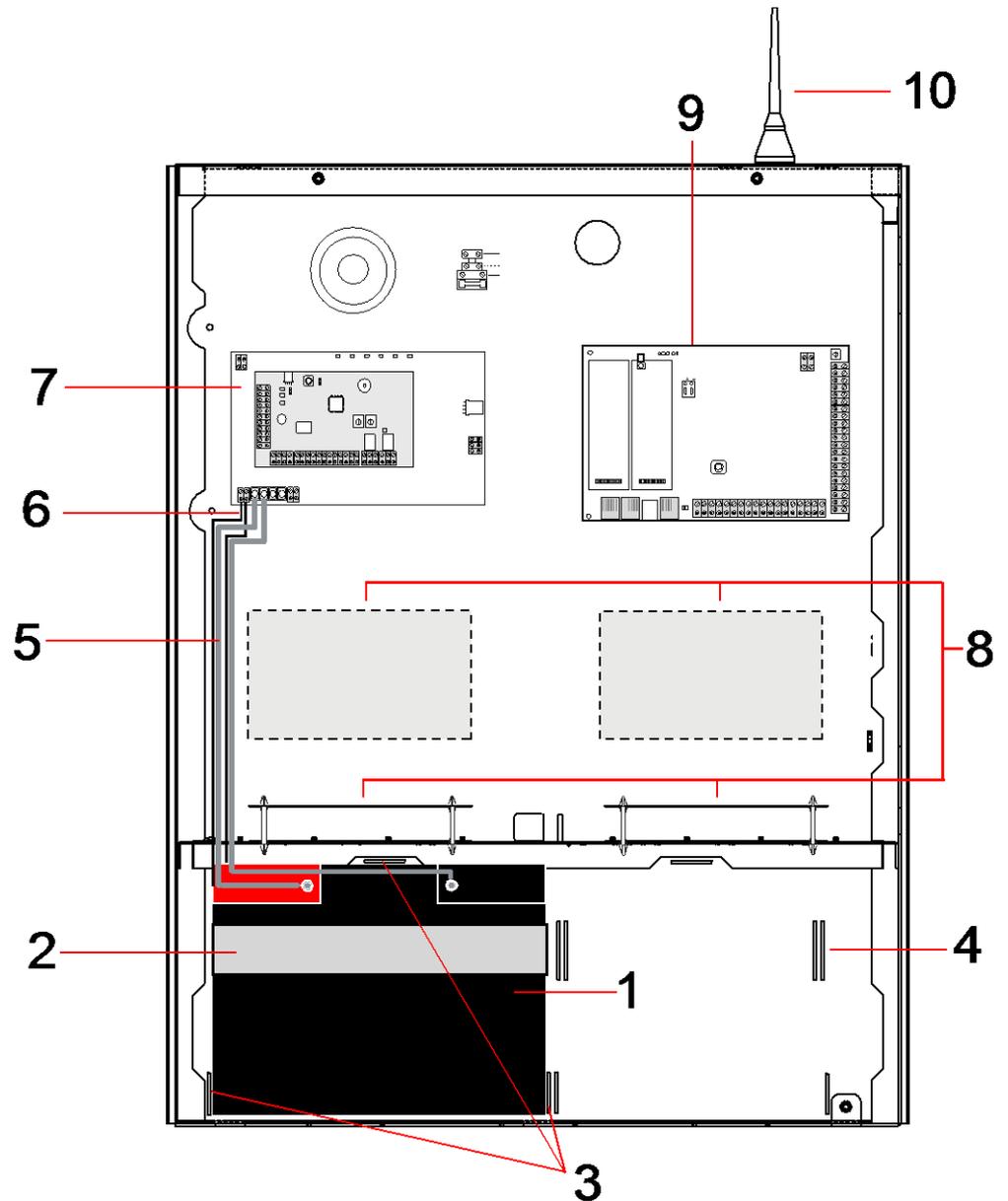
Prenez soin de replier les pattes avec précaution pour ne pas endommager la batterie. Si la batterie est endommagée ou en cas de fuite de l'électrolyte, remplacez la batterie par une batterie neuve. Éliminez l'ancienne en suivant les dispositions applicables.

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 de la centrale et le module d'alimentation SPCP355, tous deux montés sur 4 piliers de soutien. Un transpondeur à 8 entrées /2 sorties est monté sur le module d'alimentation. Quatre piliers supplémentaires sont inclus pour vous fournir l'option de monter le transpondeur à 8 entrées /2 sorties sous le panneau du module, dans le cabinet G5. Vous pouvez installer des transpondeurs supplémentaires dans le boîtier, comme illustré.

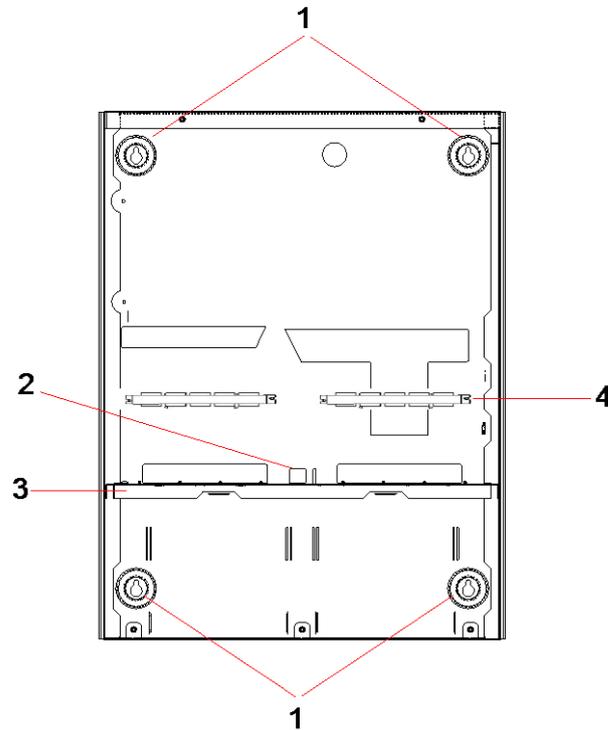


Numéro	Description	Numéro	Description
1	Batterie	6	Câbles de la température de la batterie
2	Bande d'attache de batterie	7	Module d'alimentation
3	Languettes de fixation	8	Positions en option du transpondeur
4	Trous de la bande d'attache	9	E/S Centrale
5	Câbles de la batterie	10	Antenne

Deux batteries d'une capacité maximale de 27 Ah peuvent être placées dans le compartiment prévu à cet effet situé sur 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 pré-perçés 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 firmware. 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.

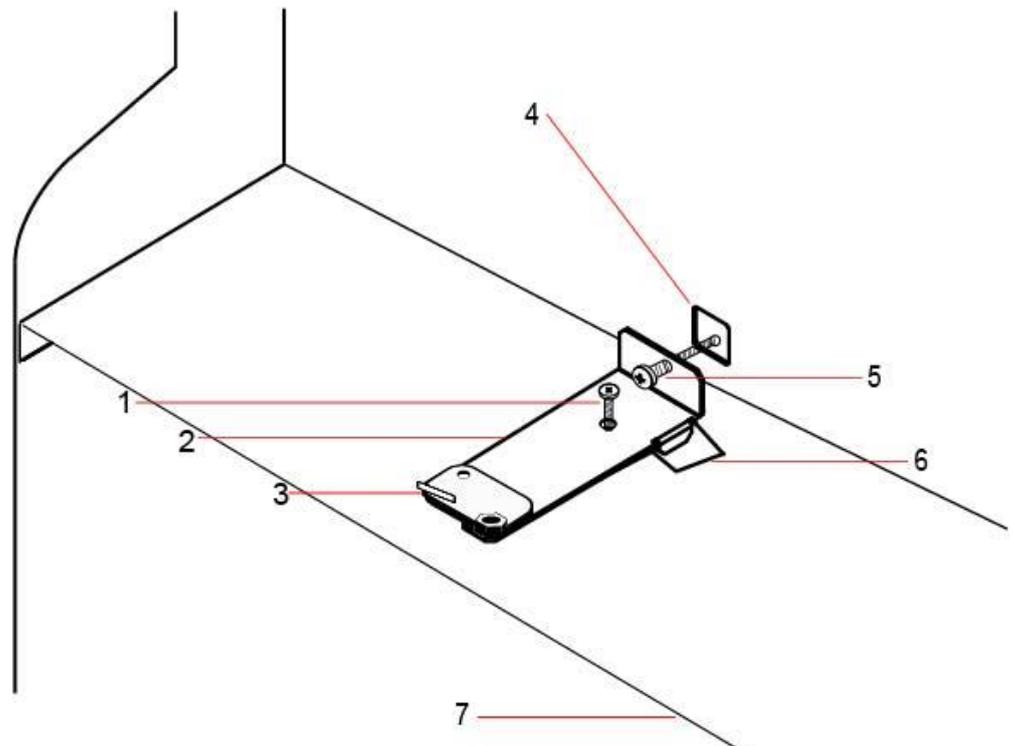
L'équerre d'autosurveillance est fermement maintenue en place à l'aide d'une vis de calage. Souvenez-vous d'enlever cette vis si vous mettez le système en service pour la protection antisabotage arrière. Ne le supprimez pas si vous n'utilisez que la protection avant.

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 pré-configuré pour l'autosurveillance avant uniquement. Pour configurer le boîtier pour les deux types de dispositifs antisabotage, enlevez le 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 aligné avec la surface du mur.
5. Déplacez l'équerre antisabotage à l'extrême gauche de la fente d'orientation et serrez le vis d'antisabotage arrière (rep. 5). L'équerre devrait être perpendiculaire au mur situé à l'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	Interrupteur d'autosurveillance	7	Étagère séparant le compartiment de la batterie
4	Découpe de l'autosurveillance arrière		

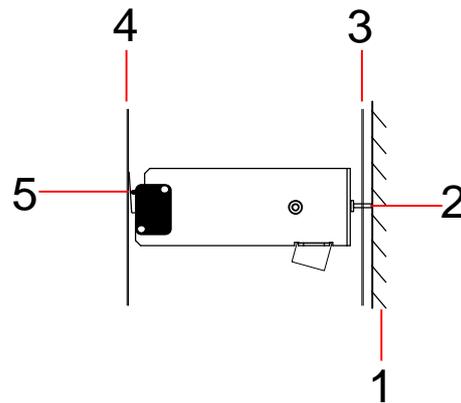


⚠ AVERTISSEMENT

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 contact d'autosurveillance arrière, sa fonctionnalité correcte doit être à nouveau testée et réajustée si nécessaire.

6.3.2.1 Fonctionnement de l'antisabotage (autosurveillance)

Interrupteur d'autosurveillance - normal



1 Mur

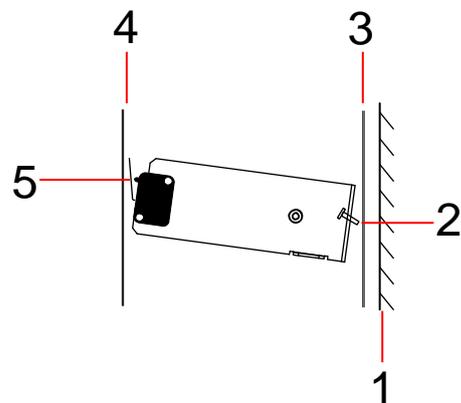
2 Vis d'autosurveillance arrière

3 Paroi arrière du boîtier

4 Couvercle du boîtier

5 Contact de l'interrupteur
d'autosurveillance fermé

Interrupteur d'autosurveillance – déplacé



- | | |
|----------------------------------|---|
| 1 Mur | 4 Couvercle du boîtier |
| 2 Vis d'autosurveillance arrière | 5 Contact de l'interrupteur d'autosurveillance ouvert |
| 3 Paroi arrière du boîtier | |

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. Ceci, à son tour, fait que l'interrupteur d'autosurveillance se détache du couvercle et ouvre le contact de l'interrupteur.



AVERTISSEMENT

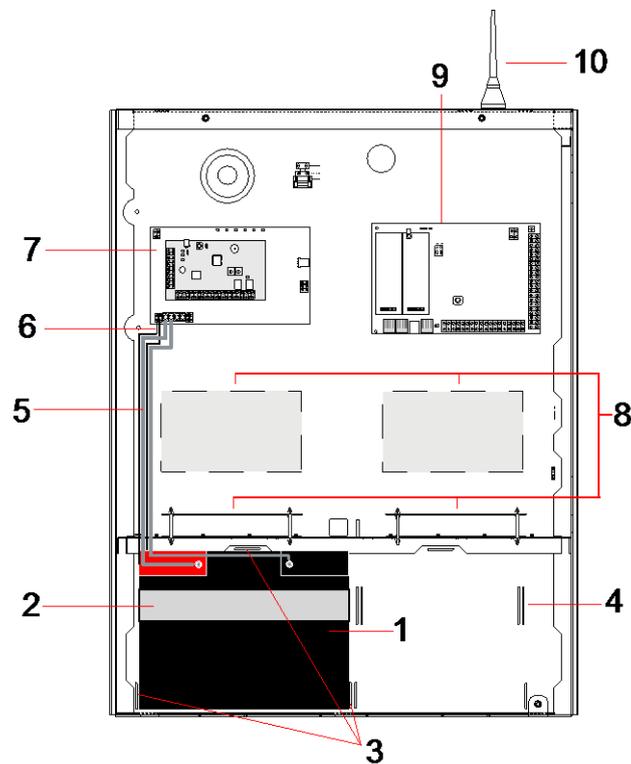
Si la vis d'autosurveillance n'est pas bien fixée au mur, la protection antisabotage n'est pas garantie.

6.3.3 Installation des batteries



AVIS

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



- | | | | |
|---|---------------------------------------|----|--|
| 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 :

- insérez les batteries dans le compartiment correspondant.
- Appuyez sur les languettes métalliques situées sur le haut et sur les deux côtés des batteries vers l'intérieur, vers les batteries.
- 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.
- Attachez-les fermement à l'aide d'une bande Velcro. Assurez-vous que la bande est serrée autour de la batterie.
- Connectez une extrémité des câbles de la batterie aux bornes + 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 (+).

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

6.4 Installation d'un clavier

Veuillez lire les instructions d'installation correspondantes.

6.5 Installation d'un transpondeur

Veuillez lire les instructions d'installation correspondantes.

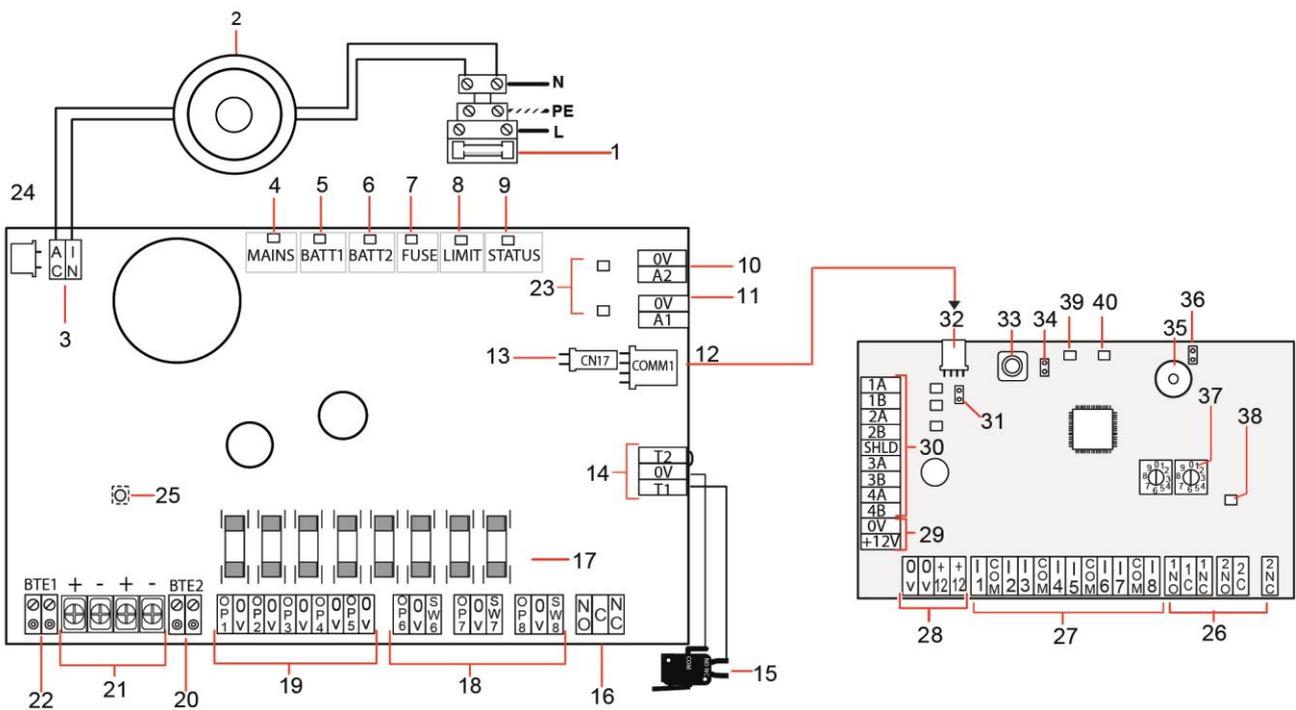
7 Alimentation Auxiliaire Supervisée

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

7.1 SPCP355.300 Smart PSU

Le SCP355 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 2 batteries de 24Ah ou 27Ah et fournit huit sorties d'alimentation et quatre sorties logiques.

Le transpondeur surveille le module d'alimentation pour détecter la présence de surcharge électrique, dysfonctionnement des fusibles, panne de courant alternatif, erreur de communication et problèmes de batterie. Le transpondeur est alimenté et reçoit des données du module d'alimentation 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
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.

Numéro	Description
	<ul style="list-style-type: none"> ● 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 [→ 54].
15	Commutateur d'antisabotage avant/arrière. Voir Montage du boîtier avec la protection antisabotage [→ 54].
16	NO / NF — sortie de relais logique NO / NF configurable. Voir Câblage des sorties [→ 66] pour de plus amples 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 12V CC 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 V CC. Voir l'avertissement sous le table 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, voir Restauration du système [→ 69].
24	Fusible PTC — fusible de 5A. Protège l'entrée d'alimentation CA (repère 3 de l'image ci-dessus). Pour plus d'informations, voir Restauration du système [→ 69].
25	Interrupteur de relance du module d'alimentation — pour plus d'informations, voir Restauration du système [→ 69].
Transpondeur	
26	NO / NC — sorties de relais logiques. Le transpondeur dispose de deux sorties de relais logiques NO / NF. Pour plus d'informations, voir Câblage des entrées [→ 65]
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, voir Câblage des entrées [→ 65]
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 Smart PSUµµµ SPCP355.
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.

Numéro	Description
	Pour plus d'informations, voir la section Câblage de l'interface X-BUS [→ 64].
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), le connecteur d'alimentation et 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 d'antisabotage dont à 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. Voir le menu X-BUS LOCALISER [→ 129] pour des informations supplémentaires.
36	JP6 — contournement de l'antisabotage arrière. Doit être mis en place.
37	Commutateurs d'adressage manuel — active le paramétrage 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 : <ul style="list-style-type: none"> ● clignotement lent (toutes les 1,5 seconde) — l'état de communication X-BUS est OK. ● Clignotement rapide (toutes les 0,2 secondes) — indique une des choses suivantes : <ul style="list-style-type: none"> – 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

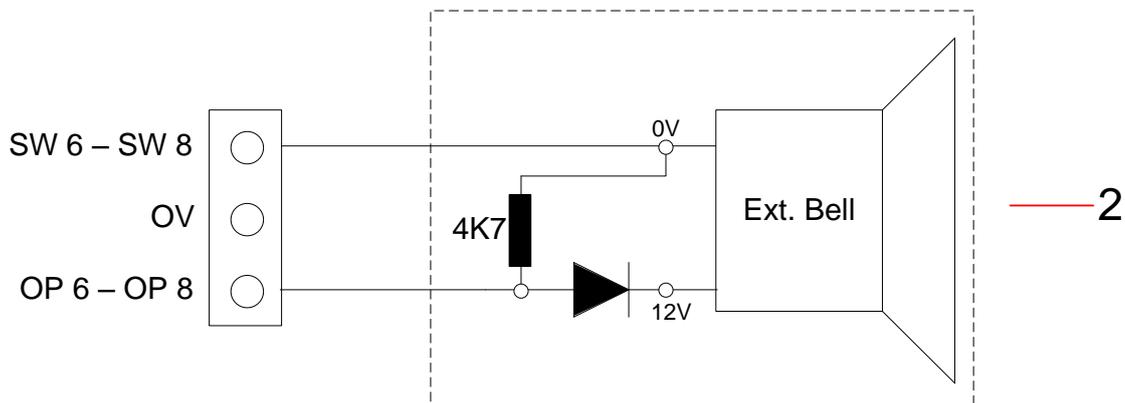
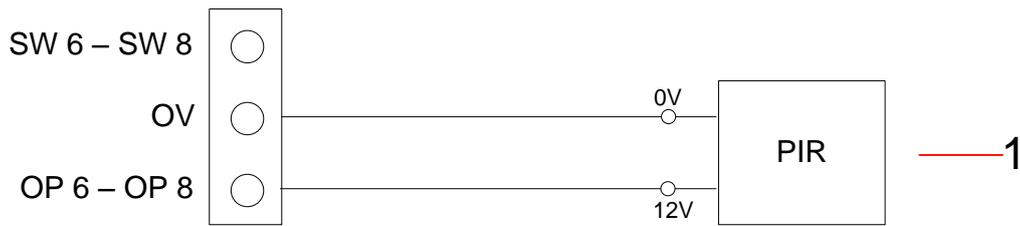
Le courant de charge maximal combiné de toutes les sorties 12V CC (OP 1 - 8) plus COMM1 ne doit pas dépasser 2,4 A. Chacune des sorties individuelles et la sortie A2 ne doit pas dépasser 300 mA. Si le courant de l'appareil nécessite plus de 300 mA, nous vous recommandons de monter les sorties en parallèle.

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, l'autosurveillance avant et arrière est traitée 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.

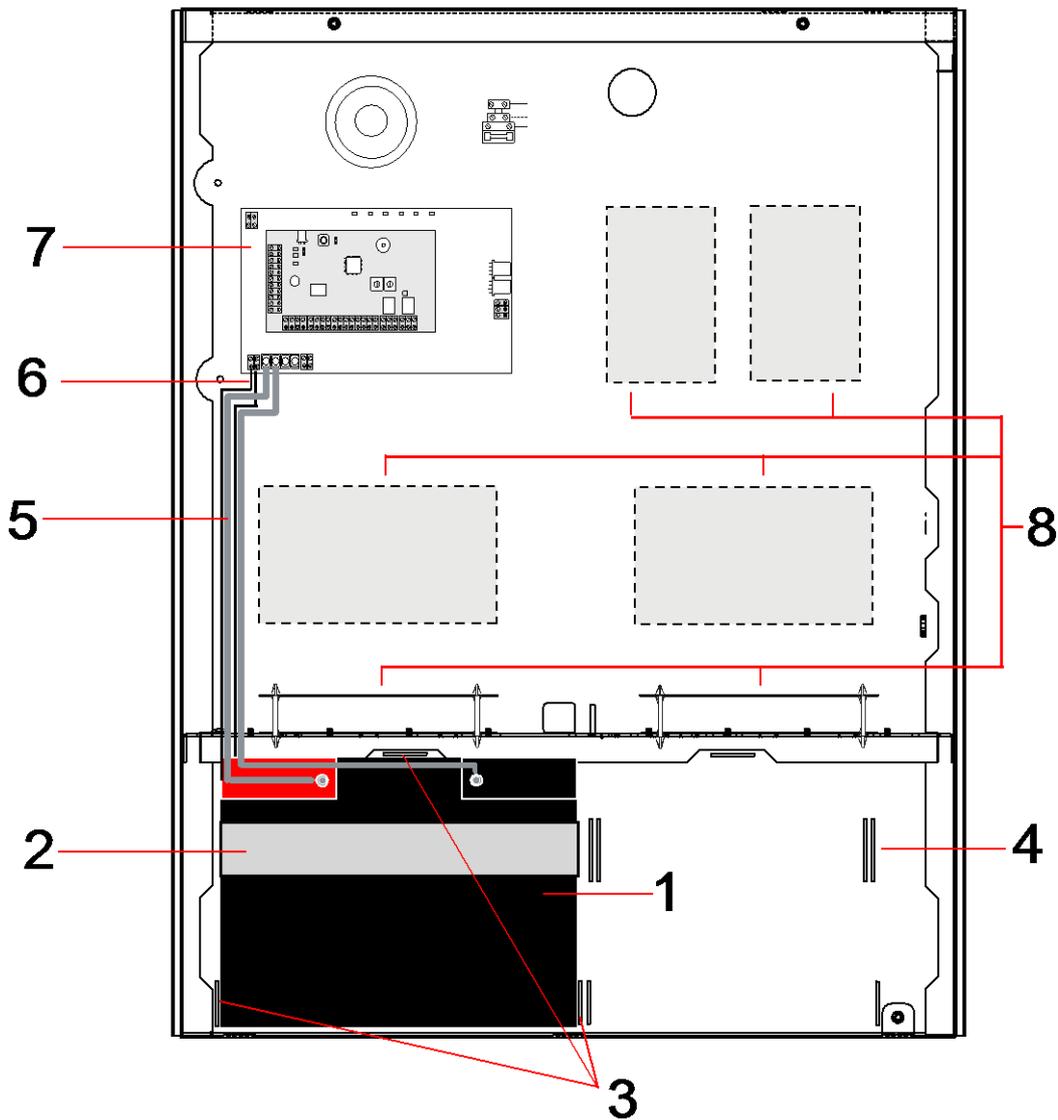


Numéro	Description
1	Sorties standard d'alimentation 12 V
2	Sortie commutée configurable et supervisée 12 V CC.

7.1.2 Batteries

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 de la SPCP355.300 Smart PSU aux batteries dans l'ordre suivant :
 - connectez tout d'abord le câble du plus (rouge).
 - connectez ensuite le câble moins (noir).



⚠ DANGER

Lorsque vous retirez les câbles de la batterie, déconnectez toujours le moins (noir) en premier avant de déconnecter le plus (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 au travers des terminaux 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 absente pendant une période prolongée, chacune des batteries fournit du courant 12 V CC au module d'alimentation pendant une période finie. Les batteries finiront par se décharger. Pour éviter qu'une batterie ne se décharge trop et qu'elle ne devienne inutilisable, le l'alimentation SPCP355.300 la déconnecte si la tension mesurée passe au-dessous de 10,5 V CC La batterie peut alors être rechargée après le retour de l'alimentation secteur.

7.1.2.4 Durée de veille de la batterie

Voir Calcul de la puissance nécessaire de la batterie [→ 353] pour les informations de veille de la batterie.

7.1.3 Câblage de l'interface X-BUS

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

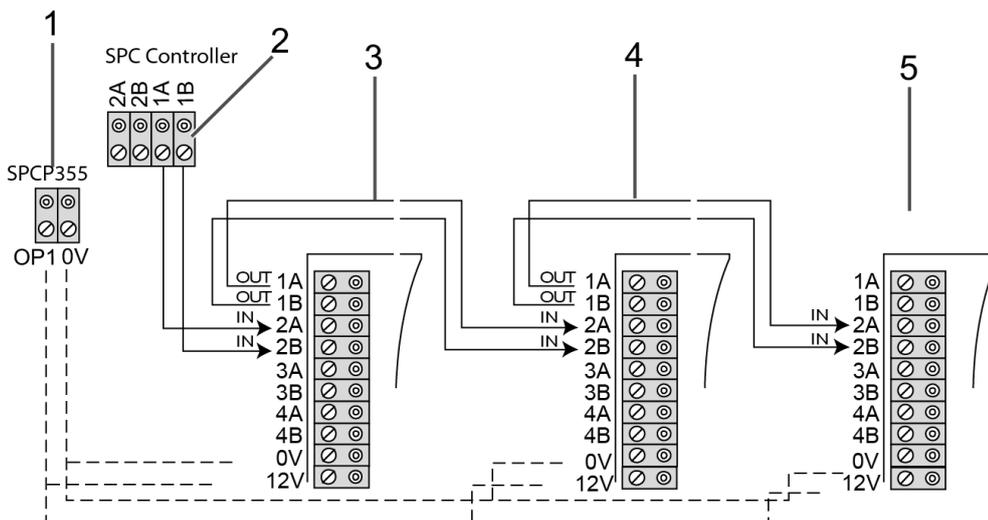
Le tableau suivant fait la liste des types et des distances de câblage recommandés :



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
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
4	Transpondeur suivant
5	Transpondeur suivant

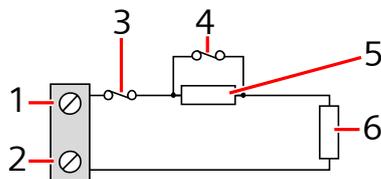
7.1.3.1 Câblage des entrées

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

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

Configuration par défaut

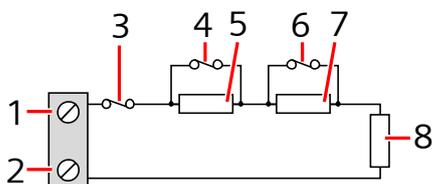
Le diagramme suivant montre la configuration par défaut, avec fin de ligne double 4K7 :



Numéro	Description
1	Entrée 1
2	COM
3	Autosurveillance
4	Alarme
5	4K7
6	EOL 4K7

Infrarouge anti-masquage (MPIR)

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



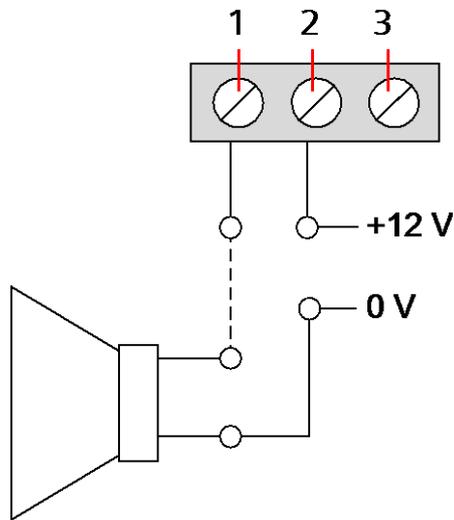
Numéro	Description
1	Entrée 2
2	COM
3	Autosurveillance
4	Alarme
5	4K7
6	Défaut détecteur
7	2K2
8	EOL 4K7

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 V CC à 1A (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) ».

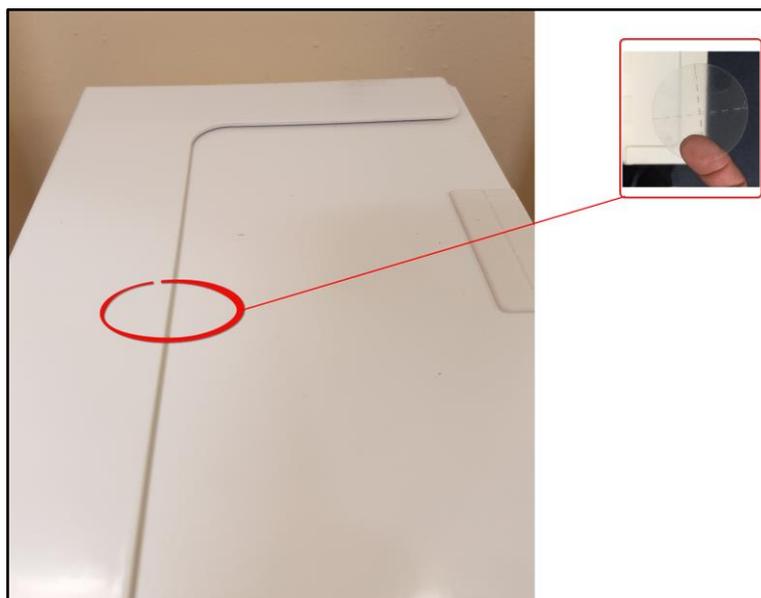
Le diagramme suivant montre le câblage d'une sortie haute active.



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

7.1.4 Conformité avec les agréments NF et A2P

Adresse de l'organisme certificateur	
CNPP Cert Pôle Européen de Sécurité - Vernon Route de la Chapelle Réanville CD 64 - 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



Pour être conforme au référentiel NF & A2P, le boîtier doit être plombé après fermeture au moyen de l'étiquette spéciale fournie.

Les produits SPC listés ont été testés conformément à la norme NF324 - H58, avec référence aux certifications EN, voir Conformité aux agréments EN50131 [→ 21] et aux spécifications RTC50131-6 et RTC50131-3.

Type de produit	Configuration	Standard	Logo
SPC6350.320 + SPCP355.300 (Cert. XXXXXXXXXXX)	60h, non monitorisé	NF Grade 3, Class 1	
SPC5350.320 + SPCP355.300 (Cert. XXXXXXXXXXX)	60h, 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	230V	BATT 1 et 2	FUSIBL E	LIMITE	ÉTAT
COULEUR	Vert	Vert	Rouge	Rouge	Vert

TÉMOIN	230V	BATT 1 et 2	FUSIBLE	LIMITE	ÉTAT
Fonctionnement					
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				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 le SPCP355.300 Smart PSU [→ 59]) permet de redémarrer le système avec seulement le courant de la batterie. Pour relancer le système, effectuez les opérations suivantes :

- ▷ l'alimentation du secteur est en panne
 - ▷ l'alimentation de la batterie est en panne
 - ▷ De nouvelles batteries sont disponibles
1. Connectez 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 de la centrale

Cette section décrit le matériel de la centrale.

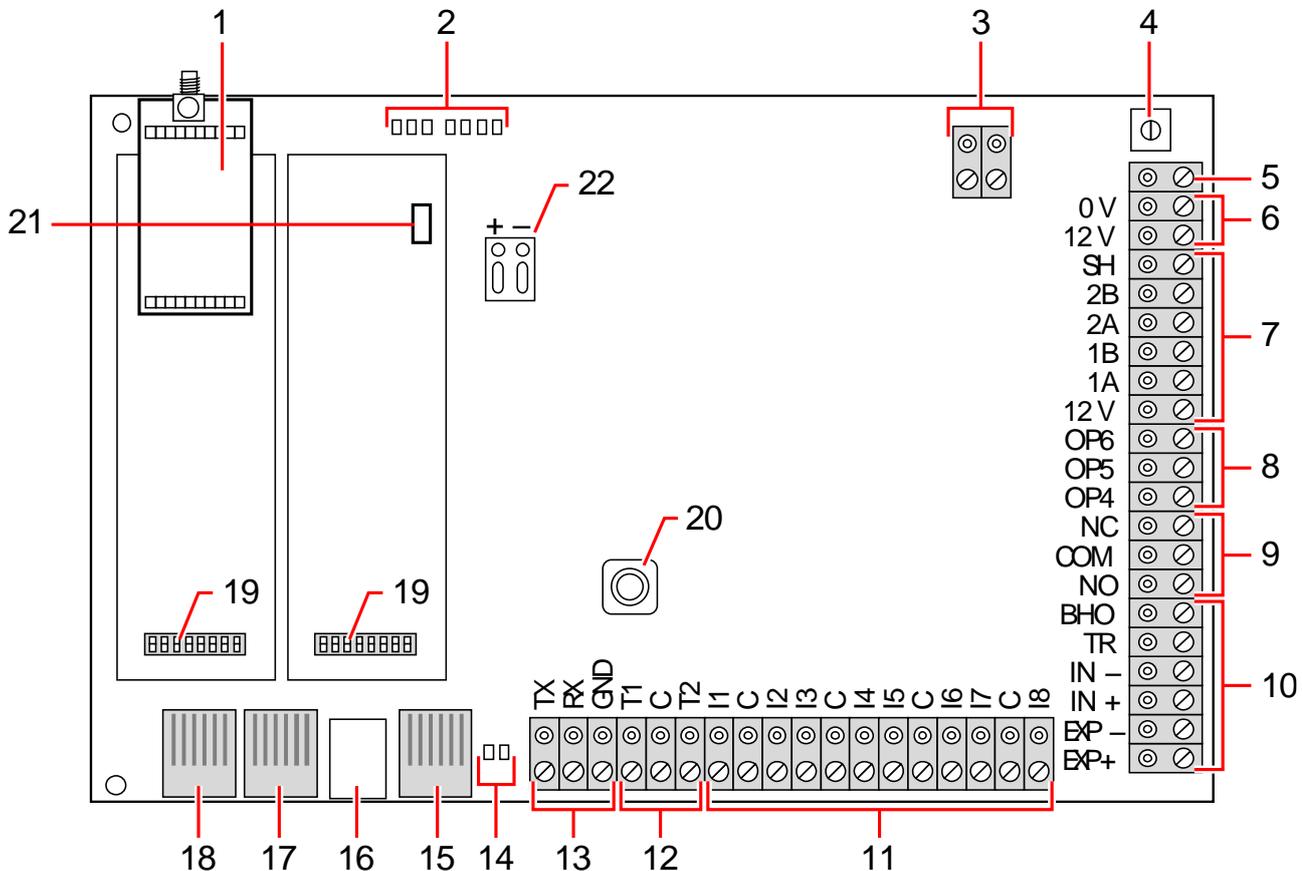
Voir aussi

- ☰ Alimentation des transpondeurs avec les bornes d'alimentation secondaires [→ 352]
- ☰ Câblage de l'interface X-BUS [→ 77]
- ☰ Câblage d'un buzzer interne [→ 93]
- ☰ Câblage des entrées de zone [→ 89]
- ☰ LED d'état de la centrale [→ 351]
- ☰ LED d'état de la centrale [→ 351]
- ☰ Alimentation des transpondeurs avec les bornes d'alimentation secondaires [→ 352]
- ☰ Câblage de l'interface X-BUS [→ 77]
- ☰ Câblage d'un buzzer interne [→ 93]
- ☰ Câblage des entrées de zone [→ 89]

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

Cette section décrit la centrale pour les modules SPC42xx, 43xx, 53xx et 63xx. Le SPC5350 et le 6350 sont décrits dans le Matériel de la centrale SPC5350 et 6350 [→ 72].

Le contrôleur SPC fournit 8 zones embarquées câblées et des zones radio optionnelles.



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	Voyants LED d'état du SPC	Ces 7 voyants LED indiquent l'état de plusieurs paramètres système décrits en page [→ 351].
3	Bornes d'entrée d'alimentation	A/C 230v entrée : La tension CA secteur est appliquée à ces connexions à deux bornes via un transformateur installé dans le boîtier du SPC. Le conducteur de terre est relié à un point de fixation du boîtier métallique. Référence 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.
4	Bouton de réinitialisation	<ul style="list-style-type: none"> ● Pour réinitialiser la centrale : <ul style="list-style-type: none"> – appuyez une fois sur ce bouton. ● Pour restaurer la configuration par défaut et redémarrer la centrale : <ul style="list-style-type: none"> – appuyez sur ce bouton et maintenez-le enfoncé jusqu'à ce qu'un message demandant si vous voulez réinitialiser le système soit affiché. – Sélectionnez OUI pour rétablir les valeurs par défaut usine. <p>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.</p> <p>Remarque : cette fonction n'est pas disponible si le mode verrouillage installateur est actif.</p>
5	Borne de mise à la terre	Cette borne n'est pas requise et ne devrait pas être utilisée.
6	Sortie auxiliaire 12 V	La centrale SPC fournit une sortie auxiliaire de courant continu de 12 V CC utilisable pour alimenter les transpondeurs et les périphériques tels que les gâches, les sirènes etc. Voir page [→ 352]. Le courant de sortie maximal est 750 mA. À noter : la quantité de courant soutiré est en fonction de la durée de maintien quand la batterie est utilisée.
7	Interface de X-BUS	Bus de communication du SPC utilisé pour mettre les transpondeurs en réseau dans le système. Voir page [→ 77]. SPC4000 n'est équipé que d'une seule interface de X-BUS.
8	Sorties intégrées	Les sorties OP4, OP5 et OP6 sont des sorties résistives à collecteur ouvert de 12 V partageant un courant nominal de 400 mA avec la sortie auxiliaire 12 V. Si ces sorties ne sont pas connectées à la borne 12 V de la centrale, mais reliées à une source d'alimentation externe, la borne 0 V de la source d'alimentation doit être connectée à la borne 0 V de la centrale et la source d'alimentation externe ne doit pas dépasser 12 V.
9	Sortie de relais	La centrale SPC possède un relais de commutation unipolaire de 1 A, utilisable pour alimenter la sortie de flash de la sirène externe.
10	Sirène intérieure / extérieure	Les sorties de sirène intérieure / 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 R>eturn = Retour anti-effraction) et EXT sont utilisées pour connecter une sirène extérieure à la centrale. Les bornes INT+ et INT- permettent de connecter des éléments internes tels qu'un buzzer. Voir page [→ 93].
11	Entrées de zone	La centrale possède 8 entrées intégrées servant à relier les zones surveillées. Plusieurs configurations de supervision différentes sont utilisables. Ces configurations peuvent être programmées dans la programmation générale. La configuration par défaut est en double fin de ligne Dual End of Line, (DEOL) avec des résistances 4K7. Voir page [→ 89].
12	Bornes anti-effraction	La centrale possède 2 bornes supplémentaires d'entrée anti-effraction servant à connecter des dispositifs anti-sabotage supplémentaires pour augmenter la protection. Ces bornes devraient être court-circuitées si elles ne sont pas utilisées.

13	Bornier du port série 2 	Le bornier du port série 2 (TX, RX, GND) constitue l'interface avec un modem externe ou un programme terminal de 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	 LED de connectivité Ethernet	Ces 2 témoins lumineux LED indiquent l'état de la connexion Ethernet. La LED de gauche indique la transmission de données sur le port Ethernet ; la LED de droite indique si la liaison Ethernet est active.
15	 Interface Ethernet	L'interface Ethernet permet de connecter la centrale à un PC pour programmer le système.
16	Interface USB	Cette interface USB sert à accéder à la programmation par navigateur Web ou à un programme de terminal.
17	Port série 2 	Ce port série RS232 peut constituer l'interface avec un modem externe ou un programme terminal de 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	Ce port série RS232 peut constituer l'interface avec un composant prenant en charge le protocole X10.
19	Modules d'extension en option	Un module primaire (emplacement gauche) et un module de secours (emplacement droit) peuvent être connectés à la centrale. Ces modules peuvent être un modem GSM ou un modem RTC augmentant les possibilités de communication. Le modem de secours ne devrait pas être connecté si le port série 2 est connecté à un modem externe ou à un autre périphérique.
20	Autoprotection frontale	Ce contact anti-effraction frontal (interrupteur & interrupteur) protège le boîtier contre les tentatives de sabotage. Remarque : l'anti-effraction avant n'est pas utilisé dans le boîtier G5.
21	Sélecteur de batterie	J12 : mettez le cavalier en place pour les batteries 17 Ah et retirez-le pour les batteries 7 Ah. À noter : ce sélecteur n'est disponible que sur la carte mère version 2.3 de la centrale. (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

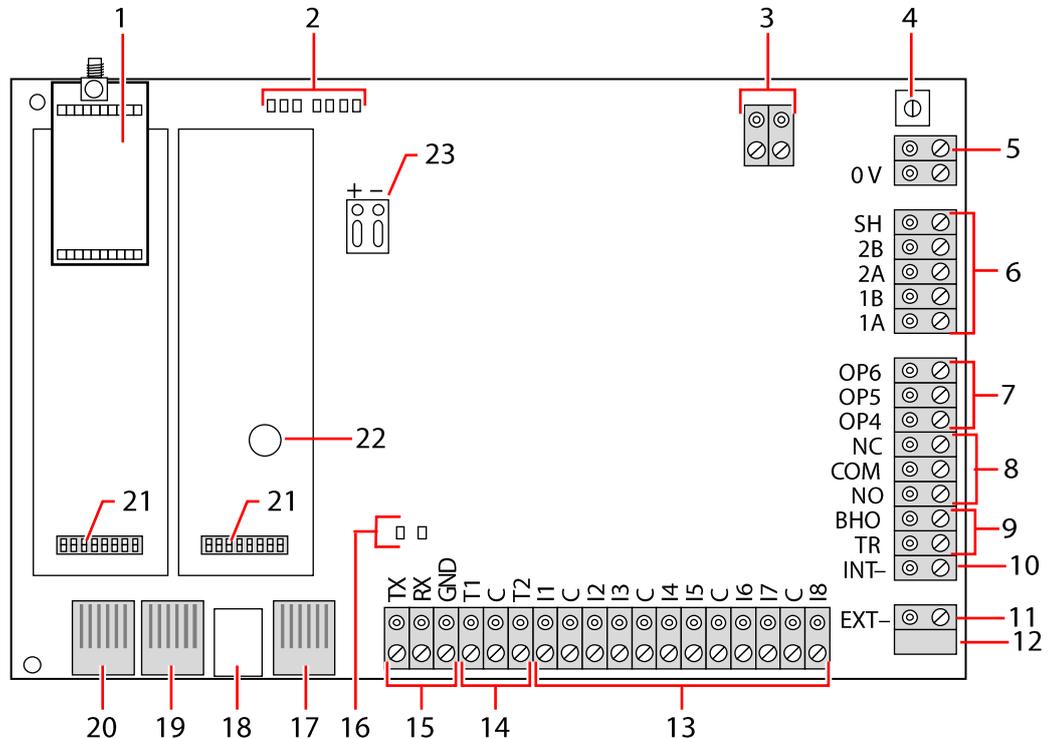
** Le module d'alimentation est valable uniquement pour les centrales SPC5350 et SPC6350.

8.2 Matériel de la centrale SPC5350 et 6350

Cette section décrit le SPC5350 et le SPC6350.



Le transpondeur qui est fixé sur la carte chargeur des boîtiers G5 est programmé à l'adresse ID1. Cette configuration ne doit pas être modifiée.



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	Voyants LED d'état du SPC	Ces 7 voyants LED indiquent l'état de plusieurs paramètres système décrits en page [→ 351].
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	<ul style="list-style-type: none"> ● Pour réinitialiser la centrale : <ul style="list-style-type: none"> – appuyez une fois sur ce bouton. ● Pour restaurer la configuration par défaut et redémarrer la centrale : <ul style="list-style-type: none"> – appuyez sur ce bouton et maintenez-le enfoncé jusqu'à ce qu'un message demandant si vous voulez réinitialiser le système soit affiché. – Sélectionnez OUI pour rétablir les valeurs par défaut usine. <p>Avvertissement : 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.</p> <p>Remarque : cette fonction n'est pas disponible si le mode verrouillage installateur est actif.</p>
5	Borne de mise à la terre	Cette borne n'est pas requise et ne devrait pas être utilisée.

6	Interface de X-BUS	Bus de communication du SPC utilisé pour mettre les transpondeurs en réseau dans le système. Voir page [→ 77]. Les terminaux 1B et 1A doivent être connectés aux terminaux de l'E/S de la centrale SPCP355.300 E/SP 2B et 2A, 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 avec le SPCP355.300 Smart PSU.
8	Sortie de relais	La centrale SPC possède un relais de commutation unipolaire de 1 A, utilisable pour alimenter la sortie de flash de la sirène externe.
9	Mise en attente de la sirène (BHO) et retour d'anti-effraction (TR)	Les sorties BHO (B ell H old O ff = Retenue de sirène) et TR (T amper R eturn = Retour d'autosurveillance) (et la sortie EXT) sont utilisées pour connecter une sirène extérieure à la centrale. Voir page [→ 93].
10	Sirène intérieure (négatif)	Le terminal 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)	Le terminal Ext- est utilisé 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	La centrale possède 8 entrées intégrées servant à relier les zones surveillées. Plusieurs configurations de supervision différentes sont utilisables. Ces configurations peuvent être programmées dans la programmation générale. La configuration par défaut est en double fin de ligne Dual End of Line , (DEOL) avec des résistances 4K7. Voir page [→ 89].
14	Bornes anti-effraction	La centrale possède 2 bornes supplémentaires d'entrée anti-effraction servant à connecter des dispositifs anti-sabotage supplémentaires pour augmenter la protection. Ces bornes devraient être court-circuitées si elles ne sont pas utilisées.
15	Bornier du port série 2	Le bornier du port série 2 (TX, RX, GND) constitue l'interface avec un modem externe ou un programme terminal de 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	Ces 2 témoins lumineux LED indiquent l'état de la connexion Ethernet. La LED de gauche indique la transmission de données sur le port Ethernet ; la LED de droite indique si la liaison Ethernet est active.
17	Interface Ethernet	L'interface Ethernet permet de connecter la centrale à un PC pour programmer le système.
18	Interface USB	Cette interface USB sert à accéder à la programmation par navigateur Web ou à un programme de terminal.
19	Port série 2	Ce port série RS232 peut constituer l'interface avec un modem externe ou un programme terminal de 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	Ce port série RS232 peut constituer l'interface avec un composant prenant en charge le protocole X10.
21	Modules d'extension en option	Un module primaire (emplacement gauche) et un module de secours (emplacement droit) peuvent être connectés à la centrale. Ces modules peuvent être un modem GSM ou un modem RTC augmentant les possibilités de communication. Le modem de secours ne devrait pas être connecté si l'interface du port série 2 est connectée à un modem externe ou à un autre périphérique.
22	Batterie d'horloge en temps réel	Batterie pour horloge en temps réel (HTR).

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

Voir aussi

- 📄 Alimentation des transpondeurs avec les bornes d'alimentation secondaires [→ 352]

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 des portes. Chacune des deux E/S de porte gère deux entrées et une sortie du contrôleur de porte. Un numéro de porte spécifique peut être attribué à une E/S de porte, ce qui permet d'utiliser les entrées et la sortie pour des fonctionnalités prédéfinies. Si un numéro de porte n'est attribué à aucune E/S de porte (l'option « Zones » est sélectionnée), les entrées et les sorties du contrôleur de porte peuvent être utilisées en guise d'entrées et de sorties sur la centrale. Dans ce cas, aucune fonctionnalité d'accès n'est disponible sur ces deux contrôleurs de porte.

Si un numéro de porte est attribué seulement à la première E/S de porte des deux contrôleurs de porte, le premier lecteur est utilisé en tant que lecteur d'entrée pour cette porte. Si un deuxième lecteur est disponible, il est utilisé en tant que 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 avec des fonctions limitées.

Si un numéro de porte est attribué à chacune des deux E/S des portes, celles-ci sont traitées indépendamment. Le premier lecteur de badge est utilisé en tant que lecteur d'entrée pour la première porte, et le deuxième en tant que lecteur d'entrée pour la deuxième porte. Toutes les entrées et sorties ont des fonctionnalités prédéfinies. En outre, les entrées du détecteur de position des deux portes sont utilisables en tant que zones d'intrusion mais avec des fonctions limitées.

Consultez l'Annexe [→ 375] pour un complément d'information à propos des lecteurs de cartes et des formats de badges.



Chaque numéro disponible peut être attribué à une zone. Cette attribution n'est pas fixe. Si le numéro 9 est attribué à une zone, la zone et un transpondeur d'entrée avec l'adresse 1 sont connectés au X-Bus (qui utilise les numéros de zone 9 à 16). La zone attribuée par les deux contrôleurs de porte obtient le numéro de zone suivant disponible. La configuration est adaptée en conséquence.

10 Câblage du système

10.1 Câblage de l'interface X-BUS

L'interface X-BUS sert à connecter les transpondeurs à la centrale. 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 ko.

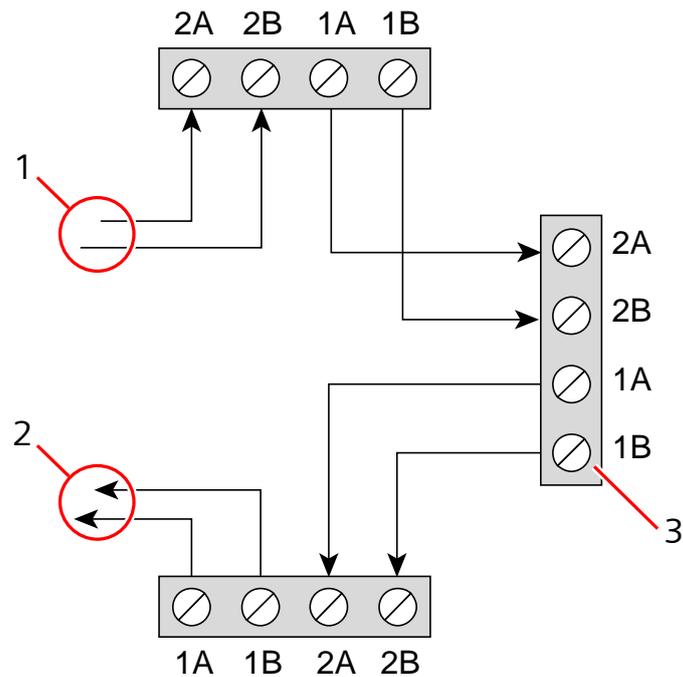
	AVIS
	<p>Le X-BUS est un bus RS-485 avec un débit en bauds de 307 Ko. La performance la plus complète possible n'est prise en charge que dans les configurations de câblage en boucle [→ 78] et en branche [→ 79] (la meilleure qualité de signal est obtenue avec la configuration en guirlande des sections isolées, avec 1 transmetteur / 1 récepteur et des résistances d'extrémité équilibrées à chaque extrémité).</p> <p>La performance dans une topologie en étoile [→ 80] ou multipoints [→ 80] est limitée, à cause des conditions non optimales de la spécification de bus RS-485 (qualité du signal réduite due au montage de plusieurs récepteurs / transmetteurs en parallèle avec des résistors d'extrémité non équilibrés).</p>

	AVIS
	Il est fortement recommandé d'utiliser une configuration en boucle [→ 78] ou en branche [→ 79].

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
Catégorie UTP : 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 topologie.



Câblage du transpondeur

1	Transpondeur précédent
2	Transpondeur suivant
3	Centrale SPC

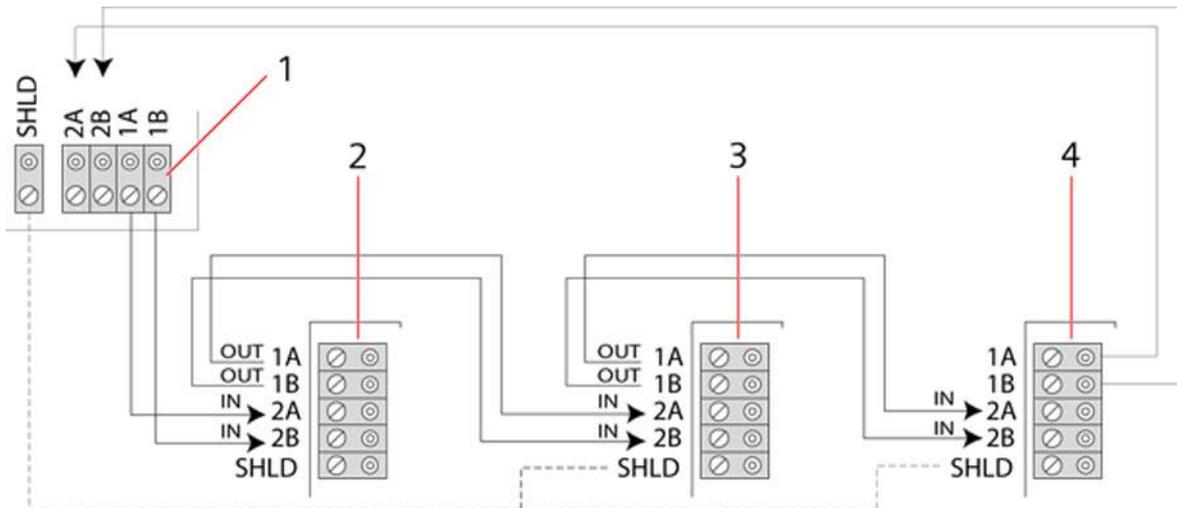
La plupart des transpondeurs sont équipés de bornes supplémentaires 3A/3B et 4A/4B pour le câblage du transpondeur en branche. Voir ici [→ 87] pour les instructions sur le câblage d'un transpondeur en branche.

10.1.1 Configuration en boucle

i	AVIS
	4000 Le SPC42xx/43xx ne prend pas en charge la configuration en boucle (uniquement 1 port X-BUS).

i	AVIS
	Tous les transpondeurs / claviers sont équipés par défaut d'un cavalier d'extrémité. En configuration en boucle, il est impératif de mettre ces cavaliers en place.

Le câblage en boucle (ou anneau) offre la plus grande sécurité tout en permettant des communications tolérant les erreurs sur le bus X-BUS. Tous les claviers et les transpondeurs sont parcourus par un courant de garde permanent, et, en cas de panne X-BUS ou de rupture de câble, le système continue de fonctionner. Tous les détecteurs sont ainsi surveillés. Ceci est réalisé en reliant 1A, 1B de la centrale à 2A, 2B du premier clavier ou transpondeur. Pour continuer, 1A, 1B du transpondeur suivant sont reliés à 2A, 2B du clavier ou du transpondeur suivant, et ainsi de suite jusqu'au dernier clavier ou transpondeur. La dernière liaison relie 1A, 1B du dernier transpondeur à 2A, 2B de la centrale. Voir le schéma de câblage dans la figure ci-dessous.



1	E/S Centrale
2-4	Transpondeurs

10.1.2 Configuration en branche

i	AVIS
	Le SPC52xx/53xx/63xx prend en charge 2 branches (2 ports X-BUS). Le SPC42xx/43xx prend en charge 1 branche (1 port X-BUS).

i	AVIS
	Tous les transpondeurs / claviers sont équipés par défaut d'un cavalier d'extrémité. En configuration en branche, il est impératif de mettre ces cavaliers en place.

Le câblage en branche (ou boucle ouverte) offre un niveau élevé de tolérance aux pannes et convient mieux à certains environnements. En cas de panne ou d'interruption du X-BUS, tous les transpondeurs et détecteurs en amont de la panne continuent d'être surveillés.

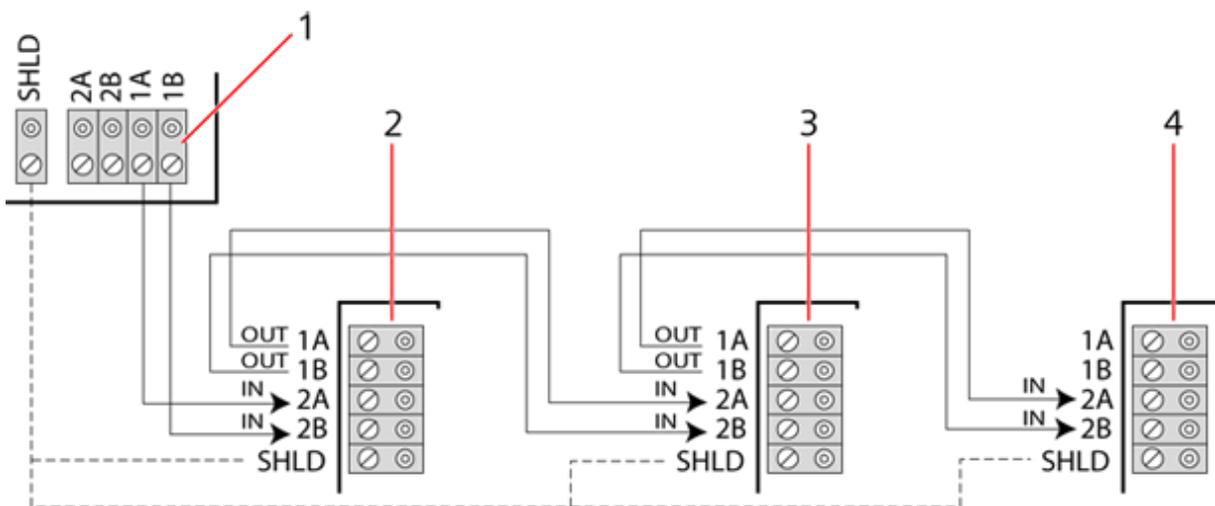
Dans cette configuration, la centrale SPC utilise un seul port X-BUS (1A/1B ou 2A/2B) pour prendre en charge un groupe de transpondeurs. Voir le schéma de

câblage dans la figure ci-dessous. Le dernier transpondeur dans une configuration en boucle ouverte n'est pas relié à la centrale et ne ferme donc pas le circuit. Il est identifié par le clignotement rapide du témoin LED (un clignotement toutes les 0,2 secondes) en Mode Paramétrage.

En mode automatique, la numérotation des transpondeurs commence avec le transpondeur le plus rapproché et se termine avec le transpondeur le plus éloigné de la centrale. Par exemple, si 6 transpondeurs sont connectés dans une configuration de boucle ouverte, le premier transpondeur en aval de la centrale sur le X-BUS est le transpondeur 1, le suivant est le transpondeur 2, et ainsi de suite jusqu'au transpondeur le plus éloigné qui aura le numéro 6.

Tous les transpondeurs/claviers possèdent par défaut un cavalier d'extrémité de ligne faisant office de bouchon (terminateur). Ceci est impératif dans le cas de la configuration en branche (chaîne), le cavalier fonctionnant comme une résistance d'extrémité annulant les échos dans le câble.

Dans un câblage en boucle, tous les transpondeurs/claviers possèdent par défaut un cavalier d'extrémité faisant office de bouchon (terminateur).



Configuration en branche

1	E/S Centrale
2-4	Transpondeurs

10.1.3 Configuration en étoile et multipoints



AVIS

Veillez lire la section concernant les exemples de câblage [→ 85] et celle sur le Blindage [→ 86] avant de commencer l'installation.

Les méthodes de câblage en étoile et multipoints permettent de reprendre des câblages existants avec des câbles à quatre âmes (en général dans les résidences individuelles) posés dans un environnement à faible bruit électrique. Ces méthodes de câblage sont limitées aux spécifications ci-dessous :

	SPC42xx/SPC43xx	SPC52xx/SPC53xx/SPC63xx
Nombre max. de	8	16 (8 par port X-BUS)

transpondeurs / claviers		
Longueur totale du câble	200 m	200 m

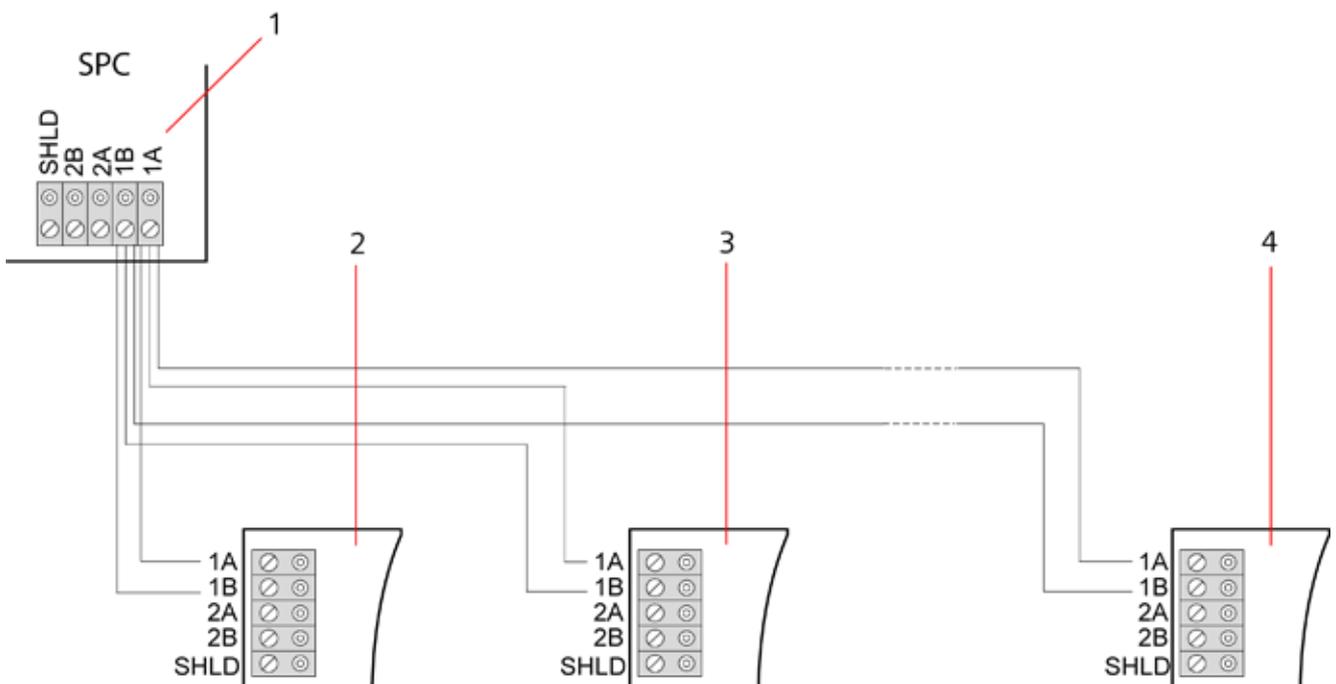
i	AVIS
	La performance en configuration de câblage en étoile ou multipoints est limitée, à cause des conditions non optimales de la spécification de bus RS-485 (qualité du signal réduite due au montage de plusieurs récepteurs / transmetteurs en parallèle avec des résistors d'extrémité non équilibrés).

Configuration en étoile

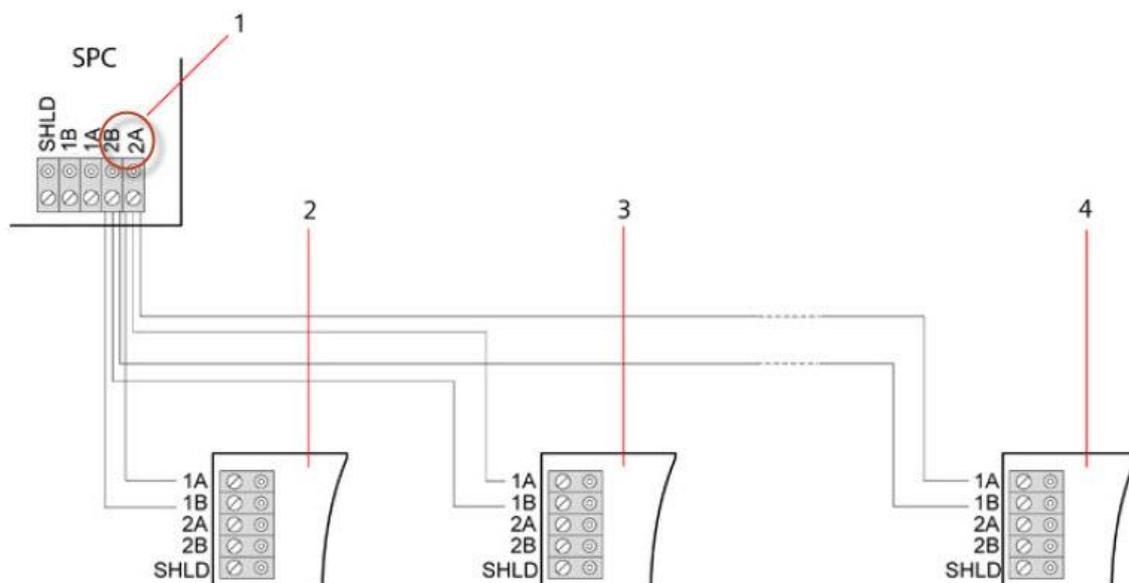
i	AVIS
	Tous les transpondeurs / claviers sont équipés par défaut d'un cavalier d'extrémité. En configuration en étoile, il est impératif de supprimer ces cavaliers.

Dans une configuration en étoile, les transpondeurs ont une liaison de retour au même port du X-BUS sur la centrale SPC. En fonction du type de transpondeurs, 2 ports peuvent être utilisés (1A/1B, 2A/2B), mais seul un port (1A/1B) doit être utilisé sur chacun des claviers ou transpondeurs.

Dans le cas d'une interruption du X-BUS, le port seul sera déconnecté et tous les autres transpondeurs et détecteurs continuent d'être surveillés. Un court-circuit dans le câble désactive tous les transpondeurs.



Configuration en étoile



Configuration en étoile 2

1	centrale SPC
2-4	Transpondeurs

Configuration multipoints

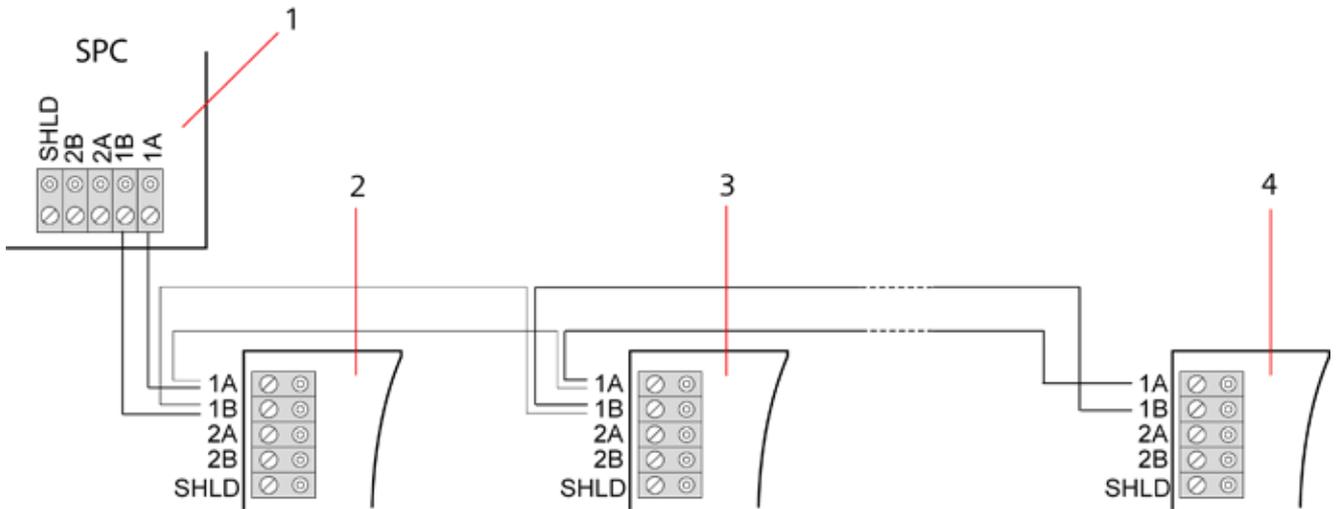


AVIS

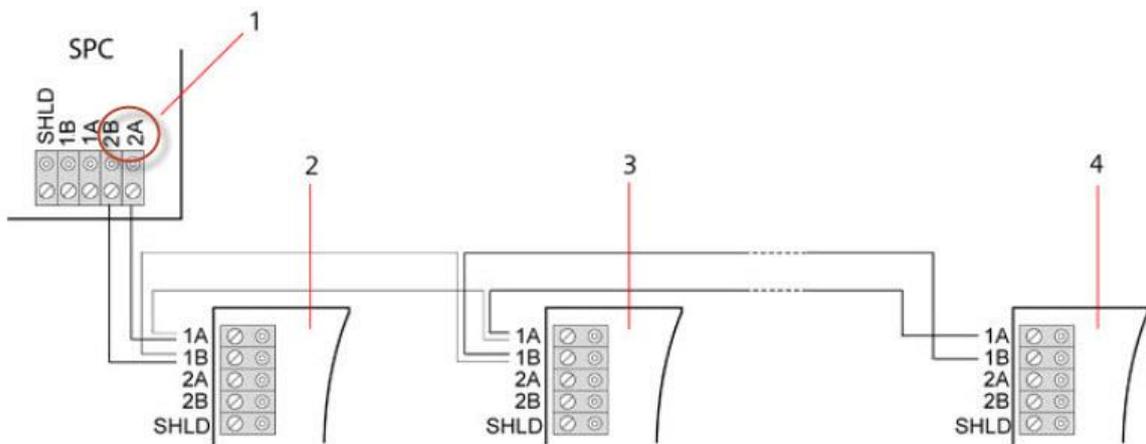
Tous les transpondeurs / claviers sont équipés par défaut d'un cavalier d'extrémité. En configuration multipoints, il est impératif de **retirer** ces cavaliers, à l'exception de celui correspondant au dernier clavier ou transpondeur.

Dans une configuration multipoints, 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 multipoints dans la seconde figure.

En cas de panne ou d'interruption du X-BUS, tous les transpondeurs et détecteurs en amont de la panne continuent d'être surveillés. Un court-circuit dans le câble désactive tous les transpondeurs.



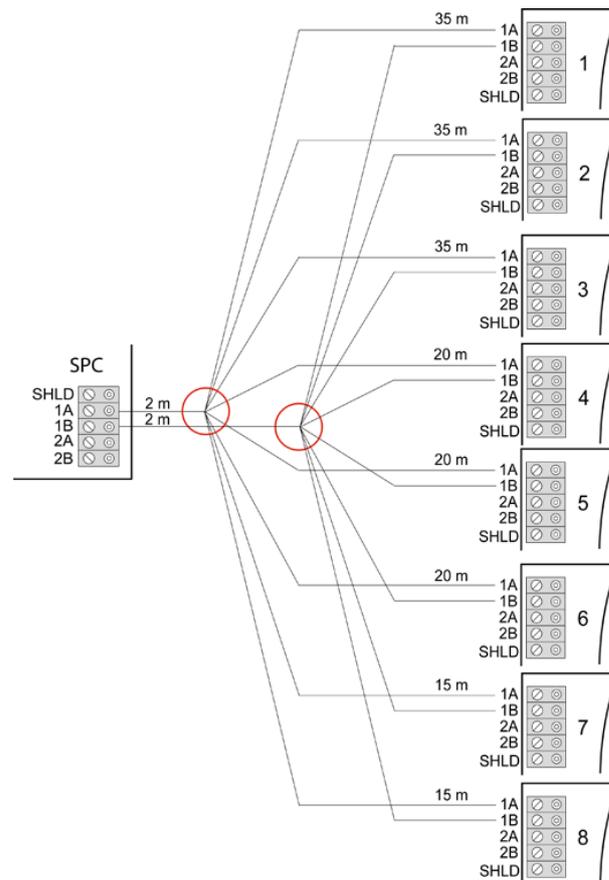
Configuration multipoints



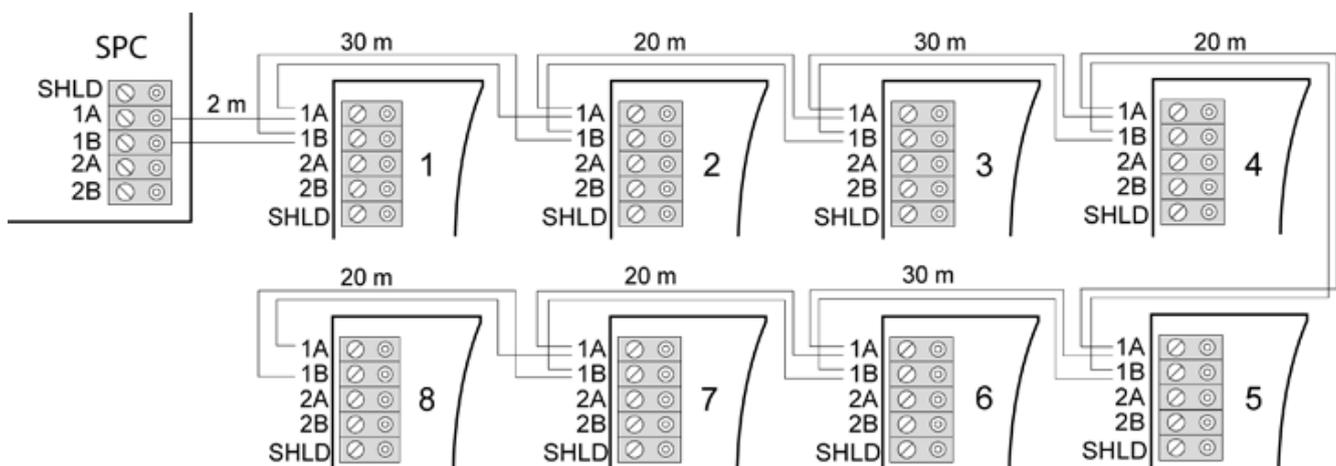
Configuration multipoints 2

1	centrale SPC
2-4	Transpondeurs

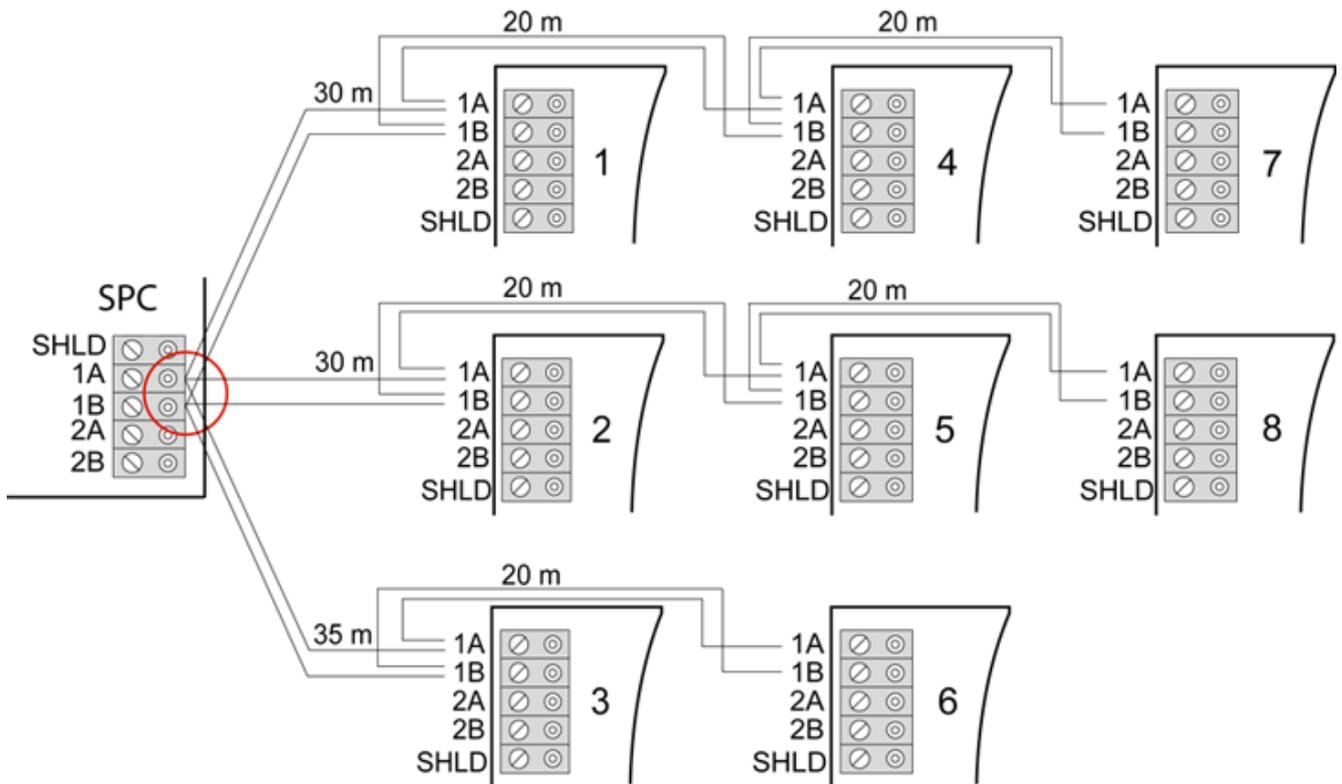
10.1.3.1 Exemples de câblage correct



Câblage en étoile



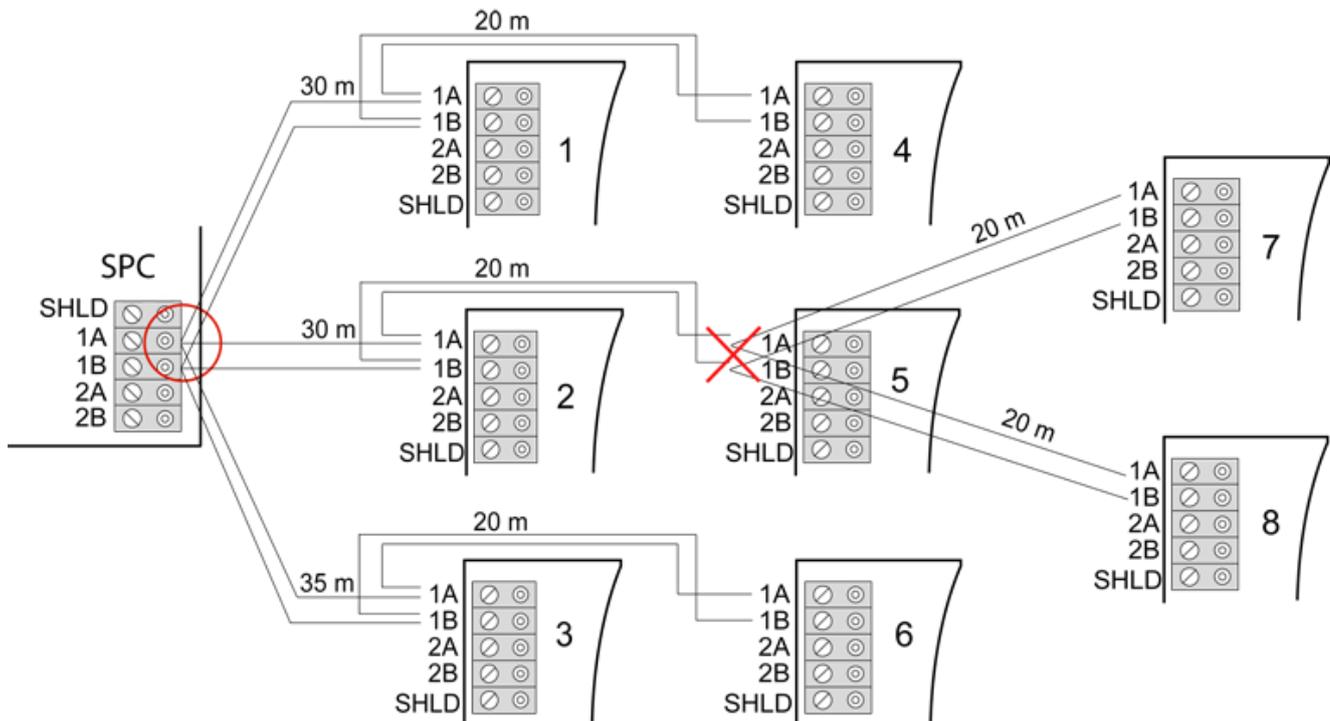
Câblage multipoints



Câblage mixte

10.1.3.2 Exemples de câblage incorrect

	<p>AVIS</p> <p>Une configuration mixte étoile / multipoints 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 multipoints, sans autre point en étoile dans le câblage.</p>
---	--



Interdiction de relier un second point en étoile



AVIS

Si le mélange de ces deux configurations n'est pas correctement câblé, 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. Si un tel comportement est observé, 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 (sites avec d'importantes interférences de champ électrique) : raccordez le blindage du câble aux bornes SHLD de la centrale et de tous les transpondeurs connectés. S'il est nécessaire de relier le blindage à la terre, on connectera un câble pour relier la borne SHLD de la centrale au plot de mise à terre du châssis. Ne reliez à la terre la borne SHLD d'AUCUN des transpondeurs.

**AVIS****Pour les câblages en étoile et multipoints**

Il n'est pas recommandé d'utiliser des câbles blindés à cause de leurs mauvaises caractéristiques électriques (capacité élevée) pour les configurations en étoile et multipoints. Toutefois, si un blindage est requis (c'est-à-dire pour les sites avec une forte interférence du 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 la numérotation des transpondeurs et des claviers varient suivant que l'adressage des transpondeurs est automatique ou manuel. Voir la description de la configuration manuelle et automatique ici [→ 126].

Pour un système avec adressage manuel, les transpondeurs et les claviers ont leur propre numérotation définie manuellement par l'installateur. Par exemple, les transpondeurs sont numérotés 01, 02, 03, et ainsi de suite. Les mêmes numéros sont attribués aux claviers.

Dans la configuration manuelle, le système attribue automatiquement des zones à chaque transpondeur. Par conséquent, les périphériques sans attribution de zone tels que les transpondeurs à 8 sorties devraient être adressés en dernier.

Pour un système avec adressage automatique, les transpondeurs et les claviers appartiennent à la même tranche de numérotation et sont numérotés par la centrale. Les transpondeurs et les claviers sont donc numérotés indistinctement 01, 02, 03, dans l'ordre de leur détection, en fonction de l'emplacement de la centrale.

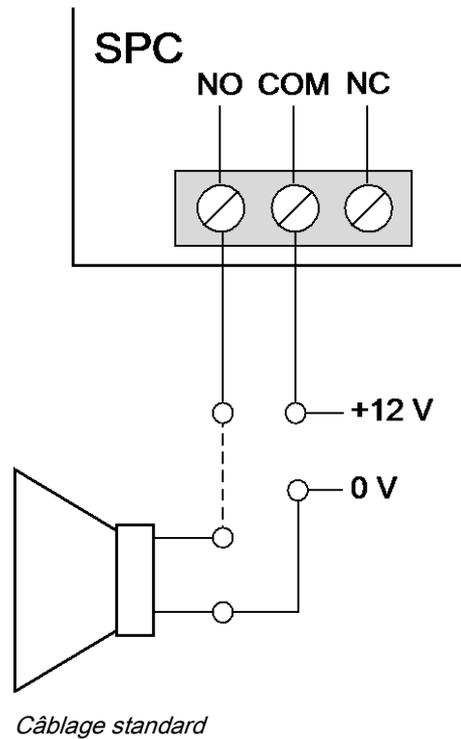
10.2 Câblage du transpondeur de branche

Le raccordement de l'interface X-BUS à 8 bornes 1A/1B à 4A/4B permet de connecter un transpondeur de branche supplémentaire.

Si la branche n'est pas utilisée, les bornes 1A/1B servent à connecter le transpondeur ou le clavier suivant. Dans ce cas, les bornes 3A/3B et 4A/4B ne sont 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
- transpondeur de module d'alimentation
- transpondeur radio
- transpondeur 2 portes

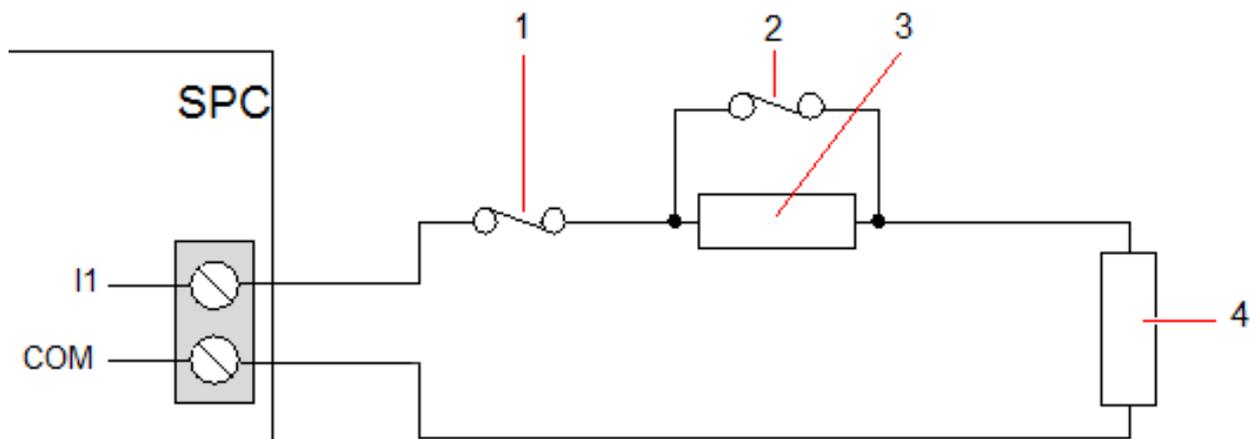


NO	Borne normalement ouverte
COM	Connexion de borne commune
NC	Borne normalement fermée

10.5 Câblage des entrées de zone

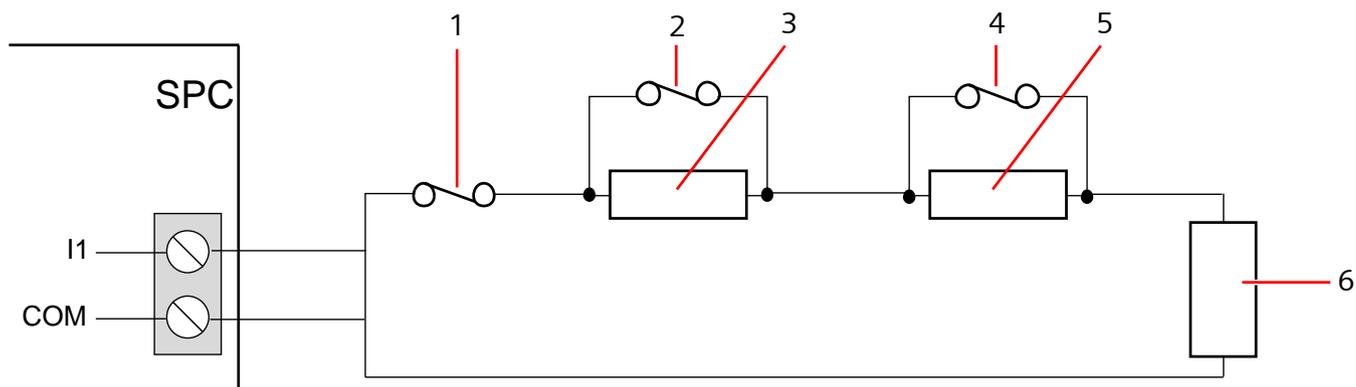
La centrale SPC possède 8 entrées des zones intégrées. Par défaut, ces entrées sont surveillées par des résistances fin de ligne. L'installateur peut choisir l'une des configurations suivantes pour câbler les entrées :

- Sans fin de ligne (NEOL)
- Fin de ligne simple (SEOL)
- Fin de ligne double (DEOL)
- Supervision infrarouge anti-masquage (MPIR)



configuration par défaut (DEOL 4K7)

1	Autosurveillance
2	Alarme
3	EOL 4K7
4	EOL 4K7



configuration infrarouge anti-masquage

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 de RFL	Courant de repos			Alarme		
	Min	Nom	Max	Min	Nom	Max
AUCUNE	0Ω (-100%)	150Ω	300Ω (+100%)	300Ω (+100%)	Non disponible	Infinie
UNIQUE_1K	700Ω (-30%)	1kΩ	1,3kΩ (+30%)	23kΩ	Non disponible	Infinie

UNIQUE_1K5	1,1kΩ (-27%)	1,5kΩ	2,1kΩ (+40%)	23kΩ	Non disponible	Infinie
UNIQUE_2K2	1,6kΩ (-28%)	2,2kΩ	2,9kΩ (+32%)	23kΩ	Non disponible	Infinie
UNIQUE_4K7	3,1kΩ (-22%)	4,7kΩ	6,3kΩ (+24%)	23kΩ	Non disponible	Infinie
UNIQUE_10K	7kΩ (-30%)	10kΩ	13kΩ (+30%)	23kΩ	Non disponible	Infinie
UNIQUE_12K	8,5kΩ (-30%)	12kΩ	15,5kΩ (+30%)	23kΩ	Non disponible	Infinie

Résistances doubles avec masquage infrarouge et défaut

Type de RFL	Courant de repos			Alarme		
	Min	Nom	Max	Min	Nom	Max
Masque_1K_1K_6K8 (1K / 1K / 6K8)	700Ω (-30%)	1kΩ	1,3kΩ (+30%)	1,5kΩ (-25%)	2kΩ	2,5kΩ (+25%)
Masque_1K_1K_2K2 (1K / 1K / 2K2)	700Ω (-30%)	1kΩ	1,3kΩ (+30%)	1,5kΩ (-25%)	2kΩ	2,6kΩ (+30%)
Masque_4K7_4K7_2K2 (4K7 / 4K7 / 2K2)	3,9kΩ (-18%)	4,7kΩ	5,6kΩ (+20%)	8,4kΩ (-11%)	9,4kΩ	10,3kΩ (+10%)

Type de RFL	Défaut			Masque		
	Min	Nom	Max	Min	Nom	Max
Masque_1K_1K_6K8	2700Ω (-69%)	8,8kΩ	12,6kΩ (+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%)

Doubles résistances de fin de ligne

Type de RFL	Courant de repos			Alarme		
	Min	Nom	Max	Min	Nom	Max
DOUBLE_1K0_470	400Ω (-20%)	470Ω	700kΩ (+40%)	1,1kΩ (-27%)	1,5kΩ	2kΩ (+34%)
DOUBLE_1K0_1K0	700Ω (-30%)	1kΩ	1,3kΩ (+30%)	1,5kΩ (-25%)	2kΩ	2,6kΩ (+30%)
DUAL_1k0_2k2	1,6kΩ (-28%)	2,2kΩ	2,9kΩ (+32%)	2,3kΩ (-29%)	3,2kΩ	4,2kΩ (+32%)
DUAL_1k5_2k2	1,6kΩ (-28%)	2,2kΩ	2,9kΩ (+32%)	2,7kΩ (-28%)	3,7kΩ	4,8kΩ (+30%)
DOUBLE_2K2_2K2	1,6kΩ (-28%)	2,2kΩ	2,9kΩ (+32%)	3,4kΩ (-23%)	4,4kΩ	5,6kΩ (+28%)
DOUBLE_2k2_4k7	4,1kΩ (-13%)	4,7kΩ	5,4kΩ (+15%)	6kΩ (-14%)	6,9kΩ	7,9kΩ (+15%)
DOUBLE_2K7_8K2	7,2 kΩ (-13%)	8,2kΩ	9,2kΩ (+13%)	9,9kΩ (-10%)	10,9kΩ	11,9kΩ (+10%)
DOUBLE_3K0_3	2,1kΩ	3,0kΩ	3,9kΩ	4,5kΩ	6kΩ	7,5kΩ

K0	(-30%)		(+30%)	(-25%)		(+25%)
DOUBLE_3K3_3 K3	2,3kΩ (-26%)	3,3kΩ	4,3kΩ (+31%)	4,9kΩ (-26%)	6,6kΩ	8,3kΩ (+26%)
DOUBLE_3K9_8 K2	7,0 kΩ (-15%)	8,2kΩ	9,5kΩ (+16%)	10,5kΩ (-14%)	12,1kΩ	13,8kΩ (+15%)
DOUBLE_4K7_2 K2	1,6kΩ (-28%)	2,2KΩ	2,9kΩ (+32%)	5kΩ (-28%)	6,9kΩ	8,8kΩ (+28%)
DOUBLE_4K7_4 K7	3,3kΩ (-30%)	4,7kΩ	6,1kΩ (+30%)	7kΩ (-26%)	9,4kΩ	11,9kΩ (+27%)
DOUBLE_5K6_5 K6	4,0kΩ (-26%)	5,6kΩ	7,2kΩ (+29%)	8,3kΩ (-26%)	11,2kΩ	14,1kΩ (+26%)
DOUBLE_6K8_4 K7	3,3kΩ (-30%)	4,7kΩ	6,1kΩ (+30%)	8,1kΩ (-30%)	11,5kΩ	14,9kΩ (+30%)
DOUBLE_2k2_1 0K	9,2kΩ (-8%)	10kΩ	10,8kΩ (+8%)	11,3 kΩ (-8%)	12,2kΩ	13,2kΩ (+9%)
DOUBLE_10k_1 0k	7,5kΩ (-25%)	10kΩ	12,5kΩ (+25%)	17kΩ (-15%)	20kΩ	23kΩ (+15%)

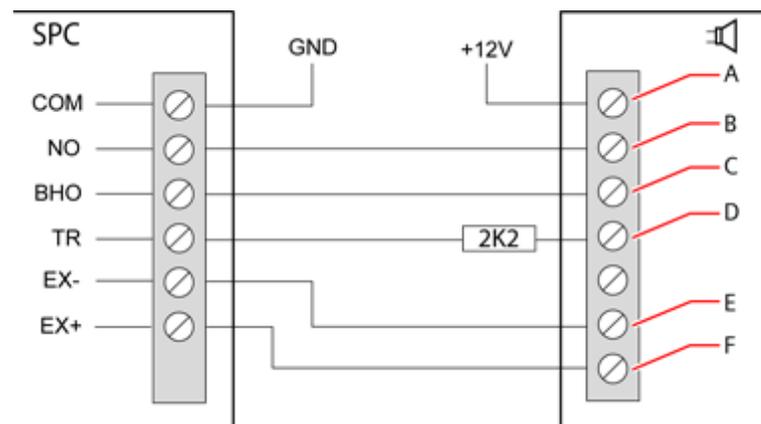


Pour tous les types de résistances de fin de ligne, une résistance inférieure à 300Ω est considéré comme un court-circuit. Si la résistance n'est pas au-dessus du seuil, elle est traitée comme déconnexion.

10.6 Câblage d'une sirène extérieure SAB

Sur une sirène extérieure raccordée à la carte de la centrale 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 de la centrale entre les bornes BHO et TR. Pour le câblage d'une sirène extérieure, connectez cette résistance en série de la borne TR de la centrale à la borne TR de l'interface de la sirène.



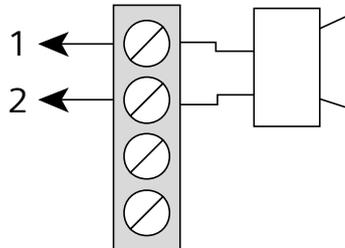
Câblage d'une sirène extérieure

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 centrale SPC, reliez les bornes IN+ et IN- directement à l'entrée 12 V du buzzer.



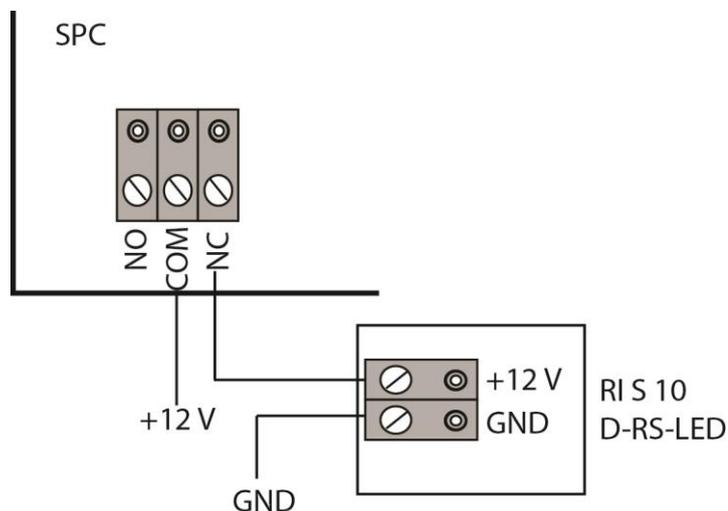
Câblage du buzzer interne (12 V)

IN-	IN- (centrale SPC)
IN+	IN+ (centrale SPC)

10.8 Câblage du Bris de verre

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

Le diagramme suivant montre comment l'interface de bris de verre 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 verre à une zone, voir la documentation spécifique au produit.

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

10.9 Installation des modules d'extension

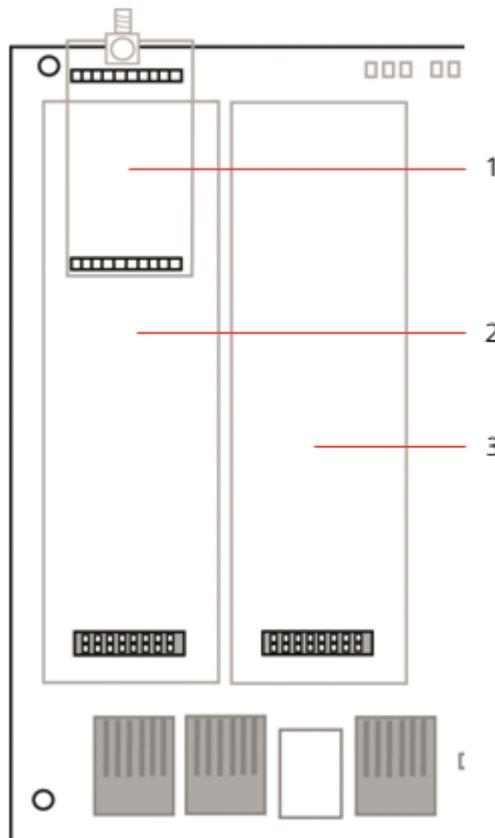
2 modems (RTC ou GSM) peuvent être installés sur la centrale pour accroître les fonctions. La figure ci-dessous montre les deux emplacements disponibles pour les modems, le module primaire (emplacement gauche) et un module de secours (emplacement droit).

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 à la centrale en mode Paramétrage. Configurez et enregistrez la configuration. Si vous ne suivez pas cette procédure, vous obtiendrez une erreur CRC.



Modules d'extension

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



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

11 Mise sous tension de la centrale SPC

La centrale SPC est alimenté par deux sources d'énergie : le secteur 230V et la batterie intégrée. Le branchement au secteur devrait être confié à un électricien qualifié. L'alimentation secteur devrait être branchée sur une ligne de dérivation isolable. Voir ici [→ 365] toutes les informations nécessaires au dimensionnement des câbles électriques, des fusibles, etc.

La centrale SPC devrait être mis sous tension dans l'ordre suivant : 1 - alimentation sur secteur, 2 - batterie intégrée. Pour assurer la conformité aux normes EN, installez une seule batterie de la capacité appropriée.

11.1 Mise sous tension avec seulement la batterie

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 puissance inférieure à 12 V sans alimentation principale.



AVIS

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 puissance 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

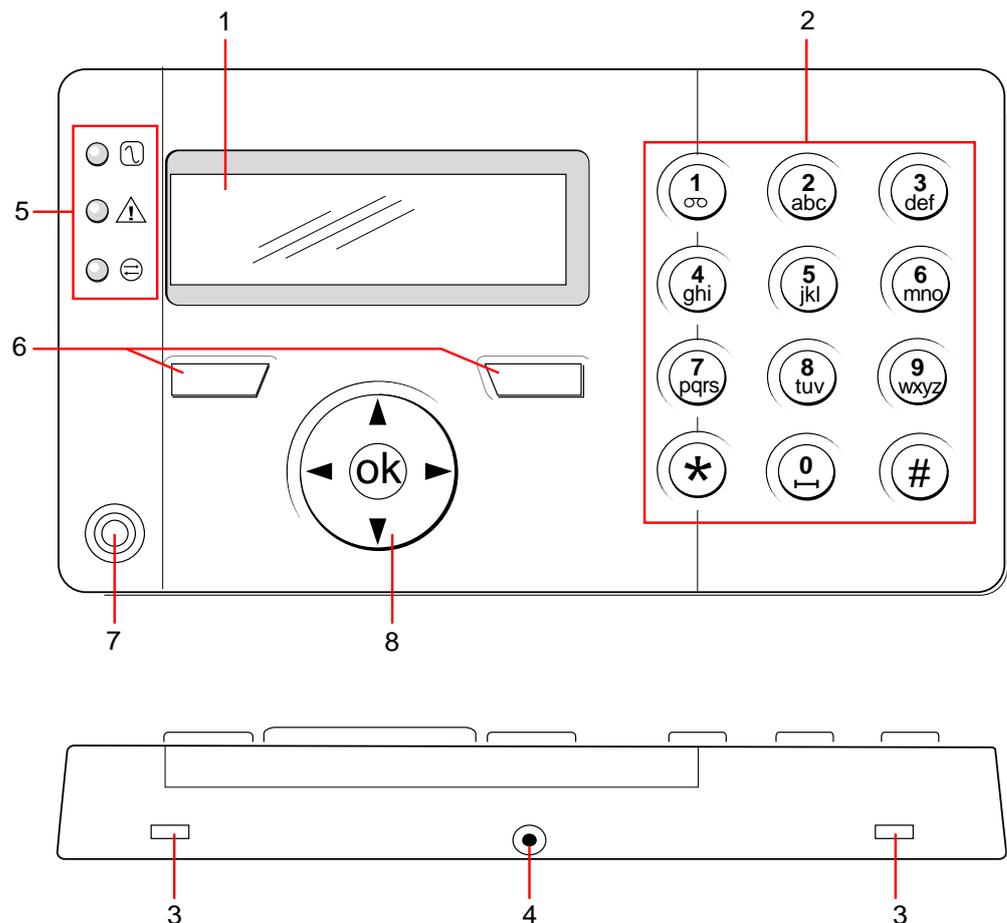
12.1.1 Introduction

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

- **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). (Veuillez vous reporter au Manuel de l'utilisateur SPCK420/421 pour obtenir de plus amples informations sur la programmation 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 ici [→ 362]).

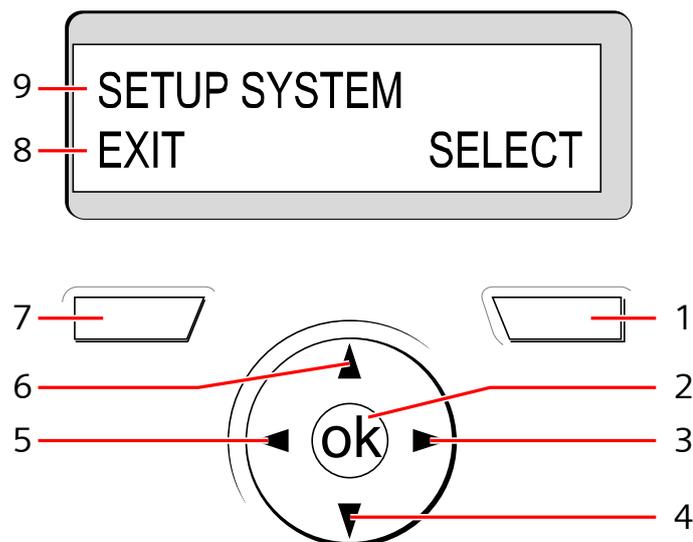


Clavier LCD

1	Écran LCD	L'afficheur (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 ajuster le contraste de l'afficheur ainsi que les conditions d'activation du rétroéclairage.
2	Touches alphanumériques	Le pavé alphanumérique permet d'entrer du texte et les valeurs numériques pendant la programmation. Les signes alphabétiques sont sélectionnés en appuyant plusieurs fois sur une touche. Pour passer des lettres minuscules aux majuscules, appuyez sur la touche dièse (#). Pour entrer un chiffre, appuyez sur la touche correspondante pendant 2 secondes.
3	Languettes d'ouverture du couvercle	Ces languettes d'ouverture du couvercle permettent d'accéder aux clips d'assemblage de l'embase et du couvercle. Insérez un tournevis plat dans la fente entre le boîtier et la base et exercez une légère pression sur le tournevis (5 mm) pour désengager le boîtier de l'embase.
4	Vis de fixation arrière	Cette vis fixe solidement le couvercle et l'embase. Enlevez la vis avant d'ouvrir le clavier.
5	Témoins LED d'état	Ces témoins lumineux fournissent une information sur l'état du système. Voir le tableau ci-dessous.
6	Touches programmables	Les touches programmables à droite et à gauche sous l'écran sont des touches contextuelles servant à naviguer dans les menus/la programmation.
7	Récepteur du lecteur de badge de proximité	Si le clavier est équipé d'un lecteur de badge de proximité (voir ici → 362)], 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 multi-fonctions	La touche de navigation multi-fonctions utilisée en combinaison avec l'afficheur constitue l'interface utilisateur servant à la programmation du système.

TÉMOIN		Etat
Alimentation secteur (Vert)		Indique si le clavier est branché sur le secteur, ou s'il y a une panne de courant. CLIGNOTEMENT : défaut secteur détecté PERMANENT : alimentation secteur sans défaut
Alerte système (Jaune)		Indique une alerte système CLIGNOTEMENT : alerte système détectée ; la nature de l'alerte et l'emplacement sont indiqués sur l'afficheur. Si le système est en service (MES), les alertes système ne sont PAS indiquées. ÉTEINT : aucune alerte détectée. Si un clavier est attribué à plus d'un secteur, le témoin LED n'indique pas d'alerte si l'un de ces secteurs est en service (MES).
État du X-BUS (Rouge)		Indique l'état des communications du X-BUS lors de la programmation en MODE PARAMETRAGE. 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 de la centrale du X-BUS soit établie.

12.1.2 Utilisation de l'interface du clavier LCD



Afficheur du clavier

1	TOUCHE PROGRAMMABLE DROITE	Cette touche est utilisée pour sélectionner l'option affichée dans la deuxième ligne à droite. Les valeurs disponibles sont : → SELECT pour sélectionner l'option affichée dans la première ligne ENTRER pour entrer la donnée affichée dans la première ligne. → SUIVANT pour voir l'alerte suivante celle affichée dans la première ligne → EFFACER pour effacer l'alerte affichée dans la première ligne → SAUVER pour enregistrer un paramètre.
2	OK	Le bouton OK a la fonction de la touche SELECT appliquée à l'option affichée dans la première ligne, et également celle d'ENTRER/SAUVER pour les données affichées dans la première ligne.
3		En mode Programmation, la touche de direction droite sert à avancer dans les menus de la même manière qu'avec l'option SELECT (touche programmable

		droite). En mode de saisie des données, appuyez sur cette touche pour déplacer le curseur d'une position vers la droite.
4	▼	En mode Programmation, la touche de direction vers le bas permet d'atteindre l'option de programmation suivante du même niveau du sous-menu. Pour faire défiler toutes les options disponibles dans le menu actif, maintenez cette touche enfoncée. En mode alphanumérique, appuyez sur cette touche pour changer la lettre majuscule sélectionnée en lettre minuscule. Quand des alertes sont affichées, la touche de direction vers le bas permet d'atteindre le message d'alerte suivant par ordre de priorité. (Voir la section Définition de la priorité d'affichage des messages).
5	◀	En mode Programmation, la touche de direction gauche permet de passer au niveau de menu précédent. Quand vous êtes au niveau supérieur du menu, appuyez sur cette touche pour quitter le mode Programmation. En mode de saisie des données, appuyez sur cette touche pour déplacer le curseur d'une position vers la gauche.
6	▲	En mode Programmation, la touche de direction vers le haut permet d'atteindre l'option de programmation précédente du même niveau du menu. Pour faire défiler toutes les options disponibles dans le menu actif, maintenez cette touche enfoncée. En mode alphanumérique, appuyez sur cette touche pour changer la lettre minuscule sélectionnée en majuscule.
7	TOUCHE PROGRAMMABLE GAUCHE	Cette touche est utilisée pour sélectionner l'option affichée dans la deuxième ligne à gauche. Les valeurs disponibles sont : → SORTIE pour quitter la programmation → RETOUR pour retourner au menu précédent
8	LIGNE INFÉRIEURE DE L'AFFICHEUR	Pendant une période d'inactivité prolongée, cette ligne est vide. En mode Programmation, cette ligne affiche les options disponibles. Ces options sont alignées au-dessus du bouton programmable droit ou gauche correspondant pour faciliter la sélection.
9	LIGNE SUPÉRIEURE DE L'AFFICHEUR	Pendant une période d'inactivité prolongée, la date et l'heure sont affichées. En mode Programmation, cette ligne affiche l'une des informations suivantes : → La fonction de programmation à sélectionner. → Le réglage actuel de la fonction sélectionnée. → La nature de l'alerte en cours pendant une condition d'alerte. (Voir ci-dessous : Définition de la priorité d'affichage des messages.)

Définition de la priorité d'affichage des messages

Les messages et alertes d'anomalie sont affichés sur le clavier dans l'ordre suivant :

- Zone
 - Alarmes
 - Autosurveillance
 - Anomalie
- Alertes secteur
 - Échec MES
 - Dépassement temps d'entrée
 - Code autosurveillance
- Alertes système
 - Alimentation
 - Batterie
 - Défaut Chargeur
 - Défaut Aux

- Fusible sirène extérieure
- Fusible sirène int.
- Autosurv. sirène
- Autosurveillance coffret
- Auxil. Autopr.1
- Auxil. Autopr.2
- Brouillage radio
- Défaut Modem 1
- Ligne Modem 1
- Défaut Modem 2
- Ligne Modem 2
- Erreur de communication
- Panique utilis.
- Défaut câble X-BUS
- Communication XBUS perdue
- XBUS Défaut 230V
- XBUS Défaut batterie
- XBUS Défaut d'alimentation électrique
- XBUS Défaut fus.
- XBUS Défaut autosurveillance
- XBUS Défaut antenne
- XBUS Problème radio
- XBUS Panique
- XBUS Feu
- XBUS Médical
- XBUS Lien alimentation
- XBUS Autosurveillance sortie
- XBUS Basse tension
- Resets ingénieur nécessaires
- Armement automatique
- Informations du système
 - Zones testées
 - Zones ouvertes
 - Etat du secteur
 - Batterie faible (détecteur)
 - Détecteur perdu
 - WPA Batterie faible
 - WPA perdu
 - WPA Test non reçu
 - Caméra offline
 - Batterie tag faible
 - Surintensité Xbus
 - Nom de l'installateur
 - N° téléphone installateur
 - Tech. autorisé

- Construct. valid
- Redémarrage
- Défaut hardware
- Surconsommation aux.
- Batterie faible
- Lien 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 décrite ci-dessous.

Saisie de valeurs numériques

En mode de saisie numérique, seules des valeurs numériques peuvent être entrées (0 - 9).

- Pour déplacer le curseur à droite ou à gauche, appuyez sur la touche de direction droite ou gauche.
- Pour quitter la fonction sans enregistrer, appuyez sur le bouton RETOUR.
- Pour enregistrer le réglage programmé, appuyez sur ENTRER ou OK.

Saisie de texte

En mode de saisie de texte, vous pouvez entrer des valeurs alphabétiques (A-Z) et des valeurs numériques (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 entrer un chiffre, appuyez sur la touche correspondante pendant 2 secondes avant de relâcher.
- Pour déplacer le curseur à droite ou à gauche, appuyez sur la touche de direction droite ou gauche.
- Pour quitter la fonction sans enregistrer, appuyez sur RETOUR.
- Pour enregistrer le réglage programmé, appuyez sur ENTRER ou OK.
- Pour changer la casse d'une lettre alphabétique, positionnez le curseur sur la lettre et appuyez sur la touche de direction bas/haut.
- Pour changer la casse de tous les caractères suivants entrés, appuyez sur la touche dièse (#), puis entrez le texte voulu.
- Pour effacer les caractères à gauche du curseur, appuyez sur la touche étoile (*).

Sélection d'une option de programmation

En mode navigation, l'installateur ou l'utilisateur sélectionne une option parmi plusieurs options prédéfinies dans une liste.

- Pour faire défiler la liste des options disponibles, appuyez sur les touches de direction haut et bas.
- Pour quitter la fonction sans enregistrer, appuyez sur RETOUR.

- Pour enregistrer l'option sélectionnée, appuyez sur SAUVER ou OK.

12.2 SPCK620/623

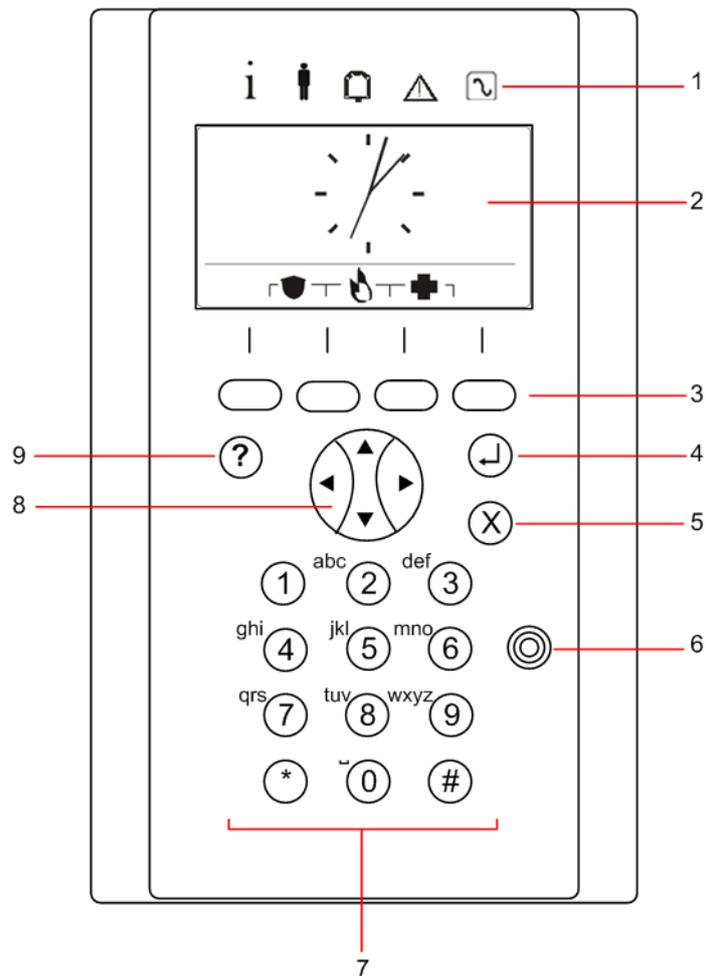
12.2.1 Introduction

Le clavier confort est une interface murale permettant :

- 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). (Veuillez vous reporter au Manuel de l'utilisateur SPC620/623 pour obtenir de plus amples informations sur la programmation utilisateur.)

Le SPCK620 possède des touches programmables et un écran LCD graphique facilitant l'utilisation. Ses fonctions peuvent être étendues en ajoutant le transpondeur d'interrupteur à clé SPCE110 ou le transpondeur d'indication SPCE120.

Le SPCK623 est équipé d'un lecteur de badges de proximité (125 kHz EM 4102) facilitant l'accès des utilisateurs, de touches programmables, d'un grand écran LCD graphique et de fonctions d'annonce vocale. Ses fonctions peuvent être étendues en ajoutant le transpondeur d'interrupteur à clé SPCE110 ou le transpondeur d'indication SPCE120.



1	Témoins LED d'état	Ces témoins lumineux fournissent une information sur l'état du système. Voir le tableau ci-dessous.
2	Écran 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). (Consultez la section sur la définition de la priorité d'affichage des messages.) Vous pouvez configurer les conditions d'activation du rétroéclairage.
3	Touches programmables	Touches contextuelles permettant de naviguer dans les menus et la programmation.
4	Touche ENTRER	Permet de confirmer un élément affiché ou la valeur entrée.
5	Touche RETOUR	<ul style="list-style-type: none"> ● Permet de retourner au menu précédent. Permet de réinitialiser les buzzers, la sirène et les alarmes dans la mémoire.
6	Récepteur du lecteur de badge de proximité	Uniquement SPCK 623 : si le clavier est équipé d'un lecteur de badge de proximité, présentez le badge, le tag ou la télécommande à moins de 1 cm de cette zone.
7	Touches alphanumériques	Le pavé alphanumérique permet d'entrer du texte et les valeurs numériques pendant la programmation. Les signes alphabétiques sont sélectionnés en appuyant plusieurs fois sur une touche. Pour passer des lettres minuscules aux majuscules, appuyez sur la touche dièse (#). Pour entrer un chiffre, appuyez sur la touche correspondante

		pendant 2 secondes.
8	Touche de navigation multifonctions	Navigation dans les menus et dans les messages d'alerte. (Voir ci-dessous : Définition de la priorité d'affichage des messages.)
9	Touche Information	Permet d'afficher les informations.

Définition de la priorité d'affichage des messages

Les messages et alertes d'anomalie sont affichés sur le clavier dans l'ordre suivant :

- Zone
 - Alarmes
 - Autosurveillance
 - Anomalie
- Alertes secteur
 - Échec MES
 - Dépassement temps d'entrée
 - Code autosurveillance
- Alertes système
 - Alimentation
 - Batterie
 - Défaut Chargeur
 - Défaut Aux
 - Fusible sirène extérieure
 - Fusible sirène int.
 - Autosurv. sirène
 - Autosurveillance coffret
 - Auxil. Autopr.1
 - Auxil. Autopr.2
 - Brouillage radio
 - Défaut Modem 1
 - Ligne Modem 1
 - Défaut Modem 2
 - Ligne Modem 2
 - Erreur de communication
 - Panique utilis.
 - Défaut câble X-BUS
 - Communication XBUS perdue
 - XBUS Défaut 230V
 - XBUS Défaut batterie
 - XBUS Défaut d'alimentation électrique
 - XBUS Défaut fus.
 - XBUS Défaut autosurveillance
 - XBUS Défaut antenne
 - XBUS Problème radio
 - XBUS Panique

- XBUS Feu
- XBUS Médical
- XBUS Lien alimentation
- XBUS Autosurveillance sortie
- XBUS Basse tension
- Resets ingénieur nécessaires
- Armement automatique
- Informations du système
 - Zones testées
 - Zones ouvertes
 - Etat du secteur
 - Batterie faible (détecteur)
 - Détecteur perdu
 - WPA Batterie faible
 - WPA perdu
 - WPA Test non reçu
 - Caméra offline
 - Batterie tag faible
 - Surintensité Xbus
 - Nom de l'installateur
 - N° téléphone installateur
 - Tech. autorisé
 - Construct. valid
 - Redémarrage
 - Défaut hardware
 - Surconsommation aux.
 - Batterie faible
 - Lien Ethernet
 - Nom du système

12.2.2 Description des témoins LED

Description	Symbol e	Couleur	Fonctionnem ent	Description
Informations	i	Bleu	Actif	Le système ou le secteur ne peut pas être mis en service. La mise en service forcée est possible (les erreurs ou les zones ouvertes peuvent être désactivées).
			Clignotant	Le système ou le secteur ne peut pas être mis en service ni être forcé (les erreurs ou les zones ouvertes ne peuvent pas être désactivées).
			Inactif	Le système ou le secteur peut être mis en service.
		Orange	Clignotant	L'installateur est sur le site.
Utilisateur		Vert	Actif	Le secteur attribué est mis hors

				surveillance.
			Clignotant	Le secteur attribué est en MES partielle A / B.
			Inactif	Le secteur attribué est en surveillance totale.
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 au bus

	AVIS
	Les témoins LED d'information, d'état du secteur, d'alarme et de défaut sont désactivés pendant que le clavier est au repos. Un code d'accès d'utilisateur doit être entré. Le réglage peut être modifié quand l'indicateur de mise sous tension est visible pendant la période de repos.

12.2.3 Description du mode d'affichage

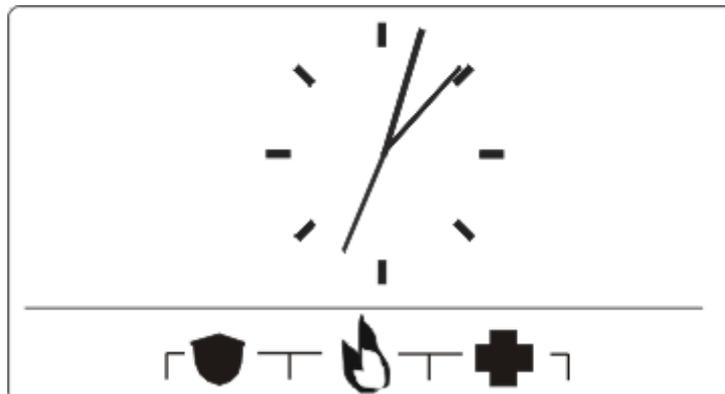
Deux modes d'affichage sont disponibles (automatiques) :

- Affichage de plusieurs secteurs : L'utilisateur peut accéder à plusieurs secteurs. Les secteurs sont affichés par groupes. Si aucun groupe de secteurs n'est configuré, seul le groupe général TOUS SECTEURS est affiché.
- Affichage d'un secteur unique : l'utilisateur ne dispose des droits que pour un secteur. En mode d'affichage d'un secteur unique, un seul secteur est affiché en lettres capitales. Il est paramétré directement.

	AVIS
	Les droits d'accès d'un utilisateur peuvent être limités par les paramètres utilisateur ou par les paramètres du clavier utilisé. Ce n'est que lorsque l'utilisateur et le clavier sur lequel il se connecte possèdent tous les deux les droits d'accès à un secteur que ce secteur est affiché. Si l'utilisateur possède les droits d'accès pour plusieurs secteurs mais que le clavier a des droits limités à 1 secteur, l'utilisateur ne pourra accéder qu'à ce seul secteur.

12.2.4 Touches de fonction au repos

Urgence

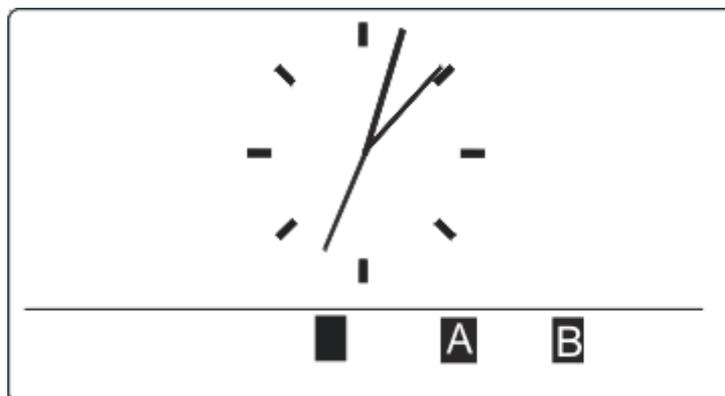


Plusieurs touches d'urgence sont affichées suivant la configuration active. Une pression simultanée sur les touches déclenche un appel d'urgence.

	Panic Alarm
	Alarme Incendie
	Medical Alarm

La procédure déclenchée dépend de la configuration du système. Demandez les détails à l'installateur.

Paramètres directs



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

13 Outils logiciels

Les outils logiciel exécutables sur PC suivants sont disponibles pour la gestion distante 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.
- **SPC Safe**
Pour la gestion distante et automatique d'un système SPC.
- **SPC Remote Maintenance**
Pour la surveillance et l'entretien distants et automatiques d'un système SPC.

14 Démarrage du système

	⚠ ATTENTION
	Le système SPC doit être installé par un installateur approuvé.

1. Connectez le clavier à l'interface X-BUS de la centrale.
2. Activez le mode de programmation Installateur en entrant le code d'installateur par défaut (1111). Pour plus de détails, voir Codes Installateur [→ 110].

14.1 Modes de programmation

Le système SPC fonctionne selon 2 modes de programmation utilisables par les installateurs autorisés : le mode Paramétrage et le mode Exploitation. Dans le navigateur, l'utilisateur ne peut se déconnecter qu'en mode Exploitation.

Mode Paramétrage



Toutes les alertes, les défauts et les alarmes d'autosurveillance doivent d'abord être isolées ou effacées avant de pouvoir quitter le mode Paramétrage.

Le mode Paramétrage offre des fonctions de programmation avancées. Toutefois, tous les paramètres d'alarme, les rapports et la programmation des sorties du système sont désactivés pendant la programmation en mode Paramétrage. Voir la description détaillée des options de menu en mode Paramétrage ici [→ 118].

Mode Exploitation

Réduit à l'utile, le mode Exploitation offre moins de fonctions de programmation et n'affecte aucune sortie programmée dans le système. Voir la description détaillée des options de menu en mode Exploitation ici [→ 117].

14.1.1 Codes 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, quelque soit le moment suivant le démarrage, tous les codes seront affublés du préfixe « 0 ». Le code par défaut de l'installateur devient donc « 01111 ».

L'augmentation du nombre de chiffres du code (voir Options Système [→ 236]) provoque l'ajout de zéros à gauche du code existant, par exemple 001111 pour un code à 6 chiffres).

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

14.2 Outils de programmation

Clavier

Le clavier permet un accès rapide sur place aux menus et à la programmation du système. L'installateur autorisé est chargé de définir des configurations initiales par défaut en utilisant le clavier. La programmation du lecteur de badge de proximité et l'attribution aux utilisateurs sont également effectuées à l'aide du clavier.

SPC Pro

Pro SPC est une application logicielle permettant de configurer les systèmes SPC en ligne et hors ligne. La programmation avec Pro SPC offre des fonctions de communication avancées et le protocole X10 que ne possède pas le clavier. La mise à niveau du firmware n'est possible qu'avec Pro SPC.

ProSPC prend en charge les connexions USB, Serial, Ethernet et modem RTC/GSM vers une centrale SPC.

14.2.1 Programmeur Rapide

Le programmeur rapide du SPC est un dispositif de stockage mobile permettant à l'installateur de télécharger et de télécharger les fichiers de configuration rapidement et efficacement. Le programmeur rapide peut être utilisé en combinaison avec tous les autres outils de programmation indiqués. Pour les détails, voir ici [→ 328].

Le programmeur rapide sert à exécuter la mise à jour du micrologiciel (firmware).

14.3 Configuration des paramètres de démarrage

Les paramètres de démarrage suivants pourront être modifiés ultérieurement lors de la programmation des fonctions du système.



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

Condition requise :

- ▷ 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 la région appropriée.
 - EUROPE, SUÈDE, SUISSE, BELGIQUE, ESPAGNE, R-U, IRLANDE, ITALIE, CANADA, USA
- 4. Choisissez le TYPE d'installation :
 - SIMPLE : appropriée pour l'utilisation par les particuliers (maisons individuelles et appartements).
 - EVOLUEE : met à disposition des types de zones supplémentaires et des descriptions (par défaut) de zone évoluée pour les 8 premières zones.
 - BANCAIRE : spécifique aux 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, Evolué et Bancaire [→ 355].

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

!	<p>AVIS</p> <p>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.</p>
----------	---

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, consultez les sections « Mise à jour des langues » pour le clavier, le navigateur et SPC Pro.
8. Saisissez la DATE et l'HEURE.
 - ⇒ Le système scanne le X-BUS à la recherche de modems.
9. Choisissez le mode adressage X-BUS :
 - MANUEL : mode recommandé pour la plupart des types d'installation, en particulier si une préconfiguration est effectuée.
 - AUTO : recommandé seulement for des installations de très petite taille.
10. Choisissez la topologie de l'installation : UNE BOUCLE (anneau) ou DEUX BRANCHES (chaîne).
 - ⇒ Le système balaye le système pour déterminer la quantité de claviers, transpondeurs, contrôleurs de portes et les entrées de zone disponibles.
11. Appuyez sur SUIVANT pour scanner tous les périphériques X-BUS.
 - ⇒ Le MODE DE PROGRAMMATION est affiché.
 - ⇒ Le paramétrage du démarrage est terminé.
12. Vérifiez les alertes dans le menu ETAT DU SYSTEME > ALERTES. Sinon, vous ne pourrez pas quitter le mode Paramétrage.
13. Configurez le système via le clavier, SPC Pro ou le navigateur web.

Voir aussi

- ▣ Paramètres par défaut des modes Simple, Evolué et Bancaire [→ 355]

14.4 Créer les utilisateurs du 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.

Consultez la section Ajouter Utilisateur :



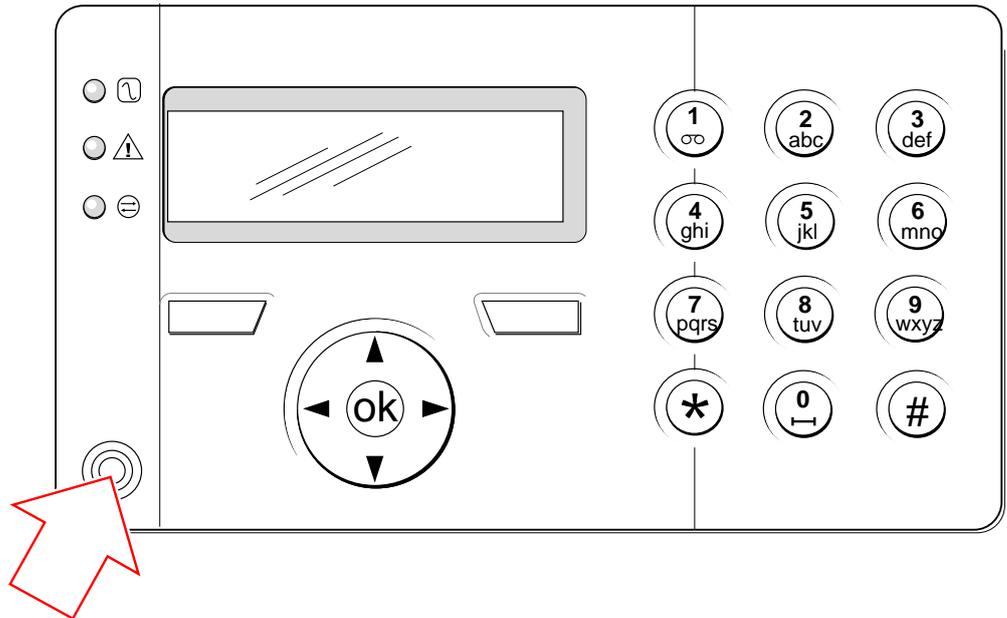
Un éventuel accès du fabricant au système (par ex. pour mise à niveau du firmware de la centrale) doit être configuré comme un droit d'utilisateur affecté à un profil d'utilisateur. Pour permettre à un utilisateur d'effectuer des mises à niveau du firmware, assurez-vous que le profil correct lui a été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

Voir aussi

- ▣ Codes Installateur [→ 110]

14.5 Programmation d'un tag PACE

Le clavier SPC possède (suivant le modèle) un lecteur de badge de proximité/tag. Les utilisateurs ayant un profil configuré de manière correspondante peuvent armer ou désarmer le système à distance, mais aussi procéder à la programmation à distance en fonction des autorisations du profil. Si un badge de proximité ou un tag ont été programmés sur le clavier, l'utilisateur peut armer/désarmer le système ou accéder à la programmation en présentant le badge ou le tag à moins de 1 cm de la zone du récepteur.



Zone du récepteur sur le clavier

Pour programmer un badge ou un tag sur le clavier :

1. Entrez le code d'installateur. (Le code par défaut est 1111. Voir Codes Installateur [→ 110].)
2. Sélectionnez le menu GESTION UTILISAT.
3. Appuyez sur SELECT.
4. Sélectionnez EDITER, puis UTILISATEUR1 dans la liste.
5. Sélectionnez TAG et appuyez sur SELECT.
6. Activez ou désactivez la prise en charge des tags PACE en utilisant les touches de direction bas/haut.
 - ⇒ Le texte PRESENTER LE TAG clignote dans la ligne supérieure de l'afficheur.
7. Présentez le badge ou le tag PACE à moins de 1 cm de la zone du récepteur du clavier.
 - ⇒ Le texte TAG CONFIGURE sur l'afficheur indique que le badge ou le tag est enregistré.

Pour désactiver un badge ou un tag avec le clavier :

1. Entrez le code d'installateur. (Le code par défaut est 1111. Voir Codes Installateur [→ 110].)
2. Sélectionnez le menu GESTION UTILISAT.
3. Appuyez sur SELECT.
4. Sélectionnez EDITER, puis UTILISATEUR1 dans la liste.
5. Sélectionnez TAG et appuyez sur SELECT.
6. Sélectionnez DEVALIDE.
 - ⇒ Le message MISE A JOUR est affiché sur le clavier.

14.6 Programmation des tags sans fil

Si un module de récepteur radio 868 MHz est installé sur le clavier ou sur la centrale, une télécommande/porte-clé radio peut être programmée avec le clavier.

Pour programmer une télécommande radio dans le système :

1. Entrez le code d'installateur (le code par défaut est 1111. (Voir Codes Installateur [→ 110]).
2. Utilisez les touches de direction bas/haut pour afficher l'option GESTION UTILISAT.
3. Appuyez sur SELECT.
4. Sélectionnez l'option EDITER et appuyez sur SELECT.
5. Sélectionnez l'utilisateur voulu et appuyez sur SELECT.
6. Sélectionnez l'option TELEC. RADIO et appuyez sur SELECT.
7. Sélectionnez VALIDE et appuyez sur SELECT.
 - ⇒ Le message APPUYER TOUCHE clignote dans la ligne supérieure de l'afficheur.
8. Appuyez sur une touche de la télécommande. Celle-ci doit être à moins de 8 mètres du clavier.
 - ⇒ Le message TELEC.CONFIGUREE indique que la télécommande est opérationnelle.

Pour désactiver une télécommande radio dans le système :

1. Entrez le code d'installateur (le code par défaut est 1111. (Voir Codes Installateur [→ 110]).
2. Utilisez les touches de direction bas/haut pour afficher l'option GESTION UTILISAT.
3. Sélectionnez l'option EDITER et appuyez sur SELECT.
4. Sélectionnez l'utilisateur voulu et appuyez sur SELECT.
5. Sélectionnez l'option TELEC. RADIO et appuyez sur SELECT.
6. Sélectionnez DESACTIVE et appuyez sur SAUVER.



Si le système ne détecte aucun récepteur radio 868 MHz, l'option TELEC. RADIO n'est pas affichée dans le menu.



Nombre de télécommandes radio par utilisateur : Une seule télécommande par utilisateur est programmable. Pour échanger les télécommandes entre les utilisateurs, répétez les étapes de programmation pour chaque nouvelle télécommande. Les anciennes télécommandes peuvent être utilisées par les autres 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. Les alertes peuvent également être effacées 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. Sélectionnez RAZ AL. TELEC. et appuyez sur SELECT.
5. Sélectionnez VALIDE et appuyez sur SAUVER.

15 Programmation en mode Exploitation avec le clavier

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

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

1. Entrez un code d'installateur valable (le code par défaut est 1111. Pour plus de détails, voir Codes Installateur [→ 110]).
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.

1	ARMEMENT	Permet de mettre le système à l'ARRET, en MES TOTALE, ou en MES PARTIELLE. Voir ici
2	INHIBER	Affiche une liste des zones désactivées du système. Voir page
3	ISOLER	Permet à l'installateur d'isoler des zones choisies. Voir ici [→ 161]
4	JOURNAL DE BORD	Affiche une liste des derniers événements détectés par le système. Voir ici [→ 161]
5	ACCES JDB	Affiche une liste des derniers accès au système. Voir ici
6	JOURNAL DES ALARMES	Affiche la liste des alarmes récentes.
7	CHANGER SON CODE	Permet à l'installateur de modifier le code d'accès d'installateur. Voir ici [→ 162]
8	GESTION UTILISAT	Permet à l'installateur de créer, de modifier ou d'effacer des utilisateurs. Voir ici [→ 163]
9	SMS	Permet à l'utilisateur d'ajouter, éditer ou supprimer les détails de SMS pour les utilisateurs. Voir SMS [→ 167]

Voir aussi

- 📖 TEST [→ 156]
- 📖 CONTROLE PORTES [→ 171]
- 📖 Programmation en mode Paramétrage avec le clavier [→ 118]
- 📖 TEXTE INSTALLAT. [→ 170]
- 📖 MODIF DATE/HEURE [→ 170]
- 📖 SMS [→ 167]

16 Programmation en mode Paramétrage avec le clavier

Cette page décrit les options de programmation en mode Paramétrage avec le clavier.

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

1. Entrez un code d'installateur valable (le code par défaut est 1111. Pour plus de détails, voir Codes Installateur [→ 110]).
 2. Appuyez sur SELECT pour accéder au MODE PARAMETRAGE.
 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).
- ⇒ Après la fin d'une opération de programmation, le message MISE A JOUR est affiché pendant un court instant.

16.1 ETAT DU SYSTEME

Le menu Etat du Système permet de consulter toutes les erreurs qui se sont produites.

Pour afficher ces erreurs :

1. sélectionnez le menu ETAT DU SYSTEME.
 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.
AFFICH ECHEC MES	Affiche toutes les zones dont l'activation a échoué. Sélectionnez chacune des zone pour afficher des détails sur la raison de la non-activation.
BATTERIE	Affiche la durée restante de batterie, le voltage 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 le temps de batterie restant sur le clavier, événement panne de secteur. Le temps est affiché 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.

	AVIS
	Les utilisateurs ne peuvent pas quitter le MODE PARAMETRAGE tant qu'un défaut est actif. Le premier défaut est affiché sur le clavier si vous essayez de quitter le mode de programmation. Vous pouvez visualiser et isoler tous les défauts sous ALERTES et AFF. ZONE OUVERT dans le menu ETAT DU SYSTEME.

16.2 OPTIONS

1. Sélectionnez OPTIONS et appuyez sur SELECT.
 2. Sélectionnez l'option de programmation souhaitée :
- ⇒ 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 dans le cadre de l'assistant de démarrage.

Variable	Description	Défaut
NIVEAU SECURITE	<p>Détermine le niveau de sécurité de l'installation SPC.</p> <ul style="list-style-type: none"> ● Irlande et Europe : <ul style="list-style-type: none"> - EN50131 GRADE 2 - EN50131 GRADE 3 - Pas de restriction ● Royaume-Uni : <ul style="list-style-type: none"> - PD6662 (basée sur EN50131 Grade 2) - PD6662 (basée sur EN50131 Grade 3) - Pas de restriction ● Suède : <ul style="list-style-type: none"> - SSF1014:3 Larmclass 1 - SSF1014:3 Larmclass 2 - Pas de restriction ● Belgique : <ul style="list-style-type: none"> - TO-14 (basée sur EN50131 Grade 2) - TO-14 (basée sur EN50131 Grade 3) - Pas de restriction ● Suisse : <ul style="list-style-type: none"> - SWISSI Cat 1 - SWISSI CAT 2 - Pas de restriction ● Espagne <ul style="list-style-type: none"> - EN50131 GRADE 2 - EN50131 Grade 3 ● Allemagne <ul style="list-style-type: none"> - VdS Classe A 	Grade : 2 Pays : non disponible

Variable	Description	Défaut
	<ul style="list-style-type: none"> - VdS Classe C - Pas de restriction ● France <ul style="list-style-type: none"> - NF type 2 - NF type 3 - Pas de restriction 	
SPECIFICITE PAYS	Détermine les contraintes locales spécifiques auxquelles répond l'installation. Les options sont ROYAUME-UNI, IRLANDE, EUROPE, SUEDE, 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 EVOLUEE (voir la ici [→ 338]), SIMPLE (voir ici [→ 337]) ou BANCAIRE.	Simple

Pour tous les détails des OPTIONS suivantes, reportez-vous au chapitre Options système [→ 236].

MES PART. A	RENOMMER TEMPORISEE Z.ACCES -> TEMPO Z.TEMPO -> IMMEDIA ALARME LOCALE
MES PART. B	RENOMMER TEMPORISEE Z.ACCES -> TEMPO Z.TEMPO -> IMMEDIA ALARME LOCALE
MSG SI APPEL CTS	AFFICHER MESSAGE (VALIDE/DEVALIDE)
CONFIRMATION	VDS DD243 : GARDA EN50131-9
CONFIRMER ZONES	Sélectionnez le NOMBRE DE ZONES.
RAZ ALARME AUTO	VALIDE/DEVALIDE
RAZ AL. TELEC.	VALIDE/DEVALIDE
CONTRAINTE	DEVALIDE CODE +1 CODE +2
REDECL.SIRENE	VALIDE/DEVALIDE
SIRENE IMMEDIATE	VALIDE/DEVALIDE
SIR. ECHEC MES	VALIDE/DEVALIDE
FLASH ECHEC MES	VALIDE/DEVALIDE
ALARME EN SORTIE	VALIDE/DEVALIDE Disponible uniquement en mode SANS RESTRICTION, ce réglage n'étant pas conforme à EN50131.
LANGUE	LANGUE SYSTEME LANGUE REPOS
TAILLE DES CODES	4 CHIFFRES 5 CHIFFRES

	6 CHIFFRES 7 CHIFFRES 8 CHIFFRES
RAZ INSTAL/UTIL	VALIDE/DEVALIDE
ACCES WEB	VALIDE/DEVALIDE Autorise/limite l'accès au navigateur Web.
AFF. ZONE OUVERT	VALIDE/DEVALIDE
ACCES INSTALLAT.	VALIDE/DEVALIDE
CONSTRUC.AUTORI. *	VALIDE/DEVALIDE
AFF. ETAT SURV.	VALIDE/DEVALIDE
RESIST. FIN LIGNE	AUCUN 1 Rés- 1K UNE RESIST. 1K5 1 Rés- 2K2 1 Rés- 4K7 UNE RESIST. 10K UNE RESIST. 12K 2 RESIST.1K0/470 2 RESIST.2K2/1K0 2 RESIST.2K2/1K0 2 RESIST.2K2/1K5 2 Rés- 2K2/2K2 2 RESIST.2K2/4K7 2R- 2K7/8K2 2 RESIST.2K2/10K 2R- 3K0/3K0 2R- 3K3/3K3 2R- 3K9/8K2 2 Rés- 4K7/2K2 2R- 4K7/4K7 2R- 5K6/5K6 2R- 6K8/4K7 2 RESIST.10K/10K Mask - 1K/1K/6K8 Mask -1K/1K/6K8 Mask - 4K7/4K7/2K2
MODE AUTH. SMS	CODE SEUL ID APPELANT SEUL CODE+ID APPELANT CODE SMS SEUL CODE SMS + ID APP.
TAG ET CODE	VALIDE/DEVALIDE
RAZ SI MHS	VALIDE/DEVALIDE Remarque :Pour être conforme à PD6662, vous devez désactiver cette option.
RAZ INSTALLATEUR	VALIDE/DEVALIDE
AP. ZONE OFFLINE	VALIDE/DEVALIDE
VERROU INSTALLAT	VALIDE/DEVALIDE Si cette option est active, le système ne peut pas être réinitialisé avec le bouton jaune de la centrale si le code d'installateur n'est pas entré sur le clavier.
CODES SECURISE	VALIDE/DEVALIDE
PARAM.HORLOGE	ETE/HIVER AUTO SYNCHRO SUR 50Hz
SUSPICION AUDIBLE	VALIDE/DEVALIDE

AFF. CAMERAS	VALIDE/DEVALIDE
TEST SISM SI MES	VALIDE/DEVALIDE
ALERT.EMPECH MES	VALIDE/DEVALIDE
ANTIMASQUE MES	DEVALIDE AUTOSURVEILLANCE DEFAULT ALARME
ANTIMASQUE MHS	DEVALIDE AUTOSURVEILLANCE DEFAULT ALARME
CONTRAINTE REDEC	VALIDE/DEVALIDE
PANIQUE REDECLEN	VALIDE/DEVALIDE
SILENCE SI ECOUT	VALIDE/DEVALIDE
TECH. SORTIR	VALIDE/DEVALIDE

* Indisponible pour le SPC42xx, SPC43xx.

16.3 TEMPORISATIONS

1. Sélectionnez TEMPORISATIONS et appuyez sur SELECT.
2. Sélectionnez l'option de programmation souhaitée :

Temporisations

Désignation des fonctions dans l'ordre suivant :

- 1^{er} rang Web/SPC Pro
- 2^{ème} rang Clavier

Temporisation	Libellé	Défaut
Audible		
Sirènes intérieures DUREE SIRENE INT	Durée d'actionnement des buzzers internes quand l'alarme est active. (1 – 15 minutes ; 0 = jamais)	15 min.
Sirènes extérieures DUREE SIRENE EXT	Durée d'actionnement des sirènes extérieures quand l'alarme est active. (1 – 15 minutes ; 0 = jamais)	15 min.
Retard sirènes extérieures RETARD SIRÈNE EXT	Le déclenchement de la sirène extérieure est temporisé. (0 – 600 secondes)	0 s
Carillon DUREE CARILLON	Durée d'actionnement de la sortie carillon en secondes quand une zone avec l'attribut Carillon est ouverte. (1 – 10 secondes)	2 s
Confirmation		
Al. Confirmée TEMPS DE CONFIRM	<ul style="list-style-type: none"> ● Remarque : Uniquement disponible si le grade de sécurité est sans restriction et que DD243 est sélectionné pour la variable Confirmation. (Voir Options Système [→ 236]) 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. (30 – 60 minutes)	30 min
Agression Confirmée	Ce temporisateur s'applique à la fonction de confirmation	480 min.

Temporisation	Libellé	Défaut
	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 – 1 200 minutes)	
Retard de transmission RETARD NUMEROTAT.	S'il est programmé, le délai de numérotation est la période prédéfinie (0 à 30 secondes) avant que le système appelle un centre de télésurveillance (CTS). Ce délai est destiné à réduire les réactions non nécessaires des centres d'appel et de la police. Toutefois, si un intrus pénètre dans une deuxième zone, le délai de numérotation est ignoré et l'appel est déclenché immédiatement. (0 – 30 secondes)	30 s
Abandon d'alarme ANNUL. D'ALARME	Après une alarme transmise, délai au cours duquel un message d'abandon d'alarme peut être transmis. (0 – 999 secondes))	30 s
MES		
Validation MES/MHS VALIDATION MES/MHS	période pour laquelle l'autorisation de validation de paramétrage est valable. Saisissez une valeur entre 10 et 250 secondes.	20 sec
Dernière issue DERNIERE ISSUE	Le délai de dernière issue est le délai de mise en marche en secondes après la fermeture d'une zone programmée avec l'attribut dernière issue. (1 – 45 secondes)	7 s
Sirène lors MES totale SIREN SI MES TOT	Active brièvement la sirène extérieure pour indiquer que la MES totale est active. (0 – 10 secondes)	0 s
Flash lors MES totale FLASH SI MES TOT	Active brièvement le flash sur la sirène extérieure pour indiquer que la MES totale est active. (0 – 10 secondes)	0 s
Armement échoué AFFICH ECHEC MES	Délai d'affichage en secondes du message d'échec de la MES sur les claviers (0 jusqu'à l'entrée du code valide). (0 – 999 secondes)	10 s
Alarme		
Double déclenchement DOUBLE DECLEENCH.	Délai maximum entre des activations de zones ayant l'attribut Double déclenchement pour déclencher une alarme. (1 – 99 secondes)	10 s
Test JOURS TEST JDB	Période en jours pendant laquelle une zone reste en test avant de revenir automatiquement en fonctionnement normal. (1 – 99 jours)	14 jours
Période de l'autotest sismique AUTOTEST SISMIC	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 DUREE TEST SISM	Temps maximum (secondes) d'attente du déclenchement du sismique lorsqu'il est sollicité par l'activation de la sortie test sismique (3 - 120 secondes)	30 s
Verrouillage Post Alarme VERROUILLAGE POST ALARME	Durée de verrouillage des accès après une alarme.	0 min
Flash sirène extérieure DUREE FLASH	Durée d'actionnement de la sortie du flash quand l'alarme est active. (1 – 15 minutes ; 0 = indéfiniment)	15 min.
Alertes		
Tempo 230V DELAI DEF.230V	Le délai entre la détection d'un défaut de l'alimentation secteur et le moment où le système déclenche une alerte. (0 – 60 minutes)	0 min.
Installateur		
Accès Ingénieur ACCES INSTALLAT.	La temporisation pour l'accès Installateur commence dès que l'utilisateur active l'accès Installateur. (0 – 999 minutes. 0 indique que l'accès au système n'est pas limité dans le	0 min.

Temporisation	Libellé	Défaut
	temps.)	
Déconnexion installateur automatique DECONNECT AUTO	La durée d'inactivité après laquelle l'installateur sera automatiquement déconnecté.	0 min.
Clavier		
Temps de saisie clavier TIMEOUT CLAVIER	Délai d'inactivité en secondes avant qu'un clavier quitte le menu actif. (10 - 300 secondes)	30 s
Langue clavier LANGUE CLAVIER	Temps en seconde pendant lequel un clavier gardera la langue Utilisateur en revenant au repos, avant de reprendre la langue par défaut, (0 - 9 999 secondes ; 0 signifie jamais).	10 sec
Feu		
Pré-alarme incendie PRE-ALARME INCENDIE	Nombre de secondes de délai avant l'envoi d'alarme d'incendie pour les zones où l'attribut « Pré-alarme incendie » est activé. (1 - 999 secondes) Voir Éditer une zone [→ 253].	30 s
Confirmation incendie CONFIRMATION FEU	Délai supplémentaire avant l'envoi du fichier d'alarme pour les zones où les attributs Pré-alarme incendie et Confirmation incendie sont activés. (1 - 999 secondes)) Voir Éditer une zone [→ 253].	120 s
CODE		
Validité code VALIDITÉ CODE	Période de temps pendant laquelle le code est valide (1 - 330)	30 Jours
Nbre maxi de changement de code NBRE MAXI DE CHANGEMENT DE CODE	Nombre de changement du code dans la période de validité (1 - 50)	5
Avertissemt Code ALERTE CODE	Temps avant expiration du code-avertissement affiché (1 - 14)	5 jours
Réglages généraux		
Durée activation sortie RF SORTIE RADIO	Temps pendant lequel les sorties radio restent actives dans le système. (0 - 999 secondes)	0 s
Limite temps syn LIMITE TEMPS SYN	Durée limite pendant laquelle aucun événement ne sera signalé. (0 - 999 sec) La synchronisation n'a lieu que si l'heure et la date du système sont hors de cette limite.	0 s
Tempo Déf.IP TEMO DÉF.IP	Timeout pour le défaut du lien Ethernet (0 = désactivé) (0 - 250)	0 sec
Camera Offline CAMERA OFFLINE	Délais avant info caméra Offline (10 - 9999)	10 sec
Délai technique TECHNIQUE DELAI	Délai en secondes pendant lequel une entrée technique doit être en défaut avant qu'une alarme soit déclenchée. (0 - 9999 secondes)	0 s
Fréquent FREQUENT 	Cet attribut s'applique uniquement à la télémaintenance. Le nombre d'heures d'ouverture d'une zone si cette zone est programmée avec l'attribut Usage fréquent . (1 - 9999 heures)	336 heures (2 semaines)
Contrainte silencieuse	Temps pendant lequel la contrainte reste silencieuse et non-restaurable depuis le clavier (0 - 999).	0 minutes
Agression/Panique silencieuse	Nombre de minutes pendant lesquelles une agression/panique reste silencieuse et non-restaurable depuis le clavier (0 - 999).	0 minutes



Les délais par défaut dépendent de la configuration par l'installateur. Les délais par défaut indiqués ne sont pas obligatoirement adaptés à chaque cas ; ils dépendent de l'ingénieur effectuant la configuration.

16.4 SECTEURS

1. Sélectionnez SECTEURS en utilisant les touches de direction bas/haut du clavier et appuyez sur SELECT.
2. Sélectionnez l'option de programmation souhaitée :

AJOUTER	<p>En mode Simple et Evolué, le type de secteur est Standard par défaut. En mode Bancaire, sélectionnez le type de secteur STANDARD, DAB, COFFRE ou EVOLUE.</p> <p>Entrez le nom du secteur et la temporisation d'entrée/sortie voulue.</p>
EDITER	<p>Éditez les réglages suivants :</p> <ul style="list-style-type: none"> ● LIBELLÉ ● ENTREE/SORTIE <ul style="list-style-type: none"> - DELAI ENTREE - DELAI SORTIE - PAS TEMPO SORTIE - MHS RADIO LIMITE ● MES PARTIELLE A/B <ul style="list-style-type: none"> - VALIDE/DEVALIDE - TEMPORISEE - Z.ACCES->TEMPO - Z.TEMPO->IMMEDIA - ALARME LOCALE - AUCUNE SIRÉNE ● SECTEURS LIES <ul style="list-style-type: none"> - SECT. - MARCHE TOTALE - MES DES DEPENDAN - EMPECHE MES - EMPECHE TTES MES - MHS - MHS DES DEPENDAN - EMPECHE MHS - EMPECHE TTES MHS ● CALENDRIER <ul style="list-style-type: none"> - CALENDRIER - MES / MHS AUTOMATIQUE - TEMPS VERROUILL - ACCES COFFRE ● TRANSMISSION <ul style="list-style-type: none"> - MES TROP TOT - MES TROP TARD - MHS TROP TOT - MHS TROP TARD

	<ul style="list-style-type: none"> ● MES/MHS <ul style="list-style-type: none"> - TEMPS DE PRESIGN - ANNUL UTILISATEU - DEROG UTILISAT. - INTER CLE - INTERVAL DEROG. - TEMPS DE DEROG. - MHS RETARDE - DUREE MHS TEMPOR - INTERVERROUILLER - DOUBLE CODE ● SORTIE RADIO
EFFACER	Sélectionnez le secteur à effacer.

Voir Ajouter / Éditer un secteur [→ 253] pour de plus amples informations sur ces options.

16.5 GROUPES SECTEURS

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

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 VALIDE ou ACTIVE comme nécessaire 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.

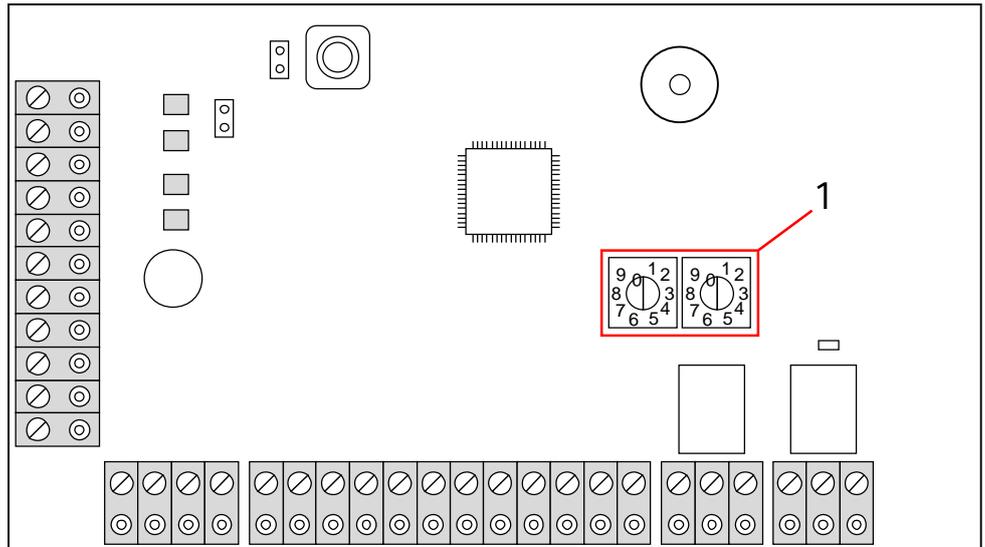
16.6 Périph. X-BUS

1. Sélectionnez XBUS en utilisant les touches de direction bas/haut et appuyez sur SELECT.
2. Sélectionnez les options de programmation souhaitées comme montré ci-dessous.

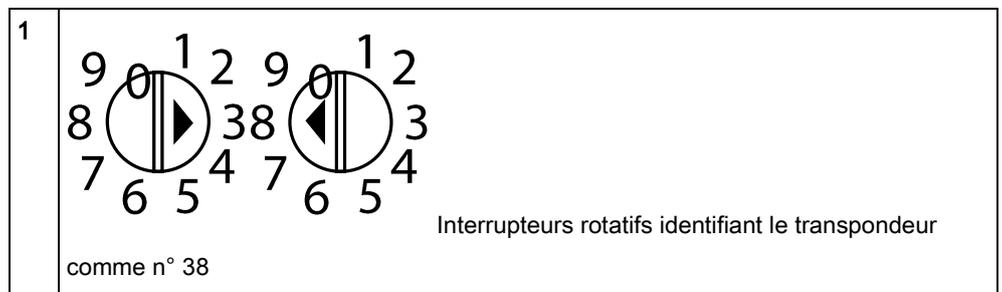
16.6.1 Adressage du X-BUS

Les transpondeurs, les claviers et les zones peuvent être configurés, localisés et surveillés en suivant les descriptions fournies dans cette section. Les paramètres du X-BUS tels que le type, les temps de communication et le nombre de tentatives sont également configurés dans ce menu.

La figure ci-dessous montre les interrupteurs rotatifs avec une flèche pointant vers un chiffre l'identifiant (dans l'exemple : 3 et 8). L'interrupteur rotatif de droite fournit le chiffre de l'unité, celui de gauche le chiffre de la dizaine. Le transpondeur dans l'exemple a le numéro 38.



Roues codeuses d'adressage



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 la centrale dans l'ordre de leur détection, c'est-à-dire en fonction de leur position relative par rapport à la centrale. Dans cette configuration, les zones sont attribuées à chaque transpondeur d'entrée.



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

16.6.2 XBUS REFRESH

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



AVIS

La fonction Reconfigurer s'applique uniquement aux zones reliées à un transpondeur par câble. Les zones radio (sans fil) d'un transpondeur et les zones de la centrale ne sont pas réactivées 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 les transpondeurs du système sont de types hétérogènes (avec et sans interrupteur rotatif), le système peut seulement 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. Sélectionnez RECONFIGURER en utilisant les touches de direction bas/haut du clavier.
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 la touche RETOUR pour quitter le menu.

16.6.4 CLAVIERS/TRANSPONDEURS/CONTROLEURS DE

PORTE

	AVIS
	Mettez à jour la version 1.1 du micrologiciel avant d'ajouter des contrôleurs de porte. Les versions plus anciennes du micrologiciel identifient les contrôleurs de porte en tant que transpondeurs d'E/S normaux et les portes doivent être ajoutées manuellement.

16.6.4.1 LOCALISER

Pour localiser un clavier/transpondeur/contrôleur de porte :

1. Sélectionnez CLAVIERS, TRANSPONDEUR ou CONTROLEUR DE PORTE et appuyez sur SELECT.
2. Sélectionnez LOCALISER et appuyez sur SELECT.
3. Sélectionnez le clavier, le transpondeur ou la centrale de porte à localiser et appuyez sur SELECT.
 - ⇒ Le périphérique sélectionné émet un bip sonore et le témoin LED s'allume pour permettre à l'installateur de le localiser visuellement.
4. Appuyez sur la touche RETOUR pour quitter le menu.
 - ⇒ Localisez les claviers en utilisant les mêmes menus mais en sélectionnant le clavier au lieu du transpondeur.

16.6.4.2 AFFICHER ETAT

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

1. Sélectionnez CLAVIERS, TRANSPONDEUR ou CONTROLEUR DE PORTE et appuyez sur SELECT.
2. Sélectionnez AFFICHER ETAT et appuyez sur SELECT.
3. Sélectionnez l'option de programmation souhaitée en utilisant les touches de direction bas/haut.
4. Appuyez sur SELECT.
 - ⇒ La liste des claviers/transpondeurs détectés est affichée.
5. Sélectionnez le clavier, le transpondeur ou la centrale de porte dans la liste et appuyez sur SELECT.
 - ⇒ Les paramètres et les propriétés affichés, le cas échéant, sont décrits dans le tableau ci-dessous.
6. Appuyez sur la touche RETOUR pour quitter le menu.

ÉTAT	En ligne ou hors ligne
N° Série	Numéro de série (utilisé pour le suivi et l'identification)
VER.	Version du Firmware

TENSION	Paramètres d'alimentation : tension en temps réel et valeurs actuelles
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. (Module d'alimentation de transpondeur seulement). Faites défiler pour afficher la tension et la charge de courant sur les sorties, l'état de la batterie. L'option Mode lien est également disponible (elle montre le paramétrage du cavalier sur la centrale pour Ah). 7Ah et 17Ah sont les options disponibles. (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 de la batterie : niveau de la batterie (ne concerne que les transpondeurs du module d'alimentation).
ETAT ENTREE	État de chaque entrée de zone associée à un transpondeur : C : Fermé, O : Ouvert, D : Déconnecté, S : Court-circuit (transpondeurs avec entrées uniquement)

16.6.4.3 ÉDITION DES CLAVIERS

Pour éditer les claviers :

1. Sélectionnez CLAVIERS -> EDITER.
2. Appuyez sur SELECT.
3. Sélectionnez le périphérique à modifier et appuyez sur SELECT.
 - ⇒ Les paramètres de configuration des claviers standard et 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.

Description	Saisissez une description unique pour identifier le clavier.
Réglage des touches de fonctions (état repos)	
Panique	Sélectionnez Activé, Désactivé ou Silencieux activé. Si validé, l'alarme de panique s'active en appuyant sur les 2 touches douces en même temps.
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	Sélectionnez lorsque le clavier est rétro-éclairé. Les options sont les suivantes : - Lorsqu'une touche est appuyée ; Toujours En service ; Toujours Hors service.
Indicateurs	Activez ou désactivez les témoins sur le clavier.
État des MES	Sélectionnez si l'état de surveillance doit être indiqué au repos.
Indications sonores	
Buzzer	Activez ou désactivez le buzzer sur le clavier.
Buzzer en MES Partielle	Activez ou désactivez le buzzer pendant la temporisation de sortie en MES Partielle.
Appuyez sur une touche	Sélectionnez si le volume des haut-parleurs est activé pour l'appui des touches.
Désactivation	
Calendrier	Sélectionnez si le clavier doit être contrôlé par le calendrier. Voir Calendrier [→ 268].
Interaction logique	Sélectionnez si le clavier doit être contrôlé par une interaction logique.

Boîtier à clé	Sélectionnez si le clavier doit être contrôlé par un boîtier à clé.
Entrée tag	Cochez cette case pour verrouiller les touches du clavier pendant la temporisation d'entrée quand un tag est configuré sur le clavier.
Secteurs	
Emplacement	Sélectionner le secteur protégé où se trouve le clavier.
Secteurs	Sélectionnez depuis le clavier les secteurs à contrôler.
Options	
Synchro Tempo sortie	Sélectionnez pour configurer un délai depuis le clavier. La localisation du clavier est ignorée et tous les secteurs appliquent le temps total de temporisation de sortie.

	<p>AVIS</p> <p>Il est recommandé de n'affecter un secteur à un clavier seulement si le clavier se trouve dans le secteur assigné et si le chemin d'entrée/sortie est défini. Si un secteur est assigné, les temporisations d'entrée et de sortie sont appliquées (si configurées) lorsque le secteur en question est armé ou désarmé. D'autres fonctions liées aux chemins d'entrée/sortie sont alors disponibles. Si aucun secteur n'est assigné, le secteur est immédiatement armé ou désarmé et les autres fonctions d'entrée/sortie ne sont pas disponibles.</p>
---	---

Paramètres du clavier de confort

Configurez les paramètres suivants du clavier de confort.

Description	Saisissez une description unique pour identifier le clavier.
Réglage des touches de fonctions (état repos)	
Panique	Sélectionnez Activé, Désactivé ou Silencieux activé. Si cette option est active, l'alarme de panique peut être activée en appuyant en même temps sur F1 et F2.
Incendie	Activez pour permettre l'activation de l'alarme incendie en appuyant en même temps sur F2 et F3
Médical	Activez pour permettre l'activation de l'alarme médicale en appuyant en même temps sur F3 et F4.
MES totale	Activez pour permettre l'activation de la MES TOTALE en appuyant deux fois sur F2.
MES Partielle A	Activez pour permettre l'activation de la MES Partielle A en appuyant deux fois sur 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.
Indications visuelles	
Rétro-éclairage	Sélectionnez lorsque le clavier est rétro-éclairé. Les options sont les suivantes : - Lorsqu'une touche est appuyée ; Toujours En service ; Toujours Hors service.
NIV.RETROECLAIR	Sélectionnez l'intensité du rétroéclairage. Plage de réglage 1 - 8 (élevé).
Indicateurs	Activez ou désactivez les témoins sur le clavier.

Etat des MES	Sélectionnez si l'état de surveillance doit être indiqué au repos (témoin).
Logo	Sélectionner si le logo doit être visible au repos.
Montre analogique	Sélectionnez la position de l'horloge si elle doit être visible au repos. Les options sont les suivantes : aligné à gauche, aligné au centre, aligné à droite ou désactivé.
Urgence	Activez si les touches fonctions Panique, Incendie ou Médicale 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	Sélectionner le volume du haut-parleur pour les indications d'alarme ou pour désactiver le son.
Entrée/sortie	Intervalle 0 - 7 (volume max.)
Carillon	Sélectionner le volume du haut-parleur pour les indications d'entrée et de sortie ou pour désactiver le son.
Appuyez sur une touche	Intervalle 0 - 7 (volume max.)
Annonce Vocale	Sélectionner le volume du haut-parleur pour le carillon ou pour désactiver le son.
Buzzer en MES Partielle	Intervalle 0 - 7 (volume max.)
Désactivation	
Calendrier	Sélectionnez si le clavier doit être contrôlé par le calendrier. Voir Calendrier.
Interaction logique	Sélectionnez si le clavier doit être contrôlé par une interaction logique.
Boîtier à clé	Sélectionnez si le clavier doit être contrôlé par un boîtier à clé.
Entrée tag	Cochez cette case pour verrouiller les touches du clavier pendant la temporisation d'entrée quand un tag est configuré sur le clavier.
Secteurs	
Emplacement	Sélectionner le secteur protégé où se trouve le clavier.
Secteurs	Sélectionnez depuis le clavier les secteurs à contrôler.
Options	
Synchro Tempo sortie	Sélectionnez pour configurer un délai depuis le clavier. La localisation du clavier est ignorée et tous les secteurs appliquent le temps total de temporisation de sortie.

**AVIS**

Il est recommandé de n'affecter un secteur à un clavier seulement si le clavier se trouve dans le secteur assigné et si le chemin d'entrée/sortie est défini. Si un secteur est assigné, les temporisations d'entrée et de sortie sont appliquées (si configurées) lorsque le secteur en question est armé ou désarmé. D'autres fonctions liées aux chemins d'entrée/sortie sont alors disponibles. Si aucun secteur n'est assigné, le secteur est immédiatement armé ou désarmé et les autres fonctions d'entrée/sortie ne sont pas disponibles.

16.6.4.4 ÉDITION DES TRANSPONDEURS

Pour éditer les transpondeurs :

1. Sélectionnez TRANSPONDEURS -> EDITER.
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.



En ce qui concerne le nom et l'identification des transpondeurs, des zones sont affectées aux transpondeurs (par groupes de 8) et identifiées par un numéro consécutif de 1 à 512. (512 est le numéro maximal pour l'identification des zones.) Ainsi, tout transpondeur identifié par un numéro supérieur à 63 n'est attribué à aucune zone.

16.6.4.4.1 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.

16.6.4.4.2 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.
ENTREE	Sélectionnez les entrées de zone.
LIMITE DU VOLUME	Sélectionnez la limite du volume.

16.6.4.4.3 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.

16.6.4.4.4 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.

16.6.4.4.5 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	<p>Vous permettent d'affecter une action à des touches spécifiques pour des zones spécifiques.</p> <p>Sélectionnez un secteur et affectez une des options suivantes à ce secteur :</p> <ul style="list-style-type: none"> ● Aucun ● 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
Indications visuelles (Mode flexible uniquement)	<p>Vous permet d'affecter un comportement spécifique à chaque LED sur le module des voyants. Chacune des LED dispose des options suivantes :</p> <ul style="list-style-type: none"> ● FONCTION — les options suivantes sont disponibles : <ul style="list-style-type: none"> – INTER CLE — 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 ététa actif. Les options disponibles sont les suivantes : <ul style="list-style-type: none"> – Permanent — toujours allumé. – Clignotement rapide / moyen / lent — variation de la vitesse du clignotement.

Nom	Description
	<ul style="list-style-type: none"> ● HORS - COULEUR — spécifiez la couleur de la désactivation ● HORS - FLASH — spécifiez le comportement de la LED en état actif. Les options disponibles sont les suivantes : <ul style="list-style-type: none"> - 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 : <ul style="list-style-type: none"> ● 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 Editer transpondeur.
ENTREE	Sélectionnez la zone

16.6.4.4.6 Édition des transpondeurs à boîtier à clé

Le tableau suivant fournit la liste des options 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.
Indications visuelles (Mode Flexible seulement)	<p>Vous permet d'affecter un comportement spécifique à chaque LED sur le transpondeur à boîtier à clé. Chacune des LED dispose des options suivantes :</p> <ul style="list-style-type: none"> ● FONCTION — les options suivantes sont disponibles : <ul style="list-style-type: none"> - INTER CLE — 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.

Nom	Description
	<ul style="list-style-type: none"> ● 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 : <ul style="list-style-type: none"> – Permanent — toujours allumé. – Clignotement rapide / moyen / lent — variation de la vitesse du clignotement. ● HORS - COULEUR — spécifiez la couleur de l'activation ● HORS - FLASH — spécifiez le comportement de la LED en état actif. Les options disponibles sont les suivantes : <ul style="list-style-type: none"> – Permanent — toujours allumé. ● Clignotement rapide / moyen / lent — variation de la vitesse du clignotement.
DESACTIVATION (Mode Flexible seulement)	<p>Sélectionnez une méthode de désactivation à partir des options disponibles :</p> <ul style="list-style-type: none"> ● Calendrier — sélectionnez un calendrier.
POSITIONS CLE	<p>Vous permet d'affecter un comportement aux positions de clé spécifiques pour des secteurs spécifiques.</p> <p>Sélectionnez un secteur pour la position de clé et affectez une des options suivantes à ce secteur :</p> <ul style="list-style-type: none"> ● Aucun ● 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 ÉDITION DES CONTRÔLEURS DE PORTE

Pour des informations détaillées sur les contrôleurs de porte, voir ici [→ 76].

1. Sélectionnez CONTROLEUR PORTE -> EDITER.
 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 porte 1 et de l'E/S de porte 2.
LECTEURS	Configuration des profils des lecteurs

Pour éditer une E/S de porte :

1. Sélectionnez 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 décrits dans le tableau ci-dessous.

ZONES	Aucune fonction d'accès n'est réalisée. Les entrées et les sorties sont utilisables normalement.
PORTE 1 – PORTE 64	Le numéro de porte choisi est attribué à l'E/S de porte.

Si l'option ZONES est sélectionnée pour une E/S de porte, les deux entrées de cette E/S doivent être configurées :

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

1. Sélectionnez l'E/S de porte à modifier et appuyez sur SELECT.
⇒ L'option ZONES est sélectionnée.
 2. Appuyez sur SELECT.
 3. Sélectionnez la zone à éditer (contact d'ouverture de porte ou bouton d'ouverture de porte).
 4. Appuyez sur SELECT.
- ⇒ Les paramètres et les propriétés affichés, le cas échéant, sont décrits dans le tableau ci-dessous.

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



Chaque numéro disponible peut être attribué à une zone. Cette attribution n'est pas fixe. Si le numéro 9 est attribué à une zone et qu'un transpondeur d'entrée avec l'adresse 1 est connecté au X-Bus (qui utilise les numéros de zone 9 à 16), la zone attribuée par les deux contrôleurs de porte obtient le numéro de zone suivant disponible. La configuration est adaptée en conséquence.

Pour modifier un profil de lecteur :

1. Sélectionnez LECTEURS.
 2. Appuyez sur SELECT.
 3. Sélectionnez le LECTEUR à modifier et appuyez sur SELECT.
- ⇒ Assignez l'un des profils suivants au lecteur :

1	Pour les lecteurs avec un voyant LED vert et un voyant LED rouge.
2	Pour les lecteurs VANDERBILT avec un voyant LED jaune (AR618X).
3	Le profil 3 est utilisé avec les lecteurs HID qui envoient un code à la centrale, comme une lecture de carte dotée d'un code site prédéfini (0)
4	Le profil 4 est utilisé avec les lecteurs HID qui envoient un code à la centrale comme carte de lecture dotée d'un code site prédéfini (255).

5	Choisir si les lecteurs Sesam sont utilisés. Pour l'homologation VDS, il est également recommandé de sélectionner l'option État MES/MHS sur voyant lecteur pour fournir une rétroaction durant la configuration.
---	---

Voir aussi

 Transpondeur de porte [→ 76]

16.6.5 MODE ADRESSAGE

Les X-BUS d'adressage peuvent être configurées de deux manières :

Adressage automatique

L'adressage automatique est applicable à des transpondeurs avec ou sans interrupteur rotatif. En mode d'adressage automatique, la centrale 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 zones 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 ((ID 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
11	89-96	24	193-200	37	297-304	50	401-408	63	505-512



Si deux périphériques du même type (par exemple deux transpondeurs) ont le même adresse, les deux émettent un bip sonore 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. Sélectionnez TYPE XBUS en utilisant les touches de direction bas/haut.
2. Appuyez sur SELECT.
3. Sélectionnez la configuration voulue :
 - BOUCLE
 - BRANCHE
4. Appuyez sur SELECT pour mettre à jour le paramètre.

16.6.7 RE-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. Sélectionnez RE-ESSAI BUS en utilisant les touches de direction bas/haut.
2. Appuyez sur SELECT.
3. Entrez le nombre de tentatives de retransmission des données.
4. Appuyez sur SELECT pour mettre à jour le paramètre.

16.6.8 TEMPO DEF. COMMS

Pour définir le délai avant qu'une erreur de communication soit enregistrée:

1. Sélectionnez TEMPO DEF. COMMS. en utilisant les touches de direction bas/haut.
2. Appuyez sur SELECT.
3. Entrez le délai voulu.
4. Appuyez sur ENTRER pour mettre à jour le paramètre.

16.7 RADIO

1. Sélectionnez RADIO et appuyez sur SELECT.
2. Sélectionnez l'option de programmation souhaitée :

DETECTEURS	<p>Il peut être nécessaire de changer le type de détecteur programmé s'il a été mal identifié lors de la programmation.</p> <p>Si aucun détecteur radio n'est enregistré, le message PAS DETECT. ACTIF est affiché sur le clavier.</p> <p>Les fonctions suivantes sont disponibles pour les capteurs :</p>
------------	--

	<ul style="list-style-type: none"> ● AJOUTER Voir AJOUTER DES DETECTEURS [→ 140] ● EDITER (Changer la zone assignée) Voir MODIFIER DÉTECTEURS (AFFECTATION DE ZONE) [→ 141] ● RETIRER Sélectionnez le périphérique ou le détecteur à effacer.
WPA	Ajoutez, modifiez ou effacez le WPA (Radio Personnel Alarme). <ul style="list-style-type: none"> ● AJOUTER Voir AJOUTER WPA [→ 141] ● MODIFIER Voir ÉDITER WPA [→ 141] ● RETIRER Sélectionnez le WPA à effacer.
ANTENNE EXTERNE	Activer ou désactiver l'antenne externe.
SUPERVISION	Active ou désactive l'autosurveillance.
FILTRE SIGNAL BAS	Activer ou désactiver le filtre de signal faible (niveaux d'intensité du signal RF: 0 et 1).
DETECT. PB RF	Activer ou désactiver le brouillage RF.
PANIQUE RADIO	Activez ou désactivez la panique radio ou activez le mode silencieux pour la panique radio.
Planification Test WPA	Entrez la durée maximale en jours séparant deux tests WPA. Vous pouvez définir un délai maxi de 365 jours.
DELAI PREV MES	Entrez une durée en minutes au bout de laquelle l'absence de message de supervision inhibe la mise en surveillance du secteur dans lequel se trouve la zone radio. Vous pouvez définir un délai maxi de 720 minutes.
DELAI RADIO PERD	Entrez une durée en minutes au bout de laquelle le périphérique radio est considéré absent en l'absence de message. La durée doit être comprise entre 20 et 720 minutes.

16.7.1 AJOUTER DES DETECTEURS

Pour ajouter un détecteur radio :

1. Sélectionnez AJOUTER et appuyez sur SELECT.
 - ⇒ Le message ACTIVER ENREG. est affiché.
 2. Appuyez sur SELECT.
 - ⇒ Le texte ACTIVER PERIPHER clignote dans la ligne supérieure de l'afficheur.
 3. Activez le périphérique radio de 3 à 5 fois de suite pour que le récepteur du clavier détecte la transmission radio du périphérique.
 - ⇒ Le texte TROUVE DETECTEUR clignote sur l'afficheur pour indiquer que le périphérique a été détecté. Le TYPE et l'ID du périphérique sont affichés en alternance.
 4. Appuyez sur ENREGIST.
 - ⇒ Un message est affiché pour vous demander de sélectionner le type de zone.
1. Appuyez sur SELECT.
 2. Sélectionnez le type de zone voulu et appuyez sur SELECT.



Pour ajouter un périphérique par AUTOSUR. ENREG., sélectionnez cette option à l'étape 2. L'enregistrement se déroule de même à l'exception d'un message demandant de définir un type de zone avant d'afficher cette donnée.

16.7.2 MODIFIER DÉTECTEURS (AFFECTATION DE ZONE)

Il peut s'avérer nécessaire de changer l'attribution de zone au capteur enregistré dans le système.

Pour changer l'attribution de zone à un détecteur radio:

1. Sélectionnez EDITER et appuyez sur SELECT.
2. Sélectionnez le détecteur à éditer et appuyez sur SELECT.
3. Sélectionnez ZONE.
4. Sélectionnez le numéro de zone voulu (seuls les numéros de zone disponibles sont affichés).
5. Appuyez sur SELECT.

16.7.3 AJOUTER WPA

!	<i>AVIS</i>
	<p>Il n'est possible de configurer un WPA ou de vérifier son état sur le clavier que si un module radio est intégré à la centrale ou si l'un des transpondeurs et la centrale sont autorisés pour le type de module(s) activé.</p>

Un WPA n'est pas affecté à un utilisateur. En général, un WPA est partagé par plusieurs personnes comme, par exemple, les vigiles travaillant en équipe. Il peut également être fixé sur une surface (sous un bureau ou derrière la caisse).

128 WPA par centrale au maximum sont autorisés.

Pour configurer le WPA depuis le clavier :

1. Sélectionnez RADIO puis WPA.
2. Sélectionnez AJOUTER pour ajouter un WPA.
3. Sélectionnez MANUEL pour saisir l'ID du WPA.
L'ID peut également être entrée automatiquement par la centrale si l'option APPRENDRE WPA est sélectionnée. L'un des boutons WPA doit être enfoncé lors de l'affichage du message ACTIVATION WPA, afin que la centrale puisse identifier le WPA. La centrale n'accepte par une WPA dont l'ID est une copie d'un WPA déjà configurée.
4. Sortez du menu AJOUTER et sélectionnez le menu MODIFIER pour configurer le WPA.

16.7.4 MODIFIER WPA

Pour configurer le WPA depuis le clavier :

1. Sélectionnez RADIO puis WPA.

2. Sélectionnez MODIFIER pour configurer un WPA.

LIBELLÉ	Saisissez un libellé unique pour identifier le WPA.
ID TRANSMETTEUR	Saisir l'ID du WPA. La centrale n'accepte pas une WPA dont l'ID est une copie d'une WPA déjà configurée.
FONCT DES BOUTON	<p>Utilisez cette section pour assignez des fonctions aux combinaisons de boutons. Les fonctions disponibles sont les suivantes : Panique, Panique silencieuse, Agression, Suspicion, Sortie RF utilisateur, Médicale. Plusieurs combinaisons de boutons peuvent être affectées à une seule fonction. Par exemple :</p> <ul style="list-style-type: none"> ● Jaune - Suspicion● ● Rouge+Vert - Holdup ● Sur les installations simples ou évoluées, la combinaison par défaut est la suivante : Rouge + Vert - Panique <p>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 [→ 272]</p>
SUPERVISER	<p>Le WPA peut être configuré pour émettre un signal de supervision intermittent. Si la supervision est activée sur le WPA (grâce à un cavalier), il émet un message de supervision toutes les 7,5 minutes environ. Le temps séparant les messages est aléatoire afin de réduire les risques de collision avec d'autres WPA.</p> <p>La fonction de supervision doit également être activée sur la centrale pour cette WPA spécifique pour une supervision correcte. Si la centrale ne reçoit pas le signal de supervision, une alarme est déclenchée : elle est affichée sur le clavier et consignée dans le journal.</p> <p>Si la supervision n'est pas activée, le WPA émet un message de supervision environ toutes les 24 heures afin de communiquer l'état de sa batterie à la centrale. Le temps séparant les messages est aléatoire afin de diminuer les risques de collision avec d'autres WPA. Sélectionnez VALIDER si la supervision a été validée pour ce WPA en particulier.</p>
TEST	Active la fonction de test du signal WPA.

Voir également

Déclencheurs [→ 272]

Configuration des temporisations WPA [→ 139]

Test WPA depuis le clavier [→ 159]

16.8 ZONES

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

LIBELLÉ	Aide à identifier la zone: entrez un nom descriptif individuel.
TYPE ZONE	Détermine le type de zone. Voir ici [→ 367].
ATTRIBUTS	Détermine les attributs de la zone. Voir ici [→ 370].
VERS SECTEUR	Détermine l'affectation entre les zones et les secteurs. Cette option est affichée uniquement si plusieurs secteurs sont définis. Cette fonction permet aux utilisateurs de regrouper des zones appartenant à un secteur particulier dans l'immeuble.



Le nombre et le type d'attributs affichés dans les menus du clavier applicables à une zone particulière varient en fonction du type de la zone. Voir ici.

16.9 PORTES

16.9.1 PORTES

1. Sélectionnez PORTES et appuyez sur SELECT.
2. Sélectionnez la porte à programmer et appuyez sur SELECT.
3. Les paramètres et les propriétés affichés peuvent être modifiés. Ce sont les suivants :
 - Description
 - Entrées DPS et DRS de la porte
 - Groupe de portes
 - Attributs porte
 - Timers porte
 - Données lecteur (Affichage seul : format du dernier badge lu avec le lecteur configuré)

Entrées de porte

Chaque porte possède 2 entrées ayant chacune une fonction prédéfinie. Ces deux entrées, le détecteur de position de porte et le bouton d'ouverture de porte, sont configurables.

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 l'entrée de détecteur de position de porte est utilisé uniquement pour les fonctions « accès », sélectionnez l'option NON ATTRIBUE. Si le détecteur de position de porte est affecté à une zone d'intrusion, celle-ci peut être configurée comme une zone normale mais avec quelques restrictions (par exemple, certains types de zone ne sont pas accessibles). Si un secteur ou le système est armé avec le lecteur de carte, l'entrée du détecteur de position de porte doit être affectée à un numéro de zone et au secteur/système devant être activé.
Description (Web et SPC Pro uniquement)	Description de la zone à laquelle le détecteur de position de porte est attribué.
Type de zone (Web et SPC Pro uniquement)	Type de la zone à laquelle le détecteur de position de porte est affecté (certains types de zones ne sont pas disponibles).
Attributs zone (Web et SPC Pro uniquement)	Les attributs de la zone à laquelle le détecteur de position de porte est affecté peuvent être modifiés.
Secteur	Le secteur auquel la zone et le lecteur de carte sont affectés. (Si le lecteur de carte est utilisé pour l'activation

Nom	Description
(Web et SPC Pro uniquement)	et la désactivation, ce secteur sera activé/désactivé).
Position porte (web) Résistance fin de ligne DPS (claviers) Contact Porte DPS (SPC Pro)	La résistance utilisée par le détecteur de position de porte. Choisissez la valeur / combinaison de la résistance utilisée.
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) Contact Porte DPS (SPC Pro)	La résistance utilisée par le bouton d'ouverture de porte. Choisissez la valeur / combinaison de la résistance utilisée.
DRS normalement ouvert	Indique si le bouton d'ouverture de porte est une entrée normalement ouverte ou non.
Pas de DRS (Web et SPC Pro 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 et SPC Pro 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 (indisponible sur SPC Pro).



Chaque numéro de zone libre peut être affecté aux zones, mais l'affectation n'est pas fixe. Si le numéro « 9 » est affecté à une zone, celle-ci et un transpondeur d'entrée avec l'adresse « 1 » sont connectés à l'X-Bus (qui utilise les numéros de zones compris entre 9 et 16). La zone affectée des deux centrales de porte se verra affectée le numéro libre suivant de zone. La configuration est adaptée en conséquence.

Groupes de portes

Une porte peut faire partie d'un groupe de portes. L'affectation à un groupe de portes peut être nécessaire si l'une des fonctions suivantes est active:

- Gardien
- Antipassback soft
- Empêche le passback
- Interverrouiller

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

Attribut	Description
	requis.
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	Le lecteur de sortie réclame un code. La porte doit posséder un lecteur d'entrée et un lecteur de sortie.
Code pour MES/MHS	Un code est requis pour armer et désarmer le secteur lié. L'utilisateur doit présenter le badge avant de taper le code.
MHS à l'extérieur (navigateur) MHS sur Lecteur d'entrée (SPCPro)	Le secteur sera mis à l'arrêt lorsqu'un badge est présenté sur le lecteur d'entrée.
MHS à l'intérieur (navigateur) MHS sur Lecteur de sortie (SPCPro)	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) MES sur Lecteur d'entrée (SPCPro)	Le secteur sera mis en surveillance lorsqu'un badge est présenté deux fois sur le lecteur d'entrée.
MES sur lecteur de sortie MES sur Lecteur de sortie (SPCPro)	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.
Urgence Un	incendie dans un secteur quelconque déverrouille la porte.
Escorte	La fonction Escorte permet à des détenteurs de carte à accès privilégié d'escorter d'autres détenteurs de carte au travers de portes spéciales. Quand cette fonction est appliquée à une porte, la badge avec les « droits d'escorte » doit être présentée en premier, puis les autres détenteurs de badge ne possédant pas ce privilège peuvent ouvrir cette même porte. Le délai entre la présentation de la carte d'escorte et celle de la carte normale est configuré pour chacune des portes.
Anti-passback*	La fonction anti-passback (protection physique) devrait 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 la présente pas pour en sortir, il viole les règles d'anti-passback. La prochaine fois qu'il tentera de pénétrer dans le même espace, une alarme d'anti-passback réelle est déclenchée, l'empêchant ainsi d'entrer dans le groupe de portes.
Antipassback soft*	Les violations des règles d'anti-passback sont

Attribut	Description
	<p>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.</p> <p>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 la présente pas pour en sortir, il viole les règles d'anti-passback. La prochaine fois qu'il tentera de pénétrer dans le même groupe de portes, une alarme d'anti-passback logiciel est déclenchée. Cependant, le détenteur de badge pourra entrer dans ce groupe de portes.</p>
Gardien*	<p>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.</p> <p>Le gardien doit pénétrer dans une pièce en premier. Les autres personnes ne 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 non-gardien.</p>
Buzzer porte	Le buzzer intégré sur la carte de circuit imprimé du contrôleur de porte retentit pendant une alarme de porte.
Ignorer les portes forcées	L'ouverture forcée d'une porte est ignorée.
Group. Interver. * (navigateur) Fonction d'interverrouillage (SPCPro)	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 portes

Temporisation	Min.	Max.	Description
Accès autorisé	1 s	255 s	Durée pendant laquelle la porte restera ouverte après que l'accès a été autorisé.
Accès refusé	1 s	255 s	Délai d'attente après un événement invalide avant que la centrale soit de nouveau prêt.
Porte ouverte	1 s	255 s	Intervalle de temps au cours duquel la porte doit être refermée pour éviter une alarme PORTE OUVERTE TROP LONGTEMPS.
Porte laissée ouverte	1 min	180 min	Intervalle de temps au cours duquel la porte doit être refermée pour éviter une alarme PORTE RESTEE OUVERTE.
Extension de temps	1 s	255 s	Délai additionnel après avoir accordé l'accès à un badge avec un attribut EXTENSION DE TEMPS.
Escorte	1 s	30 s	Délai entre la présentation d'un badge avec des privilèges

Temporisation	Min.	Max.	Description
			d'escorte et l'accès par l'utilisateur ne possédant pas ce privilège.

16.10 SORTIES

Chaque type de zone dans le système SPC est associé à un type de sortie (un témoin de marche ou un indicateur interne). Quand un type de zone est activé, par exemple quand une porte ou une fenêtre est ouverte, quand de la fumée ou une alarme est détectée etc., la sortie correspondante est activée.

1. Sélectionnez SORTIES en utilisant les touches de direction bas/haut et appuyez sur SELECT.
2. Sélectionnez CENTRALE ou TRANSPONDEUR et appuyez sur SELECT.
3. Sélectionnez le transpondeur/la sortie à programmer et appuyez sur SELECT.

⇒ Si l'activation des sorties est enregistrée dans le journal de bord du système (c'est-à-dire activé, enregistrement d'une ligne / désactivé, enregistrement), les options indiquées dans le tableau ci-dessous sont disponibles.

NOMS	Utilisé pour identifier la sortie. Entrez un nom descriptif individuel.
TYPE SORTIE	Détermine le type de sortie ; voir le tableau ici [→ 147] pour la description des types de sorties.
MODE SORTIE	Détermine le mode de sortie : en continu, impulsion ou intermittent.
POLARITE	Indique si la sortie est activée sur une polarité positive ou négative.
LOG	Indique si le journal de bord système est actif ou inactif.



Pour la procédure de test de sortie, voir ici [→ 158].

16.10.1 Types et ports de sortie

Chaque type de sortie peut être attribué à un des 6 ports de sortie physiques sur la centrale SPC ou à une sortie de l'un des transpondeurs connectés. Les types de sortie qui ne sont pas attribués à des sorties physiques jouent le rôle d'indicateurs des événements système et peuvent être connectés à un centre de télésurveillance.

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 ici [→ 367]) 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 possède ses propres sorties secteur ; s'il s'agit d'un secteur commun à d'autres secteurs, ses sorties indiquent l'état de tous les secteurs communs incluant son propre état. Exemple : si le secteur 1 est commun aux secteurs 2 et 3, et si la sirène extérieure du secteur 2 est active, alors la sortie de la sirène extérieure du secteur 1 est également active.



Certains types de sortie ne prennent en charge que des événements au niveau du système (aucun événement spécifique à un secteur). Pour des informations plus détaillées, consultez le tableau ci-dessous.

Type 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 du relais de flash (Sortie 3) sur la carte de la centrale (NO, COM, NC). 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. Le flash de la sirène extérieure est activé après un « Echec MES » si ce flash est sélectionné (case cochée) pour l'option « Echec 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 une 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.
Incendie	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.
Mémoire	La sortie est activée selon la configuration des sorties du système de gâches (voir Configuration du système de verrouillage et sorties des MES Auto [→ 217]). 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 silencieuse 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)
Test auto. du Détecteur	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 enfoncé 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 enfoncé 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 (SPC Pro — MES complète)	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 (SPC Pro — MES effectuée)	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 « Blockschloss 1 » est activée. Si le verrou du Blockschloss est fermé, une entrée « Clef 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 correspondante à la clé de mise en service en état de désactivation (fermé) et le secteur est déverrouillé. « 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 « Clef 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 désactivé. « Blockschloss 2 » est activé (si le secteur est prêt à être activé).
Élément 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 (tentative d'effraction du code)	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 : <ul style="list-style-type: none"> ● 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

Passage en 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 aussi

- 📄 Configuration les systèmes de verrouillage et sorties de MES Auto [→ 217]

16.11 COMMUNICATION

1. Sélectionnez COMMUNICATION et appuyez sur SELECT.
2. Sélectionnez l'option de programmation souhaitée en utilisant les touches de direction bas/haut.

16.11.1 PORTS SERIE

Les ports série permettent de connecter au système des PC disposant de ce port ou d'autres périphériques tels que des imprimantes.

1. Sélectionnez PORTS SERIE.
2. Appuyez sur SELECT.
3. Sélectionnez le port série à programmer.
4. Sélectionnez l'une des options de programmation décrites dans le tableau ci-dessous:
5. Appuyez sur la touche RETOUR pour quitter le menu.

TYPE	Indique le type d'appareil connecté: TERMINAL (information système) ou IMPRIMANTE (journal de bord SPC)
VITESSE (BAUDS)	Détermine la vitesse de communication entre la centrale et le périphérique. Important : la vitesse en bauds doit être configurée de manière identique sur les deux composants.
BITS DE DONNEES	Détermine la longueur du paquet de données à transmettre 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.
PARITE	Détermine la parité (paire/impair/pas de parité) du paquet de données. Important : la parité doit être configurée de manière identique sur les deux composants.
CONTROLE FLUX	Indique si les données sont contrôlés par le matériel (RTS, CTS) ou par un logiciel (Aucun). Important : le contrôle de flux doit être configuré de manière identique sur les deux composants.

16.11.2 PORTS ETHERNET

Pour programmer les ports Ethernet:

1. Sélectionnez PORT ETHERNET.
2. Appuyez sur SELECT.

- ⇒ L'option ADRESSE IP contient XXX.XXX.XXX.XXX . Complétez les chiffres inférieurs à 100 par des zéros significatifs à gauche. Exemple: 001
3. Appuyez sur SELECT et entrez l'adresse IP de votre choix.
 - ⇒ Quand vous appuyez sur la touche ENTRER, vous entendez deux bips sonores et MISE A JOUR s'affiche dans la première ligne de l'afficheur si l'adresse IP est valable. Si l'adresse IP est attribuée manuellement, elle doit être unique dans le réseau LAN ou VLAN connecté à la centrale. N'entrez pas d'adresse IP si un serveur DHCP est utilisé.
 4. Sélectionnez MASQUE SS RESEAU.
 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. Exemple: 001. Quand vous appuyez sur la touche ENTRER, vous entendez deux bips sonores et MISE A JOUR s'affiche dans la première ligne de l'afficheur si le masque de sous-réseau est valable.
 6. Sélectionnez PASSERELLE. La passerelle doit être programmée pour les accès en dehors du réseau (pour l'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. Exemple: 001. Quand vous appuyez sur la touche ENTRER, vous entendez deux bips sonores et MISE A JOUR s'affiche dans la première ligne de l'afficheur si la passerelle est valable.
 8. Sélectionnez DHCP. La fonction DHCP est active si les adresses IP dans le réseau LAN sont attribuées par un serveur DHCP. L'adresse IP doit être activée manuellement. Remarque : la passerelle doit être configurée si la centrale doit avoir un accès à l'extérieur du réseau (pour l'utilisation 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. Exemple: 001
 - ⇒ Quand vous appuyez sur la touche ENTRER, vous entendez deux bips sonores et MISE A JOUR s'affiche dans la première ligne de l'afficheur si la passerelle est valable.
 - ⇒ L'option DHCP est affichée.
 10. Sélectionnez DHCP VALIDE ou DHCP DEVALIDE à l'aide de la touche bas/haut pour activer ou désactiver la fonction DHCP.
 11. Appuyez sur SELECT.

16.11.3 MODEMS

Le SPC système 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 performante. 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). Sur la bonne réception de l'acquittement du polling (ACK) la centrale SPC met à jour l'état du chemin à 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 les temps impartis (en fonction de la catégorie d'ATP), la centrale déclare l'état du chemin comme TOMBE.

SPC supporte les interfaces de transmission suivantes:

- Ethernet
- GSM avec GPRS validé
- Modem RTC.

	AVIS
	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.

	AVIS
	Après une réinitialisation aux paramètres d'usine, pendant la procédure de paramétrage initial depuis le clavier, la centrale détecte si un modem principal ou de sauvegarde est intégré. Si tel est le cas, elle en affiche le type 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 Pour configurer un modem

Pour configurer un modem GSM ou RTC:

1. Sélectionnez MODEMS en utilisant les touches de direction bas/haut et appuyez sur SELECT.
2. Sélectionnez PREMIER ou BACKUP suivant que vous voulez configurer le modem primaire ou le modem de secours. Appuyez sur SELECT.
⇒ L'option VALIDER MODEM est affichée.
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 REPONSE	Sélectionnez MODE REPONSE pour choisir le mode selon lequel le modem doit traiter les appels reçus. REpond JAMAIS ou REpond TOUJOURS
CODE SMS REP. TECHN. ACC.	Sélectionnez VALIDER pour répondre uniquement quand l'accès ingénieur est activé.
REGLAGES SMS	Sélectionnez VALIDER SMS pour accepter les SMS pour ce MODEM.

Option de menu	Description
	<p>Uniquement pour les modems filaires (RTC). 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.</p> <p>Pour tester manuellement les SMS, sélectionnez TEST SMS puis entrez le n° de SMS.</p> <p>Pour tester automatiquement les SMS à un intervalle horaire spécifié, sélectionnez TEST AUTOMATIQUE, choisissez un INTERVALLE DE TEST puis entrez un n° de SMS.</p>
PRÉFIXE	(Modem RTC uniquement) Entrez le préfixe à composer avant le n° de SMS, le cas échéant.
SURVEIL. LIGNE	<p>Pour les RTC : Activez cette fonction pour surveiller la tension de la ligne reliée au modem.</p> <p>Modem GSM : 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.</p> <p>Entrez le nombre de secondes pour le temporisateur de surveillance (0-9999 s).</p> <p>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 (voir Options Système).</p>



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. Dans ce cas, enlevez la carte SIM et débloquent-la en utilisant un téléphone mobile. Si la carte SIM est remplacée sur le module GSM ou si une carte SIM est utilisée avec un code, il est recommandé de programmer le code avant de placer la carte dans l'emplacement SIM pour éviter d'envoyer des codes incorrects. Toutes les sources de courant (alimentation secteur et batterie) doivent être débranchées au moment d'installer la carte SIM dans l'emplacement SIM.

16.11.4 CENTRE TELESURV.

16.11.4.1 AJOUTER

Pour programmer les paramètres de la centrale de télésurveillance:

1. Sélectionnez CENTRE TELESURV. en utilisant les touches de direction bas/haut, puis AJOUTER.
2. Appuyez sur SELECT.
3. Sélectionnez l'une des options de programmation décrites dans le tableau ci-dessous:

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

N.IDENTIFICATION	Le centre de télésurveillance appelé doit disposer de cette information. Elle est utilisée pour identifier les utilisateurs chaque fois que le CTS est appelé.
NOM DU CTS	Description du centre de télésurveillance distant.
PROTOCOLE	Le protocole de communication à utiliser (SIA, Contact Id (CID), Fast Format (FF)).
1ER N. TELEPHONE	Le premier numéro de téléphone à composer pour joindre le CTS.
2EME N.TELEPHONE	Le deuxième numéro de téléphone à composer pour contacter le CTS si le premier numéro n'a pas fonctionné.
PRIORITE	Le modem (primaire ou backup) à utiliser pour communiquer avec le CTS.

16.11.4.2 EDITER

Pour éditer les paramètres de la station centrale :

- Naviguez à Centre de réception > Modifier.
- Appuyez sur SELECT.
- Sélectionnez l'une des options de programmation décrites dans le tableau ci-dessous:
- À la fin de la programmation, l'option d'effectuer un appel d'essai au centre est affichée sur le clavier.

N.IDENTIFICATION	Le centre de télésurveillance appelé doit disposer de cette information. Elle est utilisée pour identifier les utilisateurs chaque fois que le CTS est appelé.
NOM DU CTS	Description du centre de télésurveillance distant.
PROTOCOLE	Le protocole de communication à utiliser (SIA, Contact Id (CID), Fast Format (FF)).
1ER N. TELEPHONE	Le premier numéro de téléphone à composer pour joindre le CTS.
2EME N.TELEPHONE	Le deuxième numéro de téléphone à composer pour contacter le CTS si le premier numéro n'a pas fonctionné.
NBRE DE TENTATIV	Entrez le nombre de tentatives du système pour essayer de contacter son correspondant (récepteur).
INTERVALLE NUM.	Nombre de secondes d'attente entre des échecs 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 backup) à utiliser pour communiquer avec le CTS.
TEST CYCLIQUE	Définit un calendrier de test de la connexion avec le CTS. Les valeurs possibles vont du test horaire à un test tous les 30 jours.

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 TÉLÉMAINTENANCE

1. Sélectionnez TELEMAINTENANCE puis AUTOR. TELEMANT. en utilisant les touches de direction bas/haut du clavier.
2. Appuyez sur SELECT.
3. Sélectionnez DEVALIDE ou VALIDE avec les touches de direction.
4. Sélectionnez l'une des options de programmation décrites dans le tableau ci-dessous:

ID	Numéro d'identification pour la maintenance à distance. Doit correspondre à celui de SPC Pro (1 - 999999).
MOT DE PASSE	Mot de passe pour la télémaintenance. Doit être identique à celui de SPC Pro.
CONNEX.ENTRANT E	Paramètres de la connexion entrante. Pour autoriser les connexions IP demandées par le serveur de télémaintenance entrantes, sélectionnez IP ACTIVE. Si cette option est inactive, seules les connexions par modem sont établies. Entrez le PORT TCP/IP sur lequel la centrale scrute les connexions IP demandées par le serveur de télémaintenance.
CONNEX. SORTANTE	Paramètres de la connexion sortante. Choisissez un mode d'établissement des connexions sortantes avec le serveur de télémaintenance : DESACTIVE, SUR IP, SUR MODEM.

16.12 TEST

1. Sélectionnez TEST et appuyez sur SELECT.
2. Sélectionnez l'option de programmation souhaitée en utilisant les touches de direction bas/haut.

16.12.1 TEST SIRENE

Pour effectuer un test de la sirène :

1. Sélectionnez TEST -> TEST SIRENE.
 2. Appuyez sur SELECT.
- ⇒ Quand TEST SIRENE est sélectionné, les options suivantes sont accessibles : SIRENES EXTERIEURES, FLASH, SIRENES INTERIEURES, BUZZER. Chaque fois que l'une de ces options est sélectionnée, le périphérique émet une confirmation sonore pour indiquer son fonctionnement correct.

16.12.2 TEST DEPLACEMENT

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

Pour effectuer un test de déplacement :

1. Sélectionnez TEST -> TEST DEPLACEMENT.
2. Appuyez sur SELECT.
3. Le nombre de zones à tester est affiché dans le message A TESTER XX (XX étant le nombre de zones où le test de déplacement est effectué). Localisez le premier détecteur de la première zone et activez-le (ouvrez la porte ou la fenêtre).
 - ⇒ Le buzzer du clavier retentit en continu pendant env. 2 secondes pour indiquer que l'activation de la zone a été détectée. Le nombre de zones à tester restantes diminue (affichage sur le clavier).
4. Continuez avec les zones suivantes jusqu'à ce que toutes les zones du système aient été testées. Si le système ne détecte/confirmé pas l'activation de l'une des zones, vérifiez le câblage du détecteur et, le cas échéant, remplacez-le.



AVIS

Il est possible d'inclure toutes les zones dans un test de déplacement Installateur.

16.12.3 TEST ZONE

L'option TEST ZONE permet de consulter des informations d'état de chacune des zones du système.

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

1. Sélectionnez TEST -> TEST ZONE.
2. Appuyez sur SELECT.
3. Sélectionnez la zone voulue et appuyez sur SELECT.
 - ⇒ L'état de la zone et la valeur de la résistance attribuée sont affichés.
4. Appuyez sur PROCHAIN pour localiser la zone (par exemple CONTROLEUR 1 = première zone sur la centrale).
 - ⇒ Voir la description des informations d'état dans le tableau ci-dessous (applicable à deux résistances fin de ligne).

État des zones	Abréviation
INCONNU	Royaume Uni
FERMEE	FE
OUVERTE	OP
COURT-CIRCUIT	CC
DECONNECTE	CO
NBRE IMPULSION	PU
NIVEAU ATTAQUE	GR
MASQUE	AM
DEFAULT	FA

Subst. DC	DC
HORS LIMITES	HL
ZONE INSTABLE EN MES	ZONE INSTABLE EN MHS

Le fonctionnement correct de toutes les zones d'un système peut être surveillé en lançant un test de zone.

Pour effectuer un test de zone :

1. Sélectionnez TEST ZONE en utilisant les touches de direction bas-haut.
2. Appuyez sur SELECT.
3. Sélectionnez la zone voulue et appuyez sur SELECT, ou tapez directement le numéro de la zone.
 - ⇒ Si la zone se trouve à proximité du clavier, son état peut être suivi directement sur le clavier. L'état de la zone et la valeur de la résistance sont affichés en haut à droite.
4. Changez l'état d'un détecteur, par exemple ouvrez une porte pour changer l'état du contact d'ouverture de porte.
 - ⇒ Le buzzer du clavier émet des bips sonores et l'état du détecteur passe de CL (fermée) à OP (ouverte). La valeur de la résistance affichée change suivant les résistances fin de ligne utilisées.



Il est recommandé de vérifier l'état de toutes les zones du système quand l'installation est complète. Pour localiser la zone, sélectionnez PROCHAIN (à droite) sur le clavier. L'état SH ou DI indique que la zone est court-circuitée ou déconnectée.

16.12.4 TEST SORTIE

Pour tester les sorties :

1. Sélectionnez TEST SORTIE à l'aide des touches de direction bas/haut du clavier.
2. Appuyez sur SELECT.
3. Sélectionnez l'une des options CENTRALE ou TRANSPONDEUR.
4. Pour tester les sorties de la centrale, sélectionnez la sortie voulue puis appuyez sur SELECT. Pour tester les sorties du transpondeur, sélectionnez le transpondeur, 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 de bord. 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. Sélectionnez 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.

	AVIS
	Tous les types de zones peuvent être inclus dans un test JDB.

16.12.6 OPTIONS SONORES

Les options sonores sont des indicateurs acoustiques pendant un test de déplacement.

Pour activer les options sonores :

1. Sélectionnez OPTIONS SONORES en utilisant les touches de direction bas/haut.
2. Appuyez sur SELECT.
3. Déplacez le curseur sur l'une des options suivantes à l'aide des touches de navigation : TOUT, SIRENE INTERIEURE, SIRENE EXTERIEURE, CLAVIER
4. Appuyez sur SAUVER.
5. Appuyez sur la touche RETOUR pour quitter le menu.

16.12.7 IND. VISUELS

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 VISUAL IND.
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 la touche RETOUR pour quitter le menu.

16.12.8 TEST WPA

	AVIS
	Ce test doit être effectué exclusivement par un installateur ou un utilisateur en possession du droit de test du WPA. Voir Droits d'utilisateur.

Pour tester le WPA depuis le clavier :

1. sélectionnez TEST WPA et appuyez sur SELECT.
 2. Quand un message demande d'activer le 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 testées.
1. Répétez le test si nécessaire.
 2. Appuyez sur RETOUR ou X pour terminer le test.

16.12.9 TEST SISMIQUE

Pour effectuer un test sismique :

1. Sélectionnez TEST -> TEST SISMIQUE.
2. Appuyez sur SELECT.
3. Sélectionnez TEST TOUS SECTEURS ou sélectionnez un secteur voulu.
4. Si vous sélectionnez un secteur donné pour le test, vous pouvez sélectionner TEST TOUS ZONES ou une zone sismique particulière à tester.
 - ⇒ Le message TEST SISMIQUE est affiché sur le clavier pendant que le test est exécuté.
 - ⇒ En cas d'échec du test, le message SISMIQUE ERREUR est affiché. Si vous appuyez sur la touche « i » ou VOIR, la liste des zones en échec est affichée. Vous pouvez faire défiler cette liste pour la voir en entier.
 - ⇒ Si le test aboutit, TEST OK est affiché.

Voir également Test du capteur sismique [→ 343].

16.13 UTILITAIRES

1. Sélectionnez UTILITAIRES en utilisant les touches de direction bas/haut et appuyez sur SELECT.
2. Sélectionnez l'option de programmation souhaitée :

SOFTWARE SYSTEME	Affiche la version du logiciel.
PAR DEFAUT	Permet de réinitialiser les utilisateurs ou de réinitialiser le système avec les valeurs par défaut au départ usine.
BACKUP CONFIG	Permet de sauvegarder une configuration.
RESTAURER CONFIG	Permet de charger une configuration.
PROGRAMMEUR RAPIDE	<ul style="list-style-type: none"> ● CENTRALE -> CLE: Transfert des données de la centrale vers le programmeur rapide. Un message vous demande de confirmer que le nom de fichier de la nouvelle configuration est le même qu'un nom de fichier existant afin d'éviter l'écrasement des fichiers de configuration. ● CLE -> CENTRALE: Transfert des données du programmeur rapide vers la centrale. ● EFFACER FICHIERS

	<ul style="list-style-type: none"> ● MAJ FIRMWARE Remarque : si vous revenez à une version antérieure du firmware (par exemple en installant une version moins récente), le système rétablira tous les paramètres par défaut. De même, si vous revenez à une version antérieure du micrologiciel, il est important de faire de même avec le logiciel du périphérique correspondant. Dans le cas contraire, des zones peuvent apparaître déconnectées, ouvertes ou fermées. ● UPGRADE PÉRIPHÉRIQUE : ● MISE À JOUR DE LA LANGUE :
SPC PRO / SPC SAFE	<p>Pour programmer les options suivantes de SPC PRO :</p> <ul style="list-style-type: none"> ● ACCÈS ACTIVÉ : indique si SPC Pro est activé ou désactivé. ● ACCÈS INSTALLAT. : indique si l'accès installateur est actif ou inactif. ● MOT DE PASSE : permet de modifier le mot de passe système. ● IP ACTIVE : active/désactive la connexion au système par IP. ● PORT TCP/IP : Sélectionnez le Port IP de connexion pour SPC Pro/SDK.
RESET SYSTEM	Pour redémarrer le système.
LICENCE	Entrez un numéro de licence pour changer la licence du SPC. Le système n'enregistre ni ne transmet les changements de licence.

16.14 ISOLER

Les zones, les alertes système ou les alertes des périphériques reliés au X-BUS peuvent être isolées manuellement à l'aide du clavier. Le fait d'isoler une zone masque celle-ci dans le système jusqu'à ce que l'utilisateur annule l'isolation.

Pour isoler les zones, les alertes système ou les alertes des périphériques du X-BUS :

1. Sélectionnez ISOLER en utilisant les touches de direction bas/haut et appuyez sur SELECT.
2. Sélectionnez l'option souhaitée dans le tableau ci-dessous et appuyez sur SELECT.

ZONE	Sélectionnez la zone requise et basculez le paramètre de NON ISOLE à ISOLE.
SYSTEME	Isole l'alerte système voulue.
XBUS	<p>Permet d'isoler une alerte donnée par des TRANSPONDEURS ou des CLAVIERS :</p> <ul style="list-style-type: none"> ● COMM. XBUS PERDUE ● DEFAUT FUS. XBUS (uniquement pour les transpondeurs) ● AUTOSURVEILLANCE X-BUS
VOIR ISOLEES	Affiche la liste des zones, des alertes systèmes et des alertes des périphériques X-BUS isolées.

16.15 JOURNAL DE BORD

Les événements récemment journalisés par le système peuvent être consultés avec l'option JOURNAL DE BORD. Les événements clignotent, un par seconde.

1. Sélectionnez JOURNAL DE BORD en utilisant les touches bas/haut et appuyez sur SELECT.

2. Pour consulter les événements d'une date donnée, entrez la date en utilisant les touches numériques.
 - ⇒ L'événement le plus récent est affiché dans la ligne inférieure de l'afficheur. Tous les événements précédents défilent en restant affichés pendant 1 seconde (ou faites défiler en appuyant sur les touches de direction).

16.16 ACCES JDB

L'accès aux zones du système est affiché dans l'option ACCES JDB.

1. Sélectionnez ACCES JDB et appuyez sur SELECT.
2. Sélectionnez une porte du système pour laquelle vous voulez afficher les événements d'accès.
 - ⇒ Les événements d'accès les plus récents sont affichés avec la date et l'heure.
3. Faites défiler la liste des événements, ou entrez une date et appuyez sur ENTRER pour trouver un événement 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
 - Code contrainte
 - XBUS Panique
 - Panique utilis.
 - WPA Paniq.

16.18 MODIFIER CODE INSTALLATEUR

Pour modifier le code installateur :

1. Sélectionnez CHANGER SON CODE puis appuyez sur SELECT.
 - ⇒ Un code généré automatiquement est affiché.
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 configurée dans le champ Tailles des codes du menu 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 SAUVER.

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 GESTION UTILISAT

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 au système :

1. Sélectionnez le menu GESTION UTILISAT -> AJOUTER en utilisant les touches de direction bas/haut du clavier.
 - ⇒ 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 EDITER

Pour modifier un utilisateur du système:

1. Sélectionnez GESTION UTILISAT -> EDITER en utilisant les touches de direction bas/haut du clavier.
2. Appuyez sur SELECT.
3. Modifiez l'un des paramètres d'utilisateur décrits dans le tableau ci-dessous.

CHANGER LE NOM	Permet de modifier le nom d'utilisateur.
PROFIL D'UTILISATEUR	Sélectionnez le profil du nouvel utilisateur.
CONTRAINTE	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.
TAG	Permet d'activer ou de désactiver la prise en charge des tags (PACE).
TELECOMMAND E	Permet d'activer ou de désactiver l'accès par télécommande radio (clavier radio, télécommande)
MOD-TRAVAI- ISOLE	Active le test d'alerte accident.
CONTROLE D'ACCES	Si un badge n'est pas attribué à l'utilisateur: <ul style="list-style-type: none"> ● AJOUT BADGE ● ENROLEMENT BADGE Quand un badge est attribué à l'utilisateur:

	<ul style="list-style-type: none"> ● EDITER BADGE <ul style="list-style-type: none"> - NUMERO BADGE - ATTRIBUTS DU BADGE (voir Contrôle d'accès) ● RAZ BADGE ● EFFACER BADGE
LANGUE	Sélectionnez une langue pour cet utilisateur.

16.19.2.1 CONTROLE D'ACCES

Il est possible d'attribuer un badge d'accès à chacun des utilisateurs de la centrale.
 Pour configurer le contrôle d'accès pour un utilisateur:

1. Sélectionnez GESTION UTILISAT -> EDITER en utilisant les touches de direction bas/haut du clavier.
2. Appuyez sur SELECT.
3. Sélectionnez l'utilisateur à configurer et appuyez sur SELECT.
4. Sélectionnez CONTROLE D'ACCES et appuyez sur SELECT.

Pour lire les instructions sur les options de programmation du contrôle d'accès, sélectionnez les liens ci-dessous.

16.19.2.1.1 AJOUT DE BADGE en mode manuel

Si le format du numéro de badge est connu, le badge peut être créé manuellement.

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

1. Sélectionnez AJOUT BADGE en utilisant les touches de direction bas/haut du clavier.
 2. Appuyez sur SELECT.
- ⇒ Un badge vierge est créé. Il peut être édité dans l'étape suivante.

16.19.2.1.2 ENROLEMENT BADGE

	AVIS
	Seuls les badges dont le format est pris en charge peuvent être programmés par apprentissage.

Si le numéro de badge ou le format du badge est inconnu, le badge peut être lu et ses informations acquises.

1. Sélectionnez ENROLEMENT BADGE en utilisant les touches de direction bas/haut du clavier.
2. Appuyez sur SELECT.
3. Sélectionnez la porte où le badge sera présenté.
4. Appuyez sur SELECT.

	AVIS
	Le nouveau badge peut être présenté au lecteur de sortie et au lecteur d'entrée de la porte sélectionnée.

5. Présentez le badge à l'un des lecteurs de la porte sélectionnée.
- ⇒ Les informations du nouveau badge sont acquises.

16.19.2.1.3 EDITER BADGE

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

1. Sélectionnez EDITER BADGE en utilisant les touches de direction bas/haut du clavier.
2. Appuyez sur SELECT.
3. Modifiez l'un des paramètres d'utilisateur décrits dans le tableau ci-dessous.
4. Appuyez sur la touche RETOUR pour quitter le menu.

Contrôle d'accès

Attribut	Description
Numéro badge	Entrer le numéro de badge Entrez 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.
Priorité	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 : <ul style="list-style-type: none"> ● SPC4xxx – tous les utilisateurs ● SPC5xxx – 512 ● SPC6xxx - 512
Escorte	La fonction Escorte permet à des détenteurs de carte à accès privilégié d'escorter d'autres détenteurs de carte au travers de portes spéciales. 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 de la carte d'escorte et celle de la carte normale 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

Attribut	Description
	<p>badge non-gardien dans celle-ci.</p> <p>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.</p>

16.19.2.1.4 EFFACER BADGE

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

1. Sélectionnez EFFACER BADGE en utilisant les touches de direction bas/haut du clavier.
2. Appuyez sur SELECT.

16.19.2.1.5 RAZ BADGE

Si la fonction Passback physique est active dans une pièce et qu'un utilisateur quitte cette pièce sans utiliser le lecteur de sortie, cet utilisateur n'est pas autorisé à pénétrer une nouvelle fois dans cette pièce. Le badge de l'utilisateur peut être réinitialisé pour permettre à l'utilisateur de présenter son badge une nouvelle fois sans que le retour soit vérifié.

Pour réinitialiser le badge à l'aide du clavier:

1. Sélectionnez RAZ BADGE en utilisant les touches de direction bas/haut du clavier.
2. Appuyez sur SELECT.

16.19.3 EFFACER

Pour effacer un utilisateur du système:

1. Sélectionnez le menu GESTION UTILISAT -> EFFACER en utilisant les touches de direction bas/haut du clavier.
2. Appuyez sur SELECT.
 - ⇒ Une invite apparaît, vous demandant si vous confirmez votre commande de suppression.
3. Appuyez sur OUI pour effacer l'utilisateur.

16.20 PROFILS UTILISATEUR

Voir aussi

📖 Ajouter/Modifier un profil utilisateur. [→ 201]

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 PROFILES 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 EDITER

Pour modifier des profils d'utilisateur dans le système :

1. Passer à PROFILES 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.
ACCES SECTEUR	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 utilisateur [→ 201].
PORTE	Sélectionnez le type d'accès disponible pour ce profil, pour les portes configurées. Les options sont AUCUN, PAS H.LIMITE ou CALENDRIER.
CODE SITE	Saisissez un code de site pour toutes les cartes utilisant ce profil.

16.20.3 EFFACER

Pour effacer des profils d'utilisateur du système :

1. Passer à PROFILES 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

Les alertes SMS prise en charge par le système SPC doivent être communiquées par la centrale à l'installateur ainsi qu'à des téléphones portables 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 le menu OPTIONS [→ 119]), 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 aussi bien la notification que 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 :

- Activation / Désactivation
- Autoriser / interdire l'accès de l'installateur
- Autoriser / interdire l'accès du constructeur
- Activer / désactiver l'interaction logique

Événements SMS

La notification par SMS peut être configurée pour communiquer des événements tels que :

- Début d'alarme
- Alarmes confirmées
- Défaut / autosurveillance
- Activation / désactivation
- Inhibition / isolement
- Tout autre type d'événements

16.21.1 AJOUTER

- ▷ Un modem est installé et le système l'a identifié.
- ▷ La fonction **Authentification SMS** est activée dans OPTIONS [→ 119].
- 1. Passez à 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 EDITER

- ▷ Un modem est installé et le système l'a identifié.
- ▷ La fonction **Authentification SMS** est activée dans OPTIONS [→ 119].
- 1. Passez à SMS -> Editer et appuyez sur SÉLECTIONNER.
- 2. Sélectionnez un ID SMS d'ingénieur ou d'utilisateur à éditer.

ID SMS Utilisateur	ID générée par le système
NUMERO SMS	Entrez le numéro de destination du SMS (avec l'indicatif du pays à trois chiffres). Remarque : Le Numéro SMS installateur peut être supprimé fixant la valeur à 0. Les numéro SMS Utilisateur ne peuvent pas être supprimés.
Utilisateur	Sélectionnez un nouvel utilisateur pour cette ID SMS Utilisateur, le cas échéant.
Evénements SMS	Sélectionnez les événements centrale devant être envoyés par SMS à l'utilisateur ou à l'installateur.
Contrôle par SMS	Sélectionnez les opérations pouvant être effectuées à distance sur la centrale par SMS. Voir Commandes SMS [→ 206]

!	AVIS
	Les événements HOLDUP ne sont pas transmis par SMS.



Si la ligne téléphonique est reliée au RTC via un autocommutateur privé (PABX), le préfixe de prise de ligne adéquat doit précéder le numéro de l'appelé. Assurez-vous que le service Calling Line Identity (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. Passez à 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 n'est plus pris en charge à partir de la version 3.4. La fonctionnalité est conservée pour le produit, afin que la compatibilité en arrière soit maintenue.

X10 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 X10. La centrale SPC possède un port série dédié (port série 1) servant d'interface directe pour les périphériques X10 standard.

1. Sélectionnez X-10 en utilisant les touches de direction bas/haut et appuyez sur SELECT.

2. Sélectionnez l'option de programmation souhaitée :

VALIDER X-10	Permet d'activer ou de désactiver X-10.
ELEMENTS	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 MODIF DATE/HEURE

La date et l'heure du système peuvent être réglés manuellement. La date et l'heure sont affichés sur le clavier et dans le navigateur Web. Ces informations sont utilisées pour les fonctions de programmation horaire.

- Sélectionnez MODIF DATE/HEURE en utilisant les touches de direction bas/haut et appuyez sur SELECT.
 - ⇒ La date est affichée dans la ligne supérieure de l'afficheur.
- Utilisez les touches numériques pour entrer la date. Pour déplacer le curseur à droite ou à gauche, appuyez sur la touche de direction droite ou gauche.
- Appuyez sur ENTRER pour enregistrer la nouvelle date.
 - ⇒ Si vous entrez une date incorrecte, le message VALEUR INVALIDE est affiché pendant 1 seconde.
- Utilisez les touches numériques pour entrer l'heure. Pour déplacer le curseur à droite ou à gauche, appuyez sur la touche de direction droite ou gauche.
- Appuyez sur ENTRER pour enregistrer la nouvelle heure.
 - ⇒ Si vous entrez une heure incorrecte, le message VALEUR INVALIDE est affiché pendant 1 seconde.

16.24 TEXTE INSTALLAT.

Ce menu permet à l'installateur d'entrer des informations sur le système et ses données de contact.

- Sélectionnez TEXTE INSTALLAT. en utilisant les touches de direction bas/haut du clavier et appuyez sur SELECT.
- Sélectionnez l'option de programmation souhaitée :

NOM DU SITE	Utilisé pour identifier le système. Entrez un nom descriptif clair et descriptif.
NUMERO DU SITE	Permet d'identifier le système quand il connecté à un centre de télésurveillance (10 caractères max.).
NOM INSTALLATEUR	Utilisé pour contacter l'installateur.
TEL INSTALLATEUR	Utilisé pour contacter l'installateur.
AFFICH. INSTALLATEUR	Permet d'afficher ou de masquer les données de l'installateur pendant les périodes d'inactivité.



Les données de contact de l'installateur entrées dans ce menu devraient également être inscrites sur la fiche signalétique déroulante du clavier à la fin de l'installation.

16.25 CONTROLE PORTES

Cette option vous permet de commander toutes les portes du systèmes.

1. Sélectionnez CONTROLE PORTES en utilisant les touches bas/haut du clavier et appuyez sur SELECT.
2. Sélectionnez la porte à commander et appuyez sur SELECT.
3. Sélectionnez l'état à appliquer à la porte et appuyez sur SELECT. Les états sont décrits dans le tableau suivant.

NORMAL	La porte est en mode de fonctionnement normal. Un badge possédant les droits d'accès correspondants est requis pour ouvrir la porte.
DEVERR.TEMP ORAIR	La porte est ouverte seulement pendant un intervalle minuté pour permettre l'accès.
VERROUILLE	La porte est verrouillée. La porte reste fermée même si un badge avec les droits d'accès nécessaires est présenté.
DEVERROUILL E	La porte est déverrouillée.

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 de détails, voir Codes Installateur [→ 110].

Le 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 du Mode Exploitation

Ces fonctions peuvent être programmées sans que le système d'alarme doive être désactivé. Elles sont accessibles directement après la connexion en mode Installateur.

Mode Paramétrage

En mode Paramétrage, le système d'alarme doit être désactivé avant que la programmation puisse commencer. Les fonctions sont accessibles en cliquant sur le bouton Passage en mode Paramétrage.



AVIS

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 d'exploitation.

Le serveur Web sur la centrale SPC est accessible via l'interface Ethernet ou USB.

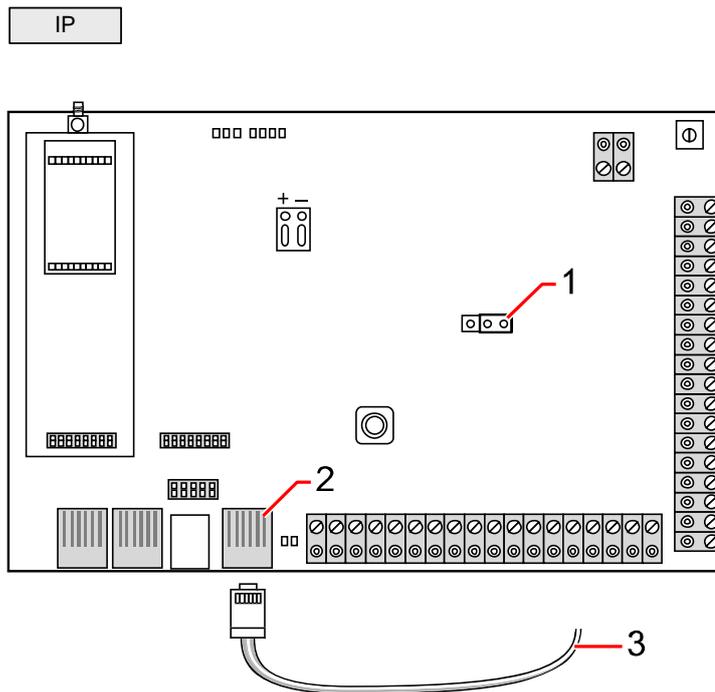


Dans le navigateur Web, les modifications doivent être enregistrées expressément en cliquant sur le bouton **Enregistrer**. Pour consulter les valeurs de programmation actives sur une page Web, cliquez sur **Rafraîchir**.

17.1 Infos sur le système

Cliquez sur l'icône ? pour voir le menu Aide qui fournit des informations actualisées sur la centrale et la fonctionnalité pour laquelle vous disposez d'une licence sur le système.

17.2 Interface Ethernet



Connectique

1	JP9 SPG4xxx
2	Port Ethernet
3	Vers le port Ethernet du PC



Si le port Ethernet du SPC doit être connecté à un réseau local (Local Area Network), consultez l'administrateur de ce réseau avant de connecter ce dernier à la centrale. Adresse IP par défaut : 192.168.1.100

Branchement du câble

- Reliez le port Ethernet de la carte de la centrale au réseau en utilisant un câble Ethernet
– OU –
Reliez le port Ethernet directement à un PC en utilisant un câble null modem.
Voir ici [→ 351].
- ⇒ Les témoins LED à droite du port Ethernet indiquent une liaison de données active (la LED droite est allumée) et un trafic de données Ethernet (la LED gauche clignote).

Détermination de l'adresse IP de la centrale SPC

1. Entrez dans le mode d'installateur (voir Codes Installateur [→ 110]).
2. Utilisez les touches de direction bas/haut pour afficher l'option COMMUNICATION et appuyez sur SELECT.
3. Sélectionnez PORT ETHERNET et appuyez sur SELECT.

4. Sélectionnez **ADRESSE IP** et appuyez sur **SELECT**.

17.3 Connexion USB à la centrale



Si la centrale est réinitialisée pendant que le câble USB est connecté, déconnectez puis reconnectez le câble.

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.

- ▷ SPC Pro doit être installé sur votre PC.
 - ▷ Un câble USB connecte 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. Appuyez sur **Suivant**.
 - ⇒ Windows XP détecte un concentrateur USB générique.
 3. Cliquez sur **Terminer**.
 - ⇒ 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 Intronet SPC USB**
 7. Cliquez sur **Suivant**.
 - ⇒ La boîte de dialogue du certificat Windows est affichée. Vanderbilt estime qu'il est sûr de continuer. Pour toute question, adressez-vous à l'administrateur réseau ou contactez un technicien Vanderbilt.
 8. Cliquez sur **Continuer**.
 - ⇒ L'installation est terminée.
 9. Cliquez sur **Terminer**.
 - ⇒ 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 demande d'entrer le nom d'utilisateur et le mot de passe de la connexion USB. Entrez les données suivantes:
 - Nom d'utilisateur : SPC
 - Mot de passe : password (par défaut)
11. Cliquez sur **Se connecter**.
 - ⇒ Le PC établit une liaison de données avec la centrale. Dès que la liaison est établie, une icône correspondante est affichée dans la barre des tâches du PC.
12. Faire un clic droit sur le lien et sélectionnez **État**.
 - ⇒ L'adresse IP du serveur est affichée dans la fenêtre des détails.
13. Entrez cette adresse dans la barre d'adresse du navigateur Web en utilisant une liaison sécurisée **hyper text transfer protocol secure** (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

- ▷ Suivez les instructions pour SPCPro de la Connexion USB sur Windows 7 pour SPCPro
 - ▷ 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 fenêtre correspondante s'ouvre.
 3. Sélectionnez l'onglet **Modems** et cliquez sur **Ajouter**.
 - ⇒ La fenêtre **The 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 **Suivant**.

7. Sélectionnez le port COM assigné à la Connexion USB sur Windows 7 pour SPCPro.
8. Cliquez sur **Suivant**, puis sur **Terminer**.
9. Retournez à l'onglet **Modems** de la fenêtre **Téléphone et modem**.
10. Sélectionnez le nouveau modem et cliquez sur **Propriétés**.
 - ⇒ La fenêtre **Propriétés de Communications cable between two computers** est affichée.
11. Dans l'onglet **Général**, cliquez sur **Modifier les paramètres** pour permettre la modification des propriétés.
12. Sélectionnez l'onglet **Modem**.
13. Modifiez la valeur dans **Vitesse maximale du port** à **115200** et cliquez sur **OK**.
14. Dans le **Panneau de contrôle**, ouvrez **Centre Réseau et partage**.
15. Cliquez sur **Modifier les paramètres de l'adaptateur**. Si un nouveau modem est présent dans la liste des connexions disponibles, passez à l'étape 23. Si le modem n'est *pas* présent, exécutez les actions suivantes :
16. dans le **Centre Réseau et partage**, cliquez sur **Configurer une connexion ou un réseau**.
17. Sélectionnez **Configurer une connexion par modem à accès à distance** puis cliquez sur **Suivant**.
18. 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**.
19. Cliquez sur **Se connecter**.
 - ⇒ Windows 7 crée la connexion.
20. Passez outre l'étape **Test de la connexion Internet**.
21. Cliquez sur **Fermer**.
22. Dans le **Centre Réseau et partage**, cliquez sur **Modifier les paramètres de l'adaptateur**.
23. Double-cliquez sur le nouveau modem.
 - ⇒ La fenêtre **Connecter nomdeconnexion** s'ouvre (le *nomdeconnexion* est le nom que vous avez défini pour le modem).
24. Cliquez sur **Propriétés**.
25. Assurez-vous que le champ **Se connecter avec** : contient les informations correctes, Communications cable between two computers (COM3), par exemple.
26. Ouvrez votre explorateur et saisissez l'adresse IP du contrôleur en vous servant de https comme protocole de connexion.
27. Cliquez sur **Continuer** si le navigateur affiche une page d'erreur de certificat.
28. Connectez-vous à la centrale.

17.4 Connexion avec le navigateur

Pour se connecter au système avec le navigateur Web:

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 Web en utilisant une liaison sécurisée avec le protocole **hyper text transfer protocol secure**. (par ex. [https:// 192.168.1.100](https://192.168.1.100)). Voir tableau ci-dessous.
 - ⇒ Un message de sécurité est affiché.
3. Cliquez sur **Continuer vers se site Web**.
 - ⇒ L'écran de connexion apparaît.

4. Entrez les données suivantes:
 - **ID utilisateur** : nom de l'utilisateur ou de l'installateur.
 - **Mot de passe** : Code Utilisateur ou Code Accès Installateur.
5. Sélectionnez la langue d'affichage des écrans du navigateur. Le paramètre de langue par défaut « Auto » chargera automatiquement la langue affectée à cet 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 (backup) / RS232	192.168.3.1 (fixé)
Modem primaire (premier)	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 Récapitulatif 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 de toutes les zones isolées et permet de retirer l'isolation ou le contournement (bypass) avant les réglages.

TOUS SECTEURS		MHS	MES Totale
Alertes système actives			
Aucun			
Avertissements et information			
Accès Installateur autorisé			
Installateur sur site			
Empêche la MES			
Zone 25: Zone 25	Activée	Inhiber	Isoler
Zone 26: Zone 26	Activée	Inhiber	Isoler
Zone 27: Zone 27	Activée	Inhiber	Isoler
Installateur sur site	Information		
Inhibe et isole			
Défaut batterie centrale	ISOLEE		Restaurer
Autosurveillance Sirène	ISOLEE		Restaurer
Autosurveillance boîtier centrale	ISOLEE		Restaurer
IO 1 Défaut batterie transpondeur X-BUS	ISOLEE		Restaurer



AVIS

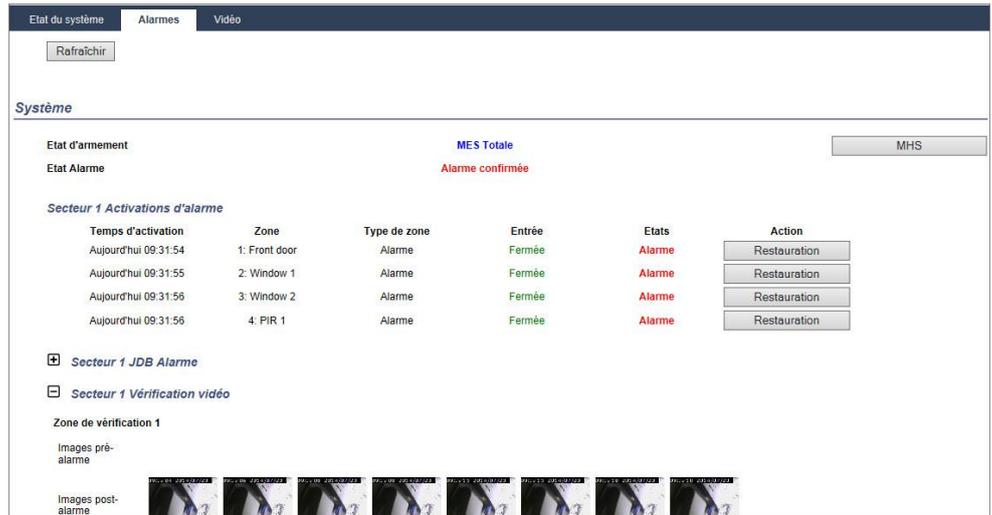
Si des alarmes sont activées sur le système, le message d'information **Voir l'onglet - Alarmes** s'affiche.

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.

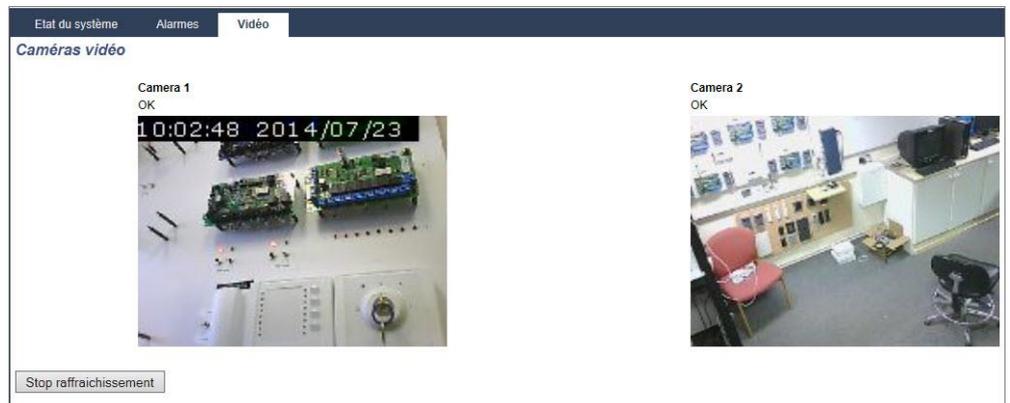
Pour chaque secteur, les états suivants sont affichés : **État d'armement**, **État Alarme**, **Activations d'alarme** et **JDB Alarme**. Les **Activations d'alarme** affichent une liste de zones en état d'alarme commandées par l'activation. Cliquez sur le bouton **Restauration** pour vider la liste. 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**. Dans l'exemple suivant, seules trois caméras sont disponibles.



Les images sont automatiquement rafraîchies à la fréquence configurée sur la caméra. (Voir Configuration de la vidéo [→ 275])

Cliquez sur **Stop rafraîchissement** pour garder l'image actuelle sur l'écran et stopper le rafraîchissement. Cliquez sur **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 sous SPC Pro et 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	Libellé
OK	La caméra se comporte normalement.

Message	Libellé
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 de forme erronée a été envoyée à la caméra. Vérifier 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 est incorrect
Inconnu	Une erreur inconnue a été renvoyée. Le modèle de caméra peut ne pas être pris en charge.

17.6 État de la centrale

17.6.1 État

Cette page fournit des informations sur l'état des composants principaux du SPC, incluant le système, l'alimentation, le X-BUS et les communications.

1. Sélectionnez **État > Hardware > État Centrale**.
2. Voir les tableaux ci-dessous pour de plus amples informations.

Hardware	Entrées & Portes	Portes	FlexC	Alertes Système
Etats Centrale				
Etats X-Bus				
Etat Radio				
Système				
Heure Système: Mer, 23 Jul 2014 10:03:40				
Autosurveillance coffret: Isolier				
Autosurveillance Aux. 1: OK				
Autosurveillance Aux. 2: OK				
Autosurveillance Sirène: Isolier				
Module Radio: SiWay - V5				
Autosurveillance Antenne: OK				
Alimentation				
Alimentation: OK				
SYNCHRO SUR 50Hz: OK (50Hz)				
Batterie: Isolier				
Tension Batterie: N/A				
Courant Batterie: N/A				
Tension auxiliaire: 13.5V				
Courant auxiliaire: 200mA				
Fusible Auxil.: OK				
Fusible sirène extérieure: OK				
Fusible sirène intérieure: OK				
X-BUS				
Etat du X-BUS: OK				
Périphériques en ligne: 11				
Périphériques Comms: OK				
Périphériques Autosurv. Coffret: Isolier				
Ethernet				
Adresse MAC: 00:0F:B6:03:1A:F1				
Adresse IP: 10.100.82.181				
Masque sous réseau: 255.255.0.0				
Passerelle: 0.0.0.0				
Reçoit: 1 M Paquets, 123 M Octets				
Transmis: 24 K Paquets, 5 M Octets				
Modem 1				
Etat Modem: Défaut: défaut ligne <input type="button" value="JDB"/>				
Type modem pluggé: IntelliModem PSTN				
Etat de la ligne: Défaut				
Appels entrants: 0 (0 Seconds)				
Appels sortants: 0 (0 Seconds)				
SMS entrant: 0				
SMS sortant: 0				
Echec essais numérotation: 0				
Modem 2				
Etat Modem: Modem hors service				
Type modem pluggé: -				
Etat de la ligne: -				
Appels entrants: -				

Actions exécutables

Les actions suivantes ne sont possibles que si une connexion a été établie.

RAZ toutes les alertes <input type="button" value="Pro"/>	Remet à zéro toutes les alertes actives sur la centrale. Ces messages d'alerte sont affichés en rouge en regard de l'élément en question.
Rafraîchir	Met à jour l'affichage après une modification de l'état. Appuyez sur ce bouton dans la fenêtre Etats pour suivre la situation en temps réel.
Mode	Permet de passer du mode Paramétrage au mode Exploitation et inversement.

Paramétrage / mode 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 fenêtre ci-dessous où figure l'état des différents tags 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 ici [→ 220]).
- Claviers (pour programmer les claviers, voir ici [→ 225]).
- Contrôleurs de porte (pour programmer les contrôleurs de porte, voir ici [→ 228]).

3. Cliquez sur l'un des paramètres identifiant un clavier/transpondeur/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.

Hardware							
Entrées & Portes							
Etats Centrale							
Etats X-Bus							
Etat Radio							
Transpondeurs							
ID	Libellé	Type	N° Série	Version	Comms.	Etats	ALIM
1	IO 1	E/S [8 Entrée / 2 Sortie]	11327907	1.11 [07AUG13]	Online	Isoler	Type 1 - V4
2	AEX 2	Audio [4 Entrée]	1434900	1.03 [13MAR13]	Online	OK	Non connecté
3	AEX 3	Audio [4 Entrée / 1 Sortie]	37070907	1.03 [13MAR13]	Online	OK	Non connecté
4	WIR 4	Radio	489907	1.11 [07AUG13]	Online	Isoler	Non connecté
5	IOA 5	E/S analysées [8 Entrée / 2 Sortie]	165074801	2.00 [09Apr14]	Online	Isoler	Non connecté
6	IO 6	E/S [8 Sortie]	443907	1.11 [07AUG13]	Online	OK	Non connecté
7	KSW 7	Boîtier à clé [1 Sortie]	226593801	1.01 [11NOV10]	Online	Isoler	Non connecté
8	IND 8	Indicateurs [1 Entrée]	223387801	1.03 [13MAR13]	Online	OK	Non connecté

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, chargeur, 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).
ALIM	Le type d'ALI affecté au transpondeur, le cas échéant. Cliquez sur le chargeur pour afficher son état.

Actions exécutables

Rafraîchir	Cliquez sur ce bouton pour mettre à jour l'affichage de l'état de la 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.

	Entrée	Etats	Action
Communication	OK	OK	Inhiber Isoler
Autosurveillance coffret	Défaut	Isoler	Restaurer
Défaut centrale fusible	OK	OK	Inhiber Isoler
Défaut 230V	OK	OK	Inhiber Isoler
En défaut ou manquant	Défaut	Isoler	Restaurer
Défaut Alim Centrale	Défaut	Isoler	Restaurer

Nom	Description
Communication	L'état physique (OK, Défaut) et l'état programmé (OK, Isolé, Inhibé) de la connexion par câble de la X-BUS au transpondeur.
Autosurveillance coffret	L'état physique et l'état programmé de l'autosurveillance du coffret.
Défaut fusible	L'état physique et l'état programmé du fusible du transpondeur.
Défaut 230V centrale	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 Chargeur	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.
Inhiber 	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 aussi

 [Etat de l'alimentation \[→ 183\]](#)

17.6.2.2 Etat de l'alimentation

La fenêtre **Etat de l'alimentation** affiche les détails sur l'état courant du module d'alimentation et ses sorties, en plus de l'état de toutes les batteries connectées.

Les types de modules d'alimentation pris en charge sont les suivants :

- SPCP332/333 Smart PSU
- SPCP355.300 Smart PSU

SPCP332/333 Smart PSU Status

L'image suivante montre l'état de la Smart PSU :

Hardware	Entrées & Portes	Portes	FlexC	Alertes Système
Etats Centrale				
Etats X-Bus				
Etat Radio				
Transpondeurs				
Claviers				
Contrôleurs de porte				

Etat de l'alimentation

Type	ALIM Vds
Version	Version Hardware: 1 Version Firmware: 1.1 [04JUL13]
Etat 230V	OK
Température	24 °C
Tension de charge	14.4 V
Courant de charge	17 mA
Etat de la charge	Charge complète
Circuit primaire	OK
Circuit de charge	OK

Batterie

	Tension	Actuel
Batterie 1	13.6V	0mA
Batterie 2	0.4V	0mA

Sorties

	Tension	Fusible	AUTOSUR.
Sortie Alim 1	OK	-Fusible OK	
Sortie Alim 2	OK	Fusible OK	

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 ou 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 de la SPCP355.300 Smart PSU :

Hardware		Entrées & Portes		Portes		FlexC		Alertes Système	
Etats Centrale		Etats X-Bus		Etat Radio					
Transpondeurs		Claviers		Contrôleurs de porte					
Etat de l'alimentation									
Type	1								
Version	4								
Etat 230V	OK								
Batterie lien	Batterie 7Ah								
Etat Batterie	En défaut ou manquant								
Tension Batterie	0.0V								
Courant Batterie	0mA								
		Tension		Actuel		Fusible			
Sortie 1		13.7V		351mA		OK			
Sortie 2		13.7V		0mA		OK			
Sortie 3		13.7V		0mA		N/A			

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.
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'auto-surveillance 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.

Hardware						
Entrées & Portes						
Portes						
FlexC						
Alertes Système						
Etats Centrale						
Etats X-Bus						
Etat Radio						
Transpondeurs						
Claviers						
Contrôleurs de porte						
ID	Libellé	Type	N° Série	Version	Comms.	Etats
1	CKP 1	Clavier confort SPCK62x	227361801	1.02 [13MAR13]	Online	OK
2	KEY 2	Claviers	559907	2.09 [13MAR13]	Online	OK

Rafraîchir

Nom	Description
ID Transpondeur	Ce numéro unique identifie le clavier.
Description	Texte descriptif du clavier (16 caractères maximum).
Type	Le type de transpondeur détecté (= clavier)
N° Série	Le numéro de série du clavier.
Version	La version du firmware du clavier.
Comms	L'état du clavier (en ligne ou hors ligne).
Etat	L'état du clavier (OK, défaut).

Actions exécutables

Rafraîchir	Cliquez sur le bouton Actualiser 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 coffret	L'état physique et l'état programmé de l'autosurveillance du coffret.
TAG	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.
Inhiber ⓘ	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.

Hardware		Entrées & Portes		Portes		FlexC		Alertes Système	
Etats Centrale		Etats X-Bus		Etat Radio					
Transpondeurs		Claviers		Contrôleurs de porte					
ID	Libellé	Type	N° Série		Version	Comms.	Etats	ALIM	
1	DC2 1	DC-2 [4 Entrée / 2 Sortie]	195309801		2.00 [07APR14]	Online	Isoler	Non connecté	
<input type="button" value="Rafraîchir"/>									

ID Transpondeur	Ce numéro unique identifie le contrôleur de porte.
Libellé	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).
Etats	L'état du contrôleur de porte (OK, Défaut).
ALIM	Indique si le contrôleur de porte est équipé d'un module d'alimentation.

Actions exécutables

Rafraîchir	Cliquez sur ce bouton pour mettre à jour l'affichage de l'état des alertes.
------------	---

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.

Hardware		Entrées & Portes		Portes		FlexC		Alertes Système	
Etats Centrale		Etats X-Bus		Etat Radio					
Transpondeurs		Claviers		Contrôleurs de porte					
Statut du Transpondeur									
Contrôleur de Porte		1 DC2 1							
Type		DC-2 [4 Entrée / 2 Sortie]							
N° Série		195309801							
Version Firmware		2.00 [07APR14]							
Tension		11.0 V							
Actuel		N/A							
		Entrée		Etats		Action			
Communication		OK		OK		<input type="button" value="Inhiber"/> <input type="button" value="Isoler"/>			
Autosurveillance coffret		Défaut		Isoler		<input type="button" value="Restaurer"/>			
Défaut centrale fusible		OK		OK		<input type="button" value="Inhiber"/> <input type="button" value="Isoler"/>			
AP faux codes		OK		OK		<input type="button" value="Inhiber"/> <input type="button" value="Isoler"/>			
<input type="button" value="Retour"/>									

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 coffret	L'état physique et l'état programmé de l'autosurveillance du coffret.
Défaut fusible	L'état physique et l'état programmé du fusible du contrôleur de porte.
Code	État du code de l'utilisateur. Plusieurs tentatives échouées ont provoqué une

autosurveillance	alarme.
------------------	---------

Actions exécutables

Effacer les alertes	Cliquez sur ce bouton pour remettre à zéro toutes les alertes sur la centrale.
Inhiber 	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**.
2. Voir le tableau ci-dessous pour de plus amples informations.

Hardware	Système	Entrées & Portes	Sorties	Portes	Secteurs	Calendriers	Changer son code	Avancé
Centrale	XBUS	Radio						
	Radio	WPA	Paramétrage Radio					
ID Détecteur	Type	Reçu	Etats	Récepteur	Signal	Enroller		
58732159	Infrarouge	23/07/2014 11:56:31	Au repos	Centrale	Haut (9)	<input type="button" value="Enroller"/>		
60304133	Infrarouge	23/07/2014 11:55:57	Ouverte	Radio 4	Haut (9)	<input type="button" value="Enroller"/>		
58740535	Infrarouge	23/07/2014 11:55:57	Ouverte	Centrale	Haut (9)	<input type="button" value="Enroller"/>		
60304133	Infrarouge	23/07/2014 11:55:57	Ouverte	Centrale	Haut (9)	<input type="button" value="Enroller"/>		
58740535	Infrarouge	23/07/2014 11:55:56	Ouverte	Centrale	Haut (9)	<input type="button" value="Enroller"/>		
60304133	Infrarouge	23/07/2014 11:55:51	Ouverte	Radio 4	Haut (9)	<input type="button" value="Enroller"/>		
26663381	Contact magnétique	23/07/2014 11:55:21	Au repos	Centrale	Haut (9)	<input type="button" value="Enroller"/>		
60306493	Infrarouge	23/07/2014 11:54:58	AUTOSUR.	Radio 4	Haut (9)	<input type="button" value="Enroller"/>		
26424404	Contact magnétique	23/07/2014 11:54:53	Au repos	Radio 4	Haut (9)	<input type="button" value="Enroller"/>		
26220868	Contact magnétique	23/07/2014 11:54:48	Au repos	Radio 4	Haut (9)	<input type="button" value="Enroller"/>		
58906531	Infrarouge	23/07/2014 11:54:37	Au repos	Radio 4	Haut (9)	<input type="button" value="Enroller"/>		

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 à laquelle le détecteur est attribué.
Batterie	L'état de la batterie dans le détecteur (le cas échéant).
Superviser	L'état 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 sur ce bouton pour afficher l'historique du détecteur radio. Voir ici [→ 190].
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 Historique - Détecteur radio X

Pour consulter un historique rapide des événements d'un détecteur radio :

1. Cliquez sur le bouton **JDB**.
2. Voir le tableau ci-dessous pour de plus amples informations.
3. Pour créer un fichier de texte contenant les données du journal, cliquez sur **Fichier Texte**.

Date/heure	La date et l'heure de l'événement journalisé.
Récepteur	L'emplacement du récepteur radio, c'est-à-dire si le module radio est installé dans le clavier, sur la centrale, ou s'il s'agit d'un transpondeur radio.
Signal	L'intensité du signal reçu par le détecteur (01=basse, 09=haute).
Etats	L'état physique du détecteur.
Batterie	L'état de la batterie connectée au détecteur (OK, Défaut).

17.6.4 Zones

Pour la configuration, voir ici [→ 253].

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.

Hardware	Entrées & Portes	Portes	FlexC	Alertes Système				
Toutes Zones		Zones X-Bus	Zones Radio					
Zones actives 41, Nbre de zones max. 512								
Zone	Type de zone	Tolérance R.	Entrée	Etats	JDB	Action		
1 Front door	Alarme	Bon [4.7kΩ]	Fermée	Alarme	JDB	Restauration		
2 Window 1	Alarme	Bon [4.7kΩ]	Fermée	Alarme	JDB	Restauration		
3 Window 2	Alarme	Bon [4.7kΩ]	Fermée	Alarme	JDB	Restauration		
4 PIR 1	Alarme	Bon [4.7kΩ]	Fermée	Alarme	JDB	Restauration		
17 Zone 17	Alarme	Bon [4.6kΩ]	Fermée	Normale	JDB	Inhiber	Isoler	Test
18 Zone 18	Alarme	Bon [4.7kΩ]	Fermée	Normale	JDB	Inhiber	Isoler	Test
19 Zone 19	Alarme	Bon [4.6kΩ]	Fermée	Normale	JDB	Inhiber	Isoler	Test
20 Zone 20	Alarme	Bon [4.7kΩ]	Fermée	Normale	JDB	Inhiber	Isoler	Test
21 Zone 21	Alarme	Bon [4.6kΩ]	Fermée	Normale	JDB	Inhiber	Isoler	Test
22 Zone 22	Alarme	Bon [4.6kΩ]	Fermée	Normale	JDB	Inhiber	Isoler	Test
23 Zone 23	Alarme	Bon [4.7kΩ]	Fermée	Normale	JDB	Inhiber	Isoler	Test
24 Zone 24	Alarme	Bon [4.7kΩ]	Fermée	Normale	JDB	Inhiber	Isoler	Test
25 Zone 25	Alarme	Bon [9.5kΩ]	Ouverte	Inhiber	JDB	Restaurer	Isoler	
26 Zone 26	Alarme	Bon [9.5kΩ]	Ouverte	Inhiber	JDB	Restaurer	Isoler	
27 Zone 27	Alarme	Bon [9.4kΩ]	Ouverte	Inhiber	JDB	Restaurer	Isoler	

Rafraîchir état auto. <input type="checkbox"/> Pro	Cochez cette case pour activer la mise à jour automatique de la synthèse des zones. Celle-ci s'applique à toutes les zones, pas seulement aux zones filtrées.
Description zone	Texte descriptif de la zone (16 caractères maximum).
Secteur	Secteurs auxquels cette zone est attribuée.
Type de zone	Le type de la zone (Alarme, Entrée/Sortie, etc.).
Tolérance R.	<p>Affiche la qualité de la résistance de fin de ligne pour la gamme de résistances indiquée. Les valeurs possibles sont :</p> <ul style="list-style-type: none"> ● 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. ● Bruité — indique un problème de détection du signal. Le câblage peut se trouver très près d'un câble secteur ou de tout autre source d'interférence. <p>Cette colonne n'est visible qu'en mode Ingénieur. Pour plus d'informations sur les valeurs nominales de la résistance et leurs gammes définies, reportez-vous à Câblage des entrées de zone [→ 89]Câblage des entrées de zone.</p>
Entrée	<p>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, Bruité). Substitution DC est une alerte antisabotage. Substitution DC vérifie périodiquement qu'aucun courant externe n'est appliqué au circuit.</p> <p>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.</p> <p>Bruité : un état Bruité se produit lorsqu'une interférence externe est induite dans le circuit d'entrée pendant une période d'échantillonnage définie.</p> <p>Hors limites : un état hors limite se produira lorsque la valeur de résistance d'entrée de zone ne se trouve pas dans les tolérances admises des valeurs actuelles de fin de ligne</p>
État	<p>L'état programmé de cette zone. Une valeur d'état de Normal signifie que la zone est programmée pour fonctionner normalement. Voici la liste complète des valeurs possibles :</p> <p>Isolée, Test, Inhibée, Changement état Zone, Alarme, Issue de secours, Défaut Avertissement, Défaut Agression, Défaut Détecteur, Défaut ligne, Panique, Agression, Technique, Médicale, Verrouillée, Défaut incendie, Détecteur masqué, Normale, Actionnée, 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.</p>

Actions exécutables

Rafraîchir	Met à jour les informations d'état affichées pour la centrale.
JDB	Cliquez sur le bouton du journal pour voir le journal de l'état d'entrée de cette zone..
INHIBEE ⓘ	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 une alerte 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 activée lors de l'activation du système.
Test	Mettez une zone en surbrillance et cliquez sur ce bouton pour exécuter un test JDB sur cette zone.
TEST SISMIQUE Pro	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 [→ 342].
Masquer entrées au repos	Cliquez sur ce bouton pour masquer toutes les entrées fermées.
Filtrer zones Pro	Sélectionnez un type de zone dans la liste déroulante. Uniquement les états de ce type de zone seront affichés dans la synthèse.

17.6.5 Portes

1. Sélectionnez **Etat > Portes**.
2. Voir les tableaux ci-dessous pour de plus amples informations.

Hardware		Entrées & Portes		Portes	FlexC	Alertes Système	
Porte	Zone	Secteur	Contact position porte (DPS)	Bouton libération porte (DRS)	Etats	JDB	Action
1	34 DOOR 1	1 Area 1	Fermée	Fermée	Porte normale	JDB	Verrouiller Déverrouiller Impulsion
2	36 DOOR 2	1 Area 1	Fermée	Fermée	Porte normale	JDB	Verrouiller Déverrouiller Impulsion

Refrâchir

Contrôle	Ce numéro identifie la porte de manière univoque.
Zone	Le numéro de zone auquel le détecteur de position de porte est attribué (uniquement si l'entrée du détecteur de position de porte est aussi utilisée pour une zone d'intrusion).
Secteur	Le secteur auquel l'entrée du détecteur de position de porte et le lecteur de badge sont attribués.
Contact position porte (DPS)	État du détecteur de position de porte.
Bouton libération porte (DRS)	État du bouton-poussoir d'ouverture de porte.
Etats	L'état de la porte (OK, défaut).
Mode porte Pro	Indique le mode de fonctionnement des portes.

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

Cet écran affiche l'état de chaque système de transmission d'alarmes (ATS) configuré sur le système.

1. Pour voir l'état d'un ATS, rendez-vous sur l'écran **FlexC - État**.
2. Le tableau ci-dessous décrit les critères d'état disponibles pour chaque ATS.

Hardware	Entrées & Portes	Portes	FlexC	Alertes Système			
FlexC - Etat							
FlexC - Système de Transmission (ATS): ATS 1							
ID d'enregistrement de l'ATS	T578-G5R9-92XG-SF2G	Numéro ID unique sous lequel s'enregistre le système de transmission (ATS) sur le récepteur (RCT).					
Etat ATS	Défaut	Montre les états du système de transmission (ATS)					
Temps depuis dernier Polling	50min 7s	Temps écoulé depuis l'envoi du dernier polling sur n'importe quel chemin de l'ATS					
Compteur File d'attente	6	Nombre d'événements dans la file d'attente pour être transmis					
File d'attente Événement	<input type="button" value="File d'attente Événement"/>	Liste des événements qui sont actuellement dans la file d'attente					
Journal de bord	<input type="button" value="Journal de bord"/>	Journal de bord de tous les événements traités par le système de transmission (ATS)					
JDB réseau	<input type="button" value="JDB réseau"/>	JDB du réseau pour ce Système de Transmission (ATS)					
Etat des Chemin de Transmission dans l'ATS							
N° Seq.	Nom du Chemin	Interface de communication	Etat du Chemin (ATP)	Dernière transmission réussie	JDB réseau	JDB Chemin	Appel Test Cyclique
1	Primary ATP 1	Ethernet	Défaut	-	<input type="button" value="JDB réseau"/>	<input type="button" value="JDB Chemin"/>	<input type="button" value="Test Manuel"/>
FlexC - Système de Transmission (ATS): ATS 2							
ID d'enregistrement de l'ATS	K6PG-K87Y-T866-385Y	Numéro ID unique sous lequel s'enregistre le système de transmission (ATS) sur le récepteur (RCT).					
Etat ATS	Défaut	Montre les états du système de transmission (ATS)					
Temps depuis dernier Polling	50min 7s	Temps écoulé depuis l'envoi du dernier polling sur n'importe quel chemin de l'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 en attente de transmission.
File d'attente Événement	Liste des événements actuellement en attente. Le tableau répertorie les éléments suivants : <ul style="list-style-type: none"> ● Séquence d'événement N° ● Horodatage Événement ● Description Événement ● Info Supplémentaire Événement ● Heure de début ● Durée de la Transmission
Journal des événements	Historique du journal pour tous les événements survenus sur le système ATS. Le tableau répertorie les mêmes champs que pour les événements en attente ci-dessus ainsi que le champ additionnel

	<p>suisant :</p> <ul style="list-style-type: none"> ● Séquence d'événement N° ● 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 Chemin de Transmission dans l'ATS	<p>Le tableau répertorie chaque chemin de l'ATS. Pour chaque ATP, le tableau montre le n° de séquence ATP, le nom ATP, interfaces de communication, l'État ATP, la dernière transmission réussie, le JDB réseau, le JDB chemin et le bouton d'Appel Test Cyclique.</p> <p>JDB réseau : Cliquez sur ce bouton pour afficher le JDB réseau.</p> <p>JDB chemin : Affiche une liste de 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.</p> <p>Bouton Test Manuel : Cliquez sur ce bouton pour effectuer un appel test. L'événement est ajouté aux événements en file d'attente.</p>

17.6.7 Défauts système

1. Sélectionnez **Etat > Défauts système**.
2. Voir les tableaux ci-dessous pour de plus amples informations.

Hardware	Entrées & Portes	Portes	FlexC	Alertes Système	Entrée	Etats	Action
					OK	OK	Inhiber Isoler
					Défaut	Isoler	Restaurer
					OK	OK	Inhiber Isoler
					OK	OK	Inhiber Isoler
					OK	OK	Inhiber Isoler
					Défaut	Isoler	Restaurer
					Défaut	Isoler	Restaurer
					OK	OK	Inhiber Isoler
					OK	OK	Inhiber Isoler
					OK	OK	Inhiber Isoler
					OK	OK	Inhiber Isoler
					OK	OK	Inhiber Isoler
					OK	OK	Inhiber Isoler
					OK	OK	Inhiber Isoler
					OK	OK	Inhiber Isoler
					OK	OK	Inhiber Isoler
					OK	OK	Inhiber Isoler
					OK	OK	Inhiber Isoler

Systeme	Description de l'alerte système.
Entrée	L'état actuel de l'alerte détecté sur la centrale (OK, Défaut).
Etats ⚠	L'état programmé de l'alerte système - cette colonne indique si l'alerte est isolée ou inhibée. L'état OK signifie que l'alerte n'est pas désactivée (voir ici).

Actions exécutables

Rafraîchir	Cliquez sur ce bouton pour mettre à jour l'affichage de l'état des alertes.
Restaurer	Cliquez sur ce bouton pour restaurer une alerte sur la centrale.
Inhiber 	Cliquez sur ce bouton pour bloquer un défaut. La fonction Inhiber désactive le défaut ou la zone considérée pendant un cycle d'armement. Elle 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

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.

JDB Système	JDB Accès	Modem 1	Modem 2
JDB Système	JDB Alarme	JDB WPA	

JDB Système

```

23/07/2014 09:35:01 FlexC Etat du Chemin (ATP) Tombé [Système (ATS)=5, ATP=1]
23/07/2014 09:35:02 FlexC Etat ATS Tombé [Système (ATS)=1]
23/07/2014 09:35:02 FlexC Etat ATS Tombé [Système (ATS)=5]
23/07/2014 09:35:02 FlexC Etat du Chemin (ATP) Tombé [Système (ATS)=1, ATP=1]
23/07/2014 09:35:11 FlexC Etat du Chemin (ATP) Tombé [Système (ATS)=3, ATP=1]
23/07/2014 09:36:00 FlexC Etat du Chemin (ATP) Tombé [Système (ATS)=2, ATP=2]
23/07/2014 09:36:32 FlexC Etat ATS Tombé [Système (ATS)=3]
23/07/2014 09:36:32 FlexC Etat ATS Tombé [Système (ATS)=8]
23/07/2014 09:36:41 FlexC Etat du Chemin (ATP) Tombé [Système (ATS)=2, ATP=1]
23/07/2014 09:36:41 FlexC Etat du Chemin (ATP) Tombé [Système (ATS)=8, ATP=1]
23/07/2014 09:39:32 FlexC Etat ATS Tombé [Système (ATS)=2]
23/07/2014 09:49:43 Centrale en mode Exploitation
23/07/2014 09:49:43 CONFIGURATION CHANGEE
23/07/2014 09:49:48 WWW FIN, Utilisateur 9999 Engineer
23/07/2014 09:51:51 WWW LOGIN OK, Utilisateur 9999 Engineer, IP 10.100.82.253
23/07/2014 09:54:43 FlexC Timeout Evènement (ATS) [Système (ATS)=1, ID de l'évènement=7004 (Accès Ingénieur dévalidé)]
23/07/2014 09:54:43 FlexC Timeout Evènement (ATS) [Système (ATS)=2, ID de l'évènement=7004 (Accès Ingénieur dévalidé)]
23/07/2014 09:54:43 FlexC Timeout Evènement (ATS) [Système (ATS)=3, ID de l'évènement=7004 (Accès Ingénieur dévalidé)]
23/07/2014 09:54:43 FlexC Timeout Evènement (ATS) [Système (ATS)=5, ID de l'évènement=7004 (Accès Ingénieur dévalidé)]
23/07/2014 09:54:43 FlexC Timeout Evènement (ATS) [Système (ATS)=8, ID de l'évènement=7004 (Accès Ingénieur dévalidé)]
23/07/2014 09:59:47 Centrale en mode Paramétrage
23/07/2014 09:59:51 Centrale en mode Exploitation
23/07/2014 09:59:54 WWW FIN, Utilisateur 9999 Engineer
23/07/2014 10:00:00 WWW LOGIN OK, Utilisateur 9999 Engineer, IP 10.100.82.253
23/07/2014 10:00:03 Centrale en mode Paramétrage
23/07/2014 10:01:03 Centrale en mode Exploitation
23/07/2014 10:01:03 CONFIGURATION CHANGEE
23/07/2014 10:01:08 WWW FIN, Utilisateur 9999 Engineer
23/07/2014 10:01:18 WWW LOGIN OK, Utilisateur 9999 Engineer, IP 10.100.82.253
23/07/2014 10:03:37 Centrale en mode Paramétrage
23/07/2014 10:04:42 FlexC Timeout Evènement (ATS) [Système (ATS)=1, ID de l'évènement=7004 (Accès Ingénieur dévalidé)]

```



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 JDB Accès

Le journal de bord contient le suivi des événements du système SPC.

- Sélectionnez **Journal > Journal des accès**.

⇒ La fenêtre suivante est affichée :

JDB Système	JDB Accès	Modem 1	Modem 2
JDB Accès			
Heure	Événement	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 des événements WPA

Ce JDB affiche tous les événements WPA du système.

- Sélectionner **JDB > JDB Système > JDB WPA**.

⇒ La fenêtre suivante est affichée :

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
- EVENEMENTS SYSTEME
 - Alarme confirmée
 - Code contrainte
 - XBUS Panique
 - Panique utilis.
 - WPA Paniq.

17.8 Utilisateur

Le tableau suivant montre le nombre maximal d'utilisateurs, de profils utilisateurs et de tags utilisateurs pour la centrale :

N° maximal	SPC4xxx	SPC5xxx	SPC6xxx
Utilisateur	100	500	2 500
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
MDT Modules	32	32	32



▲ AVERTISSEMENT

Si vous mettez à jour à partir d'une version du firmware précédent la version 3.3, veuillez noter les éléments 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 Profils Utilis. [→ 200]). Veuillez vérifier l'ensemble de la configuration utilisateur après une mise à niveau du firmware.
- L'ID Installateur par défaut est modifiée de 513 à 9999.

17.8.1 Ajouter/Éditer un utilisateur

1. Sélectionnez **Utilisateurs > Utilisateurs > Ajouter Utilisateur**.

⇒ La liste des utilisateurs configurés s'affiche.

Utilisateurs		Profils	SMS Utilisateurs	Mots de passe Web	Accès Installateur			
Editer	Effacer	Utilisateur	Nom	Alertes	Numéro de badge	Télécommande	Tag	Profils
		1	Utilisateur 1	OK	10	-	-	- Manager [2]
		2	Utilisateur 2	OK	-	-	-	- Standard user [1] - Manager [2]

Ajouter Utilisateur Tri par Nom

2. Cliquez sur le bouton **Ajouter** ou **Modifier** correspondant à l'utilisateur requis.

⇒ L'écran suivant s'affiche.

Ajouter un nouvel utilisateur au Système

Paramètres Utilisateur

ID Utilisateur:

Nom de l'utilisateur: Nom de l'utilisateur dans le système

Code PIN Utilisateur: Code PIN utilisé par l'utilisateur pour actionner le système Intrusion et le système de contrôle d'accès. Laisser à 0 si le code PIN n'est pas utilisé.

Langue: Langue utilisée par l'utilisateur

Limité entre 2 dates: / / - / /

Alertes Utilisateur

Aucun

Profils

1: Standard user 2: Manager 3: Limited user 4: Access User

3. 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.

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, ceci 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. Sélectionnez le Profil Utilisateur [→ 200] voulu pour cet utilisateur.

8. Le cas échéant, activez la contrainte (sélectionnez **Activ. Contrainte**) pour cet utilisateur. Le nombre de codes utilisateur attribué par contrainte (PIN +1 ou PIN+2) est configurable dans Options système [→ 236].



L'option Contrainte n'est disponible sur cet écran 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 (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	Entrer le numéro de badge Entrez 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.
Priorité	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 : <ul style="list-style-type: none"> ● SPC4xxx – tous les utilisateurs ● SPC5xxx – 512 ● SPC6xxx - 512
Escorte	La fonction Escorte permet à des détenteurs de carte à accès privilégié d'escorter d'autres détenteurs de carte au travers de portes spéciales. 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 de la carte d'escorte et celle de la carte normale 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 **TELECOMMANDE** — **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**
- Contrôle d'accès — Bouton **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 une carte 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 l'est également 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 **Sauver**.
L'affectation de la carte à l'utilisateur est supprimée et est supprimé du système.
3. Pour ajouter à nouveau la carte, vous devez la scannez une nouvelle fois.

17.8.2 Ajouter/Modifier un profil utilisateur.

!	AVIS
	Les profils d'utilisateurs généraux ne sont pas éditables par l'explorateur ni par SPC Pro 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.

Utilisateurs	Profils	SMS Utilisateurs	Mots de passe Web	Accès Installateur
Editer	Effacer	ID	Nom Profile Utilisateur	Comptage Utilisateur
		1	Standard user	0
		2	Manager	1
		3	Limited user	0
		4	Access User	0
<input type="button" value="Ajouter Profile Utilisateur"/>				

2. Sélectionnez **Ajouter Profil Utilisateur** ou cliquez sur le bouton **Éditer** du profil souhaité.

L'écran suivant est affiché avec les options de configuration suivantes :

- Réglages généraux
- Droits Utilisateur/Centrale
- Contrôle d'accès

Utilisateurs	Profils	SMS Utilisateurs	Mots de passe Web	Accès Installateur
Ajouter un nouveau Profil Utilisateur au système				
Paramètres généraux				
ID Profil utilisateur:	<input type="text" value="5"/>			
Nom Profil Utilisateur:	<input type="text" value="User Profile 5"/>	Nom du profil utilisateur dans le système		
Secteurs				
<input checked="" type="checkbox"/> 1: Area 1				
Calendrier				
Calendrier:	<input type="text" value="Aucun"/>	Le calendrier associé définit les croneaux horaires journaliers de limitation d'accès de l'utilisateur au système		
Droits Utilis. - Intrusion				
MHS	<input type="checkbox"/>	L'utilisateur peut mettre à l'Arrêt le système		
MES Partielle A	<input type="checkbox"/>	L'utilisateur peut mettre en Marche Partielle A le système		
MES Partielle B	<input type="checkbox"/>	L'utilisateur peut mettre en Marche Partielle B le système		
MES Totale	<input type="checkbox"/>	L'utilisateur peut mettre en Marche Totale le système		
Marche forcé	<input type="checkbox"/>	L'utilisateur peut forcer la mise en surveillance		

Réglages 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

Droit	Type de profil d'utilisateur par défaut	Description
Droits Utilis. - Intrusion		
MES totale	Limite Standard Manager	La fonction MARCHÉ 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). Si elle est sélectionnée, le buzzer retentit et un compte à rebours affiché sur le clavier indique le temps restant pour quitter les lieux. Quittez le bâtiment avant la fin du compte à rebours. Après expiration, le système est activé et l'ouverture des zones d'entrée / sortie déclenche le temporisateur d'entrée. Si le système n'est pas désactivé avant que l'expiration du délai, l'alarme est activée.
MES Partielle A	Gestionnaire standard	Le mode MES PART. A active la protection du périmètre d'un immeuble, mais autorise 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 temporisateur de sortie ; le système est activé instantanément dès que ce mode est sélectionné. Un temporisateur de sortie peut être appliqué à ce mode en activant la variable de temps MES PARTIELLE A.
MES Partielle B	Gestionnaire standard	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

Droit	Type de profil d'utilisateur par défaut	Description
		système s'active instantanément dès que ce mode est sélectionné. Un temporisateur de sortie peut être appliqué à ce mode en activant la variable MES PARTIELLE B TEMPORISÉE.
Marche forcée	Standard Manager	L'option MES FORCEE 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). En sélectionnant cette option, l'alarme est activée et la zone est inhibée pendant la période d'armement.
Mise hors surveillance	Limite Standard Manager	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 la mise en service auto	Standard* Manager	L'utilisateur peut retarder ou annuler la mise en service automatique.
Supprime le délai.	Gestionnaire standard	L'utilisateur peut neutraliser automatiquement le retard à la MHS. Disponible uniquement pour les installations bancaires. Voir Mise En/Hors surveillance [→ 259]
Restaurer	Gestionnaire standard	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.
Inhiber	Gestionnaire standard	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* Manager	Le fait d'isoler une zone la désactive jusqu'à ce que l'isolation soit annulée explicitement. Tous les types de zones du contrôleur peuvent être isolés. L'utilisation de cette fonction pour désactiver des zones en défaut ou ouvertes ne doit pas se faire à la légère ; une fois qu'une zone est isolée, le système ne la prend plus en compte et elle pourrait être oubliée lors des futures activations du système, ouvrant ainsi une brèche dans la sécurité des locaux.
Droits Utilis.- Système		
Accès Web	Standard* Manager	L'utilisateur peut accéder à la centrale via un navigateur Internet.
Voir JDB	Gestionnaire standard	Cette option affiche l'événement le plus récent sur l'afficheur du clavier. Le journal de bord [→ 161] fournit la date et l'heure de chaque événement mis dans le journal.
Utilisateur	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*	Cette fonction permet aux utilisateurs d'activer le

Droit	Type de profil d'utilisateur par défaut	Description
	Manager	service de messagerie par SMS si un modem est installé dans le système.
Réglages date	Gestionnaire standard	Cette option permet à l'utilisateur de programmer la date et l'heure du système [-> 170]. Assurez-vous que les informations de date et d'heure soient correctes ; ces champs sont affichés dans le journal des événements.
Changer code	Gestionnaire standard	Cette option du menu permet à l'utilisateur de changer son code utilisateur [-> 162]. 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.	Gestionnaire standard	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 Manager	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 permet d'activer ou de désactiver la fonction de carillon de toutes les zones.
Installateur	Gestionnaire	Cette option permet aux utilisateurs d'accorder un accès pour la programmation en mode Paramétrage. Concernant les réglementations nationales suisses CAT 1 et CAT 2 : lorsque l'accès à l'installateur est activé, tous les secteurs doivent être mis hors surveillance, sinon l'accès est refusé à l'installateur.
Upgrade	Gestionnaire	L'utilisateur peut permettre au fabricant d'accéder à la centrale pour qu'il mette le firmware à jour.
Droits Utilis. - Pilotage		
Sorties	Gestionnaire standard	L'utilisateur peut activer/désactiver les sorties configurées. Voir Éditer une sortie [-> 212].
X-10	Standard Manager Contrôle d'accès	L'utilisateur peut activer/désactiver les périphériques X-10 configurés. Remarque :X-10 n'est plus pris en charge. La fonctionnalité reste présente dans le système pour la prise en charge de l'existant seulement.
Contrôle des portes	Standard* Manager Contrôle d'accès	L'utilisateur peut verrouiller/déverrouiller les portes
COMMANDE RADIO	Standard Manager Contrôle d'accès	L'utilisateur peut contrôler la sortie radio
Droits Utilis. - Tests		
Test sirène	Gestionnaire standard	À l'aide de ce test, l'utilisateur peut effectuer tester la sirène externe, le flash, la sirène interne et le buzzer et s'assurer du bon fonctionnement de ces éléments.
Test de déplacement	Gestionnaire standard	L'utilisateur peut effectuer un test de déplacement afin de tester le fonctionnement de tous les capteurs d'alarme d'un système.
Test WPA	Gestionnaire standard	L'utilisateur peut tester un WPA.

Droit	Type de profil d'utilisateur par défaut	Description
Test auto. du Détecteur	Gestionnaire standard	L'utilisateur peut tester le détecteur sismique.
Droits Utilis. – Service Accès Installateur		
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.
* Ces fonctions ne sont pas actives par défaut pour l'utilisateur considéré, mais peuvent être activées.		

Contrôle d'accès

Contrôle d'accès

Code site: Code site de yopus les badges utilisant ce profile Utilisateur

Liste des portes d'accès:

ID Porte	Nom Porte	Accès / Calendrier
1	Door 1	Accès 24H/24H
2	Door 2	Accès 24H/24H
3	Door 3	Accès 24H/24H
4	Door 4	Accès 24H/24H

1. Entrez un **Code site**, le cas échéant, pour tous les badges affectés à ce profil d'utilisateur. Consultez la section annexe concernant les Lecteurs et formats de cartes [→ 375].
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 24H/24H (accès illimité)
 - Calendrier (si configuré)

Utilisateur

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 est affichée.

Voir aussi

- 📖 Ajouter/Modifier un profil utilisateur. [→ 201]
- 📖 Ajouter / Éditer un secteur [→ 253]

17.8.3 Programmation SMS

Quand le système SPC est équipé d'un modem, il est capable de communiquer avec l'extérieur en utilisant les fonctions de messagerie du service SMS.

- ▷ Un modem est installé et le système l'a identifié.
- ▷ La fonction **Authentification SMS** est activée. Voir page [→ 236].

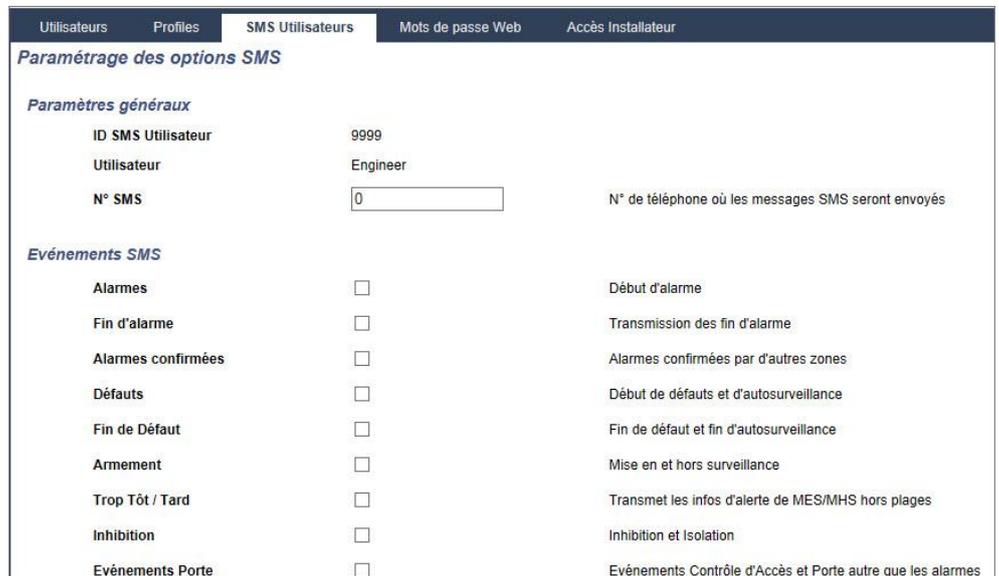
1. Sélectionnez **Utilisateurs -> SMS Utilisateurs**.

⇒ L'ID SMS Installateur et une liste d'ID SMS utilisateurs avec les données SMS correspondantes 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 infos détaillées du SMS, procédez comme suit :

ID SMS Utilisateur	ID générée par le système
NUMERO SMS	Entrez le numéro de destination du SMS (avec l'indicatif du pays à trois chiffres). Remarque : Le Numéro SMS installateur peut être supprimé fixant la valeur à 0. Les numéro SMS Utilisateur ne peuvent pas être supprimés.
Utilisateur	Sélectionnez un nouvel utilisateur pour cette ID SMS Utilisateur, le cas échéant.
Evénements SMS	Sélectionnez les événements centrale devant être envoyés par SMS à l'utilisateur ou à l'installateur.
Contrôle par SMS	Sélectionnez les opérations pouvant être effectuées à distance sur la centrale par SMS. Voir Commandes SMS [→ 206]

!	AVIS
	Les événements HOLDUP ne sont pas transmis par SMS.



Si la ligne téléphonique est reliée au RTC via un autocommutateur privé (PABX), le préfixe de prise de ligne adéquat doit précéder le numéro de l'appelé. Assurez-vous que le service Calling Line Identity (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 : **** FSET or ****.FSET. 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 ****. MARCHE 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.
**** MHS ****.MHS ****. MHS	MHS MHS	Désactive tous les secteurs auxquels l'utilisateur a accès.	Système arrêté
**** SSTA ****.SSTA ****. ÉTAT	SSTA ÉTAT	Récupère l'état des secteurs.	État du système et des secteurs ● 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 (X10) ****.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	Événements récents
**** ENGA.ON (ACCES INSTALLAT.) ****.ENGA.ON	ENGA.ON	Activer l'accès Installateur	Accès Installateur
**** ENGA.OFF ****.ENGA.OFF	ENGA.OFF	Désactiver l'accès Installateur	Interdit Ingénieur
**** 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		L'interaction logique identifiée comme S5 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		L'interaction logique identifiée comme S5 est désactivée.	État de S5 Par exemple : sortie S5 hors service
****.ASET (MES PART.A)		Autorise la MES Partielle A par SMS Il est également possible de spécifier le nom personnalisé défini dans le champ de nouveau nom de MES partielle de la fenêtre d'options. Voir Options [→ 236].	Système activé.
****.MESB (MES Partielle B)		Autorise la MES Partielle B ou l'alarme SMS Il est également possible de spécifier le nom personnalisé défini dans le champ de nouveau nom de MES partielle de la fenêtre d'options. Voir Options [→ 236]. Par exemple : ****.MESA NUIT	Ensemble système
****.RAZ ****.RESTAURER		Autorise l'effacement des alertes par SMS	



Pour la prise en compte du SMS, l'identification de l'interaction logique emploie le format SNNN, S étant l'interaction logique, et NNN les caractères numériques (uniquement les chiffres significatifs).
(Exemple : O5 pour l'interaction logique 5).

Pour la prise en compte du SMS, le périphérique X-10 emploie le format : XYNN, où X signifie X-10 ; Y est la lettre alphabétique, NN est les caractères numériques disponibles. (Exemple : XA1)

Le service SMS fonctionne sur la base d'un protocole standard utilisé par les téléphones compatibles SMS. Remarque : certains opérateurs du RTC ne proposent pas le service SMS via le RTC. Pour pouvoir envoyer des SMS par 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, 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

Liste des mots de passe d'accès installateur et les mots de passe utilisateurs créés pour l'accès à l'explorateur Web.

1. Sélectionnez **Utilisateurs -> Mots de passe Web**

Utilisateurs	Profils	SMS Utilisateurs	Mots de passe Web	Accès Installateur
Mots de passe Web Ingénieurs				
Effacer	ID	Nom de l'utilisateur		
	9999	Engineer		
Mots de passe Web Utilisateurs				
Effacer	ID	Nom de l'utilisateur		

2. Cliquez sur le bouton **Supprimer** en regard de l'Accès Installateur ou utilisateur pour supprimer le mot de passe.

17.8.6 Paramètres de configuration Installateur

1. Sélectionnez **Utilisateur > Accès Installateur**.

The screenshot shows a web interface for configuring an installer user. At the top, there are navigation tabs: 'Utilisateurs', 'Profils', 'SMS Utilisateurs', 'Mots de passe Web', and 'Accès Installateur'. The main heading is 'Editer les paramètres Installateur'. Under 'Paramètres Utilisateur', there are fields for 'ID Utilisateur' (9999), 'Nom de l'utilisateur' (Engineer), 'Code PIN Utilisateur' (with a 'Changer le code PIN' button), and 'Langue' (Anglais). Below this, 'Alertes Utilisateur' is set to 'Aucun'. The 'Contrôle d'accès' section includes checkboxes for 'Numéro de badge' (0), 'Badge inutilisé', 'Extension de temps - PMR', 'Sans code', 'Prioritaire', and 'Escorte', each with a descriptive text.

2. Le cas échéant, modifier le **Nom d'utilisateur** pour l'accès installateur.
3. Cliquez sur **Changer le code PIN** [→ 210] pour modifier le code d'accès installateur.
 - ⇒ **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) - voir Mise à jour langue [→ 325])

Contrôle d'accès

Attribut	Description
Numéro badge	Entrer le numéro de badge Entrez 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.
Priorité	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 : <ul style="list-style-type: none"> ● SPC4xxx – tous les utilisateurs ● SPC5xxx – 512 ● SPC6xxx - 512
Escorte	La fonction Escorte permet à des détenteurs de carte à accès privilégié d'escorter d'autres détenteurs de carte au travers de portes spéciales. 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 de la carte d'escorte et celle de la carte normale 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

Attribut	Description
	<p>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.</p> <p>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.</p>

17.8.6.1 Changement du code Ingénieur et du mot de passe d'accès installateur

Cette fenêtre 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.

- Changer le code comme suit :

Ancien code	Entrez le code de l'installateur valable actuellement. (chiffres seulement)
Nouveau code	Entrez le nouveau code installateur. (chiffres seulement)
Confirmer le nouveau code.	Entrez une deuxième fois le nouveau code installateur.

1. 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**.

2. 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.

- 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

17.9.1 Configurer les entrées et sorties de la centrale

17.9.1.1 Éditer une entrée

1. Sélectionnez **Configuration > Hardware > Centrale**.
⇒ La fenêtre suivante est affichée.
2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Hardware	Système	Entrées & Portes	Sorties	Portes	Secteurs	Calendriers	Changer son code	Avancé
Centrale	XBUS	Radio						
Entrée & Sortie Centrale								
Entrée	Fin de Ligne	Zone	Libellé	Type	Secteur	Attributs		
1	2 RESIST.4K7/4K7	1	Front door	Alarme	1: Area 1	...		
2	2 RESIST.4K7/4K7	2	Vault	Sismique	2: Vault	...		
3	2 RESIST.4K7/4K7	3	Window 2	Alarme	1: Area 1	...		
4	2 RESIST.4K7/4K7	4	PIR 1	Alarme	1: Area 1	...		
5	2 RESIST.4K7/4K7	5	PIR 2	Inutilisé	1: Area 1	...		
6	2 RESIST.4K7/4K7	6	Fire Exit	Inutilisé	1: Area 1	...		
7	2 RESIST.4K7/4K7	7	Fire alarm	Inutilisé	1: Area 1	...		
8	2 RESIST.4K7/4K7	8	Panic Button	Inutilisé	1: Area 1	...		
Sortie	Libellé	Type	Changer type		Attributs		Test	
1	Ext. Bell	Système - Sirène extérieure	
2	Int. Bell	Système - Sirène intérieure	
3	Strobe	Système - Flash sirène extérieure	
4	Fullset	Système - Marche totale	
5	Alarm	Système - Alarme	
6	Alarm Confirmed	Système - Alarme confirmée	

Entrée	Ce numéro ne peut pas être modifié.
Fin de ligne	Sélectionnez la résistance fin de ligne (EOL) de l'entrée de la zone (valeur par défaut : 4K7).
Analysé <input type="radio"/> Pro	Indique si le détecteur est de type inertiel/choc.
Comptage d'impulsion <input type="radio"/> Pro	Nombre d'impulsions programmé sur la centrale nécessaires pour qu'un détecteur inertiel / de choc déclenche une alarme.
Attaque <input type="radio"/> Pro	Niveau de sensibilité d'attaque brute programmé sur la centrale nécessaire pour qu'un détecteur inertiel/de choc déclenche une alarme.
Zone	Numéro de la zone sur la centrale

Description	Entrez un texte descriptif de l'entrée (16 caractères maximum). Ce texte est affiché dans le navigateur et sur le clavier.
Type	Le type de zone (voir ici [→ 367]).
Secteur	Uniquement si l'option Secteurs (multiple) est activée dans le menu Paramètres centrale > Paramètres Système > Options. Sélectionnez les secteurs auxquels cette zone est attribuée.
Attributs	Une icône dans ce champ indique que des attributs sont appliqués à cette zone (voir ici [→ 212]).

17.9.1.1.1 Zones d'entrée : attributs

Un attribut ajoutant des propriétés peut être appliqué à chaque zone du SPC.

Pour appliquer un attribut à une zone :

1. Sélectionnez **Configuration > Hardware > Centrale > Attributs**.

⇒ La fenêtre suivante est affichée :

Attribut	Libellé
<input type="checkbox"/> Accès	Quand l'attribut Accès est validé, la zone devient temporisée lorsqu'une temporisation d'entrée est en cours. Sinon, l'alarme est immédiate. De plus, en mode Partiel, le comportement de la zone change en zone <i>ENTREESORTIE</i>
<input type="checkbox"/> Exclus A	Si l'attribut Exclus A est validé pour une zone, alors aucune alarme ne sera générée si cette zone est ouverte pendant que la centrale est en mode partiel A
<input type="checkbox"/> Exclus B	Si l'attribut Exclus B est validé pour une zone, alors aucune alarme ne sera générée si cette zone est ouverte pendant que la centrale est en mode partiel B
<input type="checkbox"/> 24/24	Quand l'attribut 24/24 est validé, l'ouverture de la zone déclenchera une alarme dans tous les modes de surveillance.
<input type="checkbox"/> Locale	Quand l'attribut local est validé, une alarme générée par cette zone ne sera pas transmise.
<input type="checkbox"/> MHS locale	Quand l'attribut 'MHS Locale' est sélectionné, les alarmes ne sont transmises que lorsque le secteur associé est en MES totale ou MES partielle. (pour les entrées 24/24)
<input type="checkbox"/> Double déclenchement	Quand l'attribut double déclenchement est validé, une alarme sera générée lors de la seconde ouverture de la même entrée durant la plage de temps spécifiée pour le timer double déclenchement.
<input type="checkbox"/> Carillon	Si l'attribut carillon est validé pour une zone, l'ouverture de cette zone lorsque la centrale est hors surveillance déclenchera l'activation des buzzers internes pendant une courte période.
<input checked="" type="checkbox"/> Inhiber	Quand l'attribut inhibé est validé, un utilisateur peut inhiber cette zone.
<input type="checkbox"/> Normalement ouvert	Quand l'attribut N/O est validé, le système s'attend à ce que la sortie d'alarme du détecteur raccordé sur cette zone soit ouverte au repos (normalement ouverte).
<input type="checkbox"/> Silencieux	Si l'attribut silencieux est validé alors il n'y aura aucune indication sonore ou visuelle de l'alarme. A la mise hors surveillance, un message d'alerte sera affiché
<input type="checkbox"/> JDB	Si cet attribut est validé, alors tous les changements d'état de la zone sont historisés.
<input type="checkbox"/> Shunt	Si cet attribut est validé, lorsqu'une zone de type shunt sera activée, cette zone sera inhibée
<input type="checkbox"/> Fréquent	La zone doit être ouverte au moins 1 fois durant le temps renseigné dans le paramètre
<input type="checkbox"/> Analysé	Choisir cette option si un détecteur intertiel est utilisé
<input type="text" value="5"/> Comptage d'impulsions	Niveau comptage d'impulsion pour détecteur intertiel

2. Cochez la case en regard de l'attribut voulu.



Les attributs présentés dans cette page dépendent du type de zone sélectionné. Pour la liste des attributs pouvant être affectés, voir ici [→ 373].

17.9.1.2 Éditer une sortie

1. Sélectionnez **Configuration > Hardware > Centrale**.
2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Hardware							
Système		Entrées & Portes		Sorties		Portes	
Centrale		XBUS		Radio			
Entrée & Sortie Centrale							
Entrée	Fin de Ligne	Zone	Libellé	Type	Secteur	Attributs	
1	2 RESIST.4K7/4K7	1	Front door	Alarme	1: Area 1	...	
2	2 RESIST.4K7/4K7	2	Vault	Sismique	2: Vault	...	
3	2 RESIST.4K7/4K7	3	Window 2	Alarme	1: Area 1	...	
4	2 RESIST.4K7/4K7	4	PIR 1	Alarme	1: Area 1	...	
5	2 RESIST.4K7/4K7	5	PIR 2	Inutilisé	1: Area 1	...	
6	2 RESIST.4K7/4K7	6	Fire Exit	Inutilisé	1: Area 1	...	
7	2 RESIST.4K7/4K7	7	Fire alarm	Inutilisé	1: Area 1	...	
8	2 RESIST.4K7/4K7	8	Panic Button	Inutilisé	1: Area 1	...	
Sortie	Libellé	Type	Changer type		Attributs		Test
1	Ext. Bell	Système - Sirène extérieure
2	Int. Bell	Système - Sirène intérieure
3	Strobe	Système - Flash sirène extérieure
4	Fullset	Système - Marche totale
5	Alarm	Système - Alarme
6	Alarm Confirmed	Système - Alarme confirmée

Type Sortie	<ul style="list-style-type: none"> ● Sortie système : Sélectionnez le type dans la liste déroulante. (Voir Types et ports de sortie [→ 214]) ● Sortie secteur : Uniquement si l'option Secteurs (multiple) est activée dans le menu Paramètres centrale > Paramètres Système > Options. Sélectionnez un secteur et le type de sortie système de ce secteur. (Voir Types et ports de sortie [→ 214]) ● Zone liée : Sélectionnez la zone à mapper. ● Interaction logique : Sélectionnez l'interaction logique à mapper. ● Porte de sortie : Sélectionnez le numéro de porte et le type de sortie système de la porte. (Voir Types et ports de sortie [→ 214]) ● Boîtier à clé : sélectionnez l'ID du nœud pour le boîtier à clé et la position requise de la clé pour l'affecter à cette sortie.
Description	Entrez un texte descriptif de la sortie (16 caractères maximum). Ce texte est affiché dans le navigateur et sur le clavier.
Configuration des sorties	<ul style="list-style-type: none"> ● Mode : Sélectionnez le mode de fonctionnement. Continu: suit l'état de la sortie. Intermittente: active et désactive la sortie à l'alternat. Impulsion : génère une impulsion quand le type de sortie est activé. ● Redéclenché : cochez cette case pour redéclencher les sorties en mode Impulsion. ● On Time : Entrez la durée d'activation de la sortie en modes Impulsion et Intermittent. ● Temps Off : Entrez la durée de désactivation des sorties en mode Intermittent. ● Inverser : Cochez cette case pour inverser l'état de la sortie physique. ● Journal : Cochez cette case pour journaliser les changements d'état des sorties dans le journal des événements. ● Calendrier : Au besoin, sélectionnez le calendrier voulu. Voir ici [→ 268].

Voir aussi

📅 [Calendriers \[→ 268\]](#)

17.9.1.2.1 Types et ports de sortie

Chaque type de sortie peut être attribué à un des 6 ports de sortie physiques sur la centrale SPC ou à une sortie de l'un des transpondeurs connectés. Les types de sortie qui ne sont pas attribués à des sorties physiques jouent le rôle d'indicateurs des événements système et peuvent être connectés à un centre de télésurveillance.

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 ici [→ 367]) 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 possède ses propres sorties secteur ; s'il s'agit d'un secteur commun à d'autres secteurs, ses sorties indiquent l'état de tous les secteurs communs incluant son propre état. Exemple : si le secteur 1 est commun aux secteurs 2 et 3, et si la sirène extérieure du secteur 2 est active, alors la sortie de la sirène extérieure du secteur 1 est également active.



Certains types de sortie ne prennent en charge que des événements au niveau du système (aucun événement spécifique à un secteur). Pour des informations plus détaillées, consultez le tableau ci-dessous.

Type 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 du relais de flash (Sortie 3) sur la carte de la centrale (NO, COM, NC). 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. Le flash de la sirène extérieure est activé après un « Echec MES » si ce flash est sélectionné (case cochée) pour l'option « Echec 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 une 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.
Incendie	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.
Mémoire	La sortie est activée selon la configuration des sorties du système de gâches (voir Configuration du système de verrouillage et sorties des MES Auto [-> 217]). 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 silencieuse 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)
Test auto. du Détecteur	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 enfoncé 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 enfoncé 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 (SPC Pro — MES complète)	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 (SPC Pro — MES effectuée)	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 « Clef 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 correspondante à la clé de mise en service en état de désactivation (fermé) et le secteur est déverrouillé. « 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 « Clef 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 désactivé. « Blockschloss 2 » est activé (si le secteur est prêt à être activé).
Élément 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 (tentative d'effraction du code)	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 : <ul style="list-style-type: none"> ● 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
Passage en 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 aussi

- 📄 Configuration les systèmes de verrouillage et sorties de MES Auto [→ 217]

17.9.1.3 Configuration les systèmes de verrouillage et sorties de MES Auto

- Dans le menu **Règle**, cliquez sur **Éditer** pour l'option **Configuration des sorties** dans **Options Système**.
- ⇒ L'écran suivant s'affiche :

Hardware	Système	Entrées & Portes	Sorties	Portes	Secteurs	Calendriers	Changer son code	Avancé
Options Système		Tempos Système	Identification	Normes & Standards	Date & Heure	Langue		
Options Système								
Option	Valeur	Libellé						
Paramètres généraux								
Code Effacement alarme	<input type="checkbox"/>	Autorise l'utilisateur à effectuer un RAZ alarme installateur en utilisant un code à usage unique (fourni à distance par l'installateur)						
Autosurveillance Zone offline	<input type="checkbox"/>	Si coché, les zones des transpondeurs déconnectés du X-BUS généreront chacune une autosurveillance						
RAZ Télécommande	<input type="checkbox"/>	Si coché, une seconde MHS via une radiocommande restaurera les alertes						
LED des modules audio	<input type="checkbox"/>	Si coché, la LED des modules audio ne s'allumera pas lorsque le microphone est actif						
Transmission en mode paramétrage	<input type="checkbox"/>	La centrale transmettra toujours les activations d'alarme, les panics etc...						
Etat sorties en mode paramétrage	<input type="checkbox"/>	Les sorties et indicateurs continuent de fonctionner durant le mode paramétrage						
Sirène qd défaut de transmission	<input type="checkbox"/>	Si une alerte de défaut de transmission apparait, les sirènes extérieures seront activées						
Contrainte redéclenchable	<input checked="" type="checkbox"/>	Si coché, l'alarme contrainte se déclenche à chaque fois qu'un code sous contrainte est entré						
Panique redéclenchable	<input checked="" type="checkbox"/>	Si coché, l'alarme panique se déclenche pour chaque sollicitation des boutons panique						
Etat MES/MHS sur voyant lecteur	<input type="checkbox"/>	Si Coché, les LEDs des lecteurs indiqueront la confirmation de MES/MHS pendant quelques secondes, et la demande de Badge + Code						
Silence pendant l'écoute	<input type="checkbox"/>	Si coché, les signalisation buzzer, synthèse vocale, sirènes extérieures et intérieures seront désactivées						
Mode Sortie Watchdog	<input type="text" value="Désactiver"/>	Mode de la sortie Watchdog. Si validée, la sortie 6 de la centrale est utilisée comme sortie watchdog. Si dévalidée, la sortie 6 est gérée normalement et est librement paramétrable.						
SPCP355	<input type="checkbox"/>	Valide l'alimentation VDS						

- Sélectionnez la condition sous laquelle la sortie du verrouillage est activée :

Tempo d'entrée	Cette sortie est activée à la fin de la temporisation de sortie et désactivée au début de la temporisation d'entrée.
Issues de secours	Elle est mise en service si n'importe quelle zone d'issue de secours est active.
Mise hors surveillance	S'active si un utilisateur met momentanément le système en MHS
Alarme Reset	S'active lorsqu'une alarme est effacée momentanément
Effacement des alarmes	S'active pendant la phase de MES si les 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.

- Sélectionnez le comportement des sorties.

Actif	La sortie sera active en permanence si la phase de mise en service automatique est active.
Clavier	La sortie suivra la signalisation du clavier.
Progressive	La sortie donnera une présignalisation progressive de la MES automatique
Durée de l'impulsion	Sélectionnez la durée d'activité de la MES automatique lors de l'impulsion.

17.9.1.4 Configuration de X-10

La page de configuration de X-10 vous permet de paramétrer le comportement de X-10.

1. Sélectionnez **Configuration > Sorties > X-10**.

⇒ La fenêtre suivante est affichée :

Paramètres X-10

Valider: Cocher pour valider le X-10

JDB: Cocher cette option pour activer les commandes X-10

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. Sélectionnez le groupe (A à P) des déclencheurs de périphérique X-10 à programmer.

⇒ Une liste de déclencheurs programmables (1-16) est affichée pour chacun de ces groupes.

Unité	Actif	Libellé	Déclencheurs	Touche de raccourci	Test
1	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Editer"/>	<input type="text" value="Aucun"/>	<input type="button" value="ON"/> <input type="button" value="Off"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Editer"/>	<input type="text" value="Aucun"/>	<input type="button" value="ON"/> <input type="button" value="Off"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Editer"/>	<input type="text" value="Aucun"/>	<input type="button" value="ON"/> <input type="button" value="Off"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Editer"/>	<input type="text" value="Aucun"/>	<input type="button" value="ON"/> <input type="button" value="Off"/>
5	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Editer"/>	<input type="text" value="Aucun"/>	<input type="button" value="ON"/> <input type="button" value="Off"/>
6	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Editer"/>	<input type="text" value="Aucun"/>	<input type="button" value="ON"/> <input type="button" value="Off"/>
7	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Editer"/>	<input type="text" value="Aucun"/>	<input type="button" value="ON"/> <input type="button" value="Off"/>

Unité	Numéro (1-16) attribué au périphérique.
Actif	Ce champ indique si le périphérique est actif ou non.
Description	Ce champ contient un texte significatif servant à identifier le périphérique - par exemple : Lumière RdC (16 caractères max.).
Touche de raccourci	Ce champ contient le raccourci clavier servant à activer le périphérique X-10.

Éditer un périphérique X-10

1. Cliquez sur **Editer**.

⇒ La fenêtre suivante est affichée :

2. Pour la programmation additionnelle, voir ici [→ 272].

17.9.2 Périph. X-BUS

17.9.2.1 Transpondeurs

1. Sélectionnez **Configuration > Hardware > X-Bus > Transpondeurs**.

⇒ La fenêtre suivante est affichée :

ID	Libellé	Etats	Type	N° Série	Version	Lecteur	Radio	ALIM
1	IO 1	Online	E/S [8 Entrée / 2 Sortie]	11327907	1.11 [07AUG13]	Non connecté	Non connecté	Type 1 - V4
2	AEX 2	Online	Audio [4 Entrée]	1434900	1.03 [13MAR13]	Non connecté	Non connecté	Non connecté
3	AEX 3	Online	Audio [4 Entrée / 1 Sortie]	37070907	1.03 [13MAR13]	Non connecté	Non connecté	Non connecté
4	WIR 4	Online	Radio	489907	1.11 [07AUG13]	Non connecté	SiWay - V5	Non connecté
5	IOA 5	Online	E/S analysées [8 Entrée / 2 Sortie]	165074801	2.00 [09Apr14]	Non connecté	Non connecté	Non connecté
6	IO 6	Online	E/S [8 Sortie]	443907	1.11 [07AUG13]	Non connecté	Non connecté	Non connecté
7	KSW 7	Online	Boîtier à clé [1 Sortie]	226593801	1.01 [11NOV10]	Non connecté	Non connecté	Non connecté
8	IND 8	Online	Indicateurs [1 Entrée]	223387801	1.03 [13MAR13]	EM400	Non connecté	Non connecté



Concernant le nom et l'identification des transpondeurs :

Dans une configuration en boucle, chaque transporteur est numéroté par ordre croissant du premier (le transporteur relié aux bornes 1A 1B de la centrale) au dernier (le transporteur relié aux bornes 2A 2B de la centrale).

Exemple pour SPC63xx : les transpondeurs numérotés de 1 à 63 sont attribués à des zones (jusqu'à 8) et identifiés par un numéro de 1 à 512. (512 est le numéro maximal pour l'identification de zone.) 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 fenêtre **Configuration Transpondeur**.

- Configurez les champs suivants :

Description	Pour application sur les témoins LED des périphériques.
Volume Maxi	Transpondeurs audio seulement : volume du haut-parleur pour le transporteur audio et les satellites (WAC 11). Ils sont tous câblés en parallèle. Veuillez noter que le potentiomètre du haut-parleur sur WAC 11 permet un réglage fin du volume. La plage de réglage est comprise entre 0 mini à 7 max.ou éteint.
Canal auxiliaire	Transpondeurs audio seulement :cette option devrait être activée si les satellites (WAC 11) sont connectés sur ce transporteur. Remarque : cette option, si activée, allume les micros satellites. Les haut-parleurs satellites sont toujours activés sans tenir compte de cette option.
Fin de ligne	Sélectionnez la résistance fin de ligne (par défaut : DEOL 4K7). Ce réglage doit correspondre au câblage réel de l'entrée de la centrale ou du transpondeur. Voir ici [→ 77].
Libellé (zone)	Entrez un texte descriptif de la zone attribuée.
Type (zone)	Sélectionnez le type de zone. Voir ici [→ 370].
Secteur	Sélectionnez le secteur.
Attributs	Appliquez les attributs voulus. Voir ici [→ 367].
Sorties / ALI 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. Voir Sorties supervisées [→ 61] 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 :

- Cliquez sur **Reconfigurer** pour appliquer les modifications.

Voir aussi

📄 Câblage du système [→ 77]

📄 Attributs zone [→ 370]

📄 Type de zone [→ 367]

17.9.2.1.1 Configurer un transpondeur d'indication

L'indicateur à LED peut être configuré selon deux modes :

- Mode lié
- Mode flexible

1. Sélectionnez **Configuration > Hardware > X-Bus > Transpondeurs**.

2. Cliquez sur l'un des paramètres identifiant l'indicateur à LED.

⇒ L'écran suivant est affiché pour la configuration **Mode lié**.

The screenshot shows a web-based configuration interface for a transponder. The top navigation bar includes 'Hardware', 'Système', 'Entrées & Portes', 'Sorties', 'Portes', 'Secteurs', 'Calendriers', 'Changer son code', and 'Avancé'. Below this, there are sub-menus for 'Centrale', 'XBUS', and 'Radio'. The 'Transpondeurs' menu is active, showing sub-options for 'Claviers', 'Contrôleurs de porte', 'Plan câble', and 'Paramètres X-Bus'. The main content area is titled 'Configuration Transpondeur' and contains the following fields:

- ID Transponder:** 8
- Type:** Indicateurs [1 Entrée]
- N° Série:** 223387801
- Libellé:** IND 8 (with a text input field and the instruction 'Entrer la description du module')
- Claviers:** 1: CKP 1 (with a dropdown menu and the instruction 'Sélectionner si le module doit être limité par un code valide tapé sur un clavier')
- Touche 1:** Désactivé (with a dropdown menu and the instruction 'Sélectionner le Secteur que la touche peut activer')
- Touche 2:** Désactivé (with a dropdown menu and the instruction 'Sélectionner le Secteur que la touche peut activer')
- Touche 3:** Désactivé (with a dropdown menu and the instruction 'Sélectionner le Secteur que la touche peut activer')
- Touche 4:** Désactivé (with a dropdown menu and the instruction 'Sélectionner le Secteur que la touche peut activer')
- LEDs permanentes:** (with the instruction 'Sélectionner si les voyants LED doivent être allumés lorsque les touches sont désactivées')

At the bottom, there is a table for configuring the transponder's entry:

Entrée	Fin de Ligne	Zone	Libellé	Type	Secteur	Attributs
1	2 RESIST.4K7/4K7	33	Zone 33	Alarme	1: Area 1	...

Mode lié

1. Entrez un nom descriptif.
2. Indiquez si l'accès à l'indicateur à LED doit être protégé par un code à entrer sur le clavier.
3. Sélectionnez les secteurs à contrôler à l'aide des 4 touches de fonction.
4. Configurez l'entrée.

Mode flexible

1. Cliquez sur le bouton **Mode flexible**.
2. Configurez les champs décrits dans les tableaux ci-dessous.
3. Configurez l'entrée.



▲ AVERTISSEMENT

Votre système n'est pas conforme aux normes EN si vous activez une touche de fonction pour qu'elle active le système sans qu'un code PIN valable soit nécessaire.

Touches de fonction	
Secteur	Sélectionnez le secteur à contrôler à l'aide de la touche de fonction.
Fonction	Sélectionnez la fonction associée à la touche dans ce secteur.
Secteur	Sélectionnez un secteur si l'indicateur à LED est installé dans un secteur sécurisé.
Indication visuelle	
Indicateur LED	L'indicateur possède 8 témoins lumineux / LED sur le côté droit, et 8 sur le côté gauche.
Fonction	La fonction indiquée par 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	Appuyez sur ce bouton pour changer la fonction du témoin lumineux considéré. Cette fonction peut être activée ou utilisée pour un système, un secteur, une zone ou un boîtier à clé.
Indications sonores	
Alarmes	Sélectionnez cette option si les alarmes doivent être signalées acoustiquement.
Entrée/Sortie	Sélectionnez cette option si les entrées / sorties doivent être signalées acoustiquement.
Appuyer sur une touche	Sélectionnez cette option si la pression sur une touche doit être confirmée acoustiquement.
Désactivation	
Calendrier	Sélectionnez cette option si l'accès au transporteur d'indication doit être limité en fonction du calendrier.
Interaction logique	Sélectionnez cette option si l'accès à l'indicateur à LED doit être limité en fonction d'une interaction logique.
Boîtier à clé	Sélectionnez cette option si l'accès à l'indicateur à LED doit être limité par un contacteur à clé.
Clavier	Indiquez si l'accès à l'indicateur à LED doit être protégé par un code PIN qu'il faudrait saisir sur un clavier. (Voir avertissement ci-dessus.)
Lecteur de Badge	Sélectionnez cette option si l'indicateur à LED doit rester inactif jusqu'à ce qu'un badge ou un tag valable soit présenté au lecteur de badge intégré.

17.9.2.1.2 Configurer un transpondeur d'interrupteur à clé (boîtier à clef).

1. Sélectionnez **Paramètres > X-Bus > Transpondeurs**.
2. Cliquez sur l'un des paramètres identifiant le boîtier à clef.
 - ⇒ La boîte de dialogue suivante s'affiche.

Hardware	Système	Entrées & Portes	Sorties	Portes	Secteurs	Calendriers	Changer son code	Avancé
Centrale	XBUS	Radio						
Transpondeurs Claviers Contrôleurs de porte Plan cible Paramètres X-Bus								
Configuration Transpondeur								
ID Transponder	7							
Type	Boîtier à clé							
N° Série	226593801							
Libellé	<input type="text" value="KSW 7"/>	Entrer la description du module						
Options Serrure								
Mémoire	<input type="checkbox"/>	Sélectionner si la position de la clé doit être verrouillée en position (décocher si en impulsion)						
Tempo verrouillage	<input type="text" value="0"/>	Entrer la durée du verrouillage en secondes (0 - 9999, 0 indique que le verrou reste jusqu'à ce que la clé retrouve la même position ou change de position)						
Secteurs								
Emplacement	<input type="text" value="Aucun"/>	Sélectionner le secteur ou est placé le boîtier à clé						
Indications visuelles								
Indicateurs	Fonction	Fonction Marche			Fonction Arrêt			Changer fonction
Gauche	Désactivé	<input type="text" value="Vert"/>	<input type="text" value="Permanent"/>	<input type="text" value="Off"/>	<input type="text" value="Permanent"/>			<input type="button" value="..."/>
Droit	Désactivé	<input type="text" value="Vert"/>	<input type="text" value="Permanent"/>	<input type="text" value="Off"/>	<input type="text" value="Permanent"/>			<input type="button" value="..."/>

- Configurez les champs décrits dans les tableaux ci-dessous.

Description	Entrez une description pour le transpondeur d'interrupteur à clé.
Options Touche	
Mémoire	Sélectionnez cette option si la position de la clé doit être verrouillée.
Tempo verrouillage	Entrez la durée du verrouillage en secondes (0 - 9999, 0 indique que le verrou est appliqué jusqu'à ce que la clé soit tournée dans l'autre direction).
Secteurs	
Emplacement	Sélectionnez la zone où le boîtier à clé est localisé.
Indications visuelles	
Témoin/LED	1 témoin lumineux / LED se trouve sur le côté droit, et 1 sur le côté gauche.
Fonction	La fonction indiquée par ce témoin lumineux / 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	Appuyez sur ce bouton pour changer la fonction du témoin lumineux considéré. Cette fonction peut être activée ou utilisée pour un système, un secteur, une zone ou un boîtier à clé.
Désactivation	
Calendrier	Sélectionnez cette option si le boîtier à clé doit être limité par le calendrier.
Interaction logique	Sélectionnez cette option si le module doit être limité par une interaction logique.
Sortie	
Sortie x	Configurez et entrez un libellé pour le boîtier à clé. Voir Sortie [→ 213] pour de plus amples informations.
Fonctions du boîtier à clé	
Positions centrale, Position droite et Position gauche	Sélectionnez la Fonction assurée par cette position du boîtier à clé et le Secteur pertinent.



⚠ AVERTISSEMENT

Votre système n'est pas conforme aux normes EN si vous activez une fonction du boîtier à clé pour qu'elle active le système sans qu'un code PIN valable soit nécessaire.

17.9.2.2 Claviers

17.9.2.2.1 Éditer un clavier standard

1. Sélectionnez **Configuration > Hardware > X-Bus > Claviers**.
2. Cliquez sur l'un des paramètres identifiant le clavier standard.
3. Configurez les champs comme indiqué dans le tableau ci-dessous.

The screenshot shows the 'Configuration Clavier' page in a web browser. The navigation menu at the top includes Hardware, Système, Entrées & Portes, Sorties, Portes, Secteurs, Calendriers, and Avancé. The sub-menu includes Centrale, XBUS, and Radio. The main menu includes Transpondeurs, Claviers, Contrôleurs de porte, Plan câble, and Paramètres X-Bus. The 'Configuration Clavier' section contains the following fields:

- ID Clavier:** 2
- N° Série:** 559907
- Libellé:** KEY 2 (with a text input field and the instruction 'Entrer la description du clavier')
- Réglage des touches de fonctions (état repos):**
 - Panique:** Désactivé (dropdown menu, instruction: 'Alarme Panique par l'appui simultané de deux touches')
 - Levée de doute:** Non affecté (dropdown menu, instruction: 'Une Vérification d'alarme sera faite sur le clavier où s'est produit une alerte ou une alarme contrainte')
- Indications visuelles:**
 - Rétro-éclairage:** Lorsqu'une touche est appuyée (dropdown menu, instruction: 'Sélectionner l'option rétro-éclairage écran du clavier')
 - Indicateurs:** (instruction: 'Active les voyants visibles')
 - Etat des MES:** (instruction: 'Sélectionner si l'état de surveillance doit être indiqué au repos')
- Indications sonores:**
 - Buzzer:** (instruction: 'Active le buzzer clavier')

Description	Saisissez une description unique pour identifier le clavier.
Réglage des touches de fonctions (état repos)	
Panique	Sélectionnez Activé, Désactivé ou Silencieux activé. Si validé, l'alarme de panique s'active en appuyant sur les 2 touches douces en même temps.
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	Sélectionnez lorsque le clavier est rétro-éclairé. Les options sont les suivantes : - Lorsqu'une touche est appuyée ; Toujours En service ; Toujours Hors service.
Indicateurs	Activez ou désactivez les témoins sur le clavier.
Etat des MES	Sélectionnez si l'état de surveillance doit être indiqué au repos.
Indications sonores	
Buzzer	Activez ou désactivez le buzzer sur le clavier.
Buzzer en MES Partielle	Activez ou désactivez le buzzer pendant la temporisation de sortie en MES Partielle.
Appuyez sur une touche	Sélectionnez si le volume des haut-parleurs est activé pour l'appui des touches.
Désactivation	
Calendrier	Sélectionnez si le clavier doit être contrôlé par le calendrier. Voir Calendrier [→ 268].
Interaction logique	Sélectionnez si le clavier doit être contrôlé par une interaction logique.
Boîtier à clé	Sélectionnez si le clavier doit être contrôlé par un boîtier à clé.
Entrée tag	Cochez cette case pour verrouiller les touches du clavier pendant la temporisation d'entrée quand un tag est configuré sur le clavier.

Secteurs	
Emplacement	Sélectionner le secteur protégé où se trouve le clavier.
Secteurs	Sélectionnez depuis le clavier les secteurs à contrôler.
Options	
Synchro Tempo sortie	Sélectionnez pour configurer un délai depuis le clavier. La localisation du clavier est ignorée et tous les secteurs appliquent le temps total de temporisation de sortie.

**AVIS**

Il est recommandé de n'affecter un secteur à un clavier seulement si le clavier se trouve dans le secteur assigné et si le chemin d'entrée/sortie est défini. Si un secteur est assigné, les temporisations d'entrée et de sortie sont appliquées (si configurées) lorsque le secteur en question est armé ou désarmé. D'autres fonctions liées aux chemins d'entrée/sortie sont alors disponibles. Si aucun secteur n'est assigné, le secteur est immédiatement armé ou désarmé et les autres fonctions d'entrée/sortie ne sont pas disponibles.

Voir aussi

Calendriers [→ 268]

17.9.2.2.2 Éditer un clavier confort

1. Sélectionnez **Configuration > Hardware > X-Bus > Claviers**.
2. Cliquez sur l'un des paramètres identifiant le clavier confort.
3. Configurez les champs comme indiqué dans le tableau ci-dessous.

Hardware	Système	Entrées & Portes	Sorties	Portes	Secteurs	Calendriers	Changer son code	Avancé
Centrale	XBUS	Radio						
Transpondeurs	Claviers	Contrôleurs de porte	Plan câble	Paramètres X-Bus				

Configuration Clavier

ID Clavier	1	
N° Série	227361801	
Libellé	<input type="text" value="CKP 2"/>	Entrer la description du clavier

Réglage des touches de fonctions (état repos)

Panique	<input type="text" value="Désactivé"/>	Alarme panique en appuyant sur les touches de fonctions F1 et F2 simultanément
Feu	<input type="checkbox"/>	Alarme incendie en appuyant sur les touches de fonctions F2 et F3 simultanément
Médicale	<input type="checkbox"/>	Alarme Médicale en appuyant sur les touches fonction F3 et F4 simultanément
MES Totale	<input type="checkbox"/>	MES Totale en appuyant sur la touche fonction F2 deux fois
MES Partielle A	<input type="checkbox"/>	MES Partielle A en appuyant sur la touche F3 deux fois
MES Partielle B	<input type="checkbox"/>	MES Partielle B en appuyant sur la touche fonction F4 deux fois

Levée de doute

Levée de doute	<input type="text" value="Non affecté"/>	Une Vérification d'alarme sera faite sur le clavier où s'est produit une alerte ou une alarme contrainte
----------------	--	--

Description	Saisissez une description unique pour identifier le clavier.
Réglage des touches de fonctions (état repos)	
Panique	Sélectionnez Activé, Désactivé ou Silencieux activé. Si cette option est active, l'alarme de panique peut être activée en appuyant en même temps sur F1 et F2.
Incendie	Activez pour permettre l'activation de l'alarme incendie en appuyant en même temps sur F2 et F3
Médical	Activez pour permettre l'activation de l'alarme médicale en appuyant en même temps sur F3 et F4.
MES totale	Activez pour permettre l'activation de la MES TOTALE en appuyant deux fois sur F2.
MES Partielle A	Activez pour permettre l'activation de la MES Partielle A en appuyant deux fois sur 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.
Indications visuelles	
Rétro-éclairage	Sélectionnez lorsque le clavier est rétro-éclairé. Les options sont les suivantes : - Lorsqu'une touche est appuyée ; Toujours En service ; Toujours Hors service.
NIV.RETROECLAIR	Sélectionnez l'intensité du rétroéclairage. Plage de réglage 1 - 8 (élevé).
Indicateurs	Activez ou désactivez les témoins sur le clavier.
Etat des MES	Sélectionnez si l'état de surveillance doit être indiqué au repos (témoin).
Logo	Sélectionner si le logo doit être visible au repos.
Montre analogique	Sélectionnez la position de l'horloge si elle doit être visible au repos. Les options sont les suivantes : aligné à gauche, aligné au centre, aligné à droite ou désactivé.
Urgence	Activez si les touches fonctions Panique, Incendie ou Médicale 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	Sélectionner le volume du haut-parleur pour les indications d'alarme ou pour désactiver le son.
Entrée/sortie	Intervalle 0 - 7 (volume max.)
Carillon	Sélectionner le volume du haut-parleur pour les indications d'entrée et de sortie ou pour désactiver le son.
Appuyez sur une touche	Intervalle 0 - 7 (volume max.)
Annonce Vocale	Sélectionner le volume du haut-parleur pour le carillon ou pour désactiver le son.
Buzzer en MES Partielle	Intervalle 0 - 7 (volume max.)
Désactivation	
Calendrier	Sélectionnez si le clavier doit être contrôlé par le calendrier. Voir Calendrier.

Interaction logique	Sélectionnez si le clavier doit être contrôlé par une interaction logique.
Boîtier à clé	Sélectionnez si le clavier doit être contrôlé par un boîtier à clé.
Entrée tag	Cochez cette case pour verrouiller les touches du clavier pendant la temporisation d'entrée quand un tag est configuré sur le clavier.
Secteurs	
Emplacement	Sélectionner le secteur protégé où se trouve le clavier.
Secteurs	Sélectionnez depuis le clavier les secteurs à contrôler.
Options	
Synchro Tempo sortie	Sélectionnez pour configurer un délai depuis le clavier. La localisation du clavier est ignorée et tous les secteurs appliquent le temps total de temporisation de sortie.

**AVIS**

Il est recommandé de n'affecter un secteur à un clavier seulement si le clavier se trouve dans le secteur assigné et si le chemin d'entrée/sortie est défini. Si un secteur est assigné, les temporisations d'entrée et de sortie sont appliquées (si configurées) lorsque le secteur en question est armé ou désarmé. D'autres fonctions liées aux chemins d'entrée/sortie sont alors disponibles. Si aucun secteur n'est assigné, le secteur est immédiatement armé ou désarmé et les autres fonctions d'entrée/sortie ne sont pas disponibles.

17.9.2.3 Contrôleurs de porte

17.9.2.3.1 Édition d'un contrôleur de porte

1. Sélectionnez **Configuration > Hardware > X-Bus > Contrôleurs de porte**.
2. Cliquez sur une information affichée en bleu (par exemple le numéro de série).
3. Configurez les champs comme indiqué dans le tableau ci-dessous.

Configuration Contrôleur de Porte

ID Transponder: 1

Type: DC-2 [4 Entrée / 2 Sortie]

N° Série: 195309801

Libellé: DC2 1

Porte E/S 1 (*): Porte 1 [Editer]

Porte E/S 2 (*): Porte 2 [Editer]

Lecteur 1 (**): Défaut

Lecteur 2 (**): Défaut

(*) Choisir 'Entrées/Sorties' rends une porte non affectée. Lorsque la porte 2 n'est pas affectée, le lecteur 2 est utilisé comme lecteur de sortie pour la porte 1.

(**) Défini le comportement des sorties V0x et VAx qui pilotent les voyants indicateurs du lecteur. Les profils 3 + 4 doivent être utilisés avec des lecteurs HID avec clavier qui envoient le code PIN avec un site code prédéfini.



Concernant le nom et l'identification des transpondeurs :

Dans une configuration en boucle, chaque transporteur est numéroté par ordre croissant du premier (le transporteur relié aux bornes 1A 1B de la centrale) au dernier (le transporteur relié aux bornes 2A 2B de la centrale).

Exemple pour SPC63xx : les transpondeurs numérotés de 1 à 63 sont attribués à des zones (jusqu'à 8) et identifiés par un numéro de 1 à 512. (512 est le numéro maximal pour l'identification de zone.) Ainsi, tout transporteur identifié par un numéro supérieur à 63 n'est attribué à aucune zone.

ID Transpondeur	Numéro d'identification du contrôleur de porte réglé avec les interrupteurs rotatifs.
Type	Type du contrôleur de porte.
N° Série	Numéro de série du contrôleur de porte.
Description	Description du contrôleur de porte.
E/S de la porte 1	<ul style="list-style-type: none"> ● Si une porte est attribuée à l'E/S de porte, sélectionnez le numéro de porte correspondant. Si les deux sorties sont configurables, sélectionnez Zones / Sorties. ● Si un numéro de porte est sélectionné pour l'E/S de porte, les paramètres de la porte peuvent être modifiés en cliquant sur le bouton Editer. Cette action est identique à Paramètres > Portes. ● Si vous sélectionnez Zones / Options, les deux zones et la sortie sont configurables en cliquant sur le bouton d'édition.
E/S de la porte 2	
Profil 1	Pour les lecteurs avec un voyant LED vert et un voyant LED rouge.
Profil 2	Pour les lecteurs VANDERBILT avec un voyant LED jaune (AR618X).
Profil 3	Le profil 3 est utilisé avec les lecteurs HID qui envoient un code à la centrale, comme une lecture de carte dotée d'un code site prédéfini (0)
Profil 4	Le profil 4 est utilisé avec les lecteurs HID qui envoient un code à la centrale comme carte de lecture dotée d'un code site prédéfini (255).
Profil 5	Choisir si les lecteurs Sesam sont utilisés. Il est également recommandé de sélectionner l'option Profil Lecteur remplacé pour fournir une rétroaction durant la configuration.

Édition des zones/sorties pour les E/S d'une porte

1. Sélectionnez une Entrée/Sortie pour l'E/S de porte.
2. Cliquez sur le bouton **Éditer**.
3. Les 2 entrées et la sortie appartenant à l'E/S de porte considérée peuvent être configurées comme des entrées et des sorties normales. Voir ici [→ 262].
4. Pour que les entrées puissent être utilisées, un numéro de zone doit leur être attribué.

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 > Hardware > X-Bus > Plan de câblage**.
⇒ La fenêtre suivante est affichée :

Hardware	Système	Entrées & Portes	Sorties	Portes	Secteurs	Calendriers	Changer son code	Avancé
Centrale	XBUS	Radio						
Transpondeurs	Claviers	Contrôleurs de porte	Plan câble	Paramètres X-Bus				

Plan de câblage X-BUS

Position	ID	Etats	Type	N° Série	Libellé
1	1	Actif	E/S [8 Entrée / 2 Sortie]	11327907	IO 1
2	2	Actif	Audio [4 Entrée]	1434900	AEX 2
3	3	Actif	Audio [4 Entrée / 1 Sortie]	37070907	AEX 3
4	4	Actif	Radio	489907	WIR 4
5	5	Actif	E/S analysées [8 Entrée / 2 Sortie]	165074801	IOA 5
6	1	Actif	DC-2 [4 Entrée / 2 Sortie]	195309801	DC2 1
7	6	Actif	E/S [8 Sortie]	443907	IO 6
8	7	Actif	Boitier à clé [1 Sortie]	226593801	KSW 7
9	8	Actif	Indicateurs [1 Entrée]	223387801	IND 8
10	1	Actif	Clavier confort SPCK62x	227361801	CKP 1
11	2	Actif	Claviers	559907	KEY 2

Reconfigurer



Pour les détails sur l'interface X-BUS, voir ici [→ 77].

17.9.2.5 Paramètres

Pour configurer les connexions X-BUS :

- Sélectionnez **Configuration > Hardware > X-Bus > Paramétrage X-Bus**.
⇒ La fenêtre suivante est affichée.
- Configurez les champs comme indiqué dans le tableau ci-dessous.

Hardware	Système	Entrées & Portes	Sorties	Portes	Secteurs	Calendriers	Changer son code	Avancé
Centrale	XBUS	Radio						
Transpondeurs	Claviers	Contrôleurs de porte	Plan câble	Paramètres X-Bus				

Paramètres X-BUS

Mode adressage

Manuel - Utiliser les switches des Périphériques pour mettre une adresse d'identification

Automatique - L'identification sera fournie automatiquement

Type X-BUS

1 boucle

2 branches

Ré-essaie Nombre de tentatives de retransmissions en cas d'interférence (Par défaut : 25)

Tempo Comms Nombre de secondes durant lequel le défaut est présent avant le déclenchement d'une alerte (10 par défaut)

Sauver

Mode 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 chaîne.
Ré-essaie	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 Commun.	Délai en secondes avant qu'une erreur de communication soit enregistrée.

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**.
2. Voir le tableau ci-dessous pour de plus amples informations.

Hardware	Système	Entrées & Portes	Sorties	Portes	Secteurs	Calendriers	Changer son code	Avancé
Centrale	XBUS	Radio						
Radio	WPA	Paramétrage Radio						
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		

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 à laquelle le détecteur est attribué.
Batterie	L'état de la batterie dans le détecteur (le cas échéant).
Superviser	L'état 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 sur ce bouton pour afficher l'historique du détecteur radio. Voir ici [→ 232].
Enroller	Cliquez sur ce bouton pour ouvrir la liste des périphériques radio enregistrés.

1. Sélectionnez **État > Hardware > X-Shunt > WPA**.
2. Affiche l'identité et l'état de chaque WPA enregistré.

17.9.3.1 Historique - Détecteur radio X

Pour consulter un historique rapide des événements d'un détecteur radio :

1. Cliquez sur le bouton **JDB**.
2. Voir le tableau ci-dessous pour de plus amples informations.
3. Pour créer un fichier de texte contenant les données du journal, cliquez sur **Fichier Texte**.

Date/heure	La date et l'heure de l'événement journalisé.
Récepteur	L'emplacement du récepteur radio, c'est-à-dire si le module radio est installé dans le clavier, sur la centrale, ou s'il s'agit d'un transpondeur radio.
Signal	L'intensité du signal reçu par le détecteur (01=basse, 09=haute).
Etats	L'état physique du détecteur.
Batterie	L'état de la batterie connectée au détecteur (OK, Défaut).

17.9.3.2 Configuration d'un WPA

	<p>AVIS</p> <p>L'écran de statut et de configuration d'un WPA n'est affiché que si un module radio est intégré à la centrale ou si l'un de ses transpondeurs et la centrale sont autorisés pour le type de module(s) intégré(s).</p>
---	---

Un WPA n'est pas affecté à un utilisateur. En général, un WPA est partagé par plusieurs personnes comme, par exemple, les vigiles travaillant en équipe. Il peut également être fixé sur une surface (sous un bureau ou derrière la caisse).

128 WPA par centrale au maximum sont autorisés.

Pour configurer un WPA depuis le navigateur :

- Sélectionnez le mode Paramétrage puis les options suivantes **Configuration > Hardware > Radio > WPA.**

Hardware		Système	Entrées & Portes	Sorties	Portes	Secteurs	Calendriers	Changer son code	Avancé
Centrale		XBUS	Radio	Paramétrage Radio					
Radio	WPA	Paramétrage Radio							
WPA	Libellé	ID Transmetteur	Batterie	Supervision	Etats	Editer		Effacer	
1	WPA 1	100	OK	OK	---	Editer		Effacer	
2	WPA 2	0	OK	Désactivé	---	Editer		Effacer	
Ajouter									

Les éléments suivants peuvent être vérifiés et configurés depuis cette page :

- **État de la batterie**
La centrale reçoit le statut de batterie du WPA pour chaque image. L'état de batterie peut être OK ou Faible.
Le suivi de la batterie requiert un WPA intégrant la révision E-PC138612 de la carte de circuit imprimé ou une version plus récente
 - **Statut de Supervision**
Le statut de supervision peut correspondre à l'un des états 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 test peut correspondre à l'un des statuts 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 **Modifier** pour modifier la configuration WPA.
 2. Cliquez sur **Effacer** pour effacer le WPA du système.

17.9.3.2.1 Ajout d'un WPA

Pour ajouter un WPA au système :

- Cliquez sur **Ajouter** sur la page principale de configuration et de statut WPA.
- ⇒ La page de configuration WPA est affichée 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

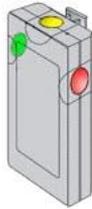
ID Transmetteur Apuyez n'importe quel bouton su WPA, puis sélectionnez 'Apprendre'

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 correspondant à la planification des tests.

Affectation de fonction aux boutons

Rouge	<input type="text" value="Aucun"/>
Vert	<input type="text" value="Aucun"/>
Jaune	<input type="text" value="Suspicion"/>
Rouge + Vert	<input type="text" value="Agression"/>
Rouge + Vert	<input type="text" value="Aucun"/>
Jaune + Vert	<input type="text" value="Aucun"/>



- Configurez le WPA à l'aide des informations suivantes :

Description/nom	Saisissez une description ou un nom unique identifiant le WPA.
ID Transmetteur	L'ID transmetteur est gravé dans le châssis du WPA et peut être entré manuellement. 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 entre automatiquement cet ID dans le champ à condition qu'aucun autre WPA ne soit défini par cette ID.
Superviser	Le WPA peut être configuré pour émettre un signal de supervision intermittent. La supervision est activée sur le WPA grâce à un cavalier. La fonction de supervision doit également être activée sur la centrale pour cette WPA spécifique pour une supervision correcte. Si la centrale ne reçoit pas le signal de supervision, une alarme est déclenchée : elle est affichée sur le clavier et consignée dans le journal. Si la supervision n'est pas activée, le WPA émet un message de supervision environ toutes les 24 heures afin de communiquer l'état de sa batterie à la centrale. Le temps séparant les messages est aléatoire afin de diminuer les risques de collision avec d'autres WPA. Cocher la case Supervision si la supervision est activée pour un WPA particulier.
Test	Cocher la case Test si un test WPA périodique est requis. a fréquence du test périodique est configurée sur la page Changer les paramètres Radio [→ 235].
Affectation des boutons	Utilisez cette section pour assignez des fonctions aux combinaisons de boutons. Les fonctions disponibles sont les suivantes : Panique, Panique silencieuse, Agression, Suspicion, Sortie RF utilisateur, Médicale. Plusieurs combinaisons peuvent être choisies pour la même fonction. L'écran ci-dessus montre les réglages par défaut de la centrale pour une installation bancaire : <ul style="list-style-type: none"> ● Jaune - Suspicion ● Rouge + Vert - Holdup Pour les installations évoluée ou simple, les combinaisons sont les suivantes :

	<ul style="list-style-type: none"> ● Rouge + Vert - Panique <p>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 [→ 272]</p>
--	---

- Cliquez sur le bouton **Sauver** pour sauvegarder les paramètres.

Voir aussi

- 📄 Modifier les paramètres radio [→ 235]
- 📄 Modifier les paramètres radio [→ 235]
- 📄 Déclencheurs [→ 272]

17.9.3.2 Modifier un WPA

Pour modifier un WPA, cliquez sur **Editer** sur la page principale de configuration et de statut du WPA.

La page **Editer** est similaire à **Ajouter** mais n'affiche pas le bouton Apprendre permettant d'entrer automatiquement l'ID du WPA.

17.9.3.3 Modifier les paramètres radio

1. Sélectionnez **Configuration > Hardware > Radio > Paramètres radio**.

The screenshot shows the 'Paramètres Radio' configuration page. The navigation menu at the top includes Hardware, Système, Entrées & Portes, Sorties, Portes, Secteurs, Calendriers, and Avancé. Under Hardware, there are sub-menus for Centrale, XBUS, and Radio. The 'Radio' sub-menu is active, showing 'Radio', 'WPA', and 'Paramétrage Radio'. The 'Paramètres Radio' section contains the following settings:

- Antenne:** Interne (dropdown menu). Description: Sélectionner le type d'antenne connectée au module radio.
- Supervision:** Autosurveillance désactivée (dropdown menu). Description: Sélectionner si le manque de supervision d'un détecteur doit déclencher une zone d'autoprotection.
- Filtre:** . Description: Si coché, les signaux reçus avec un signal nul seront ignorés.
- Détecter brouillage Radio:** . Description: Si coché, une alerte sera déclenchée lorsqu'un brouillage radio est détecté.
- RF FOB SOS:** Panique (dropdown menu). Description: Select how the SOS buttons on the RF Fob should operate.
- Plannification Test WPA:** 0 (text input). Description: Période maximale entre les tests WPA, en jours (0-365, 0 indique tests désactivés / non requis).
- Supervision RF: MES impossible:** 20 (text input). Description: Nombre de minutes sans message de supervision, qui empêchera la mise en surveillance.
- Détecteur RF perdu:** 720 (text input). Description: Nombre de minutes sans supervision après lequel le détecteur est considéré absent (la valeur 0 signifie que cette vérification n'est pas faite).

2. Voir le tableau ci-dessous pour de plus amples informations.

Antenne	Sélectionnez le type d'antenne raccordée au module radio (interne ou externe) dans la liste déroulante. Le type d'antenne requis dépend du type de module radio 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 ici [→ 245].
Filtre	Cochez cette option pour filtrer les signaux RF de basse intensité.
Détecter brouillage radio	Cochez cette option pour activer une alerte quand une interférence RF est détectée.
PANIQUE TELEC. RADIO	Sélectionnez les options de déclenchement des boutons panique de la télécommande radio :

	<ul style="list-style-type: none"> ● Désactiver ● Valider ● Validé (Silencieux) ● Médical Utilisateur ● Agression Utilisateur ● Sortie Radio
Planification Test WPA	Entrez la durée maximale en jours séparant deux tests WPA.
Supervision RF : MES impossible	<p>Entrez une durée en minutes au bout de laquelle l'absence de message de supervision inhibe la mise en surveillance de la zone du détecteur.</p> <p>Ce paramétrage s'applique uniquement aux zones d'intrusion :</p> <ul style="list-style-type: none"> ● Alarme ● Entrée/sortie ● Fin tempo de sortie ● Panique ● Holdup ● Autosurveillance ● Supervision Verrouillage ● Sismique ● Tout OK ● Autorisation avant MES/MHS ● Élément de verrouillage
Détecteur RF perdu	Entrez une durée en minutes au bout de laquelle le détecteur RF (capteur ou WPA) est considéré comme perdu.

17.9.4 Modification des paramètres système

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
Réglages généraux		
	Secteurs	<p>Sélectionnez pour autoriser plusieurs secteurs sur le système.</p> <p>Remarque : cette option n'est affichée que pour les types d'installation Résidentiel et Commercial.</p>
	Code restauré	<p>Grade 3 uniquement : Un utilisateur ne possédant pas les droits de remettre à zéro une alarme, peut toutefois la remettre à zéro 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.</p>
	Autosurveillance	Activez cette case si les zones de transpondeur hors ligne doivent générer une alarme d'anti-effraction de

Restriction	Options Système	Description
	Zone offline	zone.
	RAZ Télécommande	Si activé, la télécommande radio peut restaurer des alertes si l'on appuie sur la touche Arrêt.
Web et SPC Pro 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 : <ul style="list-style-type: none"> ● 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.
	Etat MES/MHS sur voyant lecteur	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	<p>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 :</p> <ul style="list-style-type: none"> ● 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. <p>Les options suivantes combinent l'option Validé avec le signalment d'une erreur matérielle, en cas de panne du microprocesseur principal. Si une telle panne se produit, un événement SIA est envoyé au CTS1.</p> <p>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.</p> <ul style="list-style-type: none"> ● 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. <p>L'événement SIA rapporté est HF et l'extension SIA signale un défaut matériel.</p> <p>Remarque : les défauts matériels ne sont pas signalés si</p>

Restriction	Options Système	Description
		l'ingénieur est connecté au système. Pour plus d'informations sur les CTS, voir Centre de télésurveillance (CTS) [-> 309].
	SPCP355	Activer l'alimentation électrique 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.
	Capacité de la batterie	Capacité totale des batteries en ampères-heure, seulement pour la centrale (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 est affiché sous le menu ÉTAT - BATTERIE - TEMPS BATT.
	Courant Max	Le courant total fourni par les batteries en cas de panne de 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 est affiché 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 sélectionnée 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	Options Système	Description
		restriction. Aux niveaux 2 ou 3, le type d'événement signalé est conforme aux normes de la région sélectionnée : <ul style="list-style-type: none"> ● Irlande - Alarme ● Autres régions - Alarme
Ⓣ	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 : <ul style="list-style-type: none"> ● 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 : <ul style="list-style-type: none"> ● 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 : <ul style="list-style-type: none"> ● 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 : <ul style="list-style-type: none"> ● Allemagne VDS – Autosurveillance ● Tous les autres pays - problème
Ⓣ	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 : <ul style="list-style-type: none"> ● Allemagne VDS – Autosurveillance

Restriction	Options Système	Description
		<ul style="list-style-type: none"> Tous les autres pays - problème
Ⓣ	EOL Etendu EOL Wide	Si activé, les bandes larges de résistance de fin de ligne sont utilisées.
	Suspicion Audible	Si activé, l'alerte suspicion WPA activera les voyants et le buzzer clavier. (Mode bancaire seulement).
Pro	Fin de ligne (RESISTANCE FIN DE LIGNE)	<p>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.</p> <p>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.</p>
	Test sismique si MES manuelle	Si activé, tous les sismiques de tous les secteurs activés seront testés lors de la MES (Mode bancaire seulement).
Ⓣ	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/le 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	<p>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.</p> <p>Désactivé : En cas d'activation d'une zone entrée interdite/sortie pendant la temporisation de sortie, l'alarme ne se déclenche pas.</p> <p>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.</p>
Ⓣ	Alarme activée Entrée	<p>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.</p> <p>Désactivé : En cas d'activation d'une zone entrée interdite/sortie pendant la temporisation d'entrée, l'alarme ne se déclenche pas.</p> <p>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.</p>
Confirmation		
Ⓣ	Confirmation	<p>L'option Confirmation détermine le moment à partir duquel une alarme est considérée comme étant confirmée.</p> <ul style="list-style-type: none"> BS8243 : Ceci renforce la conformité avec les exigences de police du Royaume-Uni. C'est également une contrainte spécifique pour les installations dans les entreprises du Royaume-Uni. Le texte stipule qu'une alarme n'est confirmée que si elle remplit les conditions suivantes :

Restriction	Options Système	Description
		<p>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 d'alarme. Le délai de confirmation de l'alarme doit être compris entre 30 et 60 minutes. (Voir Temporisations [→ 245])</p> <p>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.</p> <ul style="list-style-type: none"> ● 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 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. ● 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 Décret du 1er février sur l'utilisation de systèmes d'alarme dans le cadre de la sécurité privée ». Ce décret stipule qu'une alarme ne sera considérée comme alarme confirmée que si elle répond aux conditions suivantes : <ul style="list-style-type: none"> - activation de 3 zones en 30 minutes (par défaut), avec deux activations pouvant provenir du même périphérique si les types des activations différent, c'est-à-dire alarme / sabotage. - 1 activation d'alarme suivi par un défaut ATS[1] dans une période de 30 minutes (par défaut). - Un défaut ATS suivi par une condition de sabotage ou d'alarme dans une période de 30 minutes (par défaut). <p>Si la période de 30 minutes expire et que la zone est restaurée à son état physique normal, les alertes de zone seront supprimées si un utilisateur de niveau 2 peut supprimer cette alerte. Dans ce cas, la zone acceptera une nouvelle condition d'alerte qui entraînera une nouvelle activation. Alternativement, si la zone n'a pas encore été restaurée à son état physique normal, alors cette zone sera inhibée si elle peut l'être.</p> <p>Si une alerte (ATS) se produit à nouveau après la fenêtre de 30 minutes (par défaut), le délai de 30 minutes sera réinitialisé.</p> <p>L'option de confirmation EN50131-9 est automatiquement appliquée lorsque l'option Standards -> Région a pour valeur Espagne.</p> <ul style="list-style-type: none"> ● VDS Ceci mettra en vigueur la conformité avec la norme VDS.
Clavier		

Restriction	Options Système	Description
ⓘ	Toujours afficher l'état (AFFICHER ETAT)	Si activé, l'état d'armement (MES / MES partielle / MHS) du système est affiché 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 activé, un message CTS sera affiché 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.).
	Voir les caméras	Si activé, les caméra hors ligne seront affichées sur les claviers en MHS.
	Langue au repos	Sélectionnez la langue affichée au repos. <ul style="list-style-type: none"> ● Langue système paramétrée : 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.
CODE		
	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 page [→ 320] 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.
	Code contrainte	Sélectionnez l'une des fonctions Contrainte suivantes pour l'activer. <ul style="list-style-type: none"> ● 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 Editer pour sélectionner les options d'utilisation du code. <ul style="list-style-type: none"> ● 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 [→ 245]. ● 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

Restriction	Options Système	Description
		<p>d'avertissement est définie dans le champ Avertismt Code de Temporisations. Voir Temporisations [→ 245].</p> <ul style="list-style-type: none"> ● 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 [→ 245]. ● Sécuriser Code - si activé, le code sera automatiquement généré par la centrale.
Porte		
	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 carte et augmentez le nombre d'utilisateurs de cartes sur le système de 100 à 2500.
	Formats du badge	<p>Cliquez sur le bouton Modifier pour sélectionner les formats de badge autorisés sur cette centrale.</p> <p>Consultez l'Annexe du Guide d'installation et de configuration SPC pour un complément d'information à propos des lecteurs de cartes et des formats de badges.</p> <p>Remarque : En sélectionnant Wiegand, vous activez tous les formats de carte Wiegand.</p>
Web et SPC Pro 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 et SPC Pro 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.
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	<p>Activez cette fonction si vous voulez que l'installateur ne puisse accéder au système que si l'utilisateur l'autorise.</p> <p>Si désactivé, l'option du menu ACTIVE INSTALLAT du clavier n'est pas disponible.</p> <p>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.</p>
Ⓣ	Accès Constructeur	<p>Activez cette fonction si vous voulez que l'installateur ne puisse accéder au système que si l'utilisateur l'autorise.</p> <p>Si désactivé, l'option du menu ACTIVE</p>

Restriction	Options Système	Description
		CONSTRUCTEUR du 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 : <ul style="list-style-type: none"> ● Code PIN seulement : un code utilisateur valable. Voir page. ● 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 sera disponible pour la configuration par l'utilisateur si 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. Le contrôle par SMS ne sera disponible pour la configuration par l'utilisateur si cette option est sélectionnée. ● CODE PIN SMS et ID appelant
Stratégie		
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 et SPC Pro uniquement	Configuration des sorties	Cliquez sur le bouton Éditer pour configurer les paramètres de gâche et sortie MES automatique [→ 217].
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 : <ul style="list-style-type: none"> - Pas d'alarme confirmée si activée de manière interne - Block RAZ à distance - Block Isolation à distance

Restriction	Options Système	Description
		- 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
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 d'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 aussi

 Ajouter / Éditer un secteur [→ 253]

17.9.4.2 Temporisations

Cette fenêtre 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 > Temporisation Système**.
⇒ La fenêtre suivante est affichée.
2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Temporisations

Désignation des fonctions dans l'ordre suivant :

- 1^{er} rang Web/SPC Pro

● 2^{ème} rang Clavier

Temporisation	Libellé	Défaut
Audible		
Sirènes intérieures DUREE SIRENE INT	Durée d'actionnement des buzzers internes quand l'alarme est active. (1 – 15 minutes ; 0 = jamais)	15 min.
Sirènes extérieures DUREE SIRENE EXT	Durée d'actionnement des sirènes extérieures quand l'alarme est active. (1 – 15 minutes ; 0 = jamais)	15 min.
Retard sirènes extérieures RETARD SIRÈNE EXT	Le déclenchement de la sirène extérieure est temporisé. (0 – 600 secondes)	0 s
Carillon DUREE CARILLON	Durée d'actionnement de la sortie carillon en secondes quand une zone avec l'attribut Carillon est ouverte. (1 – 10 secondes)	2 s
Confirmation		
Al. Confirmée TEMPS DE CONFIRM	<ul style="list-style-type: none"> ● Remarque : Uniquement disponible si le grade de sécurité est sans restriction et que DD243 est sélectionné pour la variable Confirmation. (Voir Options Système [→ 236]) 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. (30 – 60 minutes)	30 min
Agression Confirmée	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 – 1 200 minutes)	480 min.
Retard de transmission RETARD NUMEROTAT.	S'il est programmé, le délai de numérotation est la période prédéfinie (0 à 30 secondes) avant que le système appelle un centre de télésurveillance (CTS). Ce délai est destiné à réduire les réactions non nécessaires des centres d'appel et de la police. Toutefois, si un intrus pénètre dans une deuxième zone, le délai de numérotation est ignoré et l'appel est déclenché immédiatement. (0 – 30 secondes)	30 s
Abandon d'alarme ANNUL. D'ALARME	Après une alarme transmise, délai au cours duquel un message d'abandon d'alarme peut être transmis. (0 – 999 secondes)	30 s
MES		
Validation MES/MHS VALIDATION MES/MHS	période pour laquelle l'autorisation de validation de paramétrage est valable. Saisissez une valeur entre 10 et 250 secondes.	20 sec
Dernière issue DERNIERE ISSUE	Le délai de dernière issue est le délai de mise en marche en secondes après la fermeture d'une zone programmée avec l'attribut dernière issue. (1 – 45 secondes)	7 s
Sirène lors MES totale SIREN SI MES TOT	Active brièvement la sirène extérieure pour indiquer que la MES totale est active. (0 – 10 secondes)	0 s
Flash lors MES totale FLASH SI MES TOT	Active brièvement le flash sur la sirène extérieure pour indiquer que la MES totale est active. (0 – 10 secondes)	0 s
Armement échoué AFFICH ECHEC MES	Délai d'affichage en secondes du message d'échec de la MES sur les claviers (0 jusqu'à l'entrée du code valide). (0 – 999 secondes)	10 s
Alarme		
Double déclenchement DOUBLE DECLENCH.	Délai maximum entre des activations de zones ayant l'attribut Double déclenchement pour déclencher une alarme. (1 – 99 secondes)	10 s
Test JOURS TEST JDB	Période en jours pendant laquelle une zone reste en test avant de revenir automatiquement en fonctionnement normal.	14 jours

Temporisation	Libellé	Défaut
	(1 – 99 jours)	
Période de l'autotest sismique AUTOTEST SISMIC	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 DUREE TEST SISM	Temps maximum (secondes) d'attente du déclenchement du sismique lorsqu'il est sollicité par l'activation de la sortie test sismique (3 - 120 secondes)	30 s
Verrouillage Post Alarme VERROUILLAGE POST ALARME	Durée de verrouillage des accès après une alarme.	0 min
Flash sirène extérieure DUREE FLASH	Durée d'actionnement de la sortie du flash quand l'alarme est active. (1 – 15 minutes ; 0 = indéfiniment)	15 min.
Alertes		
Tempo 230V DELAI DEF.230V	Le délai entre la détection d'un défaut de l'alimentation secteur et le moment où le système déclenche une alerte. (0 – 60 minutes)	0 min.
Installateur		
Accès Ingénieur ACCES INSTALLAT.	La temporisation pour l'accès Installateur commence 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 DECONNECT AUTO	La durée d'inactivité après laquelle l'installateur sera automatiquement déconnecté.	0 min.
Clavier		
Temps de saisie clavier TIMEOUT CLAVIER	Délai d'inactivité en secondes avant qu'un clavier quitte le menu actif. (10 - 300 secondes)	30 s
Langue clavier LANGUE CLAVIER	Temps en seconde pendant lequel un clavier gardera la langue Utilisateur en revenant au repos, avant de reprendre la langue par défaut, (0 - 9 999 secondes ; 0 signifie jamais).	10 sec
Feu		
Pré-alarme incendie PRE-ALARME INCENDIE	Nombre de secondes de délai avant l'envoi d'alarme d'incendie pour les zones où l'attribut « Pré-alarme incendie » est activé. (1 - 999 secondes) Voir Éditer une zone [→ 253].	30 s
Confirmation incendie CONFIRMATION FEU	Délai supplémentaire avant l'envoi du fichier d'alarme pour les zones où les attributs Pré-alarme incendie et Confirmation incendie sont activés. (1 – 999 secondes) Voir Éditer une zone [→ 253].	120 s
CODE		
Validité code VALIDITÉ CODE	Période de temps pendant laquelle le code est valide (1 - 330)	30 Jours
Nbre maxi de changement de code NBRE MAXI DE CHANGEMENT DE CODE	Nombre de changement du code dans la période de validité (1 - 50)	5
Avertissmt Code ALERTE CODE	Temps avant expiration du code-avertissement affiché (1 - 14)	5 jours
Réglages généraux		
Durée activation sortie RF SORTIE RADIO	Temps pendant lequel les sorties radio restent actives dans le système. (0 – 999 secondes)	0 s

Temporisation	Libellé	Défaut
Limite temps syn LIMITE TEMPS SYN	Durée limite pendant laquelle aucun événement ne sera signalé. (0 - 999 sec) La synchronisation n'a lieu que si l'heure et la date du système sont hors de cette limite.	0 s
Tempo Déf.IP TEMO DÉF.IP	Timeout pour le défaut du lien Ethernet (0 = désactivé) (0 - 250)	0 sec
Camera Offline CAMERA OFFLINE	Délais avant info caméra Offline (10 - 9999)	10 sec
Délai technique TECHNIQUE DELAI	Délai en secondes pendant lequel une entrée technique doit être en défaut avant qu'une alarme soit déclenchée. (0 - 9999 secondes)	0 s
Fréquent FREQUENT 	Cet attribut s'applique uniquement à la télémaintenance. Le nombre d'heures d'ouverture d'une zone si cette zone est programmée avec l'attribut Usage fréquent . (1 - 9999 heures)	336 heures (2 semaines)
Contrainte silencieuse	Temps pendant lequel la contrainte reste silencieuse et non-restaurable depuis le clavier (0 - 999).	0 minutes
Agression/Panique silencieuse	Nombre de minutes pendant lesquelles une agression/panique reste silencieuse et non-restaurable depuis le clavier (0 - 999).	0 minutes



Les délais par défaut dépendent de la configuration par l'installateur. Les délais par défaut indiqués ne sont pas obligatoirement adaptés à chaque cas ; ils dépendent de l'ingénieur effectuant la configuration.

17.9.4.3 Identification

1. Sélectionnez **Configuration > Système > Identification**.
⇒ La fenêtre suivante est affichée.
2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Hardware	Système	Entrées & Portes	Sorties	Portes	Secteurs	Calendriers	Changer son code	Avancé
Options Système	Tempos Système	Identification	Normes & Standards	Date & Heure	Langue			

Identification Système

Option	Valeur	Libellé
N° de site	<input type="text" value="1"/>	Numéro d'identification unique de la centrale (utilisé par FlexC et SPC PRO / SPC Safe= (1 - 999999)
Nom du site	<input type="text"/>	Description de cette Installation
Date d'installation	Jour Mois Année 9 / Jul / 2014	
Nom de l'Installateur	<input type="text"/>	Nom de l'installateur pour la maintenance
N° téléphone installateur	<input type="text"/>	N° de téléphone de l'installateur pour la maintenance
Afficher Installateur	<input type="checkbox"/>	Cocher si les coordonnées de l'installateur doivent être affichées au clavier
Verrouillage Installateur	<input type="checkbox"/>	Si coché, le code de verrouillage installateur sera requis pour restaurer le paramétrage usine de la centrale
Code verrouillage Installateur	<input type="text" value="1111"/>	Code verrouillage Installateur à 4 chiffres

N° de site	Entrez le numéro d'identification unique du site (1 - 999999).
Nom du site	Entrez le nom du site. Le nom du site doit être attribué avant l'enregistrement des données dans le système. Le site est affiché sur le clavier.
Date d'installation	Sélectionnez la date à laquelle l'installation a été effectuée.
Nom de l'Installateur	Entrez le nom de la personne ayant installé le système (pour les besoins de support technique).
N° téléphone installateur	Entrez le numéro de téléphone de la personne ayant installé le système (pour les besoins de support technique).
Afficher Installateur	Cochez cette case pour obtenir des informations détaillées de l'installation du clavier connecté à la centrale pendant que le clavier est au repos.
Verrouillage Installateur	Cochez cette case si le chargement de la configuration usine par défaut doit être protégé par le code verrouillage Installateur.
Code verrouillage Installateur	Entrez le code de verrouillage à 4 chiffres.

17.9.4.4 Normes & Standards



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/pays dans lequel le système d'alarme est installé.

1. Sélectionnez **Paramètres > Système > Normes**.
⇒ La fenêtre suivante est affichée.
2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Hardware	Système	Entrées & Portes	Sorties	Portes	Secteurs	Calendriers	Changer son code	Avancé
Options Système	Tempos Système	Identification	Normes & Standards	Date & Heure	Langue			

Options de mise en conformité du système

Type d'installation

Simple

Evoluée

Bancaire

Spécificités Pays:

Sélectionner pour conformité au référentiel UK PD6662

Sélectionner pour conformité au référentiel Irish Standard

Sélectionner pour conformité au référentiel Suédois standard SSF 1014:3

Sélectionner pour conformité au référentiel Européen

(*) Sélectionner pour conformité au référentiel Suisse

(*) Sélectionner pour conformité au référentiel INCERT Standard

(*) Choisir pour être conforme aux exigences Espagnoles

(*) Sélectionner pour la conformité au référentiel Allemand VDS

(*) Sélectionner pour la conformité au référentiel Français NF&A2P

Grade

EN50131 Grade 2

EN50131 Grade 3

Pas de restriction

(*) La sélection de ce standard régional permet de remplacer les exigences EN50131 par celles du pays concerné.



Type d'installation	Sélectionnez le type d'installation. Les options disponibles sont les suivantes : Simple, Evolue, Bancaire.
Pays	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 dans le cadre de l'assistant de démarrage. Sélectionnez le pays où le dispositif est installé et les exigences régionales que celui-ci respecte. Les options sont Royaume Uni, Irlande, Suède, Europe, Suisse, Belgique (INCERT), Allemagne (VDS) et Espagne.
Grade	<p>Sélectionnez le niveau de sécurité applicable au site.</p> <ul style="list-style-type: none"> ● Irlande et Europe : <ul style="list-style-type: none"> – EN50131 GRADE 2 – EN50131 Grade 3 – Pas de restriction ● Royaume-Uni : <ul style="list-style-type: none"> – PD6662 (basée sur EN50131 Grade 2) – PD6662 (basée sur EN50131 Grade 3) – Pas de restriction ● Suède : <ul style="list-style-type: none"> – SSF1014:3 Larmclass 1 – SSF1014:3 Larmclass 2 – Pas de restriction ● Belgique : <ul style="list-style-type: none"> – TO-14 (basée sur EN50131 Grade 2) – TO-14 (basée sur EN50131 Grade 3) – Pas de restriction ● Suisse : <ul style="list-style-type: none"> – SES EN-CH Grade 2 – SES EN-CH Grade 3 – Pas de restriction ● Espagne

	<ul style="list-style-type: none"> - EN50131 Grade 2 - EN50131 Grade 3 ● Allemagne <ul style="list-style-type: none"> - VdS Classe A - VdS Classe C - Pas de restriction ● France <ul style="list-style-type: none"> - NF&A2P - 2 Boucl. - NF&A2P - 3 Boucl. - Pas de restriction
--	---

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 pour des infos détaillées concernant les politiques de configuration du système.

17.9.4.5 Date & Heure

Cette fenêtre permet de régler la date et l'heure de la centrale. La centrale possède une horloge temps réel (**Real-Time Clock (RTC)**) alimentée par la batterie pour ne pas perdre l'information de temps et de date en cas de panne secteur.

1. Sélectionnez **Configuration > Système > Horloge**.

⇒ La fenêtre suivante est affichée.

2. Sélectionnez l'**Heure** et la **Date** dans les menus déroulants.
3. Configurez les champs suivants :

Passage automatique Heure d'Été/Hiver	Cochez cette case pour régler l'heure d'été automatiquement.
---------------------------------------	--

Synchronisé avec l'alimentation	Cochez cette case pour synchroniser la RTC avec l'onde sinusoïdale de l'alimentation secteur.
---------------------------------	---



La date et l'heure réglées sont affichées sur le clavier, dans l'interface Web et dans le journal de bord.

17.9.4.6 Langue

- Sélectionnez **Configuration > Système > Langue**.

⇒ La fenêtre de connexion suivante apparaît :

Hardware	Système	Entrées & Portes	Sorties	Portes	Secteurs	Calendriers	Changer son code	Avancé
Options Système	Tempos Système	Identification	Normes & Standards	Date & Heure	Langue			
Option langue								
Option	Valeur	Libellé						
Langue	Anglais ▼	Sélectionner la langue affichée sur les claviers, l'interface Web et le Journal de Bord, l'interface Web sera automatiquement actualisée lors de l'ouverture d'une nouvelle session						
Langue au repos	Utilise Langue Système ▼	Choisir la Langue lorsque les claviers sont au repos						

- Pour l'option **Langue**, sélectionner la langue dans le menu déroulant.
- ⇒ Les textes sur les claviers, dans l'interface Web et dans le journal de bord sont affichés dans la langue sélectionnée.
- Pour l'option **Langue au repos**, choisissez entre « Utilise Langue Système » ou « Dernière langue utilisée ».
- ⇒ La langue au repos détermine la langue utilisée pour l'affichage des claviers quand 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 si 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, quel que soit la langue spécifiée pour le système.

Voir aussi

- 📖 Langue [→ 252]
- 📖 OPTIONS [→ 119]

17.9.5 Configurer les zones, les portes et les secteurs

17.9.5.1 Éditer 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 fenêtre suivante est affichée.



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.

Hardware Système Entrées & Portes Sorties Portes Secteurs Calendriers Changer son code Avancé							
Toutes Zones Zones X-Bus Zones Radio							
Zone	Entrée	Libellé	Type	Secteur	Attributs		
1	Centrale - Entrée 1	Front door	Alarme	1: Area 1	...		
2	Centrale - Entrée 2	Vault	Sismique	2: Vault	...		
3	Centrale - Entrée 3	Window 2	Alarme	1: Area 1	...		
4	Centrale - Entrée 4	PIR 1	Alarme	1: Area 1	...		
5	Centrale - Entrée 5	PIR 2	Inutilisé	1: Area 1	...		
6	Centrale - Entrée 6	Fire Exit	Inutilisé	1: Area 1	...		
7	Centrale - Entrée 7	Fire alarm	Inutilisé	1: Area 1	...		
8	Centrale - Entrée 8	Panic Button	Inutilisé	1: Area 1	...		

Zone	Ce numéro ne peut pas être modifié.
Description	Entrez un texte unique (16 caractères max.) identifiant la zone.
Entrée	L'entrée physique est affichée en guise de référence ne peut pas être modifiée.
Type	Sélectionnez un type de zone dans la liste déroulante (voir ici [→ 367]).
Secteur	Uniquement si l'option Secteurs (multiples) est activée. En utilisant la liste déroulante, sélectionnez le secteur auquel la zone est attribuée.
Calendrier	Au besoin, sélectionnez le calendrier voulu (voir ici [→ 268]). Pro Pour le niveau 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 niveau de sécurité Pas de restriction, un calendrier peut être associé à toutes les zones indépendamment du type.
Attributs	Cochez la case voulue. Uniquement les attributs applicables au type de zone considéré sont proposés (voir Attribut de la zone [→ 370])

17.9.5.2 Ajouter / Éditer un secteur

- ▷ Uniquement si l'option **Secteurs** (multiples) est activée.

1. Sélectionnez **Configuration > Secteurs > Secteurs**.

⇒ La fenêtre suivante est affichée :

Hardware	Système	Entrées & Portes	Sorties	Portes	Secteurs	Calendriers	Changer son code	Avancé
Secteurs								
Groupes Secteur								
Secteur	Libellé			Editer	Effacer			
1	Area 1			...				
2	Vault					
3	Commercial					
4	Reception					
<input type="button" value="Sauver"/> <input type="button" value="Ajouter"/>								

- Appuyez sur **Éditer** pour éditer un secteur existant.
- Appuyez sur **Ajouter** pour ajouter un nouveau secteur. Si l'installation est de type *Simple* ou *Évolué*, un secteur est automatiquement ajouté et la fenêtre d'édition des 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.

Hardware	Système	Entrées & Portes	Sorties	Portes	Secteurs	Calendriers	Changer son code	Avancé
Secteurs								
Groupes Secteur								
Ajouter Secteur								
Libellé	<input type="text" value="Finance"/>		Description de Secteur					
Type Secteur	<input type="text" value="Standard"/>		Sélectionner le type du Secteur.					
<input type="button" value="Ajouter"/> <input type="button" value="Retour"/>								

- Saisissez une description pour le nouveau secteur et sélectionnez le type de secteur dans la liste suivante :
 - Standard - Adapté pour la majeure partie des secteurs.
 - DAB - Fournit les paramètres importants de configuration et par défaut aux DAB.
 - Coffre - Fournit les paramètres importants de configuration et par défaut aux coffres.
 - Avancé - Fournit tous les paramètres de secteur (Standard, DAB et Coffre).
- Cliquez sur le bouton **Ajouter** pour ajouter le secteur.
 - Configurez les paramètres conformément aux sections suivantes :

17.9.5.2.1 Entrée/sortie

Configurez les paramètres 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/sortie dans le secteur considéré (par défaut : 45 secondes).
Temporisation de sortie	Le temps (en secondes) accordé à l'utilisateur pour quitter un secteur

	protégé avant la MES complète. Pendant ce délai, un compte à rebours est affiché sur le clavier et le buzzer émet des bips pour rappeler à l'utilisateur que le système sera armé à la fin du délai. Le temporisateur de sortie s'applique à toutes les zones d'entrée/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 [→ 245].
MHS par radio limitée	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 : <ul style="list-style-type: none"> ● Désactiver ● MES ● Mise hors surveillance ● Mise en / hors surveillance <p>Si l'option Désactiver est sélectionnée (valeur par défaut), le système sera activé et désactivé normalement, sans modification du fonctionnement.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Vous pouvez configurer un minuteur d'activation de l'autorisation. Voir Temporisations [→ 245].</p>

17.9.5.2.2 Options MES/MHS Partielle

La configuration de la gestion de zones particulières en modes MES partielle A et MES partielle B se fait ainsi :

MES Partielle valide	Validez MES Partielle pour les opérations A et B comme demandé.
MES Part. temporisée :	Cochez la case correspondante (MES Partielle A ou B) pour appliquer le temporisateur de sortie au mode MES Partielle A ou B.
Attribut zones accès :	Cochez la case correspondante pour changer les zones d'accès en zones de type entrée/sortie en mode MES Partielle A ou B. Cette fonction est pertinente pour une installation de type Simple (en environnement résidentiel) quand un détecteur infrarouge passif (PIR) se trouve dans le couloir. Si le système est mis en surveillance partielle la nuit

	et si l'utilisateur traverse le couloir pendant ses déplacements nocturnes, le détecteur PIR dans le couloir est activé et l'alarme est déclenchée. En activant l'option Attribut zones accès, le buzzer retentit dès que le détecteur PIR est activé, avertissant ainsi l'utilisateur que l'alarme sera déclenchée s'il n'intervient pas avant la fin de la temporisation d'entrée.
Zones type Entrée/Sortie :	Cochez la case correspondante pour que les zones d'entrée/sortie se comportent comme des zones d'alarme quand le mode MES Partielle A ou B est actif. Cette fonction est pertinente pour une installation de type Simple (en environnement résidentiel) quand le système est mis 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.

17.9.5.2.3 Secteurs liés

Cette section vous permet de lier des secteurs pour la mise en marche et l'arrêt :

MES totale	MES totale de ce secteur lorsque tous les secteurs liés sont en MES totale.
MES de Tous	MES totale de tous les secteurs lorsque ce secteur est en MES totale.
Empêche la MES	Empêche la MES de ce secteur si tous les secteurs liés sont en MES totale.
Empêche la MES 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 lié sont MHS.
MHS de tous	MHS de tous les secteurs lorsque ce secteur est MHS.
Empêche la MHS	Empêche la MHS de ce secteur si l'un des secteurs lié est 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 celui-ci.

17.9.5.2.4 Calendrier

Configuration de la planification sur la base des paramètres suivants :

Calendrier	Sélectionnez un calendrier pour la planification.
Mise hors surveillance	Sélectionnez si le secteur doit être automatiquement MHS selon l'horaire spécifié dans le calendrier correspondant.
MES totale	Sélectionnez cette option pour la MES totale du secteur conformément au calendrier

	choisi. Ce secteur sera également activé lorsque le temps de MHS ou intervalle de retard sera écoulé (voir Mise En/Hors Surveillance [→ 259]). Si la durée de mise hors service dépasse le temps planifié, les paramètres du calendrier seront utilisés pour planifier le secteur.
Verrouillage horaire de la MHS	Sélectionnez cette option pour le verrouillage horaire du secteur selon le calendrier sélectionné. (Secteur de type coffre 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 n'est pas MHS à la fin de la temporisation, il ne peut pas être MHS avant le début de la période suivante de MHS verrouillée. (Secteur de type coffre en mode financier uniquement).

17.9.5.2.5 Transmission



Les paramètres de configuration de la transmission sont applicables aux secteurs standards des installations évoluées et bancaires seulement et ne sont pertinentes que si un calendrier est sélectionné. (voir la section Planification [→ 256]).

Ces paramètres autorise la transmission d'un rapport au centre de contrôle ou à une personne en particulier si la centrale est MES ou MHS hors de la planification horaire.

MES trop tôt	Permet l'envoi d'un rapport si la centrale est mise manuellement en MES Totale avant une activation programmée et avant le nombre de minutes saisi dans le champ de temporisation.
MES trop tard	Un rapport est envoyé si la centrale est mise manuellement en MES Totale après une MES programmée et après le nombre de minutes précisé dans le champ de temporisation.
MHS trop tôt	Un rapport est envoyé si la centrale est mise manuellement en MHS avant une MHS programmée et avant le nombre de minutes précisé dans le champ Temporisation.
MHS trop tard	Un rapport est envoyé si la centrale est mise manuellement en MHS avant une MHS programmée et avant le nombre de minutes précisé dans le champ Temporisation.

La communication est envoyée par SMS ou au CTS par SIA et ID de contact.

Seuls les événements configurés pour une transmission hors plage pour le secteur sont transmis.

La transmission des événements peut également être activée pour un CTS ou SMS, comme décrit dans les sections suivantes.

Activation de la transmission de MES/MHS hors plages 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'évènements pour un CTS.

Communications	FlexC	Transmission	Outils PC
CTS Analogique	EDP	CEI-ABI	
Filtrer			
Alarmes	<input checked="" type="checkbox"/>	Début d'alarme	
Fin d'alarme	<input checked="" type="checkbox"/>	Transmission des fin d'alarme	
Alarmes confirmées	<input checked="" type="checkbox"/>	Alarmes confirmées par d'autres zones	
Annul. d'alarme	<input type="checkbox"/>	Transmission de l'information 'Annulation d'alarme' au CTS	
Défauts	<input checked="" type="checkbox"/>	Début de défauts et d'autosurveillance	
Fin de Défaut	<input checked="" type="checkbox"/>	Fin de défaut et fin d'autosurveillance	
Armement	<input type="checkbox"/>	Mise en et hors surveillance	
Trop Tôt / Tard	<input checked="" type="checkbox"/>	Transmet les infos d'alerte de MES/MHS hors plages	
Inhibition	<input type="checkbox"/>	Inhibition et Isolation	
Evénements Porte	<input type="checkbox"/>	Evénements Contrôle d'Accès et Porte autre que les alarmes	
Autres	<input type="checkbox"/>	Tous autres types d'évènements	
Réseau	<input type="checkbox"/>	Transmet les connexion/deconnexion du réseau IP (grâce aux polling)	
Secteurs	<input checked="" type="checkbox"/> 1: Area 1	<input checked="" type="checkbox"/> 2: Vault	

Le paramètre **Trop tôt/tard** est activé pour la transmission de toute MES/MHS se produisant hors plages.

Activation de la transmission de MES/MHS hors plages pour SMS

Les événements SMS sont configurables sur les écrans de configuration Installateur et Utilisateur.

Pour l'accès installateur, sélectionnez **Utilisateurs -> SMS Utilisateurs > SMS installateur > Éditer** :

Utilisateurs	Profils	SMS Utilisateurs	Mots de passe Web	Accès Installateur
Paramétrage des options SMS				
Paramètres généraux				
ID SMS Utilisateur		9999		
Utilisateur		Engineer		
N° SMS		<input type="text" value="0"/>		N° de téléphone où les messages SMS seront envoyés
Événements SMS				
Alarmes	<input type="checkbox"/>			Début d'alarme
Fin d'alarme	<input type="checkbox"/>			Transmission des fin d'alarme
Alarmes confirmées	<input type="checkbox"/>			Alarmes confirmées par d'autres zones
Défauts	<input type="checkbox"/>			Début de défauts et d'autosurveillance
Fin de Défaut	<input type="checkbox"/>			Fin de défaut et fin d'autosurveillance
Armement	<input type="checkbox"/>			Mise en et hors surveillance
Trop Tôt / Tard	<input type="checkbox"/>			Transmet les infos d'alerte de MES/MHS hors plages
Inhibition	<input type="checkbox"/>			Inhibition et Isolation
Événements Porte	<input type="checkbox"/>			Événements Contrôle d'Accès et Porte autre que les alarmes

Activez Trop tot/Trop tard pour signaler toutes les activations et désactivations qui ne sont pas incluses dans la planification.

17.9.5.2.6 Mise En/Hors surveillance

Les paramètres ci-dessous (à l'exception du paramètre Interverrouillage) sont à prendre en considération seulement dans les cas suivants :

- Un calendrier est sélectionné (voir Planification [→ 256]), ou
- **Durée MHS** est activée (avec une valeur supérieure à zéro), ou
- les deux conditions ci-dessus sont remplies.

Temps de présignalisation	Durée en minutes avant l'affichage d'un message d'avertissement avant MES automatique. (0 - 30) Remarquez que la centrale est mise en service à l'heure planifiée ou à l'heure définie par le Durée du retard. Le premier avertissement est affiché à l'heure paramétrée avant l'heure planifiée. Puis l'avertissement suivant se déclenche une minute avant l'heure de la MES.
Arrêt MES Auto Utilisateur	Permet à l'utilisateur d'annuler une MES automatique en tapant un code sur le clavier.
Retard MES auto Utilisateur	Permet à un utilisateur de retarder une MES automatique en tapant un code sur le clavier.
Boîtier à clé	Permet d'annuler une MES automatique avec transpondeur d'interrupteur à clé.
Durée du retard	Entrez le nombre de minutes de retard pour

	la MES automatique. (1 - 300)
Nbre de retards consécutifs	Entrez le nombre de retards admis pour la MES automatique. (0 - 99 : 0 = illimité)
Retard de MHS	Entrez le nombre de minutes de retard pour la MHS. (0 = pas de retard)
Groupe Interverrouillage	Sélectionnez un groupe d'interverrouillage à attribuer à ce secteur. L'interverrouillage n'admet qu'un secteur à la fois dans le groupe à MHS. Utilisé surtout pour les secteurs DAB.
Durée de la MHS temporaire	Si le secteur est en MHS plus longtemps, il passe automatiquement en MES. (intervalle 0 - 120 min : 0 = désactivé).
Double code	Si cette option est activée, deux codes PIN sont requis pour mettre le secteur en MES ou en MHS depuis le clavier. Les deux codes PIN doivent être en possession d'utilisateurs qui possèdent les droits correspondant à cette action (MES et MHS). Si le second code n'est pas saisi dans les 30 secondes, ou s'il est erroné, le secteur ne passe ni en MES ni en MHS.

En cas de travail hors horaires

Un bon exemple de l'utilisation des paramètres de MES et MHS est fourni par les situations de travail hors des horaires habituels avec un calendrier paramétré pour une MES automatique à une heure donnée, alors que le personnel doit travailler plus tard que d'habitude. Il faut alors retarder la MES paramétrée.

Chaque retard est déterminé par le nombre de minutes saisi dans le champ **Durée du retard** tandis que le paramètre **Nbre de retards consécutifs** détermine le nombre de fois où la MES peut être retardée. Un utilisateur doit disposer du droit **Retard MES auto Utilisateur** pour utiliser cette fonction.

La MES peut être retardée de trois manières :

1. Taper le code sur le clavier.
DELA est une option du menu du clavier standard. Les boutons en haut du clavier confort servent à configurer la fonction de délai.
2. Avec le module à clé.
En tournant la clé dans le sens des aiguilles d'une montre, on retarde la MES du délai fixé si le nombre maximal de délais n'est pas dépassé (**Nbre de retards consécutifs**). En tournant la clé dans le sens inverse des aiguilles d'une montre, la MES est retardée de trois minutes (non-configurable). Cette opération peut être répétée autant de fois qu'on le souhaite.
3. Avec une télécommande ou un WPA ou un bouton pour activer l'action déclenchant un **Retard MES Auto**. (Voir page 172)

MHS temporaire

Pour que le système puisse passer en MHS temporaire durant 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 de la MHS**

Cette case doit être cochée pour que le secteur passe en MHS seulement pendant le temps prévu par le calendrier configuré.

3. **Durée de la MHS temporaire**

Ce paramètre doit présenter une valeur supérieure à zéro pour fixer la limite supérieure de durée de MHS du secteur concerné.

L'écran suivant présente les paramètres configurés avec les valeurs appropriées :

17.9.5.2.7 All Okay

Tout Va Bien Requis	Si sélectionné, l'utilisateur doit confirmer que tout va bien, sinon une alarme discrète sera générée Voir Éditer une Zone [→ 253] pour un complément d'information concernant la configuration d'une entrée de zone Tout Va Bien.
Tempo du TVB	Temps (seconde) requis pour activer l'entrée TVB, sinon une alarme discrète sera générée. (Plage de 1 à 999 secondes)
Type événement TVB	Sélectionnez le type d'événement à déclencher à l'expiration du délai de Tout Va Bien Requis. Les options suivantes sont disponibles : Panique (discrète), Panique et Contrainte.

17.9.5.2.8 Sortie Radio

Durée activation sortie RF	Saisissez une durée (secondes) pendant laquelle la sortie RF restera active. Une valeur de 0 seconde active / désactive la sortie.
----------------------------	---



Les autres options diverses sont décrites dans Entrée/sortie [→ 254] pour SPC Pro.

17.9.5.2.9 Zones d'évacuation incendie

Fire exit route

1 Entry



2 DOOR 2



Doors which will open when fire occurs in this area



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.
-----------------------------	--

17.9.5.2.10 Déclencheurs de MES/MHS du Secteur

La section Déclencheurs ne s'affiche que si les déclencheurs ont été définis au préalable. (Voir section Déclencheurs)

Cliquez sur **Editer** pour ajouter, modifier ou supprimer un déclencheur pour le secteur. L'écran suivant s'affiche :

Configurez le déclencheur pour le secteur en utilisant les paramètres suivants :

Déclencheur	Sélectionnez un déclencheur dans la liste déroulante.
Front	Le déclencheur peut être activé indifféremment par le front positif ou négatif du signal d'activation.
Action	<p>Il s'agit de l'action exécutée quand le déclencheur est activé. Les options sont les suivantes :</p> <ul style="list-style-type: none"> ● Mise hors surveillance ● MES Partielle A ● MES Partielle B ● MES totale ● Retard MES Auto Cette action retarde les paramètres d'alarme lorsque la temporisation de MES automatique est démarrée. Le déclencheur n'ajoute du temps que si la limite de retard n'est pas dépassée et si chaque activation d'un déclencheur ne retarde que pendant le temps défini par la Durée du retard (voir section MES/MHS [→ 259]). ● Rétablir alarme Cette action efface toutes les alarmes de la zone configurée.

Remarque : les déclencheurs ne peuvent pas être configurés depuis un clavier.

Voir aussi

📖 Déclencheurs [→ 272]

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 possède 2 entrées ayant chacune une fonction prédéfinie. Ces deux entrées, le détecteur de position de porte et le bouton d'ouverture de porte, sont configurables.

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 l'entrée de détecteur de position de porte est utilisé uniquement pour les fonctions « accès », sélectionnez l'option NON ATTRIBUE. Si le détecteur de position de porte est affecté à une zone d'intrusion, celle-ci peut être configurée comme une zone normale mais avec quelques restrictions (par exemple, certains types de zone ne sont pas accessibles). Si un secteur ou le système est armé avec le lecteur de carte, l'entrée du détecteur de position de porte doit être affectée à un numéro de zone et au secteur/système devant être activé.
Description (Web et SPC Pro uniquement)	Description de la zone à laquelle le détecteur de position de porte est attribué.
Type de zone (Web et SPC Pro uniquement)	Type de la zone à laquelle le détecteur de position de porte est affecté (certains types de zones ne sont pas disponibles).
Attributs zone (Web et SPC Pro uniquement)	Les attributs de la zone à laquelle le détecteur de position de porte est affecté peuvent être modifiés.
Secteur (Web et SPC Pro uniquement)	Le secteur auquel la zone et le lecteur de carte sont affectés. (Si le lecteur de carte est utilisé pour l'activation et la désactivation, ce secteur sera activé/désactivé).
Position porte (web) Résistance fin de ligne DPS (claviers) Contact Porte DPS (SPC Pro)	La résistance utilisée par le détecteur de position de porte. Choisissez la valeur / combinaison de la résistance utilisée.
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) Contact Porte DPS (SPC Pro)	La résistance utilisée par le bouton d'ouverture de porte. Choisissez la valeur / combinaison de la résistance utilisée.
DRS normalement ouvert	Indique si le bouton d'ouverture de porte est une entrée normalement ouverte ou non.
Pas de DRS (Web et SPC Pro 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 et SPC Pro 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 (indisponible sur SPC Pro).



Chaque numéro de zone libre peut être affecté aux zones, mais l'affectation n'est pas fixe. Si le numéro « 9 » est affecté à une zone, celle-ci et un transpondeur d'entrée avec l'adresse « 1 » sont connectés à l'X-Bus (qui utilise les numéros de zones compris entre 9 et 16). La zone affectée des deux centrales de porte se verra affectée le numéro libre suivant de zone. 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	Le lecteur de sortie réclame un code. La porte doit posséder un lecteur d'entrée et un lecteur de sortie.
Code pour MES/MHS	Un code est requis pour armer et désarmer le secteur lié. L'utilisateur doit présenter le badge avant de taper le code.
MHS à l'extérieur (navigateur) MHS sur Lecteur d'entrée (SPCPro)	Le secteur sera mis à l'arrêt lorsqu'un badge est présenté sur le lecteur d'entrée.
MHS à l'intérieur (navigateur) MHS sur Lecteur de sortie (SPCPro)	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) MES sur Lecteur d'entrée (SPCPro)	Le secteur sera mis en surveillance lorsqu'un badge est présenté deux fois sur le lecteur d'entrée.
MES sur lecteur de sortie MES sur Lecteur de sortie (SPCPro)	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.
Urgence Un	incendie dans un secteur quelconque déverrouille la porte.
Escorte	La fonction Escorte permet à des détenteurs de carte à accès privilégié d'escorter d'autres détenteurs de

Attribut	Description
	carte au travers de portes spéciales. Quand cette fonction est appliquée à une porte, la badge avec les « droits d'escorte » doit être présentée en premier, puis les autres détenteurs de badge ne possédant pas ce privilège peuvent ouvrir cette même porte. Le délai entre la présentation de la carte d'escorte et celle de la carte normale est configuré pour chacune des portes.
Anti-passback*	La fonction anti-passback (protection physique) devrait 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 la présente pas pour en sortir, il viole les règles d'anti-passback. La prochaine fois qu'il tentera de pénétrer dans le même espace, une alarme d'anti-passback réelle est déclenchée, l'empêchant ainsi d'entrer dans le groupe de portes.
Antipassback soft*	Les violations des règles d'anti-passback 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 la présente pas pour en sortir, il viole les règles d'anti-passback. La prochaine fois qu'il tentera de pénétrer dans le même groupe de portes, une alarme d'anti-passback 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 uniquement 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 intégré sur la carte de circuit imprimé du contrôleur de porte retentit pendant une alarme de porte.
Ignorer les portes forcées	L'ouverture forcée d'une porte est ignorée.
Group. Interver. * (navigateur) Fonction d'interverrouillage (SPCPro)	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 portes

Temporisation	Min.	Max.	Description
Accès autorisé	1 s	255 s	Durée pendant laquelle la porte restera ouverte après que l'accès a été autorisé.
Accès refusé	1 s	255 s	Délai d'attente après un événement invalide avant que la centrale soit de nouveau prêt.
Porte ouverte	1 s	255 s	Intervalle de temps au cours duquel la porte doit être refermée pour éviter une alarme PORTE OUVERTE TROP LONGTEMPS.
Porte laissée ouverte	1 min	180 min	Intervalle de temps au cours duquel la porte doit être refermée pour éviter une alarme PORTE RESTEE OUVERTE.
Extension de temps	1 s	255 s	Délai additionnel après avoir accordé l'accès à un badge avec un attribut EXTENSION DE TEMPS.
Escorte	1 s	30 s	Délai entre la présentation d'un badge avec des privilèges d'escorte et l'accès par l'utilisateur ne possédant pas ce privilège.

Calendriers porte

Porte verrouillée	Sélectionnez le calendrier utilisé pour verrouiller la porte pendant la durée configurée. Un badge/code n'est pas accepté pendant cette durée.
Porte verrouillée	Sélectionnez le calendrier utilisé pour déverrouiller la porte. La porte est 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 un période définie avant de se verrouiller à nouveau.
Déclencheur qui verrouille la porte	Si le déclencheur attribué est activé, la porte est verrouillée. Un badge/code n'est pas accepté.
Déclencheur qui déverrouille la porte	Si le déclencheur attribué est activé, la porte est déverrouillée. Un badge/code est requis pour ouvrir la porte.
Déclencheur mettant la porte en état de service normal	Si le déclencheur attribué est activé, la porte est remise en état de service normal. Cette action annule le verrouillage/déverrouillage de la porte. Un badge/code est requis pour ouvrir la porte.

17.9.5.3.1 Interferrouillage de porte

Cette fonction empêche l'ouverture des portes restantes d'un groupe interverrouillé si l'une des portes du groupe est ouverte.

Exemple d'application de cette fonction :

- dans les systèmes d'entrée à deux portes utilisés dans certaines banques et autres édifices. En général, un bouton ou un lecteur de carte servent à entrer, des voyants LED rouge et vert indiquant si la porte peut s'ouvrir ou non.
- dans les secteurs techniques de DAB connectant les portes des DAB. En général, toutes les portes des DAB, outre la porte d'accès au secteur, sont interverrouillées.

Pour créer une porte verrouillée :

1. Créez un groupe de portes. Voir Éditer une porte [→ 262].
2. Affectez l'attribut **Interverr.** aux portes requises du groupe. Voir Éditer une porte [→ 262].
3. Configurez une sortie porte pour le fonctionnement de la porte interverrouillée. Cette sortie s'active pour toutes les portes du groupe interverrouillé à chaque fois qu'une porte du groupe est ouverte, y compris la porte ouverte elle-même. Cette sortie peut être connectée par exemple à un voyant rouge pour indiquer que la porte ne peut pas être ouverte, et à un voyant vert pour la situation inverse.

Pour configurer une sortie pour l'interverrouillage de porte.

1. En mode paramétrage, sélectionnez **Configuration > Hardware > X-Bus > Transpondeurs**.
2. Sur l'écran **Configuration transporteur**, cliquez sur **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.

The screenshot shows a web-based configuration interface for a security system. At the top, there is a navigation bar with tabs: Hardware, Système, Entrées & Portes, Sorties, Portes, Secteurs, Calendriers, Changer son code, and Avancé. Below this, a sub-tab 'Sorties' is active, showing 'X10' as the selected device. The main content area is titled 'Type Sortie' and contains several radio button options: 'Désactivé', 'Système', 'Secteur', 'Zone', and 'Porte'. The 'Porte' option is selected. Under 'Porte', there are two dropdown menus: the first is set to 'Porte 1 DOOR 1' and the second is set to 'Interverrouillé'. Other options like 'Système' have a dropdown set to 'Sirène extérieure', and 'Secteur' has a dropdown set to '1: Area 1' with another 'Sirène extérieure' dropdown below it. 'Zone' has a dropdown set to '1 Front door'.

17.9.5.4 Ajouter un groupe de secteurs

Les groupes de secteurs peuvent être utilisés pour configurer plusieurs secteurs collectivement. Ceci évite de devoir configurer longuement un secteur après l'autre.

▷ Uniquement si l'option (multiples) **Secteurs** est activée.

- Sélectionnez **Paramètre > Secteurs > Groupes Secteur**.

1. Cliquez sur **Ajouter**.
2. Entrez une description pour le groupe.
3. Sélectionnez les secteurs devant faire partie du groupe considéré.
4. Cliquez sur **Ajouter**.



AVIS

Pour pouvoir gérer les secteurs par groupes avec le clavier Confort, activez tous les secteurs dans le champ **Secteurs** sous **Configuration > Hardware > 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, y compris déclencheurs, activations 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 est identifiée par un numéro ordinal. Une année peut avoir 52 ou 53 semaines suivant le décalage du premier lundi de l'année par rapport au 1er janvier (la semaine commence un lundi). Le système de numération du calendrier SPC respecte la norme internationale ISO8601.

Configuration des calendriers

- Sélectionnez **Configuration > Calendriers**.
⇒ La liste des calendriers configurés s'affiche :

Hardware	Système	Entrées & Portes	Sorties	Portes	Secteurs	Calendriers	Changer son code	Avancé	
		Calendrier	Libellé			Editer	Effacer		
		1	Calendrier_1			Editer	Effacer		
		2	Calendrier_2			Editer	Effacer		
		Ajouter Exceptions							

Actions exécutables

Ajouter	Ajouter un nouveau calendrier.
Jours exceptionnels	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, par exemple une zone, un secteur, un profil utilisateur, une sortie, un déclenchement, un composant de porte ou de 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

- Sélectionnez **Configuration > Calendriers > Ajouter**.

⇒ La fenêtre suivante est affichée :

- Saisir un **Libellé** du calendrier (16 caractères max)

Copie d'un calendrier

Pour faire une copie de cette structure de calendrier, cliquez sur le bouton **Retransmet**.

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.

Prog des semaines types

Assigner un type de semaine à chaque semaine du calendrier pour le configurer. Trois Semaines types maxi peuvent être définies 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 »). Le système peut gérer au maximum 64 configurations de calendriers.

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 page [→ 271]) ou de MES/MHS Automatique pour d'autres opérations de centrale (voir page [→ 271]).
⇒ 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 aussi

- 📖 MES/MHS automatiques de secteurs [→ 271]
- 📖 Autres actions des calendriers [→ 271]

17.9.6.1.1 Jours exceptionnels

Les exceptions et les jours d'exception 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 maxi pouvant être fixées 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 > Exceptions > Ajouter**.
⇒ La fenêtre suivante est affichée.
2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Hardware Système Entrées & Portes Sorties Portes Secteurs **Calendriers** Changer son code Avancé

Exceptions Calendrier

Libellé:

Date de début: Jour: 1 / Mois: Jan / Année: 2014
Date de fin: 1 / Jan / 2014

Heures: On / MHS hh:mm Off / MES hh:mm On / MHS hh:mm Off / MES hh:mm On / MHS hh:mm Off / MES hh:mm On / MHS hh:mm Off / MES hh:mm

Calendriers: 2: Calendrier_2

Description	Entrez le nom de l'exception (16 caractères maximum).
Date de début/Date de fin	Entrez la date de début et la date 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 ici [-> 271]) ou de MES/MHS Automatique pour d'autres opérations de centrale (voir ici [-> 271]).
Calendriers	Sélectionnez le(s) calendrier(s) voulus.

!	AVIS
	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

Il est possible de configurer un calendrier pour la MES automatique ou pour la MHS automatique.

Pour chaque jour de la semaine, une configuration peut comprendre au maximum 4 heures de MES et 4 heures de MHS. Les heures sont entrées au format 24 heures (hh:mm). Si l'heure est fixée sur 24, les minutes doivent être à 00 car minuit correspond à 24:00. Il est possible de définir une heure de MES sans la MHS correspondante, et vice-versa. A l'heure configurée, le secteur considéré est soit mis en surveillance, soit mis hors surveillance (si toutes les autres conditions sont réalisées). Les heures entrées ne doivent pas être vues comme une durée, mais plutôt comme un point précis au cours du temps où une action (MES/MHS) va se produire. Quand la centrale est mise hors tension ou redémarrée, l'état MES/MHS reste en mémoire et la MES ou la MHS suivante a lieu conformément à 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 heures sont entrées au format 24 heures (hh:mm). Si l'heure est fixée sur 24, les minutes doivent être à 00 car minuit correspond à 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 Changer son code

Pour changer un code PIN, voir Changement du code Ingénieur et du mot de passe d'accès installateur [→ 210].

17.9.8 Configuration des paramètres avancés

17.9.8.1 Déclencheurs

Un déclencheur est un état du système (par exemple une fermeture de porte / une heure / un événement système (alarme) / etc.) utilisable comme entrée. Les déclencheurs peuvent être associés logiquement les uns aux autres en utilisant les opérateurs logiques et/ou pour créer des sorties utilisateur. Le système prend en charge 1024 déclencheurs au maximum.

1. Sélectionnez **Configuration > Avancé > Déclencheurs**.

⇒ La fenêtre suivante est affichée.

2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Déclencheur	Le système a généré un numéro pour le nouveau déclencheur. Un déclencheur n'est activé que si l'une des deux étapes en option (calendrier/limite de temps) est configuré.
Description	Entrez une description textuelle du déclencheur.
Calendrier	Sélectionnez un calendrier, si nécessaire. Si vous en sélectionnez un, le déclencheur ne sera activé que pendant la période du calendrier. Voir ici [→ 268].
Tempo active/Temporisation	Entrez la durée en secondes pendant laquelle les conditions du déclencheur doivent être vraies avant que le déclencheur soit activé.
Limitation horaire	Sélectionnez une période entre 00:00 et 24:00 pendant laquelle le déclencheur sera seul activé. L'heure de début est incluse, l'heure de fin exclue. 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.
Conditions Déclencheur	Le déclencheur est actif quand les conditions suivantes sont satisfaites (en général, l'opération logique ET est appliquée) :

	<p>Zone – le déclencheur est actif si la zone configurée est dans un des états suivants - ouvert, fermé, court-circuit ou déconnecté.</p> <p>Porte – le déclencheur est actif si n'importe laquelle 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.</p> <p>Système – le déclencheur est actif si la sortie système est dans l'état configuré (on, off). Les sorties système disponibles sont « Sirène extérieure », « Alarme », etc.</p> <p>Zone - le déclencheur est activé si la sortie de zone est activée ou désactivée. Les sorties de secteur disponibles sont « Sirène extérieure », « Alarme », etc.</p> <p>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 télécommandes dans le système.</p> <p>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 de panique des télécommandes déclarées dans le système.</p> <p>WPA – le déclencheur est activé si un bouton ou une combinaison de boutons est enfoncé(e). Il est possible d'assigner une condition déclencheur à toutes les WPA ou à un WPA spécifique. Lorsqu'un déclencheur avec une condition de déclenchement WPA est défini, il peut être affecté à une interaction logique pour des objectifs divers, y compris l'armement d'un système, allumer des lumières ou ouvrir une porte.</p> <p>Code Clavier Valide – 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) entre un code PIN valable ou présente un tag configuré.</p> <p>Boîtier à clé – le déclencheur peut être configuré pour une position spécifique de la clé dans le boîtier.</p> <p>Heure de déclenchement – le déclencheur est activé à l'heure saisie dans la boîte prévue à cet effet au format hh:mm.</p>
--	--



⚠ AVERTISSEMENT

Votre système n'est pas conforme aux normes EN si vous activez un déclencheur pour qu'il active le système sans qu'un code PIN valable soit nécessaire.

17.9.8.2 Interactions logiques

Les déclencheurs sont utilisés avec des interactions logiques. Il s'agit de sorties virtuelles définies par l'utilisateur pouvant être associées à une sortie physique. Le système peut gérer 512 interactions logiques au maximum.



Pour une sortie en continu, quand le déclencheur est un code utilisateur valable, les deux états doivent être identiques, c'est-à-dire les deux négatifs ou les deux positifs.

1. Sélectionnez **Configuration > Avancé > Interactions logiques**.

⇒ La fenêtre suivante est affichée.

Hardware		Système		Entrées & Portes		Sorties		Portes		Secteurs		Calendriers		Changer son code		Avancé	
Déclencheurs		Intéactions logiques		Levée de doute		Licence											
Intéaction	Libellé	Protégé	Touche de raccourci	Delai	Déclencheurs	Effacer											
1	MG1	<input type="checkbox"/>	#1	0 * 100ms	Editer	Effacer											
2	MG2	<input type="checkbox"/>	#2	0 * 100ms	Editer	Effacer											
Sauver		Ajouter															

- 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.
- Cochez la case **Protégé** si vous souhaitez ne pas autoriser les utilisateurs à activer et à désactiver cette interaction, même s'ils possèdent les droits correspondants. Une interaction logique protégée n'est pas affichée sur l'écran des paramètres de **Sorties** des utilisateurs.
- Sélectionnez la touche **Raccourci clavier** voulue.
Un raccourci clavier est une combinaison [signe dièse (#) + chiffre] entrée par le clavier. Quand l'utilisateur entre un raccourci clavier valable, le système lui demande d'activer ou de désactiver la sortie.



Plusieurs sorties, des sorties X-10 et des interactions logiques, peuvent être activées en utilisant un raccourci clavier.

- Entrez une **Temporisation** pour l'interaction. L'unité de temps est le dixième de seconde.
- Cliquez sur le bouton **Déclencheurs** pour configurer les déclencheurs afin qu'ils activent ou désactivent les sorties. Dans les deux cas, un front positif ou négatif du déclencheur doit être défini. Voir Déclencheurs [→ 272] pour la configuration détaillée des déclencheurs.
- Cliquez sur **Ajouter** pour ajouter une nouvelle interaction ou sur **Sauver** pour sauvegarder les nouveaux paramètres pour une interaction existante.

Voir aussi

Déclencheurs [→ 272]

17.9.8.3 Vérification Audio/Vidéo

Pour configurer une vérification audio/vidéo sur le système SPC :

- Installez et configurez le(s) transpondeur(s) audio.
- Installez et configurez la(s) caméra(s) vidéo.
- Installez et configurez l'équipement audio.
- Configurez la(les) zone(s) de vérification.
- Testez la lecture audio dans les zones de vérification.
- Assignez une(des) zone(s) de vérification à des zones physiques.
- Configurez les paramètres de vérification.
- Visualisation d'images des zones de vérification dans un navigateur Web ou sur SPC Pro.

!	AVIS
	Les claviers et le contrôle des accès peuvent être désactivés pendant plusieurs minutes pendant l'envoi d'un fichier audio à la centrale, en fonction de la taille du fichier.

17.9.8.3.1 Configuration de la vidéo

Synthèse

Les caméras sont utilisées pour la vérification vidéo. La centrale SPC prend en charge quatre caméras maximum. Seules les caméras IP sont prises en charge et le navigateur Web doit comporter un port Ethernet.

i	AVIS
	Les caméras ne doivent pas être partagées avec d'autres applications CCTV.

Les caméras sont seulement configurables avec le navigateur Web ou SPC Pro. La configuration depuis le clavier n'est pas supportée. SPC Pro fournit une méthode plus facile de configuration et est recommandé.

La centrale prend en charge deux résolutions de caméra :

- 320x240
Cette configuration est recommandée si vous souhaitez visionner des images sur le navigateur.
- 640x480 (avec quelques restrictions).

Les caméras suivantes sont prises en charge en plus des autres caméras génériques :

- Vanderbilt CCIC1410 (caméra couleur IP 1/4" VGA)
- Vanderbilt CFMC1315 (caméra dôme 1/3" couleur intérieure 1,3 MP)

Une chaîne de commande est disponible par défaut pour accéder directement aux détails de configuration des caméras ci-dessus. Les autres caméras IP génériques nécessitent la saisie manuelle d'une chaîne de commande.

Ajout d'une caméra

1. Sélectionnez **Configuration > Avancé > Vérification > Vidéo**.

⇒ Une liste de caméras préalablement configurées est affichée avec le statut (en ligne ou hors ligne). Une caméra est en ligne si elle a fourni une image dans les 10 secondes écoulées.

Caméra	Libellé	Type	Etats	Editer	Effacer
1	Camera 1	Siemens CCIC1410	Online
2	Camera 2	Siemens CCIC1410	Online

Sauver Ajouter

2. Cliquez sur **Ajouter** pour ajouter une nouvelle caméra ou sur **Modifier** pour modifier une caméra existante.

⇒ L'écran suivant s'affiche.

Hardware		Système		Entrées & Portes		Sorties		Portes		Secteurs		Calendriers		Changer son code		Avancé		
Déclencheurs		Interactions logiques		Levée de doute		Licence												
Zones de Vérification		Audio		Vidéo														
Configuration de la caméra																		
ID Caméra	1																	
Libellé	Camera 1										Libellé de la Caméra							
Type	Siemens CCIC1410																	
IP Caméra	10.100.84.150										Adresse IP de la caméra							
Port Caméra	80										Port TCP/IP de la caméra							
Login	admin										Login pour le Login caméra (ajouté à la chaîne de commande)							
Mot de passe	●●●●●										Mise à jour comm		Mot de passe pour la caméra (ajouté à la chaîne de commande)					
Ligne de commande	/cgi-bin/stilljpeg?username=YWR										Commande à envoyer à la caméra pour obtenir les images							
Images avant l'alarme	8										Nombre d'images à enregistrer AVANT l'alarme (0 - 16).							
Intervalle avant l'alarme	1										Temps entre images avant l'alarme, en secondes (1 - 10).							
Images après l'alarme	8										Nombre d'images à enregistrer APRES l'alarme (0 - 16).							
Intervalle après l'alarme	1										Temps entre images après l'alarme, en secondes (1 - 10).							

3. Configurez la caméra avec les paramètres suivants :

ID Caméra	ID de caméra générée par le système.
Description	Saisissez une description pour identifier cette caméra.
Type	Choisissez l'un des types de caméra suivants : <ul style="list-style-type: none"> ● Générique ● Vanderbilt CCIC1410 ● Vanderbilt CFMC1315
IP Caméra	Entrez l'adresse IP de la caméra.
Port Caméra	Entrez le port TCP balayé par la caméra. Valeur par défaut de 80. Remarque : La caméra CCIC1410 peut seulement être utilisé via le port 80.
Login	Uniquement pour les caméras Vanderbilt CCIC1410 et CFMC1315. 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 commande est activé.
Mot de passe	Uniquement pour les caméras Vanderbilt CCIC1410 et CFMC1315. 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 commande est activé.
Ligne de commande	Entrez la ligne de commande à envoyer au serveur HTTP de la caméra pour obtenir des images. Cette chaîne devrait inclure le nom d'utilisateur et le mot de passe de la caméra. Consultez la documentation de la caméra pour la ligne de commande spécifique requise pour le type de caméra choisi. SPC Pro configure ce paramètre automatiquement s'il est connecté à la caméra Vanderbilt CCIC1410 ou CFMC1315 par un réseau LAN. La ligne de commande par défaut pour les caméras Vanderbilt CCIC1410 ou CFMC1315 sans mot de passe est « /cgi-bin/stilljpeg ».
Images avant l'alarme	Entrez le numéro d'images avant l'alarme à enregistrer (0 - 16). La valeur par défaut est 8.
Intervalle avant l'alarme	Entrez l'intervalle, en secondes, entre les images avant l'alarme (1 - 10). La valeur par défaut est 1 seconde.
Images après l'alarme	Entrez le numéro d'images après l'alarme à enregistrer (0 - 16). La valeur par défaut est 8.
Intervalle après l'alarme	Entrez l'intervalle, en seconde, entre les images après l'alarme (1 - 10). La valeur par défaut est 1 seconde.

17.9.8.3.2 Configuration des zones de vérification

Procédez comme suit pour créer une zone de levée de doute :

1. Rendez-vous dans les zones **Configuration > Avancé > Vérification > Vérification**.

⇒ Une liste des zones de vérification existantes est affichée.

2. Cliquez sur **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 **Sauvegarder**.
7. Assignez cette zone de vérification à une zone physique du système SPC. (Voir Éditer une zone [→ 253]).



L'entrée et la sortie audio pour la zone de vérification peuvent être testées par l'Installateur uniquement dans SPC Pro.

Voir aussi

- Éditer une zone [→ 253]

17.9.8.3.3 Configuration des paramètres de vérification

Remarque : les paramètres suivants sont applicables à toutes les zones de vérification [→ 277].

1. Sélectionnez **Configuration > Avancé > Vérification > Audio**.

⇒ L'écran suivant s'affiche.

2. Configurez les paramètres suivants.

Enregistrement avant alarme	Entrez la durée requise de l'enregistrement avant alarme, en secondes (0 - 120). Valeur par défaut de 10.
-----------------------------	---

Enregistrement après alarme	Entrez la durée requise de l'enregistrement après alarme, en secondes (0 - 120). Valeur par défaut de 30.
-----------------------------	---

17.9.8.3.4 Affichage d'images vidéo

Les images vidéo venant des caméras configurées peuvent être visionnées dans le navigateur dans les modes Paramétrage et Exploitation. Cette fonction est également disponible pour les utilisateurs disposant des droits de visualisation de vidéo dans leur profil. (Voir Paramétrage des droits utilisateur [→ 197]). Les droits d'accès à Internet doivent également être activés pour cette fonction.

Le droit de visionner des images vidéo est paramétrable depuis le clavier sous SPC Pro (Paramètres Vidéo dans le navigateur).

Pour voir des images, rendez-vous sur **SPC Accueil > Vidéo**. Voir Affichage des vidéos [→ 179].

Voir aussi

- 📄 Ajouter/Éditer un utilisateur [→ 197]
- 📄 Configuration de la vidéo [→ 275]

17.9.8.4 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, lors de l'installation de périphériques non autorisés pour SPC et devant être pris en charge par une centrale SPC.

1. Sélectionnez **Configuration > Avancé > Licence**.

The screenshot shows a web interface with a navigation menu at the top: Hardware, Système, Entrées & Portes, Sorties, Portes, Secteurs, Calendriers, Changer son code, and Avancé. Under 'Avancé', there are sub-menus: Déclencheurs, Interactions logiques, Levée de doute, and Licence. The 'Options Licence' screen displays the following information:

- N° Série: 135482801
- Clé de Licence actuelle: WIF4TQKB7F2L7QA
- Nouvelle Clé de Licence:
- A 'Sauver' button is located at the bottom left.

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

17.10.1 Paramètres de communication

17.10.1.1 Configurer les services réseau de la centrale

1. Sélectionnez **Communications > Communications > Services**.
⇒ La fenêtre suivante est affichée.
2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Services réseau

HTTP activé	<input checked="" type="checkbox"/>	Cocher pour activer le serveur web
Port HTTP	<input type="text" value="443"/>	Port d'écoute du Serveur web
TLS activé	<input checked="" type="checkbox"/>	Cocher pour activer le HTTPS pour le Web server
Telnet activé	<input type="checkbox"/>	Cocher pour valider le serveur Telnet
Port Telnet	<input type="text" value="23"/>	Port d'écoute du Serveur Telnet
SNMP activé	<input type="checkbox"/>	Cocher pour activer le protocole SNMP
Communauté SNMP	<input type="text" value="public"/>	Id de Communauté du protocole SNMP
ENMP activé	<input type="checkbox"/>	Cocher pour activer Enhanced Network Management Protocol (ENMP)
Port ENMP	<input type="text" value="1287"/>	Port d'écoute du ENMP
Modif. du mot de passe ENMP	<input type="text" value="siemens"/>	Mot de passe pour les modifications de config. réseau via ENMP
Mise à jour ENMP activé	<input checked="" type="checkbox"/>	Cocher pour autoriser les modifications de config. réseau via ENMP

HTTP activé	Cochez cette case pour activer le serveur Web incorporé de la centrale.
Port HTTP	Entrez le numéro de port balayé par le serveur Web. Par défaut, cette valeur est 443.
TLS validée	Cochez cette case pour activer le cryptage sur le serveur Web incorporé de la centrale. Cette option est activée par défaut. Quand TLS est activé, les pages Web ne peuvent être affichées qu'en utilisant le https:// avant de taper l'adresse IP.
Telnet activé	Cochez cette case pour activer le serveur Telnet. (Activé par défaut) Remarque : L'utilisation de Telnet sans avoir les connaissances nécessaires peut nuire à la configuration. Seuls des utilisateurs ayant des connaissances suffisantes, ou instruits par des personnes ayant ces connaissances devraient utiliser Telnet.
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). (Désactivé par défaut)
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 réseau faites avec le protocole ENMP.

17.10.1.2 Ethernet

IP

Le port Ethernet de la centrale peut être configuré aussi bien avec le navigateur qu'avec le clavier. Une connexion Ethernet avec la centrale SPC peut être établie en utilisant une liaison directe ou une liaison dans le réseau local.

1. Sélectionnez **Communications > Communications > Ethernet**.
⇒ La fenêtre suivante est affichée.
2. Configurez les champs comme indiqué dans le tableau ci-dessous.

IP address	Entrez l'adresse IP de la centrale.
Masque de sous-réseau	Entrez le masque de sous-réseau. Celui-ci définit le type de structure d'adresses dans le réseau local.
Passerelle	Entrez l'adresse IP de la passerelle IP (le cas échéant). Il s'agit de l'adresse par laquelle les paquets IP sont reroutés pour l'accès aux adresses IP externes dans Internet.
Valider DHCP	Cliquez sur ce bouton pour activer l'attribution dynamique de l'adresse sur la centrale.
Server DNS	Entrez l'adresse IP du serveur DNS.

17.10.1.3 Modems

La centrale SPC possède deux connecteurs d'interface pour modem (primaire et sauvegarde). Ceci vous permet d'installer les modems RTC ou GSM dans le système.



Après un retour aux paramètres d'usine, pendant la procédure de paramétrage initial depuis le clavier, la centrale détecte si un modem principal ou de sauvegarde est intégré. Si tel est le cas, elle en affiche le type 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 la section Installation des modules d'extension [→ 94])

1. Sélectionnez **Communications > Communications > Modems**.

2. Cliquez sur **Activer** puis sur **Configurer**.

The screenshot shows a web interface for configuring modems. At the top, there are tabs for 'Communications', 'FlexC', 'Transmission', and 'Outils PC'. Below these are sub-tabs for 'Services', 'Ethernet', 'Modems', and 'Ports série'. The 'Modems' tab is active, showing two modem configurations side-by-side.

Modem 1 Principal		Modem 2 secours	
Etats:	Défaut: défaut ligne	Etats:	Défaut: E51
Type:	IntelliModem PSTN	Type:	IntelliModem GSM
Version Firmware:	2.09 [28MAR14]	Version Firmware:	3.08 [13NOV13]
Version Hardware:	---	Version Hardware:	---
<input type="button" value="Configurer"/> <input type="button" value="Désactiver"/>		<input type="button" value="Configurer"/> <input type="button" value="Désactiver"/>	



La détection et la configuration par SMS ne sont pas disponibles tant que les modems ne sont pas activés et configurés.

17.10.1.3.1 Test SMS

Après avoir activé la fonction SMS pour le modem, vous pouvez la tester en envoyant un message court à un destinataire existant.

1. Entrez le numéro du téléphone mobile (incluant l'indicatif du pays à trois chiffres) et le texte du message dans les champs respectifs.
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. Remarque : 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 / autocommutateur 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).

17.10.1.3.2 Fonction SMS

Quand la centrale SPC est équipée d'un modem, elle est capable de communiquer avec l'extérieur en utilisant les fonctions de messagerie du service SMS. Les opérations suivantes sont nécessaires pour configurer la fonction SMS :

- Modem compatible SMS. Voir ici.
- Authentification SMS. Voir ici.
- Configuration du contrôle par SMS en mode Paramétrage. Voir ici.

- Configuration du contrôle par SMS en mode Exploitation. Voir ici.
- Suivant la configuration, les fonctions incluent les ressources suivantes :
- Notification des événements. Voir ici.
 - Commandes à distance (des commandes à distance choisies peuvent être attribuées à l'utilisateur). Voir ici.

17.10.1.3.3 Options système SMS

Après l'installation d'un modem et l'activation de la fonction SMS, le mode d'authentification des correspondants doit être configuré.

1. Sélectionnez **Paramètres > Système > Système > Options**.
2. Sélectionnez l'option souhaitée dans la liste déroulante **Authentification SMS** :
 - **Code seul**: un code utilisateur valable. Voir ici [→ 113].
 - **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. Cette option doit être active si l'utilisateur doit pouvoir configurer la fonction CONTROLE PAR SMS.
 - **Code PIN et ID appelant**
 - **Code PIN SMS seul** : Code PIN valable configuré pour l'utilisateur, différent du code de connexion de l'utilisateur. Voir ici. Cette option doit être active si l'utilisateur doit pouvoir configurer la fonction CONTROLE PAR SMS.
 - **CODE PIN SMS et ID appelant**

17.10.1.3.4 Commandes SMS

Les fonctions SMS peuvent être activées dès que le contrôle par SMS est configuré. Suivant cette configuration, les commandes envoyées sont authentifiées soit par un code, soit par le numéro de téléphone de l'appelant. Pour les détails sur l'authentification SMS, voir la page [• 136]).

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 les commandes avec un code, le format du texte est le code suivi d'un espace ou d'un point. Exemple : **** représente le code, et « commande » représente la commande : ****.commande ou **** commande.

Par exemple, la commande « HELP » est envoyée sous forme du texte suivant : **** HELP ou ****.HELP.

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 (MES TOTALE) ****.MEST	MEST	Mise en surveillance totale	Date/heure du système mis sous surveillance. Le cas échéant, les zones ouvertes / zones à MES forcée
****MESA (MES		Autorise la mise en service	

PART A) ****.MESA		partielle A par SMS	
**** MESB (MES Part B) ****.MESB			
**** MHS ****.MHS	MHS	Mise hors service	Système arrêté
**** ETAT (ETAT) ****.ETAT	ETAT	État affiché	État du système et des secteurs affectés
**** XA1.ON ****.XA1.ON		Le tag 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	Événements récents
**** ENG.ON ****.ENG.ON	ENG.ON	Activer l'accès Installateur	État de l'accès Installateur
**** ENG.OFF ****.ENG.OFF	ENG.OFF	Désactiver l'accès Installateur	État Installateur
**** MANA.ON ****.MANA.ON		Activer l'accès Constructeur	État de l'accès Constructeur
**** MAN.OFF ****.MAN.OFF		Désactiver l'accès Constructeur	État de l'accès Constructeur
**** S5.ON ****.05.ON		La sortie identifiée comme O5 est activée.	État de S5
**** S5.OFF ****.05.OFF		La sortie identifiée comme O5 est désactivée.	État de S5



Pour la confirmation du SMS, l'identification de la sortie emploie le format ONNN, O étant la sortie, et NNN les caractères numériques (uniquement les chiffres significatifs). Exemple : O5 pour la sortie 5.

Pour la prise en compte du SMS, le tag X-10 emploie le format : XYNN, où X signifie X-10 ; Y est la lettre alphabétique, NN représente les caractères numériques disponibles. Exemple : XA1.

17.10.1.3.5 Modem RTC

1. Sélectionnez **Communications > Communications > Modems > Configurer**.
2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Communications		FlexC	Transmission	Outils PC
Services		Ethernet	Modems	Ports série
Paramètres Modem RTC [Principal]				
Pays	Irlandais ▼			
Appels entrants	<input checked="" type="radio"/> Pas de réponse aux appels entrants <input type="radio"/> Réponse après 1 Sonnerie ▼ <input type="radio"/> Réponse si raccroché après une sonnerie puis ré-appel immédiat <input type="checkbox"/> Réponse uniquement quand l'accès ingénieur est activé			
Préfixe	<input type="text"/> Numéro du préfixe si nécessaire, sinon laisser blanc			
Surveillance ligne	Désactivé ▼			
Surveillance timer	<input type="text" value="0"/> 0 à 9999 secondes			
Délais Défaut Modem	<input type="text" value="60"/> Temps avant l'apparition de l'alerte système 0 à 9999 secondes			
SMS Activation	<input type="checkbox"/>			
Serveur SMS	<input type="text" value="17409900"/>			
SMS automatisé	Désactivé ▼			
N° de SMS automatisé	<input type="text"/>			
Heure du test automatique	---			

Paramètres modem

Pays	Sélectionnez le pays dans lequel le SPC est installé.
Code PIN SIM	Uniquement pour les modems GSM. Entrez le code de la carte SIM installée dans le module GSM.
Autoriser roaming	Sélectionnez pour activer l'itinérance GSM. Remarque : La modification de ce paramètre réinitialise le modem. Remarque : Pris en charge par les modems GSM v3.08 ou supérieurs.
Appels entrants	Le modem peut être programmé pour prendre les appels selon plusieurs modes différents : <ul style="list-style-type: none"> ● Pas de réponse aux appels entrants : le modem ne décroche jamais. ● Réponse après x sonneries : sélectionnez le nombre de sonneries avant que le modem décroche. ● Réponse après que le correspondant ait appelé le modem, ait raccroché après 1 sonnerie seulement, puis ait rappelé immédiatement le modem. Le système SPC peut répondre à l'appel automatiquement après avoir été mis dans ce mode. ● Réponse uniquement quand l'accès ingénieur est activé
Préfixe	Entrez le numéro requis pour l'accès en ligne (par ex. par connexion PBX).
Surveillance ligne	Modem RTC : Activez cette fonction pour surveiller la tension de la ligne reliée au modem. Modem GSM : Activez cette fonction pour surveiller la tension du GSM relié au modem. L'option MES TOTALE n'est efficace 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. (Voir Options Système [→ 236])
Surveillance timer	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 - 9999 secondes). 60 secondes par défaut.
SMS Activation	<p>Cochez cette case pour activer la fonction SMS du système.</p> <p>Remarque : Le service SMS fonctionne sur la base d'un protocole standard utilisé par les téléphones compatibles SMS. Remarque : 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 :</p> <p>Le numéro de téléphone de l'appelant (ID appelant) doit être activé sur la ligne téléphonique.</p> <p>Ligne téléphonique directe - ne fonctionne pas via une centrale téléphonique / auto-commutateur privé ni d'autres équipements de télécommunications.</p> <p>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).</p> <p>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.</p>
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.
Heure du test automatique	Affiche l'heure du dernier test SMS.
Version puce GSM	Affiche le numéro de version de GSM WISMO. Si aucun numéro de version n'est disponible, « --- » s'affiche.
GPRS Point d'Accès (APN)	Uniquement pour les modems GSM. Les coordonnées du Point d'accès sont communiquées par le fournisseur d'accès.
Point Accès GPRS Nom utilisateur	Uniquement pour les modems GSM. Les coordonnées du Point d'accès sont communiquées par le fournisseur d'accès.
GPRS Mot de passe Point d'Accès	Uniquement pour les modems GSM. Les coordonnées du Point d'accès sont communiquées par le fournisseur d'accès.

Cliquez sur **SMS test** pour envoyer un SMS pour tester le système.

Remarque : 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 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 l'opérateur SMS couvrant le secteur dans lequel le SPC est installé doit être programmé. Le système SPC compose ce numéro automatiquement pour se connecter au serveur SMS chaque fois que la fonction SMS est activée. La fonction d'identification de l'appelant (Calling Line Identity) doit être disponible sur la ligne RTC pour pouvoir utiliser cette fonction. Dans chaque pays, les opérateurs SMS ont un numéro de téléphone unique.



Cette fonction n'est pas disponible dans tous les pays. Veuillez contacter votre revendeur local pour les informations détaillées (prise en charge de la fonction, opérateur recommandé).



Consultez les opérateurs de votre pays pour demander les détails sur la disponibilité du service et le numéro du serveur SMS.
Les conditions techniques requises pour le fonctionnement du service avec certains serveurs SMS peuvent varier. Demandez les conditions techniques requises à votre opérateur SMS local.

17.10.1.3.6 Modem GSM

▷ Un modem GSM doit être installé et fonctionner correctement.

1. Sélectionnez **Communications > Communications > Modems > Configurer**.

⇒ La fenêtre suivante est affichée :

Communications		FlexC	Transmission	Outils PC
Services		Ethernet	Modems	Ports série
Paramètres Modem GSM [Sauvegarde]				
Pays	Irlandais ▼			
Code PIN SIM	<input type="text"/>			
Autorise Roaming	<input type="checkbox"/>			
Appels entrants	<input checked="" type="radio"/> Pas de réponse aux appels entrants <input type="radio"/> Réponse aux appels entrant <input type="checkbox"/> Réponse uniquement quand l'accès ingénieur est activé			
Surveillance ligne	Désactivé ▼			
Surveillance timer	<input type="text" value="0"/> 0 à 9999 secondes			
Délais Défaut Modem	<input type="text" value="60"/> Temps avant l'apparition de l'alerte système 0 à 9999 secondes			
SMS Activation	<input type="checkbox"/>			
SMS automatisé	Désactivé ▼			
N° de SMS automatisé	<input type="text"/>			
Heure du test automatique	---			
Version du Chip GSM	---			

2. Configurez les champs suivants :

Paramètres modem

Pays	Sélectionnez le pays dans lequel le SPC est installé.
Code PIN SIM	Uniquement pour les modems GSM. Entrez le code de la carte SIM installée dans le module GSM.

Autoriser roaming	Sélectionnez pour activer l'itinérance GSM. Remarque : La modification de ce paramètre réinitialise le modem. Remarque : Pris en charge par les modems GSM v3.08 ou supérieurs.
Appels entrants	Le modem peut être programmé pour prendre les appels selon plusieurs modes différents : <ul style="list-style-type: none"> ● Pas de réponse aux appels entrants : le modem ne décroche jamais. ● Réponse après x sonneries : sélectionnez le nombre de sonneries avant que le modem décroche. ● Réponse après que le correspondant ait appelé le modem, ait raccroché après 1 sonnerie seulement, puis ait rappelé immédiatement le modem. Le système SPC peut répondre à l'appel automatiquement après avoir été mis dans ce mode. ● Réponse uniquement quand l'accès ingénieur est activé
Préfixe	Entrez le numéro requis pour l'accès en ligne (par ex. par connexion PBX).
Surveillance ligne	Modem RTC : Activez cette fonction pour surveiller la tension de la ligne reliée au modem. Modem GSM : Activez cette fonction pour surveiller la tension du GSM relié au modem. L'option MES TOTALE n'est efficace 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. (Voir Options Système [→ 236])
Surveillance timer	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 - 9999 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. Remarque : 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.
Heure du test automatique	Affiche l'heure du dernier test SMS.
Version puce GSM	Affiche le numéro de version de GSM WISMO. Si aucun numéro de version n'est disponible, « --- » s'affiche.
GPRS Point d'Accès (APN)	Uniquement pour les modems GSM. Les coordonnées du Point d'accès sont communiquées par le fournisseur d'accès.
Point Accès GPRS Nom utilisateur	Uniquement pour les modems GSM. Les coordonnées du Point d'accès sont communiquées par le fournisseur d'accès.

GPRS Mot de passe Point d'Accès	Uniquement pour les modems GSM. Les coordonnées du Point d'accès sont communiquées par le fournisseur d'accès.
---------------------------------	--

Cliquez sur **SMS test** pour envoyer un SMS pour tester le système.

Remarque : 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.

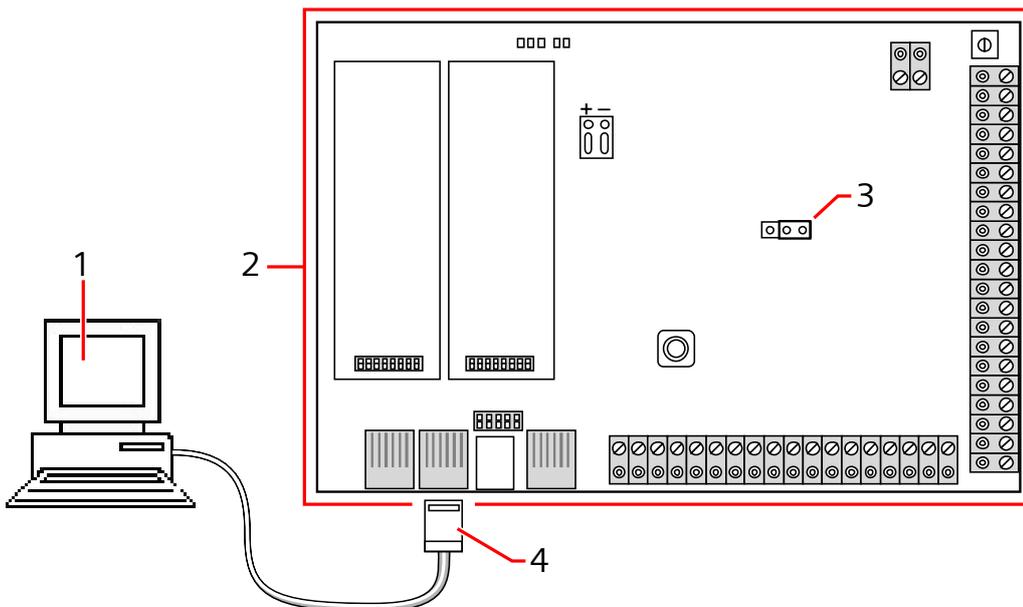


Le test SMS sert uniquement à vérifier que la fonction SMS fonctionne correctement. Utilisez un message court avec des caractères alphabétiques (A-Z) pour tester la fonction.

17.10.1.4 Ports série

La centrale SPC propose 2 ports série (RS232) dotés des fonctions suivantes :

- **X10** : le port série 1 est une interface dédiée prenant en charge le protocole X10. Ce protocole permet l'utilisation du câblage existant dans l'immeuble 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 de la centrale SPC.
- **Journalisation des événements** : l'interface du port série 2 permet de relier la centrale à un port série d'un PC ou d'une imprimante. Avec cette connexion, un programme terminal peut être configuré pour recevoir un JDB des événements du système de la centrale SPC.
- **Informations sur le système** : avec un émulateur de terminal, le port série 2 constitue également une interface permettant d'exécuter des commandes afin d'interroger la centrale pour obtenir des informations spécifiques du 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 sur lequel un émulateur de terminal est exécuté
2	SPC E/S Centrale

3	JP9 4000
4	RS232

Pour configurer les ports série :

- Sélectionnez **Communications > Communications > Ports série**.

Les paramètres sont affichés en fonction du type de connexion utilisé sur les ports. Les paramètres sont décrits dans les sections suivantes :

17.10.1.5 Enregistrement du portail SPC

IP

Le Portail SPC vous permet de vous connecter à distance via Internet au serveur Web incorporé à la centrale SPC, sans avoir besoin de connaître l'adresse IP du SPC sur le WAN. Le serveur de portail SPC est un serveur externe avec une adresse IP fixe, capable de balayer les centrales SPC sur des numéros de port spécifiés. Le numéro de port par défaut balayé par le serveur de Portail est 80, et le port WAN par défaut (l'adresse du port du SPC dans la perspective du réseau externe) est 443.

1. Sélectionnez **Communications > Communications > Portail**.
⇒ La fenêtre suivante est affichée.
2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Validé	Cochez cette case pour activer l'utilisation du Portail.
Port Portail	Entrez le numéro de port balayé par le serveur de portail (valeur par défaut : 80).
Portail URL ou Adresse IP	Entrez l'adresse IP fixe du service de portail SPC (87.192.253.140 - contactez Vanderbilt pour demander confirmation de cette information). L'adresse IP du serveur de portail peut aussi être indiquée sous forme de nom DNS. Remarque : dans ce cas, un serveur DNS doit être configuré dans l'onglet Ethernet .
Adresse IP WAN	Si votre fournisseur d'accès Internet a attribué une adresse IP fixe à votre connexion Internet, entrez-la ici. Si vous n'avez pas d'adresse IP fixe, laissez ce champ vide.
Port WAN	Conservez la valeur par défaut (443) sauf instruction contraire de votre administrateur réseau.
Mise à jour Intervalle	Entrez l'intervalle de temps pour l'enregistrement de vos paramètres de portail.

17.10.2 FlexC®

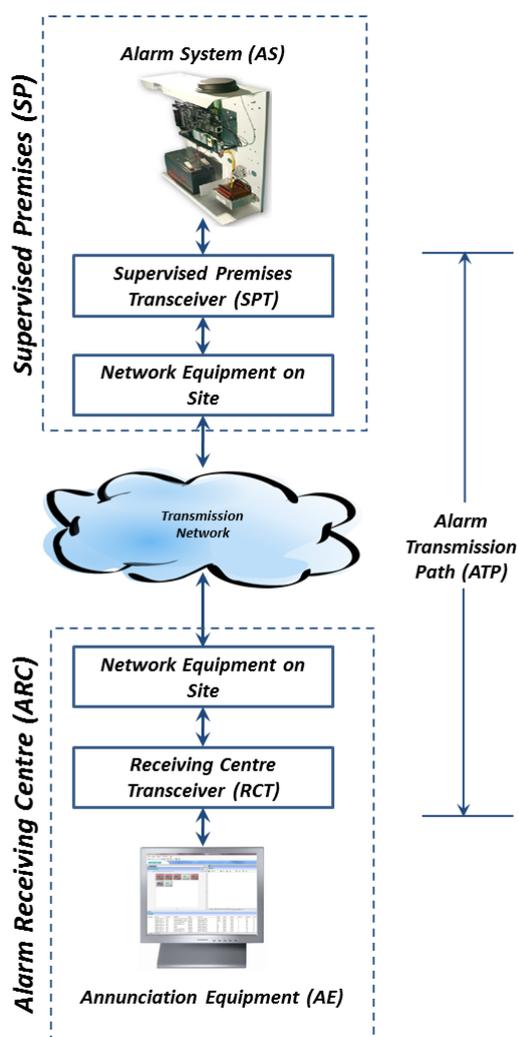
Le Protocole de Communication de Sécurité Flexible de la centrale permet les communications pour un système de transmission d'alarmes à chemin unique ou multiple (ATS) basé sur un protocole Internet (IP) . Un système de transmission d'alarme (ATS) est une voie de communication fiable entre un transmetteur supervisé (SPT, par ex. centrale avec Ethernet intégré) et un frontal de réception (RCT, par ex. SPC Com XT). Un ATS FlexC consiste en un chemin de

transmission d'alarmes principal (ATP) et d'un maximum de neuf chemins de transmission d'alarmes de secours (ATP). Il active les fonctions suivantes :

- le transfert de données bidirectionnel entre le SP, par exemple la centrale SPC par Ethernet et RCT, par exemple, le serveur SPC Com XT.
- 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 aussi

- 📄 Configuration Démarrage Rapide ATP pour système de transmission conforme EN50136 [→ 291]
- 📄 Configuration de profils d'événement [→ 303]
- 📄 Définition de l'exception d'événement. [→ 305]
- 📄 Configuration de profils d'événement [→ 307]
- 📄 FlexC - État [→ 193]
- 📄 Configurer un système de transmission ATS conforme EN50136-1 ou un ATS personnalisé. [→ 293]

17.10.2.1 Mode de fonctionnement

Le système utilise la méthode d'acquiescement après enregistrement lors de la transmission des événements.

La central d'alarme SPC envoie les événements vers le frontal SPC Com XT et demande un acquiescement du frontal avant de déclarer que l'événement est correctement transmis. SPC Com XT acquiesce l'événement seulement après qu'il ait été enregistré dans la base de données SQL et transmis sur l'interface 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 :

- Écran de configuration Démarrage Rapide pour **système de transmission à chemin unique conforme EN50136, système de transmission à chemin double et ATS double chemin-double récepteur**
 - 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), rendez-vous 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, récepteurs principaux et secours

The screenshot displays the 'Configuration du Chemin - Système de Transmission EN50136' interface. It is organized into several sections:

- Identification Centrale:** Includes 'Nom de l'ATS' (Systeme (ATS) 3) and 'Code Client-Identifiant' (0).
- Identifiant du Récepteur RCT:** Includes 'ID Récepteur' (1), 'Adresse IP ou URL Récepteur' (0.0.0.0), and 'Port IP Récep.' (52000).
- Ident. du récepteur de secours:** Includes 'ID Récepteur' (1), 'Adresse IP ou URL Récepteur' (0.0.0.0), and 'Port IP Récep.' (52000).
- Interface du Chemin:** Includes 'Catégorie EN50136 Syst. Transm' (ATS Double Chemin: DP3), 'Interface Principale' (Ethernet), and 'Interface de Secours' (Ethernet).

Buttons for 'Retour' and 'Sauver' are located at the bottom left. A gear icon is visible in the bottom right corner of the interface.

1. Complétez les champs de l'écran **Configuration ATP - ATS conforme EN50136** figurant dans le tableau ci-dessous. Au minimum, il faut compléter le champ **Adresse IP ou URL récepteur** 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 de la de secours. L'opérateur RCT doit entrer cette **ID d'enregistrement de l'ATS**, par exemple, dans SPC Com XT.
2. Cliquez sur **Enregistrer**. L'écran **Configuration système de transmission ATS** affiche l'**ID d'enregistrement de l'ATS** et l'ATP principal configuré ou les ATP principaux et secours dans la **Table de séquence d'événement**.
3. Sur l'écran **Configuration de l'ATS**, cliquez sur **Sauver** pour valider le réglage par défaut, par exemple, le **Profil Evénements par défaut**, le **Profil Commandes par défaut** (y compris le **Nom utilisateur pour commandes FlexC** et le **Mot de passe commande FlexC**) et le **Cryptage automatique** sans mot de passe. Pour modifier les paramètres, voir Configurer un système de transmission ATS conforme EN50136-1 ou un ATS personnalisé. [→ 293].
4. Cliquez sur **Retour**. L'ATS est affiché dans la fenêtre **Syst. de transmission configuré**.

Identification de la centrale	
Nom de l'ATS	Renseignez le nom de l'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 identifiant la centrale sur le récepteur. Entrez 0 si vous n'avez pas de code client-Identifiant. Dans ce cas, vous pouvez charger la centrale avec l' ID d'enregistrement de l'ATS . Pour un système de transmission EN50136, l' ID d'enregistrement de l'ATS est automatiquement créée lorsque vous cliquez sur Sauver . 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 <i>Manuel d'installation et de configuration de SPC</i> .
Adresse IP ou URL Récepteur	Entrez l' Adresse IP ou URL récepteur pour la localisation du serveur RCT (par ex. serveur SPC Com XT).
Port IP Récep.	Entrez le port IP 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 EN50136 (SP1-SP6, DP1-DP4). Pour la description des catégories, voir Tempos des catégories d'ATS [→ 383].

Interface principale	Sélectionnez Interface principale pour appliquer le chemin de communication de l'élément suivant à l'interface principale : <ul style="list-style-type: none"> ● 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 : <ul style="list-style-type: none"> ● 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 TX). Il combine un chemin simple ou multiple entre une centrale SPC et un récepteur. On peut ajouter au système de transmission un maximum de 10 chemins.

!	<p>AVIS</p> <p>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 [→ 291].</p>
----------	---

1. Pour configurer un système de transmission ATS, rendez-vous sur **Communications - FlexC - FlexC ATS**.
2. Sélectionnez l'une des options suivantes :
 - **Ajouter ATS à chemin unique**
 - **Ajouter ATS à double chemin**
 - **Ajout ATS double chemin-double récepteur**
 - **Ajouter un ATS personnalisé.**
1. Pour un ATS conforme EN50136, il faut commencer par régler les paramètres sur l'écran **Configuration ATP - EN50136**. Voir Configuration Démarrage Rapide ATP pour système de transmission conforme EN50136 [→ 291].
2. L'écran **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**.

Communications	FlexC	Transmission	Outils PC
FlexC - Système de Transmission (ATS)	Profils d'Événement	Profil Commande	FlexC - Aide

Configuration de l'ATS [Système (ATS) 4]

Chemin supprimé

Identification

Nom de l'ATS Entrez le nom du Système de Transmission d'Alarme (ATS)

ID d'enregistrement de l'ATS Numéro ID unique sous lequel s'enregistre le système de transmission (ATS) sur le récepteur (RCT).

Table de séquence d'événement

Éditer	Effacer	Remonte	Descent	N° Seq.	Nom	Interface de communication	Catégories du Chemin	Etats	Timeout du polling en mode actif (s)	Timeout Événement (s)
Ajouter Récepteur FlexC		Ajouter Récepteur Analogique								

Profils ATS

Profil d'Événement Choisir le profil d'événement qui définit quels événements et comment ils seront transmis par ce Système de Transmission (ATS)

Profil Commande Choisir le profil de commande qui définira le jeu de commandes autorisées sur ce Système de Transmission (ATS)

Défauts de l'ATS

Timeout Polling ATS Secondes Un Timeout Polling ATS est généré si aucun message de polling n'a été acquité sur aucun chemin de transmission durant cette période (0= calcul automatique du temps)

Timeout événement ATS Secondes Un Timeout événement ATS est généré si un événement n'a été acquité sur aucun chemin de transmission durant ce temps

Génère un Défaut de Transm. Choisir si le système générera un Défaut de Transmission sur un Timeout ATS d'événement ou sur un Timeout ATS de polling

Événements remis en file d'attente Choisir si l'événement est remis en file d'attente ou abandonné après un timeout de transmission ATS

Délais de remise en file d'attente Secondes Temps d'attente avant de remettre en file d'attente de transmission un événement qui avait échoué sur l'ATS par timeout.

Temps maxi de remise en file Secondes Période de temps qu'un événement sera conservé dans la file d'attente avant d'être supprimé.

Détails de l'installation

Détails de l'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. 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.
2. Pour ajouter 1 chemin principal et jusqu'à 9 chemins de secours à l'ATS, cliquez sur **Ajouter un chemin au récepteur FlexC** ou cliquez sur **Ajouter Récepteur FlexC** [→ 295], voir **Ajouter un chemin au CTS analogique**.
3. 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 [→ 303].
4. 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 [→ 307].
5. Complétez les champs **Défauts de l'ATS** comme indiqué dans la fenêtre ci-dessous.
6. Cliquez sur **Éditer Détails Installation** pour terminer les réglages permettant d'identifier une centrale et un opérateur RCT. Voir Éditer Détails Installation [→ 301].
7. Cliquez sur **Sauver** et **Retour** pour revenir à la page **Configuration de l'ATS**. Le nouvel ATS est affiché dans la fenêtre **Syst. de transmission configuré**.
8. 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.

!	AVIS
	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 forcer la centrale à utiliser cette ID d'enregistrement de l'ATS . L'opérateur CMS doit également saisir cette ID d'enregistrement de l'ATS dans le récepteur (par ex. SPC Com XT. Voir le <i>Manuel d'installation et de configuration de SPC Com XT</i>).

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. Par défaut : 300 secondes.
Génère un Défaut de Transm.	Sélectionnez le résultat : le système peut créer un FTC ou un événement timeout de l'ATS.
Événements remis en file 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 après la remise en file d'attente de transmission d'un événement qui avait échoué sur l'ATS par expiration du délai d'attente. Par défaut : 300 secondes.
Temps max. de remise en file	Durée pendant laquelle un événement est conservé dans la file d'attente avant d'être supprimé. Par défaut : 86400 secondes.

Voir aussi

- 📄 [Tempos des catégories d' ATS \[→ 383\]](#)
- 📄 [Ajouter Récepteur Analogique \[→ 300\]](#)

17.10.2.2.1 Ajouter Récepteur FlexC

Ajouter 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**.

Communications FlexC Transmission Outils PC

FlexC - Système de Transmission (ATS) Profils d'Événement Profile Commande FlexC - Aide

Configuration du Chemin - FlexC - Récepteur

Identification Centrale

N° Séquence ATP: 3 N° de séquence du Chemin (ATP) dans la configuration du Système de Transmission (ATS) (1 pour Principal, 2-10 pour les Secours)

Nom du Chemin: Secours ATP 3 Nom du Chemin de transmission (ATP)

Code Client- Identifiant: 0 Numéro unique qui identifie la centrale sur le récepteur (1-99999999, 0= auto assigné)

Identifiant du Récepteur RCT

ID Récepteur: 1 Numéro unique donné au récepteur (No ID du récepteur SPC ComXT de 1-99999999)

Adresse IP ou URL Récepteur: 0.0.0.0 Adresse IP fixe ou URL du récepteur d'alarme (par exemple SPC ComXT)

Port IP Récep.: 52000 Port TCP du récepteur (par exemple le port IP que SPC ComXT utilise pour recevoir les événements)

Interface du Chemin

Interface de communication: Ethernet Interface utilisée par le Chemin de Transmission pour communiquer

Catégories du Chemin: Cat 5 [Ethernet] Choisir la catégorie de Supervision du chemin de transmission (ATP)

Avancé

Paramètres avancés du Chemin ATP: Paramètres avancés du Chemin ATP La programmation avancée ne doit être utilisée que par des personnes expérimentées qui connaissent les impacts de ce qu'ils modifient. Il n'est pas recommandé de changer la programmation Avancée.

Retour Sauver

1. Configurez les champs ATP décrits dans le tableau ci-dessous.
2. 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 [→ 297].
3. Cliquez sur **Enregistrer**.



⚠ 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.

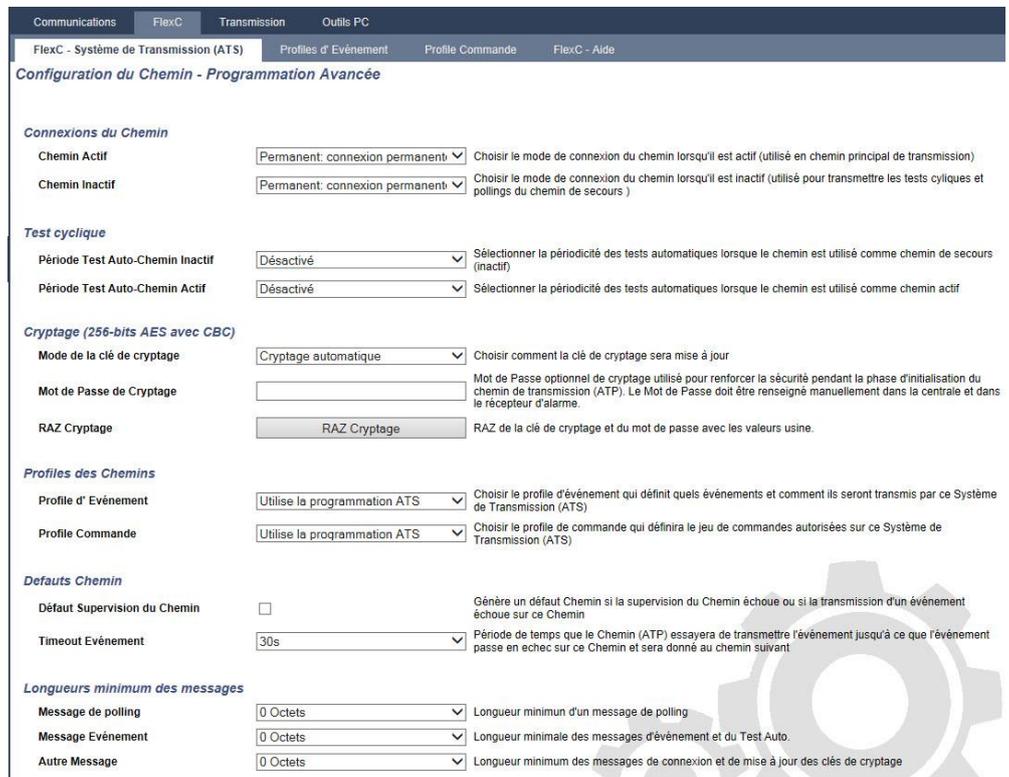
Identification de la centrale	
N° Séquence ATP	Ce champ affiche le numéro de séquence du chemin ATP dans la configuration du système de transmission ATS. 1 pour principal, 2 - 10 pour les secours.
ID Unique Chemin	Quand on sauve un chemin ATP, le système assigne une ID unique au chemin. Le chemin est 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 <i>Manuel d'installation et de configuration de SPC Com XT</i> .
Interface du chemin	
Interface de communication	Dans la liste déroulante, sélectionnez l'interface utilisée par ce chemin pour la communication. <ul style="list-style-type: none"> ● 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 [→ 384].
Avancé	
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.

17.10.2.2.1.1 Configurer les paramètres avancés du Chemin ATP

	<p>⚠ AVERTISSEMENT</p> <p>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.</p>
--	--

1. Cliquez sur Paramètres avancés du Chemin ATP.



The screenshot shows the 'Configuration du Chemin - Programmation Avancée' page. It includes sections for 'Connexions du Chemin', 'Test cyclique', 'Cryptage (256-bits AES avec CBC)', 'Profils des Chemins', 'Defaults Chemin', and 'Longeurs minimum des messages'. Each section contains dropdown menus, text boxes, and checkboxes with descriptive text.

1. Configurez les champs décrits dans le tableau ci-dessous.

2. Cliquez sur **Enregistrer**.

Connexions du Chemin	
Chemin Actif	<p>Choisir le mode de connexion ATP quand le chemin ATP fonctionne comme chemin de communication principal.</p> <ul style="list-style-type: none"> ● Permanent : Connexion permanente ● Temporaire : 1 seconde ● Temporaire : 20 secondes ● Temporaire : 80 secondes ● Temporaire : 3 minutes ● Temporaire : 10 minutes ● Temporaire : 30 minutes
Connexion ATP inactive	<p>Choisir le mode de connexion ATP quand le chemin ATP fonctionne comme chemin de communication de secours.</p> <ul style="list-style-type: none"> ● Permanent : Connexion permanente ● Temporaire : 1 seconde ● Temporaire : 20 secondes ● Temporaire : 80 secondes ● Temporaire : 3 minutes ● Temporaire : 10 minutes ● Temporaire : 30 minutes
Test cyclique	
Mode d'appel de test (chemin inactif)	<p>Sélectionnez la périodicité des tests cycliques lorsque le chemin est utilisé comme chemin inactif.</p> <ul style="list-style-type: none"> ● Désactivé ● 10 minutes ● 1 heure ● 4 heures ● 24 heures ● 48 heures ● 7 jours ● 30 jours
Mode d'appel de test (chemin actif)	<p>Sélectionnez la périodicité des tests lorsque le chemin est utilisé comme chemin actif.</p> <ul style="list-style-type: none"> ● 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	<p>Choisissez le mode de mise à jour du cryptage.</p> <ul style="list-style-type: none"> ● Cryptage automatique ● Cryptage automatique avec mises à jour ● Cryptage Manuel <p>Remarque : le cryptage automatique utilise la clé par défaut et la met à jour une fois. Le cryptage automatique avec mises à jour</p>

	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). <ul style="list-style-type: none"> ● 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). <ul style="list-style-type: none"> ● 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.
Evénement 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. <ul style="list-style-type: none"> ● 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. <ul style="list-style-type: none"> ● 0 octet ● 64 octets ● 128 octets ● 256 octets ● 512 octets
Message Événement	Longueur minimale du message d'événement et de test automatique. <ul style="list-style-type: none"> ● 0 octet ● 64 octets ● 128 octets ● 256 octets ● 512 octets

Autres messages	<p>Longueur minimale du message de connexion, de mise à jour et des clés de cryptage.</p> <ul style="list-style-type: none"> ● 0 octet ● 64 octets ● 128 octets ● 256 octets ● 512 octets
-----------------	--

17.10.2.2.2 Ajouter Récepteur Analogique

Si une connexion entre la centrale et le récepteur d'alarme (par ex. SPC Com XT) n'est plus établie, FlexC peut habiliter une connexion ATP entre la centrale et un récepteur analogique. Il est possible de configurer jusqu'à 10 chemins pour chaque système de transmission.

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.
3. Cliquez sur **Enregistrer**.

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	<p>Sélectionnez le type de modem à utiliser.</p> <ul style="list-style-type: none"> ● Modem 1 ● Modem 2
Test cyclique	
Mode d'appel de test (chemin inactif)	<p>Sélectionnez la périodicité des tests lorsque le chemin est utilisé comme chemin inactif. Par défaut : 24 heures.</p> <ul style="list-style-type: none"> ● Appel test cyclique désactivé ● 10 minutes ● 1 heure ● 24 heures ● 48 heures ● 7 jours ● 30 jours.
Mode d'appel de test (chemin actif)	<p>Sélectionnez le mode d'émission des appels de test lorsque le chemin est utilisé comme chemin actif. Par défaut : 24 heures.</p> <ul style="list-style-type: none"> ● Appel test cyclique désactivé ● 10 minutes ● 1 heure

	<ul style="list-style-type: none"> ● 24 heures ● 48 heures ● 7 jours ● 30 jours.
Heure du premier test	<p>Heure du premier Test après RAZ ou initialisation du système (ATS).</p> <ul style="list-style-type: none"> ● Envoyer immédiatement (par défaut) ● ou ● Choisissez un intervalle d'une demi-heure entre 0:00 et 23:30.
Protocole pour l'événement	
Protocole	<p>Protocole utilisé en communication.</p> <ul style="list-style-type: none"> ● SIA ● SIA étendu 1 ● SIA étendu 2 ● ID du contact
Profil d'événement	<p>Choisir le profil d'événement qui définit quels événements et comment ils seront transmis par ce système de transmission (ATS).</p> <ul style="list-style-type: none"> ● 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	<p>Génère un défaut chemin si la supervision du chemin échoue ou si la transmission d'un événement échoue sur ce chemin.</p>
Événement Timeout	<p>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. Par défaut : 2 minutes.</p> <ul style="list-style-type: none"> ● 30 secondes ● 60 secondes ● 90 secondes ● 2 minutes ● 3 minutes ● 5 minutes ● 10 minutes

17.10.2.2.3 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 Installation**.

Détails de l'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.

ID Syst. de Transmission (ATS) 0 Numéro d'Identification du Système de Transmission ATS (1-999999999)

ID Société 0 IDentifiant de la Société

Nom de Société Nom donné pour la Société

Adresse Installation ATS Entrer l'adresse de l'installation du Système de Transmission d'Alarme (ATS)

Coordonnées GPS Les coordonnées GPS de l'installation

Installateur de l'ATS Le nom de l'Installateur du Système de Transmission (ATS)

Téléphone Installateur 1 Le numéro de téléphone de l'Installateur du Système de Transmission (ATS)

Téléphone Installateur 2 Le numéro de téléphone de l'Installateur du Système de Transmission (ATS)

Notes Toute autre information devant être transmise au récepteur

Retour Sauver

1. Complétez les champs de la fenêtre ci-dessous.
2. Cliquez sur **Enregistrer**.

ID Syst. de Transmission (ATS)	Numéro d'identification du système de transmission ATS (1-999999999).
ID Société	ID de la société (1 - 99999999).
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.

17.10.2.4 Exportation et importation d'un système ATS

Les fichiers ATS se terminent par l'extension .xml. 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, rendez-vous sur **Communications - FlexC - FlexC ATS**.
2. Dans la fenêtre **Syst. de Transmission configurés**, sélectionnez l'ATS à exporter puis cliquez sur **Exporter Système de Transmission (ATS)** (flèche verte).

FlexC - Système de Transmission (ATS) | Profils d'Événement | Profile Commande | FlexC - Aide

Configuration de l'ATS

ATS supprimé

Syst. de Transmission configurés

Editer	Effacer	Exporter Système de Transmission (ATS)	ID	Nom de l'ATS	ID d'enregistrement de l'ATS	Increment ATP	Timeout Polling ATS	Timeout événement ATS	Génère un Défaut de Transm.
			2	ATS Dual Path	59R8-KP2K-P36R-2RP2	2	360	300	Oui
			3	ATS 1	YXGS-97TX-T3XG-8G5X	1	180	300	Oui

Ajouter ATS au Portail
Ajouter un ATS au portail SPC

Ajouter un ATS conforme EN50136
Ajouter un système de transmission à simple chemin conforme EN50136-1:2012
Ajouter un système de transmission (ATS) avec chemin principal et secours conforme EN50136-1:2012
Ajouter un (ATS) double chemin - double récepteur conforme EN50136-1:2012

Ajouter un ATS personnalisé
Ajouter un Système de Transmission. Jusqu'à 10 Chemins (ATP) peuvent être ajoutés par Sys. Trans(ATS)

Importer un Système de Transmission (ATS)
Importer dans la centrale un Système de Transmission déjà pré-défini

3. Enregistrez le fichier sous le nom par défaut **export_flexc.xml** ou renommez-le.
 4. On peut ouvrir le fichier dans le Bloc-Notes.
 5. Pour importer un ATS dans le système, rendez-vous 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 .xml).
 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.

17.10.2.5 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 de plus amples informations, voir Définition de l'exception d'événement. [→ 305].

	<p>AVIS</p> <p>Pour voir une liste des événements, rendez-vous sur Communications - FlexC - Profils d'événements. Cliquez sur Éditer (crayon bleu) pour afficher un profil d'événement. Cliquez sur Afficher la table complète des États situé en bas de l'écran.</p>
--	---



AVIS

Pour créer rapidement un nouveau profil d'événement, rendez-vous sur **Communications - FlexC - Profils d'événement**. Dans le tableau **Profils d'événement**, sélectionnez un profil d'événement et cliquez sur Éditer (crayon bleu). Cliquez sur **Dupliquer** situé en bas de l'écran. Vous pouvez maintenant procéder aux modifications requises.

1. Pour configurer pas à pas des profils d'événement FlexC, rendez-vous sur **Communications - FlexC - Profils d'événement**.
2. Cliquez sur **Ajouter**. La fenêtre **Profils d'événement** s'affiche.

Communications	FlexC	Transmission	Outils PC
FlexC - Système de Transmission (ATS)	Profils d' Evénement	Profile Commande	FlexC - Aide

Profils d' Evénement

Exception Evénement supprimé

Identification

Nom Norm du Profile d' Evénement

Filtrer

Intrusion / Incendie / Médical

Groupes de filtre	Transmet l'événement	Compteur d'exception d'événement	Ajouter Exception Evénement
Alarmes confirmées	<input checked="" type="checkbox"/>	0	- Sélectionner Evénements à ajouter i Ajouter
Alarme Intrusion	<input checked="" type="checkbox"/>	0	- Sélectionner Evénements à ajouter i Ajouter
Fin d'Alarme Intrusion	<input checked="" type="checkbox"/>	0	- Sélectionner Evénements à ajouter i Ajouter
Panique / Agression / Contrainte	<input checked="" type="checkbox"/>	0	- Sélectionner Evénements à ajouter i Ajouter
Début et Fin d'alarme Incendie	<input checked="" type="checkbox"/>	0	- Sélectionner Evénements à ajouter i Ajouter
Alarme et Fin d'alarme Médicale	<input checked="" type="checkbox"/>	0	- Sélectionner Evénements à ajouter i Ajouter
Autosurveillances	<input checked="" type="checkbox"/>	0	- Sélectionner Evénements à ajouter i Ajouter
RAZ des autosurveillance	<input checked="" type="checkbox"/>	0	- Sélectionner Evénements à ajouter i Ajouter
Armement	<input checked="" type="checkbox"/>	0	- Sélectionner Evénements à ajouter i Ajouter

Supervision Système

Groupes de filtre	Transmet l'événement	Compteur d'exception d'événement	Ajouter Exception Evénement
Défauts	<input checked="" type="checkbox"/>	0	- Sélectionner Evénements à ajouter i Ajouter
RAZ Défauts	<input checked="" type="checkbox"/>	0	- Sélectionner Evénements à ajouter i Ajouter
Réseau	<input checked="" type="checkbox"/>	0	- Sélectionner Evénements à ajouter i Ajouter
Test cyclique	<input checked="" type="checkbox"/>	0	- Sélectionner Evénements à ajouter i Ajouter
Connexion de l'Installateur au système	<input checked="" type="checkbox"/>	0	- Sélectionner Evénements à ajouter i Ajouter
Information Système	<input checked="" type="checkbox"/>	0	- Sélectionner Evénements à ajouter i Ajouter
Inhibe et isole	<input checked="" type="checkbox"/>	0	- Sélectionner Evénements à ajouter i Ajouter
Zone en Test de Marche	<input checked="" type="checkbox"/>	0	- Sélectionner Evénements à ajouter i Ajouter
Changement état Zone	<input checked="" type="checkbox"/>	0	- Sélectionner Evénements à ajouter i Ajouter
Caméra	<input checked="" type="checkbox"/>	0	- Sélectionner Evénements à ajouter i Ajouter

Porte et Utilisateur

Groupes de filtre	Transmet l'événement	Compteur d'exception d'événement	Ajouter Exception Evénement
Avertissements Porte	<input checked="" type="checkbox"/>	0	- Sélectionner Evénements à ajouter i Ajouter
Information Porte	<input checked="" type="checkbox"/>	0	- Sélectionner Evénements à ajouter i Ajouter
Information Utilisateur	<input checked="" type="checkbox"/>	0	- Sélectionner Evénements à ajouter i Ajouter

Filtre sur Secteur

1: Area 1

Retour Sauver Dupliquer Afficher la table complète des E

1. Entrez un **Nom** permettant d'identifier l'événement.
2. Choisissez les groupes de filtre d'événement affectés à ce profil en cochant les cases **Transmet l'événement**.
3. 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**.
4. Cliquez sur **Ajouter** pour voir s'afficher l'écran **Définition de l'exception d'événement**. Voir Définition de l'exception d'événement. [→ 305].
5. Pour appliquer un profil d'événement à un secteur, choisissez le secteur dans **Filtre sur Secteur**.
6. Cliquez sur **Sauver** puis sur **Retour**. Le nouveau profil est affiché dans la fenêtre **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** de l'écran **Profils d'événement**.

	AVIS
	On ne peut pas supprimer les Profil Événements par défaut et Profil Événement par défaut pour le Portail , ni aucun profil d'événement assigné 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.

17.10.2.4.1 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
- Adresses 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 à l'ID de zone 101 - 109.

Communications FlexC Transmission Outils PC

FlexC - Système de Transmission (ATS) Profils d'Évènement Profile Commande FlexC - Aide

Définition de l'exception d'évènement

Identification

Nom Nom donné à l'exception d'évènement

ID de l'évènement Numéro d'Identification de l'évènement dans le système

Description Evènement Description de l'évènement

Filtrer

Transmet l'évènement Cocher si l'évènement est normalement transmis

Valider Filtre des Exceptions Cocher pour valider le filtre sur les Exceptions

DISABLED="disabled"

si (≤ Zone ID ≤)

alors

Format Evènement

Code Evènement SIA Code Evènement qui sera transmis pour représenter l'évènement

Code/ Qualifier de l'évènement en CID / Code / Qualifier utilisé en Contact ID pour transmettre l'évènement

Valider Redéfinition Exception Cocher pour valider la redéfinition des exceptions

si (≤ Zone ID ≤)

alors Redéfinit le Code Evènement SIA vers

et Redéfinit le Code Evènement / Qualifier Contact ID vers /

et Redéfinit Adresse Evènement vers -

1. Pour configurer une **Définition de l'exception sur évènement**, renseignez les champs décrits dans la fenêtre ci-dessous.
2. Cliquez sur **Enregistrer**.
3. Cliquez sur **Retour** pour revenir à l'écran **Profils d'évènement**.
 - ⇒ Le nom de chaque exception s'affiche dans la fenêtre **Exception sur évènement**, située en bas de l'écran. La fenêtre présente les paramètres des champs **Transmet l'évènement**, **Filtre des exceptions**, **Code évènement (SIA/CID)** et **Redéfinition de l'exception** pour l'évènement concerné.

Filtre sur Secteur

1: Area 1

Exceptions d'évènement

Editer	Effacer	Nom de l'exception d'évènement	Transmet l'évènement	Filtre des Exceptions	Code Evènement (SIA / CID)	Redéfinit Exception
ID de l'évènement 1000 :Alarme Intrusion [Alarme Zone]						
		Alarme Intrusion	Oui	Ne transmet pas l'évènement [1-9]	BA / 130	[1-9] → YZ/230 [101-109]

1. Cliquez sur l'icône **Éditer** pour effectuer des changements ou sur **Supprimer** pour supprimer une **exception sur évènement**.
2. Pour appliquer le profil d'évènement à un secteur, cochez la case correspondant à ce secteur.
3. Cliquez sur **Sauver** pour sauver le profil d'évènement.
4. Cliquez sur **Retour** pour voir le profil dans la fenêtre **Profils d'évènement**.

Identification	
Nom	Entrez le nom de l'exception sur évènement.
ID de l'évènement	L'ID de l'évènement sur le système. Affiché en

	lecture seule.
Description Événement	Description de l'événement. Affiché en lecture seule.
Filtre d'événements	
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 (Transmet l'événement), 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 ($0 \leq \text{Zone ID} \leq 9999$) 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 <i>Zone ID 1 - 9</i> pour cet événement. Inversement, si vous décidez de ne pas transmettre un événement type BA, vous pouvez décider de transmettre <i>l'identificateur de zone (Zone ID) 1 - 9</i> pour cet événement.
Format d'événement	
Code événement SIA	Le code événement SIA par défaut transmis pour représenter l'événement. Champ en lecture seule.
Code/Qualifier de l'événement en CID.	Code/Qualifier utilisé en contact ID pour représenter l'événement. Champ en lecture seule.
Valider Redéfinition Exception	Cochez pour redéfinir le code/qualifier (qualificatif) SIA et CID par défaut ainsi que l'adresse d'événement par des valeurs personnalisées, par exemple, pour redéfinir <i>Zone ID 1 - 9</i> vers <i>Zone ID 101 - 109</i> . Les champs ci-dessous sont affichés s'ils sont activés.
si ($0 \leq \text{Zone ID} \leq 9999$)	Renseignez l'intervalle d'adresses à redéfinir pour un événement, par exemple, pour redéfinir <i>Zone ID 1 - 9</i> vers <i>Zone ID 101 - 109</i> , saisir un chiffre compris entre <i>1</i> et <i>9</i> . 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/qualifier événement contact ID vers	redéfinit le code/qualifier événement CID par défaut vers un code/qualifier événement CID personnalisé.
et redéfinit adresse événement vers	Renseignez un nouvel intervalle d'adresses, par exemple, si vous souhaitez redéfinir <i>Zone ID 1 - 9</i> vers <i>Zone ID 101 - 109</i> , entrez <i>101 et 109</i> .

17.10.2.6 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.

**AVIS**

Pour créer rapidement un nouveau profil d'événement, allez à **Communications - FlexC - Profils de commande**. Dans la fenêtre **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 maintenant procéder aux modifications requises.

- Pour ajouter un profil de commande pas à pas, rendez-vous à **Communications - FlexC - Profils de commande**.

Editer	Effacer	ID	Nom Profile Commande	Commandes validées	Commandes mises au JDB
		1	Default Command Profile	23	4
		2	Default Portal Command Profile	25	5
		3	All Commands	73	73
		4	Command Profile 4	53	27

Ajouter

- Cliquez sur **Ajouter**.

Profils de commande

Identification

Nom: Nom donné au profil de commande

Authentication Profile Command

Mode Authentification: Mode utilisé pour authentifier les Droits de l'Utilisateur se servant du profil de commande FlexML

Nom Utilisateur pour Commandes: Nom de l'Utilisateur pour le profil des Commandes

Mot de Passe Commande: Mot de passe de l'Utilisateur -Profil des Commandes

Flux temps réel

Mode Audio Temps réel: Sélectionner les paramètres de confidentialité pour les transmissions Audio/vidéo temps réelles vers ce récepteur.

Filtre Commande

Commandes Système	Autorise Commande	JDB Commande
Lit Résumé Centrale	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Mise à la date et heure du système	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Accorde l'accès Installateur	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Accorde l'accès Fabricant	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

1. Entrez un **Nom** permettant d'identifier le profil de commande.
2. 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.

!	<p>AVIS</p> <p>Le Nom Utilisateur pour Commandes par défaut fournit un utilisateur prêt à l'emploi qui active, rapidement et aisément, 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).</p>
----------	---

3. Renseignez le nom d'utilisateur du profil de commande dans le champ **Nom utilisateur pour commandes**. Il doit correspondre au **Nom d'utilisateur d'Authentification** du SPC Com XT.
4. 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.
5. Sélectionnez le **Mode Audio Temps réel** (Désactivé, Seulement après l'alarme, Toujours disponible, Système est en service total) pour déterminer les options de confidentialité de transmission. L'option **Toujours disponible** crée le plus gros volume de données.
6. Sous **Filtre Commande**, sélectionnez les commandes à activer. Pour obtenir la liste complète des commandes disponibles, voir FlexC - Commandes [→ 382].
7. Sélectionnez la commande à journaliser.
8. Cliquez sur **Enregistrer**.
9. Cliquez sur **Retour** pour voir le profil de commande dans le tableau **Profils de commande**.
10. Pour modifier un profil de commande, cliquez sur **Éditer** (crayon), à côté d'un profil.

17.10.3 Transmission

17.10.3.1 Centre de télésurveillance (CTS)

La centrale SPC est capable de communiquer des informations à un correspondant distant quand un événement / une alarme donnée est déclenché sur la centrale.

Ce correspondant peut être un centre de télésurveillance (CTS). Celui-ci doit être configuré au préalable sur la centrale pour que la communication à distance puisse se faire.

17.10.3.1.1 Ajouter / éditer un CTS au moyen d'un SIA ou CID

- ▷ Un modem RTC ou GSM doit être installé et fonctionner correctement.
- 1. Sélectionnez **Communications > Transmission > CTS Analogique**.
 - ⇒ La fenêtre suivante est affichée :

Communications		FlexC	Transmission	Outils PC					
CTS Analogique		EDP	CEI-ABI						
ID	N° d'identification	Libellé	Dernier appel	Statut dernier appel	Test cyclique	Heure du test automatique	JDB	Editer	Effacer
1	1	ARC	Aucun	N/A	Modem 1	---
2	2	ABC	Aucun	N/A	Modem 1	---
3	3	XYZ	Aucun	N/A	Modem 1	---

Rafraîchir Ajouter

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 fenêtre contenant les enregistrements de tous les appels de test déclenchés manuellement ou automatiquement est affichée.
4. Pour ajouter ou éditer un CTS, cliquez sur **Ajouter** – OU – Cliquez sur **Editer**.
⇒ La fenêtre suivante est affichée.
5. Configurez les champs comme indiqué dans le tableau ci-dessous.

Communications		FlexC	Transmission	Outils PC	
CTS Analogique		EDP	CEI-ABI		
Ajouter un Centre de Télésurveillance					
Libellé	<input type="text"/>	Identification du Centre de Télésurveillance			
N° d'identification	<input type="text" value="1"/>	Numéro de Compte			
Protocole	<input type="text" value="SIA"/>	Protocole utilisé en communication			
Prioritaire	<input type="text" value="Principal"/>	Priorité au CTS			
N° de téléphone 1	<input type="text"/>	N° de téléphone 1			
N° de téléphone 2	<input type="text"/>	N° de téléphone 2			
Nbre de tentatives	<input type="text" value="8"/>	Nombre de tentatives de numérotation pour se connecter au récepteur			
Intervalle de numérotation	<input type="text" value="0"/>	Nombre de secondes d'attente après échec de numérotation (0 - 999)			
Test cyclique	<input type="text" value="Désactivé"/>	Intervalle entre les tests automatiques			
	<input type="checkbox"/>	Si coché, l'état de tous les modems sera testé			

Ajouter

Description	Entrez une description du centre de réception distant de l'alarme.
N° Compte	Entrez votre numéro de compte. Le centre de télésurveillance appelé doit disposer de cette information. Elle est utilisée pour vous identifier chaque fois que vous appelez le CTS. Pour un compte ID de contact, un maximum de 6 caractères est admis.
Protocole	Entrez le protocole de communication à utiliser (SIA, SIA étendu, Contact Id (CID), Format rapide (FF)). Remarque : SPCPrend en charge le protocole SIA étendu. Sélectionnez ce protocole pour envoyer des descriptions supplémentaires des événements SIA en clair au CTS.
Prioritaire	Sélectionnez le niveau de priorité du CTS (primaire ou secondaire).
Numéro de téléphone 1	Entrez le premier numéro de téléphone à composer pour joindre le CTS. Ce numéro de téléphone est utilisé en premier pour appeler le CTS, avant d'en utiliser un autre.

Numéro de téléphone 2	Entrez 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 a conduit à un échec.
Tentatives de numérotation	Entrez le nombre de tentatives du système pour essayer de contacter son correspondant (récepteur). (La valeur par défaut est 8).
Délai de numérotation	Nombre de secondes d'attente après échec de numérotation (0 - 999).
Interval num.	Nombre de secondes d'attente entre des échecs de numérotation. (0 - 999)
Test cyclique	Activez le test cyclique en sélectionnant un intervalle de temps. Le modem 1 appelle le CTS primaire automatiquement.
Tester tout	Cochez cette case si vous voulez également effectuer un appel de test automatique du modem 2 au CTS secondaire.

- Cliquez sur le bouton **Ajouter** pour saisir ces informations sur le système.
 - ⇒ La liste des comptes de CTS configurés est affichée, précisant la date et l'état du dernier appel du CTS.

17.10.3.1.2 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 fenêtre suivante est affichée :

Communications		FlexC	Transmission	Outils PC
CTS Analogique		EDP	CEI-ABI	
Filtrer				
Alarmes	<input checked="" type="checkbox"/>	Début d'alarme		
Fin d'alarme	<input checked="" type="checkbox"/>	Transmission des fin d'alarme		
Alarmes confirmées	<input checked="" type="checkbox"/>	Alarmes confirmées par d'autres zones		
Annul. d'alarme	<input type="checkbox"/>	Transmission de l'information 'Annulation d'alarme' au CTS		
Défauts	<input checked="" type="checkbox"/>	Début de défauts et d'autosurveillance		
Fin de Défaut	<input checked="" type="checkbox"/>	Fin de défaut et fin d'autosurveillance		
Armement	<input type="checkbox"/>	Mise en et hors surveillance		
Trop Tôt / Tard	<input type="checkbox"/>	Transmet les infos d'alerte de MES/MHS hors plages		
Inhibition	<input type="checkbox"/>	Inhibition et Isolation		
Evénements Porte	<input type="checkbox"/>	Evénements Contrôle d'Accès et Porte autre que les alarmes		
Autres	<input type="checkbox"/>	Tous autres types d'événements		
Réseau	<input type="checkbox"/>	Transmet les connexion/deconnexion du réseau IP (grâce aux polling)		
Secteurs	<input checked="" type="checkbox"/>	1: Area 1	<input checked="" type="checkbox"/>	2: Vault

2. Configurez les champs suivants :

Vérifiez toutes les cases suivantes si vous souhaitez lancer un appel distant vers un récepteur CTS pour notifier un événement particulier.

Alarmes	Les alarmes sont activées.
Fin d'alarme	Les alarmes système sont restaurées.
Alarmes confirmées	Alarmes confirmées pour de multiples zones
Annulation d'alarme	Événements d'annulation d'alarme. Les alarmes sont annulées après qu'un code utilisateur valide a été saisi à l'aide du clavier à la suite d'une alarme confirmée ou non confirmée.
Défauts	Les défauts et l'autosurveillance sont activés.
Fin de Défaut	Les défauts et l'autosurveillance sont restaurés.
Paramètres	Le système est MES et MHS.
Trop Tôt / Tard	Activation et désactivation non planifiées du système.
Inhibition	Exécution des opérations d'inhibition et d'isolement sur le système.
Événements Porte	Événements Porte activés. Requiert le protocole SIA.
Autres	Tous les autres types d'événements sont détectés sur le système.
Réseau	Transmet les connexions/déconnexions du réseau IP (grâce au polling).
Secteurs	Sélectionnez les secteurs spécifiques concernés par les événements ci-dessus.



En ajoutant un centre de télésurveillance (CTS) distinct pour chaque secteur défini et en programmant chaque secteur de manière que les données soient transmises à son CTS dédié, il est possible de réaliser une approximation d'un système partagé. L'avantage des systèmes partagés est la possibilité de gérer chaque secteur de manière séparée.

17.10.3.1.3 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 :

- Sélectionnez **Communications - Transmission - CTS Analogique - Éditer - Filtrer**.
- 1. Une liste des huit canaux disponibles est affichée avec les conditions d'alarme programmables pour chaque canal. Sélectionnez les conditions d'alarme voulues pour chaque canal. Pour voir une description de chaque condition, voir Types et ports de sortie [→ 214].
- 2. Dans le menu déroulant **Champ**, sélectionnez **Système** ou un secteur particulier auquel appliquer les paramètres choisis.
- 3. Cliquez sur le bouton **Test** situé près du premier canal pour tester l'activation de l'alarme.
 - ⇒ L'icône de l'ampoule est activée.
- 4. 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.
- 5. Continuer à tester les autres canaux.

17.10.3.2 Configuration d'un EDP

IP

Le système est capable de communiquer des informations au serveur SPC Com à distance en utilisant un protocole propre à Vanderbilt : EDP (**E**nhanced **D**atagram **P**rotocol). Après avoir configuré un correspondant EDP (récepteur) dans le système, celui-ci peut être programmé pour déclencher automatiquement des appels de données vers le serveur distant SPC Com chaque fois qu'un événement tel qu'une alarme, une mise en surveillance ou une mise hors surveillance est déclenché. Les appels au serveur distant peuvent emprunter les canaux de communication suivants :

- **RTC** (modem RTC requis)
- **GSM** (modem GSM requis)
- **Internet** (interface Ethernet)

Si vous utilisez le réseau RTC, assurez-vous que le modem RTC est installé et configuré correctement, et que les bornes A, B du modem soient raccordées à une ligne RTC en service.

Si vous utilisez le réseau GSM, assurez-vous que le modem GSM soit installé et configuré correctement. Une connexion IP avec un serveur peut être établie via Internet en utilisant une adresse IP publique fixe.

Si vous voulez utiliser une connexion IP, assurez-vous que l'interface Ethernet soit configurée correctement (voir ici [→ 173]) et que l'accès Internet soit activé sur le routeur.

17.10.3.2.1 Ajouter un récepteur EDP

1. Sélectionnez **Communications > Transmission > EDP**.

⇒ La fenêtre suivante est affichée :

Communications		FlexC	Transmission	Outils PC				
CTS Analogique		EDP	CEI-ABI					
ID	Récepteur	Libellé	Statut réseau	Etat Appel Modem	Dernier appel	Test	Editer	Effacer
1	2	EDP2	Défaut	N/A	Aucun

Rafraîchir Paramètres Ajouter



8 récepteurs max. peuvent être ajoutés au système SPC.

2. Cliquez sur **Ajouter**.
 ⇒ La fenêtre suivante est affichée.
3. Voir le tableau ci-dessous pour de plus amples informations.

Communications		FlexC	Transmission	Outils PC					
CTS Analogique		EDP	CEI-ABI						
ID	Récepteur	Libellé	Statut réseau	Etat Appel Modem	Dernier appel	Test	Editer	Effacer	
1	2	EDP2	Défaut	N/A	Aucun	
Rafraîchir		Paramètres		Ajouter					

Description	Entrez une description du récepteur.
ID récepteur	Entrez un numéro unique utilisé par EDP pour identifier le récepteur.

Voir aussi

Édition des paramètres du récepteur EDP [→ 314]

17.10.3.2.2 Édition des paramètres du récepteur EDP

- Sélectionnez **Communications > Transmission > EDP > Éditer**.
⇒ La fenêtre suivante est affichée.
- Configurez les champs comme indiqué dans le tableau ci-dessous.

Communications		FlexC	Transmission	Outils PC	
CTS Analogique		EDP	CEI-ABI		
Editer un récepteur					
Libellé	<input type="text" value="EDP2"/>	Description du récepteur			
ID Récepteur	<input type="text" value="2"/>	Identification numérique utilisée par l'EDP pour identifier le récepteur (1 - 999997)			
Version de Protocole	<input type="text" value="Version 2"/>	Sélectionner la version du protocole EDP à utiliser avec ce récepteur			
Sécurité					
Commandes activées	<input checked="" type="checkbox"/>	Cocher si les commandes externes sont autorisées depuis ce récepteur			
Changer les codes Utilisateur	<input type="checkbox"/>	Cocher si le changement des codes Utilisateur est autorisé depuis ce récepteur EDP.			
Clavier virtuel	<input type="checkbox"/>	Cocher pour autoriser l'accès d'un clavier virtuel depuis ce récepteur EDP.			
Flux temps réel	<input type="text" value="Seulement après l'alarme"/>	Sélectionner les paramètres de confidentialité pour les transmissions Audio/vidéo temps réels vers ce récepteur.			
Cryptage activé	<input type="checkbox"/>	Cocher si les données entrantes et sortantes du récepteur sont cryptées			
Réseau					
Réseau activé	<input type="checkbox"/>	Cocher si les événements doivent être transmis via réseau Ethernet			

Description	Éditez le nom du récepteur EDP. Le nom choisi peut comporter 16 caractères au maximum.
ID récepteur	Éditez l'ID du récepteur EDP. L'intervalle va de 1 à 999997 (999998 et 999999 sont réservés à des utilisations particulières).
Version de Protocole	Sélectionnez la version du protocole EDP à utiliser avec le récepteur EDP. Les options suivantes sont disponibles : Version 1 ou Version 2. Étant basée sur un protocole plus sûr, la version 2 est recommandée si elle est prise en charge.
Compatibilité VdS 2471	(Norme Vds seulement) Si cette option est sélectionnée, le récepteur EDP mettra en œuvre

	<p>les paramètres suivants pour ce récepteur :</p> <ul style="list-style-type: none"> ● 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 que les commandes soient acceptées par le récepteur.
Changer les codes Utilisateur	Cochez cette case pour permettre le changement des codes PIN à distance. Cette fonction est applicable seulement si les commandes sont activées depuis le récepteur.
Cryptage activé	Cochez cette case pour activer le cryptage des données envoyées ou reçues par le récepteur.
Clef de cryptage	Entrez la clé hexadécimale (max. 32 chiffres) utilisée pour crypter les données. Remarque : la même clé doit être utilisée sur le récepteur.
Clavier virtuel	Active l'accès à la centrale depuis un clavier virtuel, par exemple un module logiciel PC qui ressemble et se comporte comme un clavier SPC. Disponible avec le client Com. SPC.
Flux temps réel/Mode de diffusion	Spécifie lorsque le flux en temps réel audio et vidéo est disponible. Les options sont les suivantes : Jamais, Toujours ou Seulement après l'alarme. Le paramètre par défaut est « Uniquement » après un événement d'alarme. Remarque : ce paramètre a des implications évidentes sur la vie privée et ne devrait être activé seulement à bon escient et dans le respect des lois et réglementations locales.
Réseau (s'applique uniquement à la connexion Ethernet).	
Réseau activé	Cochez cette case pour activer la transmission des événements dans le réseau.
Protocole réseau	Sélectionnez le type de protocole pour le récepteur. Les options suivantes sont disponibles : UDP et TCP. TCP est recommandé s'il est pris en charge par le récepteur.
Adress IP récepteur	Entrez l'adresse IP du récepteur.
Port IP récepteur	Entrez le port IP balayé par le récepteur EDP.
Toujours connecté	Si activé, la centrale est en contact permanent avec le récepteur. Si désactivé, la centrale prend contact avec le récepteur seulement après un événement d'alarme.
Centrale maître	Si activé, la centrale est maître des messages d'interrogation. Seulement applicable 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. Seulement applicable 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 GPRS).	
Trans. par Modem activée	Cochez cette case pour activer la transmission des événements par modem.

Type d'appel	Sélectionnez le type d'appel utilisé quand le canal de numérotation téléphonique est activé. Sélectionnez GPRS.
Protocole GPRS	Sélectionnez le protocole de la couche de transport utilisé par la connexion GPRS. Les options suivantes sont disponibles : UDP et TCP. Applicable seulement si l'appel est du type GPRS.
Adresse GPRS	Entrez l'adresse IP du récepteur EDP pour les connexions GPRS. Applicable seulement si l'appel est du type GPRS.
Port GPRS	Entrez le port balayé par le récepteur EDP pour détecter les connexions GPRS. Les options sont les suivantes : UDP ou TCP. Applicable seulement si l'appel est du type GPRS. La valeur par défaut est 50000.
Tempo de raccroché GPRS	Saisissez la période en secondes après laquelle il sera mis fin à l'appel GPRS. (0 = rester connecté jusqu'à ce que la connexion IP fonctionne)
Autoconnexion GPRS	Cochez cette boîte pour déclencher automatiquement un appel GPRS au serveur si une erreur du réseau IP se produit.
Numérotation sur défaut réseau	Cochez cette case pour signaler des défauts réseau sur un test d'essai 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 coupée.
Adresse réseau*	Entrez l'adresse IP du récepteur. Entrez cette adresse uniquement si la connexion au récepteur EDP est faite via l'interface Ethernet. Laissez ce champ vide si vous utilisez l'un des modems de la centrale.
N° de téléphone*	Entrez le premier numéro de téléphone composé par les modems pour contacter le récepteur.
N° de téléphone 2*	Entrez le deuxième numéro de téléphone composé par les modems pour contacter le récepteur si la connexion ne peut pas être établie avec le premier numéro.
Evénements	
Récepteur principal	Cochez cette case pour indiquer qu'il s'agit du récepteur principal. Si la case est décochée, il s'agit d'un récepteur secondaire.
Evénements gardés en attente	Cochez cette case pour replacer les événements non transmis dans la file d'attente.
Vérification	Cochez cette case si les vérifications d'audio/vidéo doivent être envoyées sur ce récepteur.
Filter	Cliquez sur ce bouton pour filtrer les types d'événements déclenchant un appel EDP. Voir Éditer les paramètres du filtre d'événement [→ 316].



* L'appel EDP via RTC n'est pas pris en charge dans cette version.

Voir aussi

Programmation SMS [→ 204]

17.10.3.2.3 Éditer les paramètres du filtre d'événements

1. Sélectionnez **Communications > Transmission > EDP > Éditer > Filtrer**

⇒ La fenêtre suivante est affichée.

2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Communications	FlexC	Transmission	Outils PC
CTS Analogique	EDP	CEI-ABI	
Filtrer			
Alarmes	<input checked="" type="checkbox"/>	Début d'alarme	
Fin d'alarme	<input checked="" type="checkbox"/>	Transmission des fin d'alarme	
Alarmes confirmées	<input checked="" type="checkbox"/>	Alarmes confirmées par d'autres zones	
Annul. d'alarme	<input type="checkbox"/>	Transmission de l'information 'Annulation d'alarme' au CTS	
Défauts	<input checked="" type="checkbox"/>	Début de défauts et d'autosurveillance	
Fin de Défaut	<input checked="" type="checkbox"/>	Fin de défaut et fin d'autosurveillance	
Etat de zone	<input type="checkbox"/>	Transmet tous les changements d'état des entrées	
Armement	<input type="checkbox"/>	Mise en et hors surveillance	
Trop Tôt / Tard	<input type="checkbox"/>	Transmet les infos d'alerte de MES/MHS hors plages	
Inhibition	<input type="checkbox"/>	Inhibition et Isolation	
Evénements Porte	<input type="checkbox"/>	Evénements Contrôle d'Accès et Porte autre que les alarmes	
Autres	<input type="checkbox"/>	Tous autres types d'événements	
Autre (non standard)	<input type="checkbox"/>	Utiliser des code SIA non standard avec SPC COMXT.	
Réseau	<input type="checkbox"/>	Transmet les connexion/deconnexion du réseau IP (grâce aux polling)	
Secteurs	<input checked="" type="checkbox"/> 1: Area 1	<input checked="" type="checkbox"/> 2: Vault	

Cochez une des boîtes suivantes si vous désirez effectuer un appel distant vers un récepteur EDP pour notifier un événement particulier.

Alarmes	Les alarmes sont activées.
Fin d'alarme	Les alarmes système sont restaurées.
Alarmes confirmées	Alarmes confirmées pour de multiples zones
Annulation d'alarme	Événements d'annulation d'alarme. Les alarmes sont annulées après qu'un code utilisateur valide a été saisi à l'aide du clavier à la suite d'une alarme confirmée ou non confirmée.
Défauts	Les défauts et l'autosurveillance sont activés.
Fin de Défaut	Les défauts et l'autosurveillance sont restaurés.
Etat de zone	Transmettre tous les changements d'état d'entrée de zone.
Paramètres	Le système est MES et MHS.
Trop Tôt / Tard	Activation et désactivation non planifiées du système.
Inhibition	Exécution des opérations d'inhibition et d'isolement sur le système.
Evénements Porte	Evénements Porte activés. Requier le protocole SIA.
Autres	Tous les autres types d'événements sont détectés sur le système.
Autre (non standard)	Les codes SIA non pris en charge sont utilisés avec SPC COM XT, y

	compris les événements de caméra en ligne / hors ligne.
Réseau	Transmet les connexions/déconnexions du réseau IP (grâce au polling).
Secteurs	Sélectionnez les secteurs spécifiques concernés par les événements ci-dessus.

17.10.3.2.4 Éditer les paramètres EDP

1. Sélectionnez **Communications > Transmission > EDP > Paramètres**.
⇒ La fenêtre suivante est affichée.
2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Communications	FlexC	Transmission	Outils PC
CTS Analogique	EDP	CEI-ABI	
Paramètres EDP coté centrale			
Valider	<input type="checkbox"/>	Cocher pour activer EDP	
ID EDP Centrale	<input type="text" value="1000"/>	Identification numérique utilisée par EDP pour l'identification unique de l'installation (1 - 999997)	
Port IP centrale	<input type="text" value="50000"/>	Port pour la réception des paquets IP (50000 par défaut) (1 - 65535)	
Limite packet	<input type="text" value="1440"/>	Nombre maximum d'octets d'un paquet EDP pour la transmission. (500 - 1440)	
Evènement Timeout	<input type="text" value="10"/>	Nombre de secondes entre retransmissions d'évènements non acquittés (1 - 199)	
Compteur d'essais	<input type="text" value="10"/>	Nombre maximum de retransmissions (0 - 199)	
Nbre de tentatives	<input type="text" value="10"/>	Nombre maximum de tentatives de numérotations avant la suspension de la numérotation du Modem (1 - 199)	
Délai de numérotation	<input type="text" value="30"/>	Nombre de secondes d'attente avant re-numérotation en cas d'échec de numérotation (1 - 199)	
Suspension numérotation	<input type="text" value="480"/>	Nbre de secondes de suspension de la numérotation quand le nbre maximum d'échec de numérotations a été atteint (0 = Pas d'arrêt) (0 - 999999)	
Mise au JDB			
Etat des communications	<input type="checkbox"/>	Mise au JDB de tous les changements sur l'état de la communication.	
Commandes EDP	<input type="checkbox"/>	Mise au JDB toutes les commandes exécutée via EDP.	
Evenements A/V	<input type="checkbox"/>	Mise au JDB lorsque les événements de levée de doute Audio/Vidéo sont envoyés au récepteur.	

Valider	Cochez cette case pour activer EDP dans le système.
ID EDP Centrale	Entrez un identifiant numérique utilisé par le récepteur EDP pour identification unique de la centrale.
Port IP de la centrale	Sélectionnez le port IP pour la réception des paquets IP. La valeur par défaut est 50000.
Limite packet	Nombre maximum d'octets d'un paquet EDP pour la transmission.
Evènement Timeout	Entrez le délai d'attente en secondes avant la retransmission d'un événement non acquitté.
Compteur d'essais	Entrez le nombre maximal de tentatives de transmission d'un événement.
Tentatives de numérotation	Entrez le nombre maximal d'échecs de numérotation avant que le système bloque le modem. La durée du blocage est fixée dans l'option Délai de fermeture.
Délai de numérotation	Entrez le délai d'attente en secondes entre un échec de numérotation et la tentative suivante.
Suspension numérotation	Entrez la durée en secondes pendant laquelle le système interdit toute nouvelle tentative de numérotation une fois que le nombre maximal de tentatives est atteint. Si vous ne voulez pas limiter le nombre de tentatives, entrez 0 (zéro).

Mise au JDB

Etat des communications	Mise au JDB de tous les changements sur l'état de la communication.
Commandes EDP	Mise au JDB toutes les commandes exécutées via EDP.
Evenements A/V	Mise au JDB lorsque les événements de levée de doute Audio/Vidéo sont envoyés au récepteur.
Flux A/V	Mise au JDB lorsque débute la levée de doute temps réelle.
Clavier utilise	Mise au JDB lorsque le clavier virtuel est activé.

17.10.4 Outils PC

17.10.4.1 SPC Pro / SPC Safe

1. Sélectionnez **Communications > Outils PC > SPC Pro/SPC Safe**.
2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Valider	Cochez cette case pour autoriser SPC Pro à se connecter à la centrale.
Accès Ingénieur	Cochez cette case si l'accès Installateur est requis pour autoriser SPC Pro à se connecter à la centrale.
Mot de passe	Entrez le mot de passe de la connexion SPC Pro. La centrale vérifie le mot de passe chaque fois que SPC Pro essaie de se connecter. Si le mot de passe entré dans ce champ est identique au mot de passe programmé sur la centrale, la connexion est autorisée (par défaut :).
Autorise IP	Cochez cette case pour autoriser les connexions à la centrale avec le protocole IP.
Port IP	Sélectionnez le port IP utilisé par SPC Pro pour se connecter à la centrale.

SPC Safe

Pour plus d'informations sur la configuration de SPC Safe, veuillez vous reporter au *Manuel d'installation et de configuration du SPCS410*.

1. Cliquez sur le bouton **Valide SPC Safe**.
2. Configurez les champs comme indiqué dans le tableau ci-dessous.

Communications	FlexC®	Transmission	Outils PC
SPC Pro / SPC Safe	SPC Manager	Télemaintenance	
SPC Pro / SPC Safe			
Paramètres généraux			
Valide l'accès	<input checked="" type="checkbox"/>	Cocher pour autoriser SPC Pro/SPC Safe à se connecter à la centrale	
Accès Installateur	<input checked="" type="checkbox"/>	Cocher si l'accès installateur doit être validé sur SPC Pro/SPC Safe pour se connecter.	
Mot de passe	<input type="text" value="password"/>	Mot de passe utilisé par SPC Pro/SPC Safe.	
Réglage connexion entrante			
Autorise IP (*)	<input checked="" type="checkbox"/>	Cocher pour autoriser SPC Pro/SPC Safe à se connecter via IP	
Port TCP/IP (*)	<input type="text" value="50000"/>	Port TCP sur lequel la centrale écoute les connexions entrantes depuis SPC Pro/SPC Safe.	
(*) Note: cela affecte aussi la maintenance à distance.			
<input type="button" value="Sauver"/> <input type="button" value="Valide SPC Safe"/>			

Valider	Cochez cette case pour autoriser Pro à se connecter à la centrale.
Accès Ingénieur	Cochez cette case si l'accès Installateur est requis pour autoriser Pro à se connecter à la centrale.
Mot de passe	Entrez le mot de passe de la connexion Pro. La centrale vérifie le mot de passe chaque fois que Pro essaie de se connecter. Si le mot de passe entré dans ce champ est identique au mot de passe programmé sur la centrale, la connexion est autorisée (par défaut :).
N° de site	Entrez le numéro d'identification de l'installation (ce numéro peut aussi être entré dans la page Identification Système).
Valide l'envoi	Cocher pour autoriser la centrale à contacter le serveur après que sa configuration ai été modifiée.
Intervalle d'envoi	Entrez le délai en minutes entre la dernière modification de la configuration et le moment où la centrale doit contacter le serveur pour transmettre sa configuration (min: 1, max.: 120).
Autorise IP	Cochez cette case pour autoriser les connexions à la centrale avec le protocole IP.
Port TCP/IP	Sélectionnez le port IP utilisé par SPC Safe pour se connecter à la centrale (le port IP de la centrale).
Adresse serveur	Entrez le nom d'hôte, l'URL ou l'adresse IP du serveur SPC Safe (par exemple l'adresse IP de votre PC).
Port TCP/IP serveur	Entrez le port TCP du serveur SPC (par exemple le port IP de votre PC).

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.

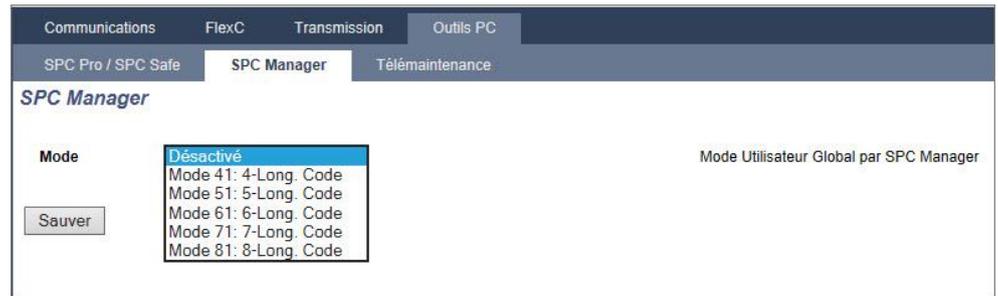
Mode51 : Les codes PIN de 5 caractères activent un total de 10 000 utilisateurs généraux.

Mode61 : les codes PIN de 6 caractères activent 100 000 utilisateurs généraux.
 Mode71 : les codes PIN de 7 caractères activent 1 000 000 d'utilisateurs généraux.
 Mode81 : Les codes PIN de 8 caractères activent 10 000 000 d'utilisateurs généraux.

En mode SPC Manager, des zéros sont ajoutés devant les 4 ou 5 caractères du code utilisateur. Par exemple, en **Mode71 : le code à 7 caractères** 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 **Sauvegarder**.
 - ⇒ 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.

	AVIS
	Les modes SPC Manager ne peuvent pas être changés s'il existe des utilisateurs généraux dans le système.

17.10.4.3 Télémaintenance

Pour de plus amples informations, veuillez vous reporter au manuel de configuration de la télémaintenance.

17.10.4.3.1 Rapport de télémaintenance

Un rapport de télémaintenance peut être obtenu directement par le SPC Pro de la centrale.

- ▷ SPC Pro doit être en ligne sur la centrale.
- ▷ L'option **Télémaintenance** doit être activée.

1. Cliquez sur le menu **Avancé**.
2. Sélectionnez l'option **Obtenir rapport de maintenance de la centrale** dans le menu.

Pour un complément d'information concernant cette option, veuillez consulter le manuel SPC de télémaintenance.

17.11 Opération sur les 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 firmware périphérique et de la langue de la centrale. Consultez la Mise à jour des fichiers [→ 322].
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. Consultez la Utilisation du gestionnaire de fichiers [→ 327].
Gestionnaire Page Web	Sélectionnez la disposition à appliquer aux pages Web dans le navigateur SPC. Choisissez entre Modern Blue et Menus groupés puis cliquez sur Sauver .
Audio	Téléchargez ou testez un fichier audio sur le SPC. Le fichier doit être créé par SPC Audio Pro Manager. Cliquez sur Parcourir puis sur Upload pour ajouter un fichier audio au SPC. Ceci fait, cliquez sur Test pour valider le fichier audio.
Programmeur Rapide	Gestion des fichiers du programmeur rapide. Consultez la Utilisation de la clé de programmation rapide [→ 328].
Défaut	Rétablit la configuration usine par défaut du système SPC. AVIS ! L'adresse IP est conservée pour permettre la connexion à l'interface Web après le chargement de la configuration usine à partir de cette page Web.
Reset	Redémarre la centrale.
Règle 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**.

⇒ L'écran suivant s'affiche :

Mise à jour | Gestionnaire de Fichiers | Gestionnaire Page Web | Audio | Programmeur Rapide | Défaut | Reset

Opérations de mise à jour de la centrale

Version actuelle: 3.6.0 - RC.18388

Mise à jour Firmware Centrale

Mise à jour Fichier: Browse...

Mise à jour du Firmware des Périphériques

Mise à jour Fichier: Browse...

Mise à jour des fichiers langues

Mise à jour Fichier: Browse...

Voir aussi

- 📖 Options [→ 236]
- 📖 Utilisation de la clé de programmation rapide [→ 328]

17.11.1.1 Mise à jour du firmware

	AVIS
	L'accès du fabricant est requis pour effectuer la mise à jour. Il doit être valide à la fois pour la mise à jour du firmware de la centrale et de celui des périphériques. Voir Options Système [→ 236].

Le firmware pour SPC est formé de deux fichiers distincts :

- Fichier firmware de la centrale
Contient uniquement le logiciel pour l'UC de la centrale. Le nom de fichier a l'extension *.fw.
- Le fichier du firmware des périphériques
contient le logiciel 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 jour séparément.

	AVIS
	Il est recommandé que tous les firmware des tags soient mis à jour après la mise à jour d'un nouveau firmware centrale.

Remarque : Le firmware accepte également les mises à jour effectuées par le biais de SPC Pro et du programmeur rapide.

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**.

⇒ L'écran suivant s'affiche :



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 fenêtre de confirmation s'affiche.

3. Cliquez sur **Confirmer** pour confirmer l'installation d'une nouvelle version du firmware de la centrale.

- ⇒ Lorsque le firmware de la centrale est mis à jour, le système affiche un message annonçant sa remise à zéro. Il faut se connecter de nouveau pour poursuivre l'opération.

	<p>⚠ AVERTISSEMENT</p> <p>Si vous revenez à une version antérieure du firmware, le système rétablira tous les paramètres par défaut. De même, si vous revenez à une version antérieure du micrologiciel, il est important de faire de même avec le logiciel du périphérique correspondant. Dans le cas contraire, des zones peuvent apparaître déconnectées, ouvertes ou fermées.</p>
---	--

	<p>⚠ AVERTISSEMENT</p> <p>Si vous mettez à jour à partir d'une version du firmware précédent la version 3.3, veuillez noter les éléments suivants :</p> <ul style="list-style-type: none"> - 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 Profils Utilis. [→ 200]). Veuillez vérifier l'ensemble de la configuration utilisateur après une mise à niveau du firmware. - L'ID Installateur par défaut est modifiée de 513 à 9999.
---	---

Mise à jour des micrologiciels de périphériques

Le firmware des périphériques est mis à jour en suivant la même procédure que pour le firmware de la centrale.

Le fichier de firmware des périphériques n'est enregistré que temporairement parmi les fichiers système. Lorsqu'un nouveau fichier firmware de périphériques est téléchargé, la version actuelle et la nouvelle version du firmware de chaque périphérique et modem sont affichés comme suit :

Mise à jour						
Gestionnaire de Fichiers						
Mise à jour périphérique						
Mise à jour firmware Périphériques X-BUS						
ID	Type	N° Série	Version actuelle	Version actuelle	Version actuelle	Action
1	E/S [8 Entrée / 2 Sortie]	11327907	1.11 [07AUG13]	1.11 [07AUG13]	1.11 [07AUG13]	Identique
2	Audio [4 Entrée]	1434900	1.03 [13MAR13]	1.03 [13MAR13]	1.03 [13MAR13]	Identique
3	Audio [4 Entrée / 1 Sortie]	37070907	1.03 [13MAR13]	1.03 [13MAR13]	1.03 [13MAR13]	Identique
4	Radio	489907	1.11 [07AUG13]	1.11 [07AUG13]	1.11 [07AUG13]	Identique
5	E/S analysées [8 Entrée / 2 Sortie]	165074801	2.00 [09Apr14]	2.00 [09Apr14]	2.00 [09Apr14]	Identique
1	DC-2 [4 Entrée / 2 Sortie]	195309801	2.00 [07APR14]	2.00 [07APR14]	2.00 [07APR14]	Identique
6	E/S [8 Sortie]	443907	1.11 [07AUG13]	1.11 [07AUG13]	1.11 [07AUG13]	Identique
7	Boîtier à clé [1 Sortie]	226593801	1.01 [11NOV10]	1.01 [11NOV10]	1.01 [11NOV10]	Identique
8	Indicateurs [1 Entrée]	223387801	1.03 [13MAR13]	1.03 [13MAR13]	1.03 [13MAR13]	Identique
1	Clavier confort SPCK62x	227361801	1.02 [13MAR13]	1.02 [13MAR13]	1.02 [13MAR13]	Identique
2	Claviers	559907	2.09 [13MAR13]	2.09 [13MAR13]	2.09 [13MAR13]	Identique
Mise à jour Modem						
Slot Modem	Type	Version actuelle	Version actuelle	Version actuelle	Version actuelle	Action
Slot Modem 1	IntelliModem PSTN	2.09 [28MAR14]	2.09 [28MAR14]	2.09 [28MAR14]	2.09 [28MAR14]	Identique
Retour		Mise à jour cor				

- 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 tags.

⇒ Si le firmware d'un périphérique correspondant au fichier .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 celle de la centrale, un message d'avertissement est affiché.

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.

Le firmware des périphériques accepte également les mises à jour effectuées par le biais de SPC Pro et du programmeur rapide [→ 328].

Mise à niveau du firmware du SPCP355.300 ALIM classic

Pour mettre à niveau le SPCP355.300 ALIM classic, vous devez vous assurer des éléments suivants :



Le firmware du SPCP355.300 ALIM classic ne peut être mis à niveau que via le navigateur. Vous ne pouvez pas utiliser SPCPro pour cette tâche.

- L'alimentation secteur doit être connectée.



Cette procédure de mise à niveau peut prendre jusqu'à 2 minutes. N'effectuez aucune action au sein du 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 aussi

- 📄 Ajouter/Modifier un profil utilisateur. [→ 200]

17.11.1.2 Mise à jour des langues

Vous pouvez télécharger un fichier de langue personnalisé (*.clng) sur la centrale. Ce fichier ne concerne que le firmware de la centrale et n'est pas disponible pour SPC Pro ni SPC Safe.

!	AVIS
	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 :

- 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.

Langue	ID	Taille (octets)	Lignes texte manquantes	Version actuelle	Version actuelle	Mise à jour
Anglais	0	N/A	0	3.6.0	3.6.0	<input checked="" type="checkbox"/>
Danois	9	41338	-	---	3.6.0	<input type="checkbox"/>
Hollandais	13	40637	-	---	3.6.0	<input type="checkbox"/>
Finlandais	4	43580	-	---	3.6.0	<input type="checkbox"/>
Flandmand	17	40637	-	---	3.6.0	<input type="checkbox"/>
Français	2	44567	6	3.6.0	3.6.0	<input checked="" type="checkbox"/>
Allemand	15	44533	6	3.6.0	3.6.0	<input checked="" type="checkbox"/>
Italien	3	42863	6	3.6.0	3.6.0	<input checked="" type="checkbox"/>
Norvégien	8	39819	-	---	3.6.0	<input type="checkbox"/>
Polonais	11	44085	-	---	3.6.0	<input type="checkbox"/>
Espagnol	1	36553	6	3.6.0	3.6.0	<input checked="" type="checkbox"/>
Suédois	7	40418	-	---	3.6.0	<input type="checkbox"/>

- Cochez la case en regard de la langue à installer.



4 langues au maximum peuvent être installées.

- Cliquez le bouton **Mise à jour éléments sélectionnés**.

⇒ La fenêtre **Confirmer MàJ Langue** montre les langues en cours d'installation.

- 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 :

- 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.

- Décochez les cases des langues à supprimer.
- Cliquez le bouton **Mise à jour éléments sélectionnés**.

⇒ La fenêtre **Confirmer MàJ Langue** s'affiche. Pour supprimer une langue, la centrale désinstalle d'abord toutes les langues puis réinstalle les langues choisies. Dans l'exemple ci-dessous, le flamand est en cours de suppression.

Mise à jour | Gestionnaire de Fichiers | Gestionnaire Page Web | Audio | Programmeur Rapide | Défaut | Reset

Confirmer MàJ Langue

Le fichier langue va être effacé:

ID	Langue	Version actuelle
1	Espagnol	3.6.0
2	Français	3.6.0
3	Italien	3.6.0
15	Allemand	3.6.0

Le fichier langue a été installé:

ID	Langue	Version actuelle
2	Français	3.6.0
15	Allemand	3.6.0
3	Italien	3.6.0
1	Espagnol	3.6.0

Taille (octets) 189148
Espace libre après MàJ (octets) 326682

4. Cliquez sur le bouton **Confirmer** pour confirmer la langue à supprimer.

Les fichiers langue peuvent également être importés par le biais du programmeur rapide [→ 328].

Voir Langues [→ 252] pour un complément d'information concernant la sélection des langues « Système » et « Langue au repos » dans le navigateur.

Voir OPTIONS [→ 119] pour un complément d'information concernant la sélection des langues « Système » et « Langue au repos » avec le clavier.

Voir aussi

Langue [→ 252]

17.11.2 Utilisation du gestionnaire de fichiers

- Sélectionnez **Fichier -> Gestionnaire de Fichiers**.

⇒ Un écran affiche les détails de la configuration du système, de la langue et des fichiers de suivi.

Mise à jour | Gestionnaire de Fichiers | Gestionnaire Page Web | Audio | Programmeur Rapide | Défaut | Reset

Fichiers système

Libellé	Taille (octets)	Date	Effacer
Fichier de configuration du système	7564	23/07/14 10:51:54	-
Fichier de sauvegarde de la config. système	671	07/06/12 12:37:01	...
Fichier des langues	187471	23/07/14 09:24:45	...
Total utilisé	195706		
Espace libre	328371		

Fichier de configuration du système

Download: Charge le fichier dans le PC où il pourra être enregistré comme sauvegarde.

Upload: Charge un fichier du PC vers la centrale

Sauvegarde: Crée un fichier de sauvegarde dans la centrale qui pourra servir ultérieurement.

Restauration: Remplace les paramètres actuels de la centrale avec le fichier de sauvegarde mémorisé dans la centrale.

Fichier de configuration du système

Les options suivantes sont disponibles pour la gestion du fichier de configuration système :

Download	Récupère un fichier de configuration stocké sur la centrale. Remarque : si un message d'erreur est affiché quand vous cliquez sur le bouton Download, procédez comme suit: <ol style="list-style-type: none"> 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 nouveau sur Download . <p>Lors du téléchargement sortant d'un fichier de configuration, les paramètres de configuration sont stockés dans un fichier .cfg. Ce fichier peut être chargé sur d'autres centrales pour éviter les longues procédures de programmation.</p>
Upload	Charge le fichier de configuration dans la centrale.
Secours	Sauvegarde la configuration dans une mémoire flash.
Restaurer	Charge la configuration sauvegardée dans la mémoire flash.

Données utilisateur

Les options suivantes sont disponibles pour la gestion des données utilisateur :

Download	Cliquez sur le bouton pour télécharger les données utilisateur de la centrale. Une boîte de dialogue demande si vous voulez sauver le fichier user.csv .
Upload	Cliquez sur Parcourir pour télécharger les données utilisateur sur la centrale. Elles doivent se trouver dans un fichier au format .csv .

17.12 Utilisation de la clé de programmation rapide

Le programmeur rapide du SPC est un dispositif de stockage mobile permettant à l'installateur de télécharger et de télédécharger les fichiers de configuration rapidement et efficacement. Elle possède deux interfaces se trouvant chacune à une extrémité de la clé:

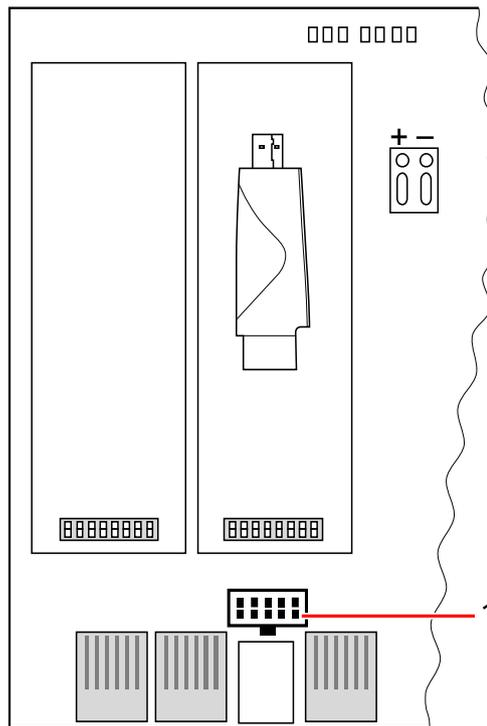
Interface de la centrale SPC

Ce connecteur série à 10 broches se trouve en haut du programmeur rapide. Il est inséré directement sur l'interface correspondante de la carte de circuit imprimé de la centrale. Après avoir inséré le programmeur rapide, l'installateur peut charger et récupérer les fichiers directement sur le programmeur en utilisant l'interface de programmation du navigateur.

Interface USB PC

Le connecteur USB se trouve en bas du programmeur rapide. Il est connecté directement sur un port USB d'un PC. Le fichier de configuration et autres fichiers ne peuvent être copiés qu'entre le PC et le programmeur rapide à l'aide de l'interface de programmation SPC Pro.

17.12.1 Connecter la clé de programmation à la centrale rapide



Interface de la clé de programmation rapide

1	Interface de la clé de programmation rapide
---	---

Pour connecter la clé de programmation SPC à la centrale :

1. Ouvrez l'enceinte de la centrale SPC et localisez l'interface de la clé de programmation.
AVIS ! N'éteignez pas la centrale.
 2. Aligned la clé de programmation rapide sur son interface sur la carte de circuit imprimé de la centrale SPC en tournant le connecteur série 10 broches vers le bas.
 3. Vérifiez que les broches soient parfaitement alignées sur les trous du socle puis enfoncez la clé sans forcer.
- ⇒ Le voyant LED de la clé clignote pendant l'accès aux données.
ATTENTION ! Ne retirez pas la clé de programmation rapide pendant que le voyant LED clignote..
- ⇒ La clé de programmation est à présent connectée à la centrale.



Pour enlever la clé de programmation, retirez-la tout droit de l'interface.

17.12.2 Installation de la clé de programmation rapide sur un PC

Pour Windows XP

- ▷ SPCPro doit être installé sur le PC avec Windows XP.

1. Connectez le programmeur rapide à une interface USB sur le PC.
⇒ L'assistant **Nouveau matériel détecté** est affiché.
2. Appuyez sur **Suivant**.
3. Cliquez sur **Continuer** .
⇒ À la fin de l'installation, une fenêtre indique que l'installation est complète.
4. Cliquez sur **Finish**.

Pour Windows 7

- ▷ Vous devez posséder des droits d'administrateur.
- ▷ SPCPro doit être installé sur le PC avec Windows 7.
- Connectez le programmeur rapide à une interface USB sur le PC.
⇒ Les pilotes sont installés automatiquement.

Voir le programmeur rapide SPC.

- Ouvrez le menu Windows **Démarrer > Panneau de configuration > Système > Gestionnaire de périphériques**.
- ⇒ Le pilote de la clé de programmation figure dans la catégorie Ports (COM & LPT) en tant que **SPC USB Fast Programmer (COM X)** (X = numéro du port com).

17.12.3 Gestion des fichiers de la clé de programmation rapide

La mise à jour du firmware et l'importation de la langue particulière de la centrale et des périphériques peuvent être réalisées avec la clé de programmation rapide et SPC Pro.

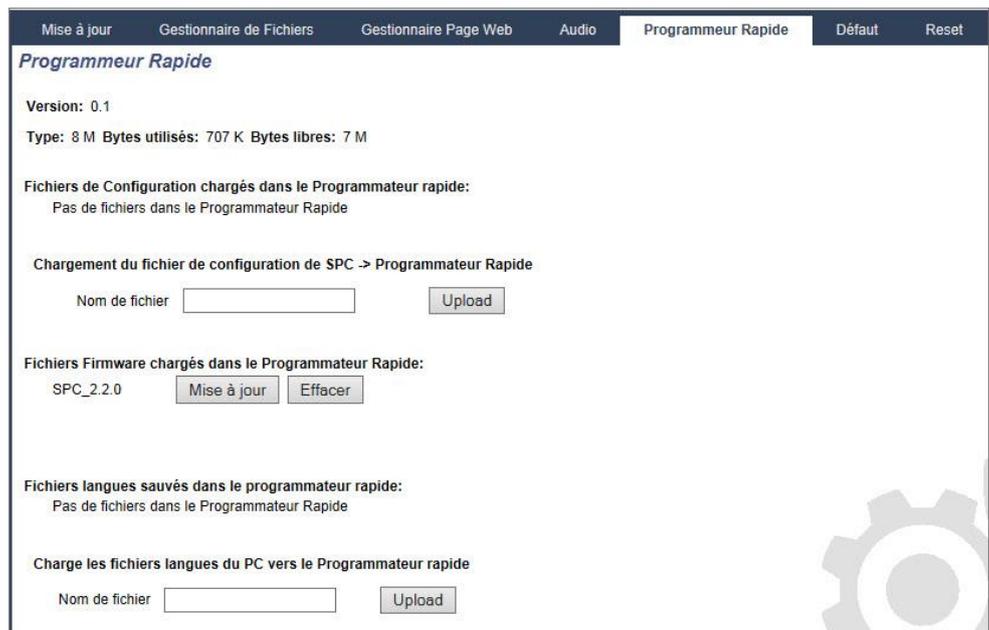
17.12.3.1 Configurez la clé de programmation rapide à l'aide du clavier

1. Accédez au mode Paramétrage puis sélectionnez le menu UTILITAIRES > CLE PROGRAMMAT.
2. Appuyez sur SELECT.
3. Sélectionnez l'option voulue:

CENTRALE -> CLE	Sélectionnez le fichier voulu dans la liste.
CLE -> CENTRALE	Sélectionnez le fichier voulu dans la liste.
EFFACER FICHIERS	Sélectionnez le fichier voulu dans la liste.
UPGRADE FIRMWARE	La centrale recherche un fichier de firmware valable. Si ce fichier est disponible, l'utilisateur est autorisé à le sélectionner et à procéder à la mise à jour de la centrale.
UPGRADE PÉRIPHÉRIQUE	La centrale recherche un fichier de firmware valable. Si ce fichier est disponible, l'utilisateur est autorisé à le sélectionner et à procéder à la mise à jour de la centrale.
MISE À JOUR DE LA LANGUE	Une liste des fichiers langue disponibles dans le programmeur rapide est affichée. Sélectionnez la langue voulue et appuyez sur SELECT pour importer le fichier.

17.12.3.2 Accès à la clé de programmation rapide à l'aide du navigateur

1. Accédez au mode Paramétrage dans le navigateur et affichez la page de programmation **Fichier**.
 2. Cliquez sur **Programmeur rapide**.
- ⇒ Les options de chargement et de récupération des fichiers sont affichées.



Téléchargement des fichiers de configuration sur la centrale

La liste des fichiers de configuration enregistrés sur la clé de programmation est affichée ainsi que les options de les récupérer ou de les effacer.

Mise à jour des fichiers de configuration de la clé de programmation rapide

Pour télécharger les fichiers du SPC vers la clé de programmation rapide, on vous demandera d'effacer les fichiers existants sur celle-ci avant d'enregistrer le nouveau fichier.

Pour télécharger un fichier configuration du programmeur rapide vers le SPC, saisissez le nom de fichier dans la boîte de dialogue et cliquez sur **Upload**.

Pour une description détaillée de l'utilisation de la clé de programmation rapide avec SPC Pro, consultez le *Manuel de configuration de SPC Pro*.

Mise à jour du firmware

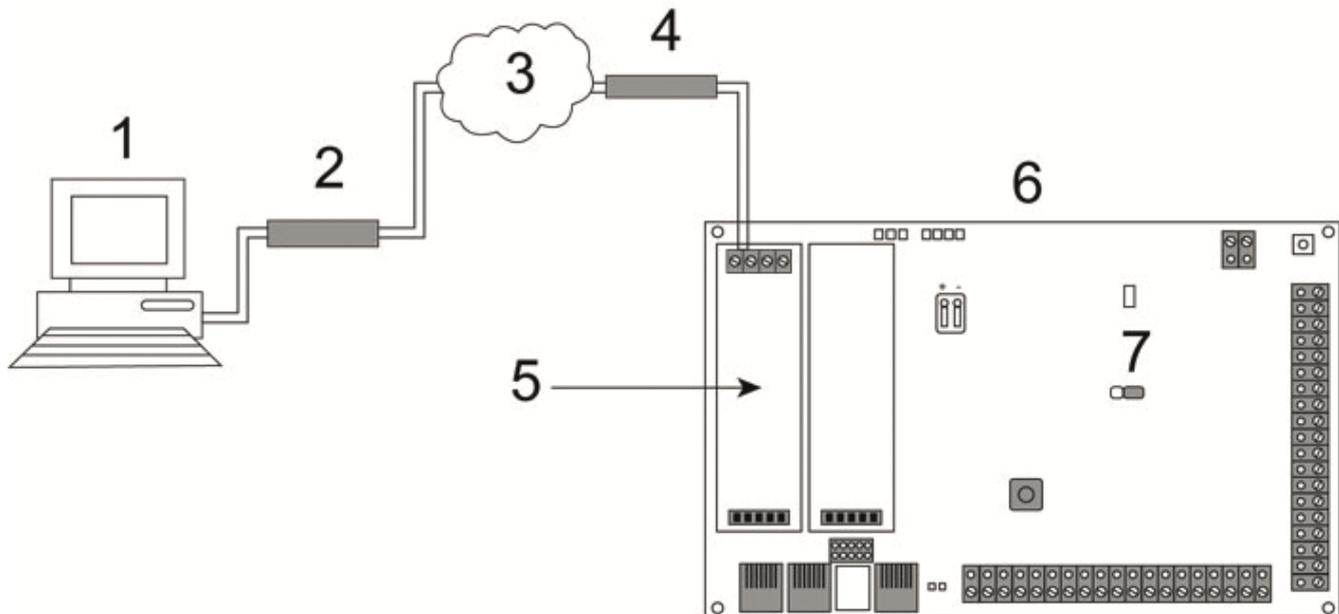
!	AVIS
	L'Accès Constructeur est obligatoire pour intervenir sur le firmware.

Une liste des fichiers de langues disponibles sur la clé de programmation rapide est affichée.

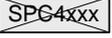
Pour mettre à jour le firmware, cliquez sur le bouton **Upgrade** correspondant au fichier firmware requis.

18 Accès à distance au serveur Web

18.1 Connexion RTC



Connexion RTC

1	PC distant avec le navigateur
2	Modem RTC
3	Réseau RTC
4	Ligne téléphonique
5	Modem RTC
6	Centrale SPC
7	JP9  SPC4xxx

Le serveur Web sur la centrale est accessible avec une connexion à distance établie dans le réseau téléphonique commuté. Un modem RTC doit être installé sur la centrale et relié à la ligne téléphonique (voir l'illustration).

Le correspondant distant doit avoir un PC équipé d'un modem RTC relié à la ligne téléphonique.

Pour accéder à distance à la centrale :

1. Installez un modem RTC dans la centrale (voir le manuel d'installation correspondant).
2. Reliez les bornes A/B en haut du modem au réseau RTC en utilisant un câble téléphonique.
3. Accédez au mode Paramétrage en utilisant le clavier et configurez le modem (primaire ou de secours) pour qu'il décroche aux appels reçus.
4. Sur le clavier, sélectionnez **MODE PARAMETRAGE > COMMUNICATIONS > MODEMS**.
5. Effectuez les réglages suivants :

- **VALIDER MODEM** : Activation
 - **Type** : Affiche le type de modem (RTC).
 - **CODE PAYS** : Sélectionnez le code du pays (Irlande, Royaume-Uni, Europe).
 - **MODE REPONSE** : Sélectionnez le mode de réponse aux appels entrants.
 - **SONNERIES MODEM** : Sélectionnez le nombre de sonneries avant de décrocher (8 sonneries max.).
6. Créez une connexion d'accès à distance sur le PC distant en utilisant le numéro de téléphone de la ligne reliée au modem RTC de la centrale. 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 sélectionnant **Démarrer > Panneau de configuration > Connexions réseau > Créer une nouvelle connexion** (dans la barre de navigation Gestion du réseau).
2. Dans la fenêtre **Type de connexion réseau**, sélectionnez **Etablir 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**, entrez le nom de la connexion, par exemple Accès à distance au SPC.
6. Dans la fenêtre **Entrez le numéro de téléphone à composer**, entrez le numéro de téléphone de la ligne RTC reliée au modem RTC.
7. Dans la fenêtre **Disponibilité de connexion**, indiquez si cette connexion doit être partagée par tous les utilisateurs.
8. Dans la fenêtre **Information de compte internet**, entrez les données suivantes :
 - Nom d'utilisateur : SPC
 - Mot de passe : password (par défaut)
 - Confirmer le mot de passe : password⇒ La fenêtre **Fin de l'Assistant Nouvelle connexion** est affichée.
9. Cliquez sur **Terminer** pour enregistrer la connexion sur le PC.



Il est recommandé de changer le code par défaut et de le conserver en un endroit sûr, puisque Vanderbilt est incapable de récupérer ce nouveau code. En cas d'oubli du code, seule une remise à zéro du système avec les paramètres par défaut permet de pouvoir utiliser l'appareil, ce qui entraîne la perte des paramètres programmés. Les paramètres programmés peuvent être rétablis si une sauvegarde est disponible.

Pour activer la connexion d'accès à distance :

- Cliquez sur l'icône correspondante dans la liste affichée en sélectionnant **Panneau de configuration > Connexions réseau**.

- ⇒ Le PC passe un appel de données à la ligne du PSTN connectée au module SPC PSTN.
- ⇒ Le PSTN du SPC décroche après le nombre de sonneries configuré et établit une liaison IP avec l'ordinateur distant.
- ⇒ Le système SPC attribue automatiquement une adresse IP au PC distant.



Sous certains systèmes d'exploitation Windows, une boîte de dialogue concernant la certification Windows est affichée. Vanderbilt estime qu'il est sûr de continuer. Pour toute question, adressez-vous à l'administrateur réseau ou contactez un technicien Vanderbilt autorisé.

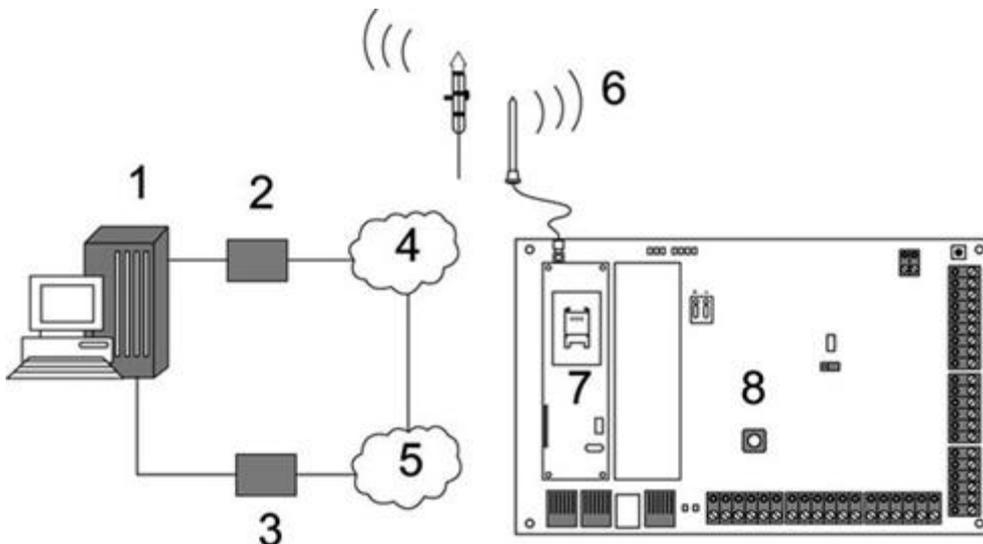
Pour obtenir cette adresse IP :

1. Cliquez sur l'icône de la connexion avec le bouton droit de votre souris.
2. Cliquez sur l'onglet **Propriétés**.
 - ⇒ L'adresse IP est affichée en tant qu'adresse IP du serveur.
1. Entrez cette adresse IP dans la barre d'adresse du navigateur Web et validez.
2. Si l'icône de la connexion d'accès à distance est affichée dans la barre des tâches de Windows, ouvrez le navigateur et entrez l'adresse IP du SPC.
 - ⇒ La fenêtre de connexion du navigateur est affichée.



Pour savoir comment configurer une connexion d'accès à distance sous un système d'exploitation différent, lisez l'aide de ce système d'exploitation.

18.2 Connexion GSM



Connexion GSM

1	PC distant avec le navigateur
2	Modem GSM
3	Modem RTC

4	Réseau GSM
5	Réseau RTC
6	antenne externe
7	Modem GSM
8	Centrale SPC

Le serveur Web sur la centrale est accessible avec une connexion à distance établie dans le réseau cellulaire GSM. Un modem GSM (avec une carte SIM) doit être installé dans la centrale pour que la communication puisse être établie avec le SPC (voir l'illustration). L'option de transmission de données doit être activée sur la carte SIM et le numéro de données doit être utilisé.

Le correspondant distant doit avoir un PC équipé d'un modem RTC ou GSM relié à la ligne téléphonique. Si un modem RTC est installé, il doit être relié à une ligne RTC active.

Pour accéder à distance à la centrale :

1. Installez un modem GSM dans la centrale (voir le manuel d'installation correspondant).
2. Accédez au mode Paramétrage en utilisant le clavier et configurez le modem (primaire ou de secours) pour qu'il décroche aux appels reçus.
3. Sur le clavier, sélectionnez le menu suivant en utilisant les touches de direction bas/haut : MODE PARAMETRAGE > COMMUNICATION > MODEMS, et configurez le système selon les indications ci-dessous :

VALIDER MODEM	Activez l'option MODEM VALIDE.
Type	Affiche le type de modem (GSM).
CODE PAYS	Sélectionnez le code du pays.
MODE REPONSE	Sélectionnez le mode de réponse aux appels entrants.
SONNERIES MODEM	Sélectionnez le nombre de sonneries avant de décrocher (8 sonneries max.).

Sous Windows XP :

1. Ouvrez l'Assistant Nouvelle connexion en sélectionnant **Démarrer > Panneau de configuration > Connexions réseau > Créer une nouvelle connexion** (dans la barre de navigation Gestion du réseau).
2. Dans la fenêtre **Type de connexion réseau**, sélectionnez **Etablir 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**, entrez le nom de la connexion, par exemple Accès à distance au SPC.
6. Dans la fenêtre **Entrez le numéro de téléphone à composer**, entrez le numéro de téléphone de la ligne RTC reliée au modem RTC.
7. Dans la fenêtre **Disponibilité de connexion**, indiquez si cette connexion doit être partagée par tous les utilisateurs.
8. Dans la fenêtre **Information de compte internet**, entrez les données suivantes :

- Nom d'utilisateur : SPC
- Mot de passe : password (par défaut)
- Confirmer le mot de passe : password
- ⇒ La fenêtre **Fin de l'Assistant Nouvelle connexion** est affichée.

9. Cliquez sur **Terminer** pour enregistrer la connexion sur le PC.



Il est recommandé de changer le code par défaut et de le conserver en un endroit sûr, puisque Vanderbilt

est incapable de récupérer ce nouveau code. En cas d'oubli du code, seule une remise à zéro du système avec les paramètres par défaut permet de pouvoir utiliser l'appareil, ce qui entraîne la perte des paramètres programmés. Les paramètres programmés peuvent être rétablis si une sauvegarde est disponible.

Pour activer la connexion d'accès à distance :

- Cliquez sur l'icône correspondante dans la liste affichée en sélectionnant **Panneau de configuration > Connexions réseau**.
 - ⇒ Le PC passe un appel de données à la ligne du PSTN connectée au module SPC PSTN.
 - ⇒ Le PSTN du SPC décroche après le nombre de sonneries configuré et établit une liaison IP avec l'ordinateur distant.
 - ⇒ Le système SPC attribue automatiquement une adresse IP au PC distant.



Sous certains systèmes d'exploitation Windows, une boîte de dialogue concernant la certification Windows est affichée. Vanderbilt

estime qu'il est sûr de continuer. Pour toute question, adressez-vous à l'administrateur réseau ou contactez un technicien Vanderbilt autorisé.

Pour obtenir cette adresse IP :

1. Cliquez sur l'icône de la connexion avec le bouton droit de votre souris.
2. Cliquez sur l'onglet **Propriétés**.
 - ⇒ L'adresse IP est affichée en tant qu'adresse IP du serveur.
1. Entrez cette adresse IP dans la barre d'adresse du navigateur Web et validez.
2. Si l'icône de la connexion d'accès à distance est affichée dans la barre des tâches de Windows, ouvrez le navigateur et entrez l'adresse IP du SPC.
 - ⇒ La fenêtre de connexion du navigateur est affichée.



Pour savoir comment configurer une connexion d'accès à distance sous un système d'exploitation différent, lisez l'aide de ce système d'exploitation.

19 Fonctions d'alarme anti-intrusion

Le système SPC peut fonctionner selon trois modes différents, le mode **Bancaire**, **Evolué** et le mode **Simple**, chacun prenant en charge plusieurs secteurs.

Chaque secteur peut fonctionner selon 4 modes d'alarme différents. Les modes Evolué et Bancaire propose davantage de types d'alarme programmables que le mode Simple. Les noms et les types de zone par défaut pour chaque mode peuvent être consultés ici [→ 355].

19.1 Fonctionnement en mode Bancaire

Le mode Bancaire est adapté aux banques et aux établissements financiers équipés de secteurs sûrs spéciaux, comme les coffres et les DAB.

Chaque secteur défini dans le système prend en charge les modes d'alarme indiqués ci-dessous.

Mode d'alarme	Description
MHS	Le secteur est mis hors surveillance, une alarme n'est déclenchée que dans les zones d'alarme du type 24/24.
MES PART. A	Ce mode active la protection du périmètre d'un immeuble, mais autorise 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, un temporisateur de sortie n'est pas actif, l'activation est instantanée quand l'utilisateur sélectionne ce mode. Au besoin, un temporisateur de sortie peut être appliqué à ce mode en activant le paramètre TEMPORISATION dans les options de la MES partielle A.
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, un temporisateur de sortie n'est pas actif, l'activation est instantanée quand l'utilisateur sélectionne ce mode. Au besoin, un temporisateur de sortie peut être appliqué à ce mode en activant le paramètre TEMPORISATION dans les options de la MES partielle B.
MES TOTALE	La mise en surveillance totale du secteur est sans restriction, l'ouverture d'une zone d'entrée/de sortie lance le temporisateur d'entrée. L'alarme est activée si le temporisateur n'est pas arrêté avant la fin du délai.

19.2 Mode Evolué

Le mode Evolué est adapté aux installations en environnement commercial/industriel avec de nombreux secteurs et de nombreuses zones d'alarme. Chaque secteur défini dans le système prend en charge les modes d'alarme indiqués ci-dessous.

Mode d'alarme	Description
MHS	Le secteur est mis hors surveillance, une alarme n'est déclenchée que dans les zones d'alarme du type 24/24.
MES PART. A	Ce mode active la protection du périmètre d'un immeuble, mais autorise 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, un temporisateur de sortie n'est pas actif, l'activation est instantanée quand l'utilisateur sélectionne ce mode. Au besoin, un temporisateur de sortie peut être appliqué à ce mode en activant le paramètre TEMPORISATION dans les options de la MES partielle A.
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, un temporisateur de sortie n'est pas actif, l'activation est instantanée quand l'utilisateur sélectionne ce mode. Au besoin, un temporisateur de sortie

Mode d'alarme	Description
	peut être appliqué à ce mode en activant le paramètre TEMPORISATION dans les options de la MES partielle B.
MES TOTALE	La mise en surveillance totale du secteur est sans restriction, l'ouverture d'une zone d'entrée/de sortie lance le temporisateur d'entrée. L'alarme est activée si le temporisateur n'est pas arrêté avant la fin du délai.

19.3 Mode Simple

Le mode Simple est adapté aux installations en environnement résidentiel avec peu de secteurs et un nombre peu élevé à moyen de zones d'alarme. Chaque secteur défini dans le système prend en charge les modes d'alarme indiqués ci-dessous.

Mode d'alarme	Description
MHS	Le secteur est mis hors surveillance, une alarme n'est déclenchée que dans les zones d'alarme du type 24/24.
MES PART. A	Ce mode active la protection du périmètre d'un immeuble, mais autorise le libre déplacement dans les zones d'entrée et d'accès (par exemple la porte principale et le couloir d'entrée). Les zones exclues (attribut de zone EXCLUS A) ne sont pas protégées dans ce mode. Aucun temporisateur de sortie n'est associé à ce mode, l'activation est instantanée lorsque l'utilisateur sélectionne ce mode.
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, un temporisateur de sortie n'est pas actif, l'activation est instantanée quand l'utilisateur sélectionne ce mode. Au besoin, un temporisateur de sortie peut être appliqué à ce mode en activant le paramètre TEMPORISATION dans les options de la MES partielle B.
MES TOTALE	La mise en surveillance totale du secteur est sans restriction, l'ouverture d'une zone d'entrée/de sortie lance le temporisateur d'entrée. L'alarme est activée si le temporisateur n'est pas arrêté avant la fin du délai.

19.4 Alarmes totales et locales

Le type d'alarme généré par le système SPC varie suivant le type de zone où l'alarme est activée. La majorité des alarmes incluent une indication visuelle (flash) et acoustique (sirène) d'une intrusion dans les locaux ou dans l'immeuble.

Par défaut, les 3 premières sorties physiques de la centrale SPC sont attribuées à la sirène extérieure, à la sirène intérieure et au flash de la sirène extérieure. Quand elles sont activées, ces trois sorties sont suffisantes pour signaler une alarme aux personnes se trouvant à l'intérieur ou dans les environs immédiats de l'immeuble ou des locaux où l'intrusion a eu lieu.

Les alarmes totales et locales sur le SPC activent les sorties physiques suivantes :

- Sortie 1 de la centrale : Sirène extérieure
- Sortie 2 de la centrale : Sirène intérieure
- Sortie 3 de la centrale : Flash

Pour les détails sur le câblage des sirènes et des flashes, voir ici [→ 77].

Une **Alarme totale** est transmise au centre de télésurveillance (CTS) si la transmission est configurée.

Une **Alarme locale** n'est pas transmise au CTS.

Une **Alarme silencieuse** n'active pas les sorties 1 – 3 (pas d'indication visuelle ni acoustique de l'alarme). L'alarme est transmise 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

20.1 Utilisation d'un secteur commun

Les secteurs communs sont utilisés pour activer plusieurs secteurs d'un site en même temps. Un utilisateur attribué à un secteur commun est autorisé à ACTIVER TOUS les secteurs faisant partie du secteur commun (même les secteurs qui ne sont pas attribués à cet utilisateur). Toutefois, les utilisateurs ne peuvent DESACTIVER que les secteurs qui leur sont attribués.

Les secteurs communs devraient seulement être utilisés si un clavier unique est installé dans la zone d'accès principal et si tous les utilisateurs dans l'immeuble se partagent ce clavier.

Scénario : 2 services d'une entreprise (Comptabilité et Vente) ont un passage d'accès commun à l'immeuble (porte principale).

Dans ce cas, créez 3 secteurs dans le système (Secteur commun, Comptabilité, Vente). Le secteur commun doit inclure le passage d'accès principal (porte principale). Attribuez les zones de la Comptabilité au Secteur 2, et les zones de la Vente au Secteur 3. Installez un clavier à la porte principale et attribuez-le à tous les trois secteurs. Créez 2 utilisateurs (au moins) dans le système, un pour chaque service, et attribuez-les à leur secteur respectif et au secteur commun.

Opération : Activation du système

Le responsable du service Comptabilité quitte le bureau à 17:00 heures. Quand il tape son code sur le clavier, le menu MES TOTALE propose les 3 options suivantes :

- **TOUTES ZONES :** active tous les secteurs attribués au secteur commun (Secteur commun, Comptabilité, Vente) et tous les autres secteurs attribués au responsable (dans cet exemple, pas d'autres secteurs). Le temporisateur de sortie de la porte principale indique à l'utilisateur de quitter l'immeuble.
- **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.

Quand le dernier employé du service Vente quitte le bureau, il ferme toutes les portes et fenêtres dans le SECTEUR 3 et tape son code sur le clavier. Le menu MARCHE TOTALE propose les 3 options suivantes :

- **TOUTES ZONES :** active tous les secteurs attribués au secteur commun (Secteur commun, Comptabilité, Vente) et tous les autres secteurs attribués à l'employé du service Vente (dans cet exemple, pas d'autres secteurs). Le temporisateur de sortie de la porte principale indique à l'utilisateur de quitter l'immeuble.
- **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.

Opération : Désactivation 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 :

- **TOUTES ZONES** : désactive tous les secteurs attribués à la Comptabilité (Secteur commun, Comptabilité) et les autres secteurs attribués au responsable. Dans ce cas, aucun autre secteur ne lui est attribué.
REMARQUE : Le responsable du service Comptabilité ne peut PAS désactiver le secteur Vente.
- **COMMUN** : désactive UNIQUEMENT le secteur commun (réception). Ceci permet de mettre la réception hors surveillance pendant que les bureaux des services Comptabilité et Vente restent armés.
- **COMPTABILITÉ** : désactive le secteur Comptabilité et le secteur commun (réception). Dans ce cas, le secteur Vente reste activé et l'accès par la porte principale est toujours possible.

Utilisation des secteurs communs :

- Zone d'armement par clé

Si l'itinéraire d'entrée/de sortie dans le secteur commun est programmé en tant que zone d'armement par clé et que cette zone est activée, tous les secteurs dans le secteur commun sont mis en surveillance. La désactivation de la zone d'armement par clé met HORS SURVEILLANCE tous les secteurs dans le secteur commun.

- Plusieurs claviers

Si les secteurs attribués au secteur commun ont leurs propres claviers pour l'entrée/sortie, il importe que les temporisations de sortie programmées pour ces secteurs soient suffisamment longues pour que les utilisateurs puissent atteindre la sortie du secteur commun. En effet, dans le cas où le secteur qui vient d'être activé est le dernier secteur non armé du système, ceci déclencherait l'activation de tout le secteur commun.



En général, il est recommandé d'utiliser des secteurs communs sur les sites où un seul clavier est installé au point d'accès commun, c'est-à-dire à la porte d'accès principale.

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 n'est disponible que sur les installations dont la centrale est de type Bancaire.

Vous disposez de plusieurs méthodes pour tester les détecteurs sismiques. Le moyen le plus simple consiste à frapper un mur ou un dispositif de sécurité et de voir si la zone s'ouvre sous l'effet d'un test de déplacement. Ce type de test est disponible avec tous les détecteurs sismiques, quels qu'ils soient.

Si le détecteur sismique est installé avec un transmetteur de test, les options suivantes sont disponibles :

- Test manuel lancé depuis le clavier ou avec SPC Pro (non pris en charge par le navigateur) ;
- Test automatique programmé à une fréquence donnée ou lorsque la centrale est configurée depuis le clavier.

Le transmetteur de test est un petit capteur vibrant à haute fréquence fixé à proximité du détecteur sur la même paroi. Le transmetteur de test est câblé sur une sortie de la centrale ou d'un transpondeur.

Configuration des détecteurs sismiques dans la centrale

1. Configuration d'une zone sismique. Les détecteurs sismiques doivent être affectés à une zone. (Voir Éditer une porte [→ 253]).

Hardware							Système							Entrées & Portes							Sorties							Portes							Secteurs							Calendriers							Changer son code							Avancé						
Toutes Zones														Zones X-Bus														Zones Radio																																		
Zone	Entrée	Libellé	Type	Secteur	Attributs																																																									
1	Centrale - Entrée 1	Front door	Alarme	1: Area 1	...																																																									
2	Centrale - Entrée 2	Vault	Sismique	2: Vault	...																																																									

2. Configurez les attributs de zone.

Hardware		Système		Entrées & Portes		Sorties		Portes		Secteurs		Calendriers		Changer son code		Avancé	
Centrale																	
XBUS																	
Radio																	
Attributs - Zone 2																	
Attribut	Libellé																
<input type="checkbox"/> 24/24	Quand l'attribut 24/24 est validé, l'ouverture de la zone déclenchera une alarme dans tous les modes de surveillance.																
<input type="checkbox"/> MHS locale	Quand l'attribut 'MHS Locale' est sélectionné, les alarmes ne sont transmises que lorsque le secteur associé est en MES totale ou MES partielle. (pour les entrées 24/24)																
<input checked="" type="checkbox"/> Inhiber	Quand l'attribut inhibité est validé, un utilisateur peut inhiber cette zone.																
<input type="checkbox"/> JDB	Si cet attribut est validé, alors tous les changements d'état de la zone sont historisés.																
<input type="checkbox"/> Test Sismique	Si coché, les détecteurs sismiques seront testés automatiquement, voir le temps 'périodicité test sismique' dans l'onglet TEMPORISATIONS																
Calendrier																	
<input type="text" value="1: Vault"/>	Valider si la zone est limitée par un calendrier																
Levée de doute																	
<input type="text" value="1: Verificat 1"/>	Sélectionner si l'entrée est liée à la zone de vérification d'alarme et déclenche une vérification Audio/vidéo.																

3. L'attribut **Test sismique** active le test automatique du détecteur.
4. Sélectionnez un calendrier de contrôle de la zone sismique, le cas échéant.
5. Affecte cette zone à une zone de vérification si une vérification audio/vidéo est requise.
6. Configurez les temporisations pour préciser la fréquence des tests de zones sismiques (7 jours par défaut) et la durée des tests. (L'attribut de zone Test auto. du Détecteur doit être activé.) (Voir Temporisations [→ 245])

Période de l'autotest sismique	<input type="text" value="168"/> Heures	Périodicité myenne des tests de détecteurs sismiques (la périodicité est aléatoire). Pour valider les tests auto, l'attribut 'Test auto du détecteur' doit être sélectionné. (12 - 240)
Durée du test sismique	<input type="text" value="30"/> Secondes	Temps maximum (secondes) d'attente du déclenchement du sismique lorsqu'il est sollicité par l'activation de la sortie test sismique (3 - 120)

- Configurez une sortie pour tester une zone sismique. (Voir Types de sorties et Ports de sortie [→ 214])

La sortie peut être affectée à un système ou à un secteur, si la centrale est configurée pour utiliser des secteurs, ce qui est en général le cas dans les environnements bancaires. La sortie ne doit être affectée au système que si la centrale n'utilise pas de secteurs.

Avec le clavier

- Sélectionnez **MODE PARAMETRAGE >ZONES >(sélectionnez une zone) >TYPE ZONE > SISMIQUE**
- Sélectionnez **MODE PARAMETRAGE >ZONES >(sélectionnez une zone) >ATTRIBUTS>AUTOTEST SISMIC**

Voir aussi

- 📄 Temporisations [→ 245]
- 📄 Types et ports de sortie [→ 214]
- 📄 Éditer une zone [→ 253]

21.1 Test du capteur sismique

Les zones sismiques doivent être configurées afin que les tests manuels et automatiques soient disponibles. Que le test soit manuel ou automatique, le résultat est sauvegardé dans le JDB.

Le test sismique concerne une ou plusieurs zones sismiques. Pendant un test de zone, les autres zones du secteur sont temporairement désactivées, car il n'y a qu'une sortie de test sismique par secteur.

21.1.1 Procédure de test manuel et automatique

Un test manuel ou automatique se déroule comme suit :

- La centrale active la sortie Test sismique pour le(s) secteur(s) auquel appartient la ou les zones à tester.
- 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.
- 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 (par ex. si 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 capteurs sismiques sont testés périodiquement ou après une configuration du système depuis le clavier.

Test automatique périodique

Des tests automatiques périodiques sont effectués dans toutes les zones sismiques pour lesquelles les tests automatiques sont activés.

Les tests automatiques sont effectués aléatoirement pendant la période configurée et sont indépendants pour chaque secteur.

Toutes les zones sismiques du même secteur (pour lesquelles les tests automatiques sont activés) sont testées simultanément.

L'option de configuration **Période de l'autotest sismique** du menu Temporisations [→ 245] détermine la période moyenne de test pour les tests automatiques des capteurs sismiques. La valeur par défaut est fixée à 168 heures (soit 7 jours) ; des valeurs comprises dans l'intervalle 12 - 240 heures sont admises.

L'heure du test est aléatoire et déterminée dans l'intervalle fixé +/- 15%. Par exemple, si un test est planifié tous les 24 heures, il peut intervenir entre 20,4 et 27,6 heures après le test précédent.

Un test sismique est effectué après un redémarrage si l'option gérant les tests automatiques est activée. Si la centrale était en mode Paramétrage avant le redémarrage, le test est effectué seulement si la centrale n'est plus en mode Paramétrage après le redémarrage.

En cas d'échec du test sismique, un problème est signalé (code SIA BT). L'événement Restauration correspondant est signalé également (code SIA BJ).

Test automatique lors de la MES

L'option **Test sismique lors MES manuelle** est configurable dans l'onglet Options Système [→ 236]. Si activé, toutes les zones sismiques de tous les secteurs à configurer sont testées avant la séquence habituelle de MES. Cela ne concerne que le clavier.

Pendant le test, la mention AUTOTEST SISMIQUE est affichée sur le clavier. En cas de succès du test, la procédure de de MES se poursuit normalement.

Si tous les secteurs, un groupe de secteurs ou un seul secteur sont sélectionnés pour configuration et qu'un test sismique échoue, la mention ÉCHEC SISMIQUE s'affiche. En appuyant sur **Retour**, une liste des zones en échec s'affiche. Naviguez dans la liste à l'aide des flèches haut et bas.

En fonction de l'attribut **Inhibé** affecté à une zone sismique en échec et du profil utilisateur, les situations suivantes peuvent se produire :

- Si l'attribut **Inhibé** est appliqué à toutes les zones sismiques ayant échoué au test et que le profil utilisateur possède le droit **Inhiber** :

1. Appuyez sur **Retour** sur l'une des zones en échec.
 - ⇒ Le message MES FORCEE TOUT? s'affiche.
2. Appuyez de nouveau sur **Retour** pour inhiber toutes les zones sismiques en échec. (Vous pouvez également revenir au menu précédent.)
 - ⇒ La configuration se déroule normalement.
 - Si l'attribut **Inhibé** n'est pas appliqué à toutes les zones sismiques ayant échoué au test ou si le profil utilisateur ne possède pas le droit **Inhiber** :
 - Appuyez sur **Retour**.
 - ⇒ Le message FAIL TO SET s'affiche et aucun secteur n'est configuré.

Aucun test sismique automatique n'est prévu pour les secteurs auto-configuré, quelle qu'en soit la raison (par exemple, les secteurs activés par un calendrier ou un déclencheur). De même, aucun test sismique automatique n'a lieu lorsque le système est configuré avec SPC Com, avec SPC Pro ou le navigateur. Cependant, un test sismique auto se déclenche en cas d'utilisation d'un clavier virtuel avec SPC Com ou SPC Pro.

Aucun événement n'est transmis si la configuration des tests après MES échoue.

La temporisation de test automatique du système périodique est effectuée après la configuration.

21.1.3 Test manuel des détecteurs

Pour effectuer un test manuel des détecteurs, sélectionnez l'option TEST>TEST SISMIQUE dans le menu TEST sur le clavier.

Un test sismique manuel avec le clavier peut être effectué par un installateur en mode Paramétrage et par l'utilisateur type Manager ou Standard :

- un installateur est autorisé à tester tous les détecteurs dans tous les secteurs configurés dans le système avec n'importe quel clavier.
- un utilisateur n'est autorisé à tester que les détecteurs des secteurs qui lui sont attribués, avec le clavier spécifique qu'il utilise.

Pour effectuer un test sismique en mode Paramétrage, sélectionnez MODE PARAMETRAGE ⇒ TEST ⇒ TEST SISMIQUE.

Pour effectuer un test sismique en mode Utilisateur, sélectionnez MENUS ⇒ TEST ⇒ TEST SISMIQUE.

Remarque : les instructions suivantes concernent à la fois les modes Paramétrage et Utilisateur. Attention : seules certaines options sont disponibles pour l'utilisateur.

Les options suivantes sont disponibles dans le menu TEST SISMIQUE :

- TEST TOUTES ZONES
Tester les zones sismiques dans tous les secteurs disponibles si plus d'un secteur contient des zones sismiques.
- *NOM DU SECTEUR*
Les noms des secteurs contenant des zones sismiques sont listés individuellement. Si un secteur donné est sélectionné, les options suivantes sont disponibles :
 - TEST TOUS ZONES
Teste toutes les zones sismiques du secteur s'il existe plus d'une zone sismique.
 - *NOM DE ZONE*
Les noms de toutes les zones sismiques sont listés et peuvent être sélectionnés pour un test individuel.

Le message TEST SISMIQUE est affiché sur le clavier pendant que le test est exécuté.

En cas d'échec du test, le message SISMIQUE ERREUR est affiché. Si vous appuyez sur la touche « i » ou VOIR, la liste des zones en échec est affichée. Vous pouvez faire défiler cette liste pour la voir en entier.

Si le test aboutit, TEST OK est affiché.

Les entrées sont journalisées avec les détails suivants :

- l'utilisateur qui a démarré le test
- résultat (OK ou ECHEC)
- numéro et nom de secteur et de zone

aucun événement n'est signalé 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.

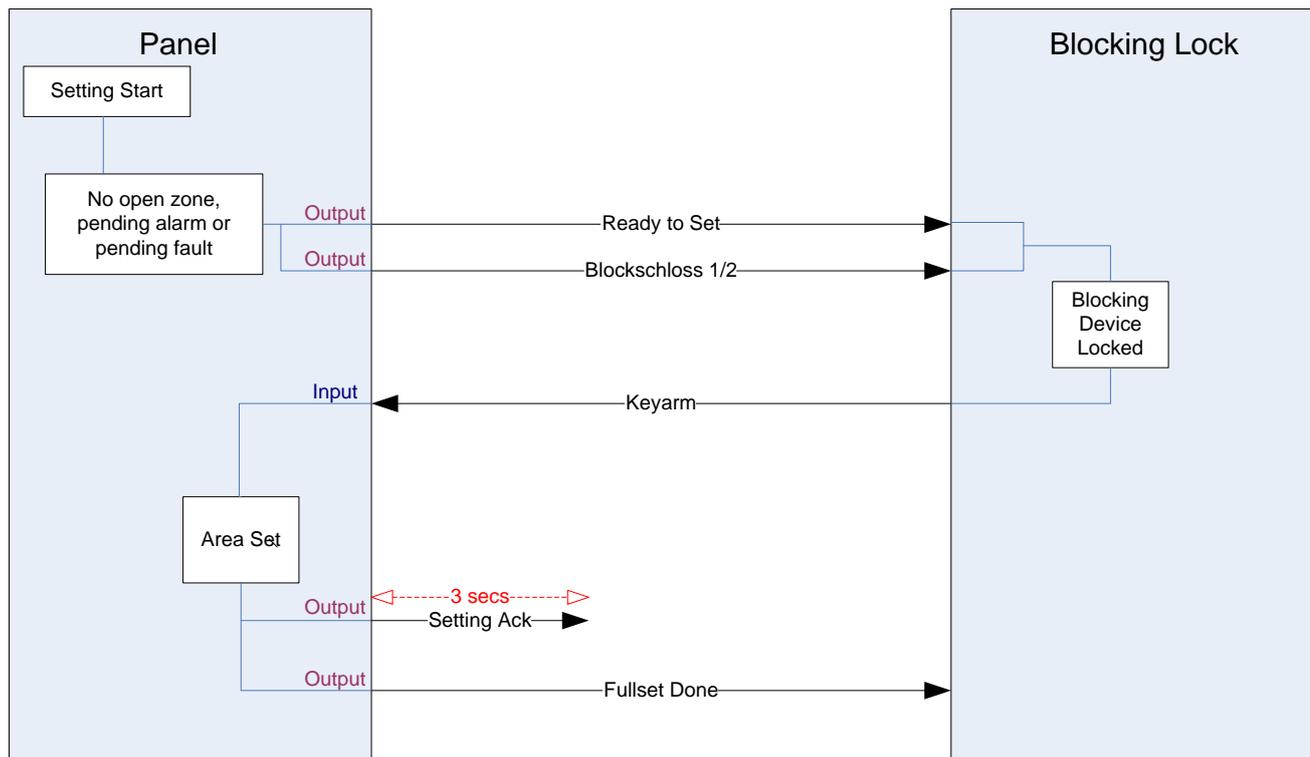
22.1 Verrouillage de blocage

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 si le signal MES possible est disponible à partir du panneau de contrôle. Ceci 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 à 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 d'acquis de mise en service 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 activé 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. Suite au changement sur le type d'entrée de la clé de mise en service, le secteur est désactivé. Blockschloss 1 est désactivé si le secteur est prêt à l'activation alors que Blockschloss 2 est activé si le secteur est prêt à l'activation.



Les exigences en matière de configuration pour un verrouillage de blocage sont les suivantes :

- Sorties :
 - Prêtes à l'activation
 - Acquis de MES
 - MES totale faite
 - Blockschloss 1/2
- Entrées
 - Clef de MES

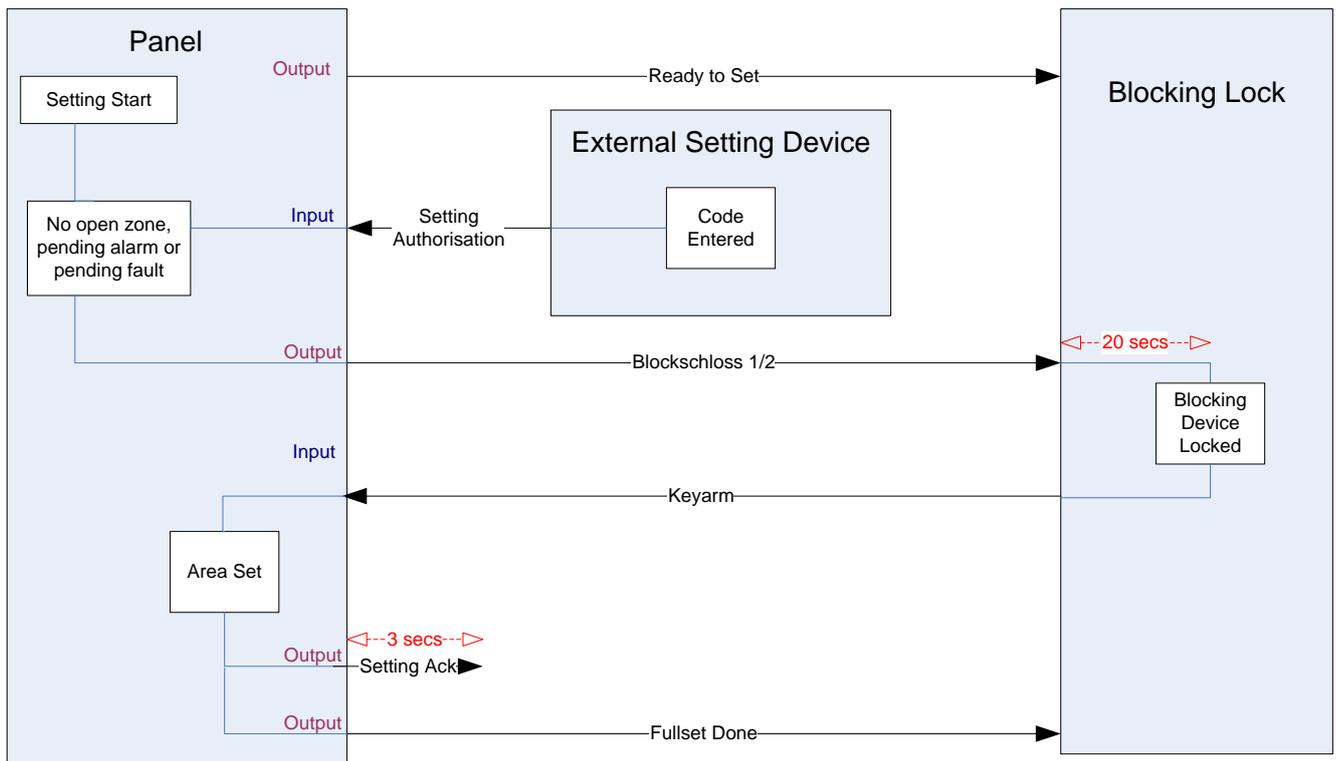
22.2 Activation autorisée du verrouillage de blocage

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 à carte ou à 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 avant MES/MHS
 - MES
 - MES et MHS (nécessaire pour VdS)
 - Mise hors surveillance
- Sorties :
 - Prêtes à l'activation
 - Acquis de MES
 - MES totale faite
- Entrées
 - Clef de MES

22.3 Élément de verrouillage

Pour VdS, il est obligatoire d'empêcher l'entrée dans un secteur activé. Ceci est fait en utilisant un élément de verrouillage monté dans le cadre de la porte. Il consiste en un petit écrou en plastique qui bloque la porte dans un état MES. La position de l'écrou 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 est situé au sein d'un secteur, le minuteur de sortie est restreint à un minimum de 4 secondes de façon à ce que l'élément de verrouillage puisse être activé. Lorsque le minuteur atteint quatre secondes, l'élément de verrouillage sera activé pendant trois secondes. Une fois cette durée

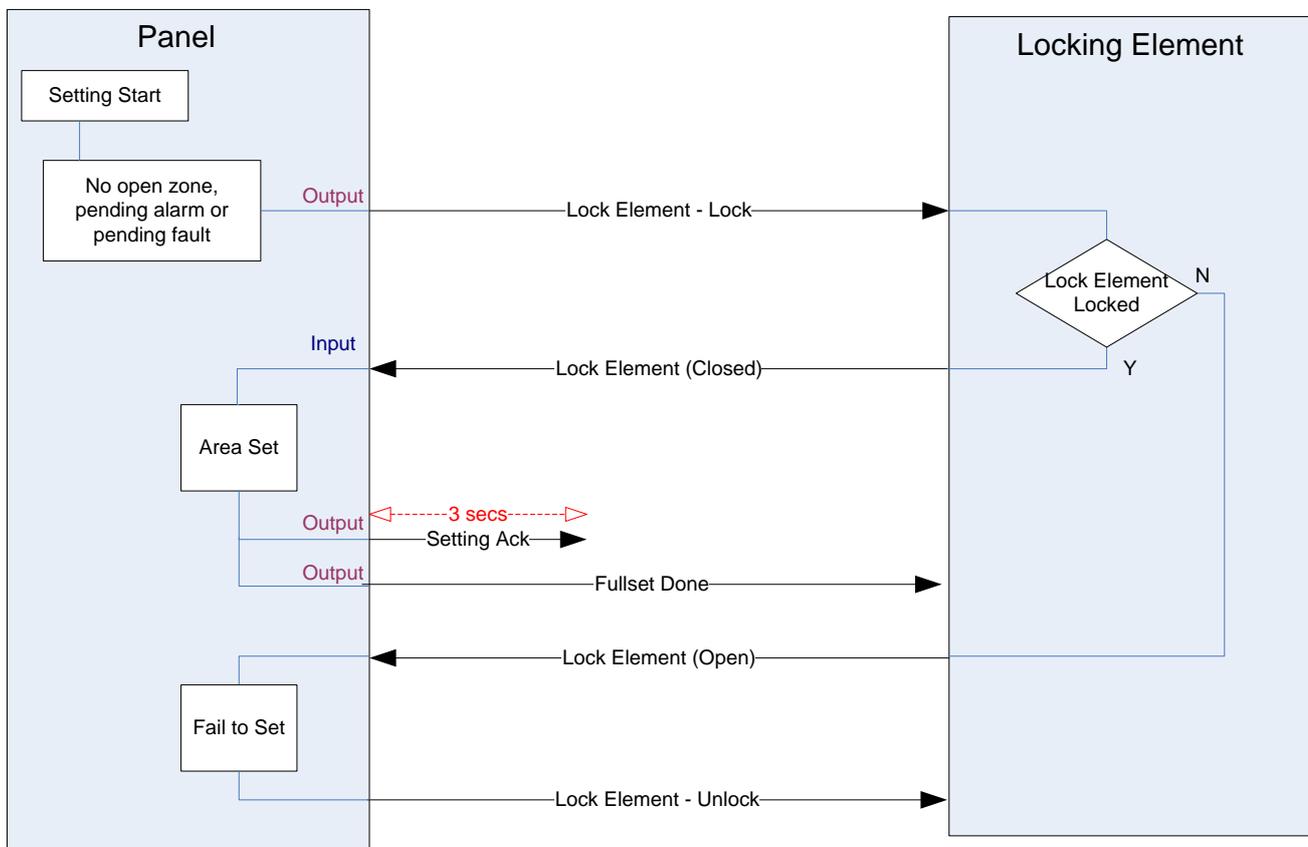
atteinte, la sortie de l'élément de verrouillage doit être en état fermé. Le système sera alors activé.

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 de l'élément de verrouillage (si elle est configurée) ne se trouve pas en état fermé lorsque le minuteur 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

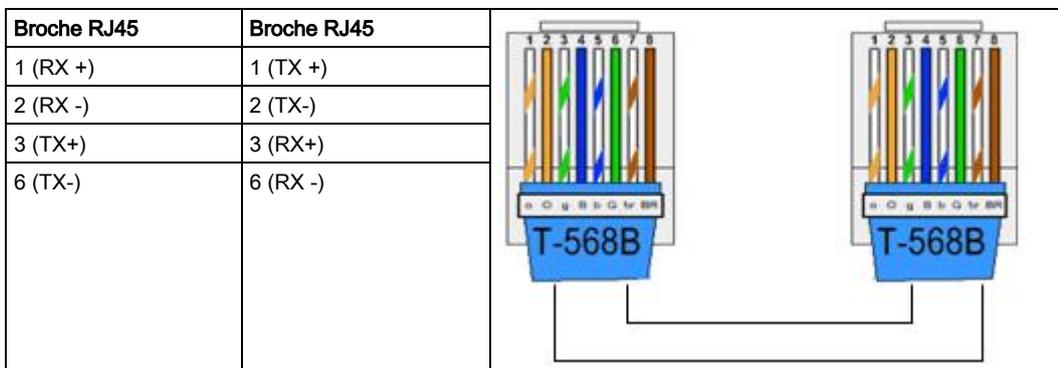
23.1 Connexions des câbles réseau

IP

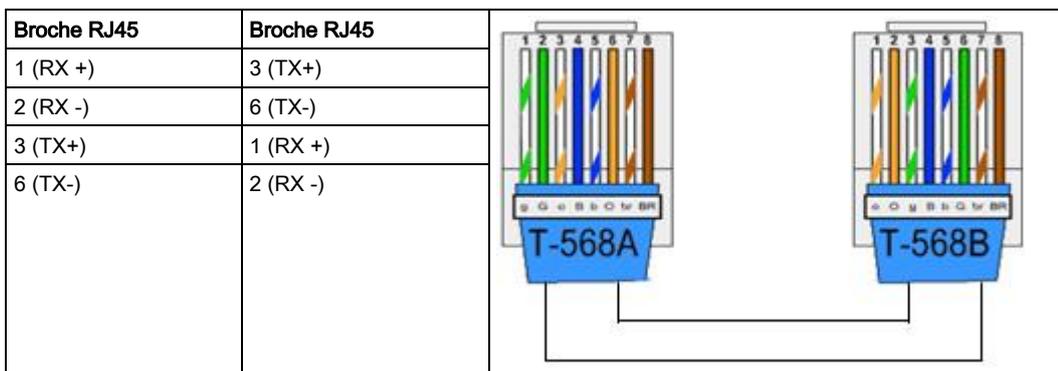
Un PC peut être connecté au SPC soit via le réseau local (LAN), soit directement à l'interface Ethernet du SPC. Les tableaux ci-dessous illustrent les deux cas sous forme graphique.

- Si SPC est connecté au réseau via un concentrateur, utilisez un câble droit entre le concentrateur et le PC.
- Si le contrôleur n'est pas connecté à un réseau (par exemple, si un concentrateur ou un switch n'est pas utilisé), il faudra alors connecter un câble null modem entre la centrale SPC et le PC.

Pour connecter le SPC à un PC via un concentrateur, utilisez un câble droit.



Pour connecter la centrale SPC directement à un PC, utilisez un câble null modem.



23.2 LED d'état de la centrale

TÉMOIN	Fonction
Témoins 1	Données radio CLIGNOTEMENT : une donnée radio est reçue par le module radio ÉTEINT : aucune donnée radio n'est en cours de réception.
Témoins 2	État de la batterie ALLUME : la tension de la batterie est inférieure au niveau de décharge profonde (10,9 V) ÉTEINT : OK.

Témoin 3	Alimentation secteur ALLUMÉ : panne de secteur ÉTEINT : alimentation secteur OK.
Témoin 4	État du X-BUS ALLUMÉ : la configuration X-BUS est une configuration en boucle ÉTEINT : la configuration X-BUS est une configuration en branche CLIGNOTEMENT : transpondeurs de fin de ligne détectés, ou rupture de câble.
Témoin 5	Erreur du système ALLUMÉ : un défaut de matériel a été détecté sur la carte ÉTEINT : pas de défaut de matériel détecté
Témoin 6	Accès en écriture à la mémoire flash ALLUMÉ : le système enregistre sur la mémoire flash ÉTEINT : pas d'enregistrement sur la mémoire flash
Témoin 7	Battement de coeur CLIGNOTEMENT : le système fonctionne normalement

ALLUME 	ARRÊT 	CLIGNOTEMENT : 
--	---	--

23.3 Alimentation des transpondeurs avec les bornes d'alimentation secondaires

Pour calculer le nombre de transpondeurs / claviers pouvant être alimentés sans problème par les terminaux d'alimentation auxiliaires 12 V CC, 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 V CC.

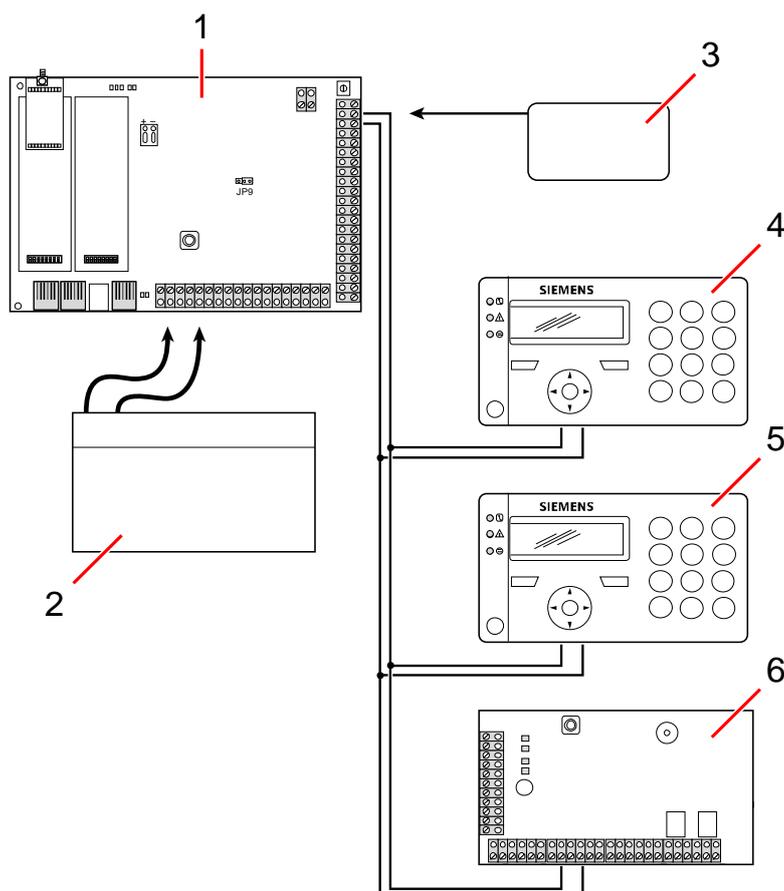


Veillez vous référer à Caractéristiques techniques pour le courant auxiliaire spécifique et à la fiche de données ou d'instruction d'installation des modules, claviers et transpondeurs pour la consommation courante.

$$\text{Courant du transpondeur 1 (mA)} + \text{courant du transpondeur 2 (mA)} + \dots < \text{puissance auxiliaire}$$

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 V CC 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 avec les bornes d'alimentation secondaires

1	Centrale SPC
2	Batterie
3	Bornes d'alimentation secondaire 12 V
4	Clavier
5	Clavier
6	Transpondeur E/S

23.4 Calcul de la puissance nécessaire de la batterie

Il importe que la puissance disponible pour alimenter tous les périphériques pendant une panne de courant secteur soit suffisante. Pour que cette condition soit réalisée, connectez toujours la batterie et le chargeur appropriés.

Le tableau ci-dessous fournit une valeur approximative du courant de chargement maximal que chaque type de batterie peut fournir pendant les périodes de disponibilité indiquées.

Les valeurs approximatives ci-dessous se basent sur le fait que la carte de circuit imprimé de la centrale SPC utilise sa charge maximale (toutes les entrées connectées ont une résistance fin de ligne) et la puissance de sortie utile de la batterie est 85 % de sa capacité maximale.

0,85 x capacité de la batterie (Ah)	-	(Icentr + Isirène)	=	I _{max}
Temps (heures)				

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

Icentr = courant de repos (en A) pour la centrale SPC

Isirène = courant de repos (en A) pour les sirènes extérieures et intérieures raccordées

I_{max} = 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	AUCUN	RTC	GSM	RTC+GSM
Durée de veille				
12 h	356 mA	331 mA	226 mA	201 mA
30 h	58 mA	33 mA	Non disponible	Non disponible

Quantité de courant de la sortie Aux en utilisant une batterie de 17 Ah (SPC523x)

COMMS	AUCUN	RTC	GSM	RTC+GSM
Durée de veille				
12 h	750 mA	750 mA	750 mA	750 mA
30 h	342 mA	317 mA	212 mA	187 mA

Quantité de courant de la sortie Aux en utilisant une batterie de 7 Ah (SPC432x/532x)

COMMS	AUCUN	RTC	GSM	RTC+GSM
Durée de veille				
12 h	326 mA	301 mA	196 mA	171 mA
30 h	28 mA	Non disponible	Non disponible	Non disponible

Quantité de courant de la sortie Aux en utilisant une batterie de 17 Ah (SPC533x/633x)

COMMS	AUCUN	RTC	GSM	RTC+GSM
Durée de veille	mA	mA	mA	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	AUCUN	RTC	GSM	RTC+GSM
Durée de veille	mA	mA	mA	mA
12 h	1 650	1 625	1 610	1 585
24 h	650	625	610	585
30 h	450	425	410	385
60h	50	25	10	Non disponible

Quantité de courant de la sortie Aux en utilisant deux batteries de 24 Ah (SPC535x/635x)

COMMS	AUCUN	RTC	GSM	RTC+GSM
Durée de veille	mA	mA	mA	mA
12 h	2 205	2 180	2 165	2 140
24 h	1 650	1 625	1 610	1 585
30 h	1 250	1 225	1 210	1 185
60h	450	425	410	385

Quantité de courant de la sortie Aux en utilisant une batterie de 27 Ah (SPC535x/635x)

COMMS	AUCUN	RTC	GSM	RTC+GSM
Durée de veille	mA	mA	mA	mA
12 h	1 900	1 875	1 860	1 835
24 h	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	AUCUN	RTC	GSM	RTC+GSM
Durée de veille	mA	mA	mA	mA
12 h	2 205	2 180	2 165	2 140
24 h	1 900	1 875	1 860	1 835
30 h	1 450	1 425	1 410	1 385
60h	550	525	510	485

« Non disponible » indique que la batterie sélectionnée n'a même pas la capacité nécessaire pour alimenter la centrale SPC pendant la durée de veille voulue. Voir la charge maximale des périphériques et des modules ici [→ 353].



N'utiliser que des batteries à cellule scellée régulée par soupapes.

Pour la conformité aux normes EN, la batterie doit fournir le courant requis pendant la durée de veille requise.

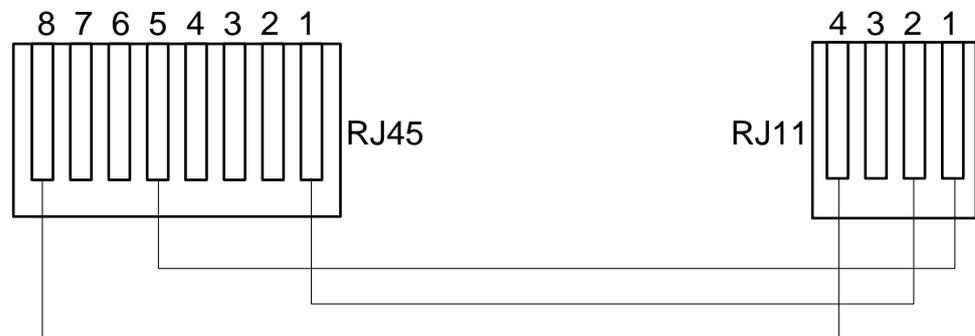
23.5 Paramètres par défaut des modes Simple, Evolué et Bancaire

Ce tableau indique le nom et le type de zone par défaut de la centrale pour chaque mode d'installation. Toutes les zones sur les transpondeurs connectés doivent être

considérées comme inutilisées jusqu'à ce qu'elles soient configurées explicitement par l'installateur.

Fonction	Mode Simple	Mode Evolué	Mode Bancaire
<i>Nom de la zone</i>			
Centrale - 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 devant	INFRAROUGE 1	INFRAROUGE 1
Centrale - Zone 5	Escalier arrière	Infrarouge 2	Infrarouge 2
Centrale - Zone 6	Infrar. couloir	Sortie incendie	Sortie incendie
Centrale - Zone 7	Infrar. réception	Alarme Incendie	Alarme Incendie
Centrale - Zone 8	Bouton panique	Bouton panique	Bouton panique
<i>Type de zone</i>			
Centrale - 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 X-10



Câblage de l'interface X-10 sur la centrale

Code PIN	RJ45	RJ11
TX	8	4
TERRE	5	1
RX	1	2

23.7 Codes SIA

LIBELLÉ	CODE
FIN DEFAULT 230V	AR

LIBELLÉ	CODE
DEFAUT 230V	AT
ALARME INTRUSION	BA
COMMUTATION INTRUSION	BB
ANNULATION D'ALARME	BC
ANOMALIE SWINGER	BD
FIN ANOMALIE SWINGER	BE
FIN ANOMALIE INTRUSION	BJ
FIN D'ALARME INTRUSION	BR
ANOMALIE INTRUSION	BT
ALARME INTRUSION DE-INHIBEE	BU
ALARME INTRUSION VERIFIEE	BV
TEST ALARME INTRUSION	BX
PROBLEME LORS DE LA MES	CD
MES FORCEE	CF
SECTEUR EN SERVICE	CG
ECHEC MES	CI
MES TROP TOT	CK
MES TRANSMISE	FE
MES AUTOMATIQUE	CP
MES A DISTANCE	CQ
MES PAR BOITIER A CLE	CS
MHS TROP TARD	CT
ACCES FERME	DC
ACCES REFUSE	DD
PORTE FORCEE	DF
ACCES AUTORISE	DG
ACCES REFUSE : ANTIPASSBACK	CO
PORTE RESTEE OUV	DN
ACCES OUVERT	DO
FIN D'ALARME PORTE	DR
DEMANDE DE SORTIE	DX
ALARME SORTIE	EA
FIN D'EXTENSION AUTOSURV.	EJ
EXTENSION ABSENTE	EM
FIN EXPANSION ABSENTE	FR
FIN D'ALARME EXTENSIO	ER
AUTOSURV. PÉRIPHÉRIQUE EXTENSION	ES
ANOMALIE EXTENSION	ET
ALARME INCENDIE	FA
COMMUTATION INCENDIE	FB
ANNULATION INCENDIE	FC

LIBELLÉ	CODE
FIN ANOMALIE INCENDIE	FJ
FIN D'ALARME INCENDIE	FR
FIRE TROUBLE	FT
FIRE UNBYPASS	FU
HOLDUP ALARM	HA
HOLDUP BYPASS	HB
HOLDUP TROUBLE RESTORE	HJ
HOLDUP RESTORAL	HR
HOLDUP TROUBLE	HT
HOLDUP UNBYPASS	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
LOCAL PROGRAMMING ENDED	LX
ALARME MEDICALE	MA
MEDICAL BYPASS	MB
MEDICAL TROUBLE RESTORE	MJ
MEDICAL RESTORAL	MR
MEDICAL TROUBLE	MT
MEDICAL UNBYPASS	MU
PÉRIMÉTRIE ARMÉE	NL
FIN LIEN RÉSEAU IP	N°
FIN LIEN RÉSEAU GPRS	N°
ECHEC LIEN RÉSEAU IP	NT
ECHEC LIEN RÉSEAU GPRS	NT
OUVERTURE AUTOMATIQUE	OA
OPEN AREA	OG
MHS TROP TOT	OK
OPENING REPORT	OP
OPENING KEYSWITCH	OS
MES TROP TARD	OT
REMOTE OPENING	OQ
DISARM FROM ALARM	OR
PANIQUE	PA
PANIC BYPASS	PB
PANIC TROUBLE RESTORE	PJ
PANIC RESTORAL	PR

LIBELLÉ	CODE
PANIC TROUBLE	PT
PANIC UNBYPASS	PU
RELAY CLOSE	RC
REMOTE RESET	RN
RELAY OPEN	RO
TEST CYCLIQUE	RP
POWERUP	RR
REMOTE PROGRAM SUCCESS	RS
DATA LOST	RT
MANUAL TEST	RX
AUTOSURVEILLANCE	TA
TAMPER BYPASS	TB
TAMPER RESTORAL	TR
TAMPER UNBYPASS	TU
TEST CALL	TX
UNTYPED ALARM	UA
UNTYPED BYPASS	UB
UNTYPED TROUBLE RESTORE	UJ
UNTYPED RESTORAL	UR
UNTYPED TROUBLE	UT
UNTYPED UNBYPASS	UU
DEFAUT SIRENE	YA
RF INTERFERENCE RESTORAL	XH
RF TAMPER RESTORAL	XJ
LECTEUR VERROUILLÉ	RL
LECTEUR DÉVERROUILLÉ	RG
CLAVIER DÉVERROUILLÉ	KG
BROU.RF	XQ
RF TAMPER	XS
COMMUNICATION FAIL	YC
DÉFAUT CHECKSUM	YF
BELL RESTORED	YH
COMMUNICATION RESTORAL	YK
BATTERIE ABSENTE	YM
PSU TROUBLE	YP
PSU RESTORAL	YQ
FIN DÉFAUT BATTERIE	YR
COMMUNICATION TROUBLE	YS
DÉFAUT BATTERIE	YT
WATCHDOG RESET	YW
SERVICE REQUIRED	YX

LIBELLÉ	CODE
SERVICE EFFECTUÉ	YZ
ÉVÉNEMENTS SIA SPÉCIAUX	
CONTRAINTE	HA
CONTRAINTE UTILISATEUR	HR
ALARME PANIQUE CLAVIER	PA
PANIC RESTORAL	PR
ALARME PANIQUE CLAVIER	PA
ALARME INCENDIE CLAVIER	FA
FIN D'ALARME INCENDIE	FR
ALARME MEDICALE CLAVIER	MA
FIN ALARME MÉDICALE	MR
PTI PANIQUE	PA
PTI TILT	MA
PTI CLIP CEIN	HA
FIN PTI PANIQUE	PR
FIN PTI TILT	MR
FIN PTI CLIP CEIN	HR
WPA PANIQ.	PA
FIN WPA PANIQ.	PR
WPA AGRESS	HA
FIN WPA AGRESS	HR
CHANGER CODE UTILISATEUR	JV
CODE EFFACÉ	
CODES SIA NON STANDARD POUR RAPPORT D'ÉTAT DE ZONE	
ZONE OUVERTE	ZO
ZONE FERMEE	ZC
ZONE COURT-CIRCUIT	ZX
ZONE DISCONT.	ZD
ZONE MASQUÉE	ZM
ZONE DE MARCHE	TP
DÉBUT TEST DE MARCHE	ZK
FIN TEST DE MARCHE	TC
ZONE BATT FAIBLE	XT
ZONE FIN DÉFAUT BATT FAIBLE	XR
AUTRES CODES SIA NON STANDARD	
CAMERA ONLINE	CU
CAMERA OFFLINE	CV
ALERTE FERMÉE	SD
ALERTE RÉOUVERTE	DI
X-BUS ALERTE FERMÉE	NB
XBUS ALERTE RÉOUVERTE	NO

LIBELLÉ	CODE
BADGE INCONNU	AU
ACCÈS UTILISATEUR	JP
FIN D'ACCÈS UTILISATEUR	ZG
BASSE TENSION	XD
RESTORAL BASSE TENSION	XG
CHARGE PROFONDE	XK
VEROUILLE	WW

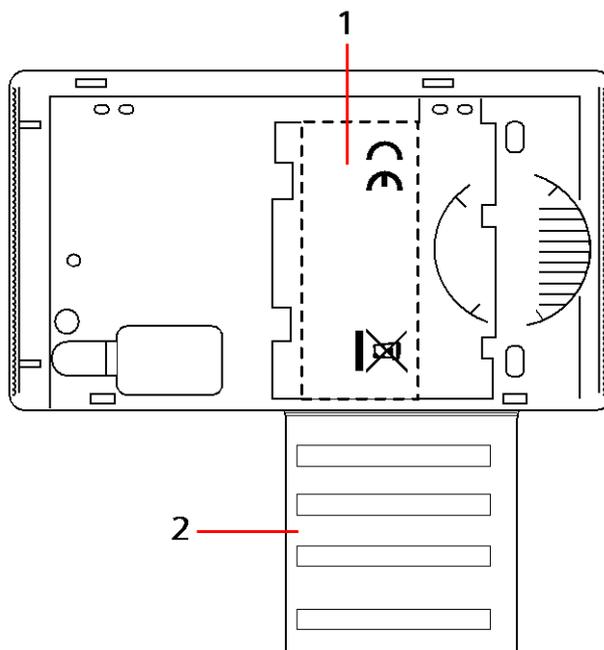
23.8 Codes CID

CODE	EVEN. CID	LIBELLÉ
100	MEDICAL	Alarme et fin d'alarme médicale et homme mort
110	FEU	
120	PANIQUE	
121	CONTRA	
129	AGRESSION CONFIRMÉE	Voir Exigences en matière de configuration pour la conformité avec la PD 6662:2010 [→ 28]
130	INTRUSION	
134	ENTRÉE/SORTIE	
137	AUTOSURVEILLANCE	Défaut et fin de défaut Autosurv. coffret et auxiliaire
139	VERIFIE	Alarme confirmée
144	DETECTEUR AUTOSURV.	Défaut et fin de défaut autosurv. de zone
150	NON INTRUSION	
300	ANOMALIE SYSTEME	Défaut et fin de défaut alim.
301	PERTE AC	Défaut et fin de défaut alim. secteur
302	BATTERIE FAIBLE	
305	RESET	Réinitialisation du système
311	BATTERIE DÉCHARGÉE	Défaut et fin de défaut alim. batterie
312	ALIM. SURCONSOMMATION	Défaut et fin de défaut fusibles alim. internes, externes et auxiliaires
320	BUZZER	Défaut et fin de défaut sirène autosurv.
330	ANOMALIE SYSTEME CENTRALE	Défaut et fin de défaut alim.
333	DEFAUT TRANSPONDEUR	Défaut et fin de défaut câble X-Bus et transp. communications
338	BATT. TRANSP.	Défaut et fin de défaut batterie transp. X-Bus
341	AUTOSURV. TRANSP.	Alarme et fin d'alarme transp. X-Bus et antenne transp. radio
342	230 V TRANSP.	Défaut et fin de défaut nœud secteur. X-Bus
344	BROU.RF	Défaut et fin de défaut brou. RF

351	TELCO 1	Défaut et fin de défaut modem primaire
352	TELCO 2	Défaut et fin de défaut modem secondaire
376	HOLDUP TROUBLE	
380	ANOMALIE DETECTEUR	
401	OUVRIRFERMER	MHS, POST-ALARME ET MES TOTALE
406	ANNUL. D'ALARME	Annulation de l'alarme.
451	OUVRIRFERMER TROP TOT	
452	OUVRIRFERMER TROP TARD	
453	ECHEC MES	MHS trop tard
454	ECHEC MES	MES trop tard
456	EVEN. MES PARTIELLE	MES Partielle A et B
461	CODETRANSP.	User code transp.
466	SERVICE	Mode Installateur DEVALIDE ou VALIDE.
570	BYPASS	Zone inhibée et désinhibée, zone isolée et non isolée
601	MANUAL TEST	Test manuel modem
602	AUTOTEST	Test automatique modem
607	TEST DEPLACEMENT	
613	ZONE DÉPLACEMENT	
614	ZONE INCENDIE DÉPLACEMENT	
615	ZONE PANIQUE DÉPLACEMENT	
625	RESET HEURE	Mise à l'heure

23.9 Vue d'ensemble des types de claviers

Type de clavier	N° de modèle	Fonctions de base	Lecteur de proximité	Audio
Clavier standard	SPCK420	✓	-	-
Clavier avec tag PACE	SPCK421	✓	✓	-
Clavier confort	SPCK620	✓		-
Clavier confort avec audio/CR	SPCK623	✓	✓	✓



Fiche signalétique du clavier SPCK420/421

1	Fiche signalétique 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 prend en charge des codes PIN entre 4 et 8 caractères par utilisateur (code Installateur ou Utilisateur). Le nombre maximum de combinaisons/variations logiques de chaque caractère numérique du code est indiqué dans le tableau ci-dessous.

Nombre de caractères numériques	Nombre de variations	Plus grand code valable
4	10 000	9999
5	100 000	99999
6	1 000 000	999999
7	10 000 000	9999999
8	100 000 000	99999999

La formule permettant de calculer le nombre maximum de combinaisons/variations logiques est la suivante :

$$10^{\text{Nb caractères}} = \text{nombre de variations (y compris le code Installateur ou Utilisateur)}$$

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. Voir Code Ingénieur [→ 110] pour plus d'informations.

23.11 Codes 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 demande 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 (p.ex. 2906, 2907) ne peuvent pas être utilisés, puisqu'un événement « contrainte utilisateur » est déclenché lorsque ce code est tapé sur le clavier.

Après configuration du système pour PIN+1 ou PIN+2 dans Options Système [→ 236] et que des utilisateurs sont activés pour la contrainte (voir Utilisateurs [→ 197]), aucune modification n'est **possible** sauf si tous les utilisateurs sont supprimés et que les codes sont réaffectés.

23.12 Inhibitions automatiques

Le système prend en charge des inhibitions automatiques dans les cas ci-dessous.

23.12.1 Zones

Avec les options Royaume-Uni et évolué activées (voir Normes & Standards [→ 249]), 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 le cycle de mise en surveillance.

23.12.2 Codes PIN d'accès

Pour les systèmes Grade 2: Après 10 tentatives infructueuse de saisie du 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 infructueuse de saisie du 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.

23.12.3 Accès Ingénieur

Un installateur ne peut accéder au système que s'il est autorisé par un utilisateur de type Manager (voir l'attribut « Installateur » de l'onglet Droits utilisateur) et uniquement pour une durée limitée (voir « Accès Installateur » dans Temporisations [→ 245]).

23.12.4 Déconnexion de l'utilisateur clavier

Si le clavier est inutilisé pendant une durée donnée (voir « Temps de saisie clavier » dans Tempos [→ 245]), l'utilisateur est automatiquement déconnecté.

23.13 Raccordement de la centrale au secteur

Conditions requises :

Un dispositif de séparation des circuits, dans un endroit accessible facilement, doit être incorporé au câblage du bâtiment. Il doit être capable de séparer les deux phases en même temps. Les dispositifs acceptés sont les interrupteurs, les coupe-circuits, ou des dispositifs similaires.

- La section minimale des conducteurs utilisés pour le raccordement à l'alimentation est de 1,5 mm carrés.
- Les coupe-circuits doivent avoir une capacité maximale de 16 ampères.

Le câble d'arrivée d'alimentation est attaché sur un coude métallique en V de l'embase au moyen d'un attache-câble, de manière que le coude se trouve entre le câble et l'attache-câble. Assurez-vous que l'attache-câble soit appliqué à l'isolation supplémentaire du câble d'alimentation, c'est-à-dire la chemise extérieure en PVC. L'attache-câble doit être extrêmement bien serré : le câble doit être parfaitement immobilisé en cas de traction sur le câble.

Le conducteur de terre protecteur devrait être monté sur le bornier de façon à ce que si le câble d'arrivée d'alimentation glisse de son ancrage et exerce une tension sur les conducteurs, le conducteur de terre protecteur sera le dernier élément à devoir supporter l'effort.

Le câble d'arrivée d'alimentation doit être homologué et doit être du type HO5 VV-F ou HO5 VVH2-F2.

L'attache-câble (collier serre-câble) en plastique doit répondre au niveau d'inflammabilité V-1.

23.14 Maintenance de la centrale

La maintenance du système doit être effectuée conformément au plan de maintenance établi. Les seules pièces de la centrale pouvant être remplacées sont les fusibles, la batterie de veille et la pile de date et d'heure (sur la carte de circuit imprimé).

Il est recommandé de vérifier les points suivants pour un contrôle de maintenance :

- Vérifier le journal de bord des événements pour savoir si un test de batterie de veille a échoué depuis la dernière maintenance - en cas d'échec des tests de batterie de veille, vérifier la batterie.
- Remplacer la batterie de veille selon le plan de maintenance pour assurer qu'elle ait une capacité suffisante pour alimenter le système pendant la durée configurée. 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.

	AVIS
	La nouvelle batterie devrait avoir la même capacité ou une capacité supérieure (voir la capacité maximale).

- Si le fusible principal déclenche, vérifiez le système pour en trouver la cause. Le fusible doit être remplacé par un fusible ayant les mêmes caractéristiques. Ces caractéristiques sont indiquées sur l'étiquette du système à l'arrière du boîtier.
- La pile bouton lithium pour l'horloge installée sur la carte de circuit intégré est utilisée uniquement quand le système est hors tension. Cette pile a une durée de vie d'environ 5 ans. Effectuez un contrôle visuel de cette pile une fois par an, et mettez le système hors tension pour voir s'il conserve la date et l'heure. Si le système perd la date et l'heure, remplacez la pile par une nouvelle pile bouton lithium type CR1216.
- Vérifier toutes les connexions électriques pour assurer que l'isolation soit en bon état et qu'il n'y ait pas de risque de court-circuit ni de débranchement.
- Il est aussi recommandé de lire les notes de mise à jour du micrologiciel pour savoir si une nouvelle mise à jour améliorant la sécurité du système est disponible.
- Vérifier que les fixations physiques soient intactes. Toute fixation rompue doit être remplacée par une pièce similaire.

23.15 Maintenance du chargeur (Smart PSU)

La maintenance du système doit être effectuée conformément au plan de maintenance établi. Les seules pièces remplaçables du chargeur (Smart PSU) sont les fusibles et la batterie de veille.

Il est recommandé de vérifier les points suivants pour un contrôle de maintenance :

- Vérifier le journal de bord des événements de la centrale pour savoir si un test de batterie de veille a échoué depuis la dernière maintenance - en cas d'échec des tests de batterie de veille, vérifier la batterie.
- Remplacer la batterie de veille selon le plan de maintenance pour assurer qu'elle ait une capacité suffisante pour alimenter le système pendant la durée configurée. 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.

	AVIS
	La nouvelle batterie devrait avoir la même capacité ou une capacité supérieure (voir la capacité maximale).

- Vérifier que les voyants LED de la carte du module d'alimentation ont les états prévus. Pour de plus amples informations, lire la documentation du chargeur.
- Si le fusible principal déclenche, vérifiez le système pour en trouver la cause. Le fusible doit être remplacé par un fusible ayant les mêmes caractéristiques. Ces caractéristiques sont indiquées sur l'étiquette du système à l'arrière du boîtier.
- Vérifier toutes les connexions électriques pour assurer que l'isolation soit en bon état et qu'il n'y ait pas de risque de court-circuit ni de débranchement.

- Il est aussi recommandé de lire les notes de mise à jour du micrologiciel pour savoir si une nouvelle mise à jour améliorant la sécurité du système est disponible.
- Vérifier que les fixations physiques soient intactes. Toute fixation rompue doit être remplacée par une pièce similaire.

23.16 Type 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 gérée 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 attribuée 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 événement Ouvert, Déconnecté, ou Autosurveillance dans n'importe quel mode (sauf si le système est mis hors surveillance) déclenche une alarme totale immédiate. Quand le système est hors surveillance, un événement Autosurveillance est journalisé, ce qui entraîne le message d'alerte AUTOSURVEILLANCE 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 Incendie surveillent la déclaration d'un incendie pendant 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.
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 télémessure. 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 un mode hors surveillance, et une alarme totale dans tous les autres modes.
PANIQUE	Agression	Ce type de zone est actif pendant 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.
HOLDUP / AGRESSION	Agression	Ce type de zone est actif pendant 24 heures sur 24. Il est activé par un bouton. Quand une zone de type Holdup (clavier : 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.
AUTOSURVEILLAN CE	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 : <ul style="list-style-type: none"> ● 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.
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 : <ul style="list-style-type: none"> ● 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.
ARMEMENT PAR CLE	Intrusion	Ce type de zone est normalement utilisé en combinaison avec un mécanisme de verrouillage par clé. Une zone d'armement par clé ACTIVE le système / le secteur / les secteurs communs quand elle est OUVRETE, et DESACTIVE le système / le secteur / les secteurs communs quand elle est FERMEE. <ul style="list-style-type: none"> ● 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 de façon à activer le système sans saisir tout d'abord un code PIN valable sur un périphérique externe.
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. Le type Zone de panne déclenche une sortie de panne. Lorsque le système est armé, une sortie de défaut est déclenchée. À la fois 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 Secteurs [→ 253] 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.
DEFAUT HOLDUP	Défaut	Les zones de panne de holdup sont des zones 24/24, utilisées pour un périphérique de signalisation de holdup, comme une WPA. Le type Zone de panne déclenche une sortie de panne. Lorsque le système est armé, une sortie de défaut est déclenchée. À la fois 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 de panne d'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 panne. Lorsque le système est armé, une sortie de défaut est déclenchée. À la fois 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 l'activation. L'option d'activation doit être sélectionnée pour l'attribut « Autorisation avant MES/MHS » pour le secteur.
ELEMENT DE	Intrusion	En cas d'utilisation d'un élément de verrouillage (écrou) avec un Blockschloss, ce type de zone signale la position de l'élément de

VERROUILLAGE		verrouillage à la centrale (verrouillée ou déverrouillée). Cet écrou verrouille la porte en état activé. Ce signal est contrôlé pendant le processus d'activation. Si l'information « verrouillée » n'est pas reçue, l'activation échoue.
BRIS DE VITRE	Intrusion	<p>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.</p> <ul style="list-style-type: none"> ● Ce type de zone est disponible sur les centrales et les contrôleurs. 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.

23.17 Attributs zone

Dans le système SPC, les attributs de zone déterminent la manière dont les types de zones programmés fonctionnent.

Attribut de zone	Description
Accès	<p>Quand l'attribut ACCES est appliqué à une zone, une alarme n'est pas générée au moment d'ouvrir cette zone tant que la temporisation d'entrée ou de sortie est en cours. Quand le système est en MES totale, l'attribut ACCES n'est pas actif et l'ouverture de la zone déclenche une alarme totale. L'attribut ACCES est le plus souvent utilisé pour les détecteurs PIR installés à proximité d'une zone d'entrée/sortie. Il autorise les déplacements dans le secteur d'accès pendant le compte à rebours de la temporisation d'entrée ou de sortie.</p> <p>L'attribut ACCES est valable uniquement pour les types de zone Alarme.</p> <p>Tous les périphériques connectés (sirènes intérieures et extérieures buzzers, flash) sont actifs.</p> <p>REMARQUE : en mode MES partielle, une zone Alarme avec l'attribut ACCES peut être changée automatiquement en zone Entrée/sortie si l'option Attribut zones accès est active.</p>
Exclus A	<p>Quand l'attribut EXCLUS A est appliqué à une zone, une alarme n'est pas générée par l'ouverture de cette zone pendant que la centrale est en mode MES partielle A. L'attribut EXCLUS A est valable uniquement pour les zones de type Alarme et Entrée/sortie.</p> <p>Une alarme totale est générée au moment de l'ouverture d'une zone ayant l'attribut EXCLUS A si le système est en mode MES totale ou MES partielle B (sirènes intérieures et extérieures, flash).</p>
Exclus B	<p>Quand l'attribut EXCLUS B est appliqué à une zone, une alarme n'est pas générée par l'ouverture de cette zone pendant que la centrale est en mode MES partielle B. L'attribut EXCLUS B est valable uniquement pour les zones de type Alarme et Entrée/sortie.</p> <p>Une alarme totale est générée au moment de l'ouverture d'une zone ayant l'attribut EXCLUS B si le système est en mode MES totale ou MES partielle A.</p>

	(sirènes intérieures et extérieures, flash).
24 Heure	Une zone avec l'attribut 24/24 est active en permanence et déclenche une alarme totale si elle est ouverte indépendamment du mode du système. Cet attribut ne peut être appliqué qu'au type de zone Alarme. Génère une alarme totale dans les modes MHS, MES totale et MES partielle. REMARQUE : l'attribut 24/24 est prioritaire par rapport à tous les autres attributs appliqués à une zone d'alarme particulière.
Locale	Quand l'attribut LOCAL est appliqué, une alarme générée par l'ouverture d'une zone ne déclenche pas la transmission externe de l'événement. L'attribut LOCAL est valable pour les types de zone Alarme, Entrée/sortie, Incendie, Issue de secours et Médical.
MHS locale	Si cet attribut est appliqué, l'alarme générée par l'ouverture de la zone quand le secteur est MES totale ou MES partielle est transmise par la voie habituelle. Cependant, si le secteur est MHS, seule une alarme locale est déclenchée, par exemple le buzzer du clavier, le clignotement d'un voyant et l'affichage de la zone. Cet attribut n'est applicable qu'aux zones Alarme, Incendie et aux zones sismiques.
Double déclenchement	Utilisez cet attribut pour des détecteurs problématiques. Par exemple, certains détecteurs peuvent générer des signaux d'activation parasites, déclenchant ainsi des fausses alarmes dans le système. Une zone avec l'attribut DOUBLE DECLENCHEMENT 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 page [→ 245]). Deux ouvertures pendant ce délai génèrent une alarme. Toutes les zones DOUBLE DECLENCHEMENT ouvertes sont journalisées quand le système est mis en surveillance.
Carillon	Quand l'attribut CARILLON est appliqué à une zone, toute ouverture de cette zone pendant que le système est hors surveillance active les buzzers internes brièvement (env. 2 secondes). L'attribut CARILLON est valable pour les zones de type Alarme, Entrée/sortie, et Technique.
Inhiber	Quand l'attribut INHIBE est appliqué, l'utilisateur peut inhiber cette zone. La fonction Inhiber désactive le défaut ou la zone pour une seule période de MES.
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 sensé être activé si les contacts sont fermés sur le périphérique.
Silencieux	Si l'attribut SILENCIEUX est actif, l'alarme est déclenchée sans indication acoustique ni visuelle. L'alarme est transmise au centre de télésurveillance. Un message d'avertissement est affiché sur l'afficheur quand le système est hors surveillance.
Journal	Si cet attribut est appliqué, tous les changements d'état des zones sont journalisés.
Ouverte en sortie	Si cet attribut est validé, la zone sera affichée si elle est ouverte pendant la MES.
Fréquent	Cet attribut s'applique uniquement à la télémaintenance*. Quand cet attribut est appliqué à une zone, celle-ci doit être ouverte pour la télémaintenance pendant la période définie.
Fin de ligne	L'attribut FIN DE LIGNE permet plusieurs configurations de câblage de zone d'entrée du système.
Analysé	L'attribut ANALYSE doit être appliqué à une zone reliée à un détecteur inertiel. Les paramètres Comptage d'impulsions et Niveau attaque sont à régler pour chaque détecteur inertiel du système en fonction des résultats du calibrage du périphérique.
Comptage d'impulsion	Niveau de déclenchement du comptage d'impulsions pour les détecteurs inertiels analysés.
Attaque	Niveau de déclenchement du niveau d'attaque pour les détecteurs inertiels.

Dernière issue	L'attribut DERNIERE ISSUE ne peut être appliqué qu'au type de zone Entrée/sortie. Utilisez cet attribut pour ignorer le compte à rebours standard du temporisateur de sortie en mode MES totale. Quand tous les autres chemins d'entrée/sortie dans l'immeuble sont fermés, activez la MES totale du système et fermez la dernière zone d'entrée/sortie. Dès que la porte est fermée, le compte à rebours du délai Tempo dernière issue commence avant d'activer le système.
Shunt	Quand l'attribut SHUNT est appliqué à une zone, celle-ci est inhibée chaque fois qu'une zone de type Shunt est ouverte. Cet attribut fournit un mécanisme pour former un groupe de zones inhibées simultanément au moment où quelqu'un ouvre une zone de type Shunt.
Transmission seule	Cet attribut s'applique uniquement au type de zone Incendie. Quand il est appliqué à une zone, l'activation de la zone Incendie déclenche uniquement la transmission de l'événement au centre de télésurveillance. Aucune alarme n'est générée sur le site.
Seulement ouvert	Cet attribut s'applique uniquement au type de zone ARMEMENT PAR CLE. Si l'attribut SEULEMENT OUVERT (clavier : OUVERTURE SEULE) est appliqué, l'état d'armement de l'immeuble alterne chaque fois qu'on l'ouvre. (Voir la description du type de zone Armement par clé).
Mise en surveillance possible	Cet attribut s'applique uniquement au type de zone ARMEMENT PAR CLE. Si l'attribut MISE EN SURVEILLANCE POSSIBLE (clavier: MHS TOTALE ACTIV) est appliqué, l'activation de la zone met le système/secteur en surveillance totale. Sélectionnez cet attribut si vous voulez que l'utilisateur ne puisse mettre le système en MES TOTALE que s'il se trouve dans une zone d'armement par clé.
Mise hors surveillance possible	Cet attribut s'applique uniquement au type de zone ARMEMENT PAR CLE. Si cet attribut est appliqué, l'activation de la zone met le système/secteur hors surveillance. Sélectionnez cet attribut si vous voulez que l'utilisateur ne puisse désactiver le système que s'il se trouve dans une zone d'armement par clé.
Zone technique Transmis	Cet attribut permet de transmettre une alarme au CTS en FF, CID, SIA et SIA étendu quand une zone est ouverte, indépendamment du mode du système. Quand des secteurs sont sélectionnés, l'alarme est transmise uniquement au CTS auquel le secteur est attribué. Le code transmis serait UA (Unknown Alarm, alarme inconnue) suivi du numéro de zone (et suivi du texte si SIA étendu est sélectionné). Un SMS est également envoyé à l'utilisateur et à l'installateur si cette option est active quand le filtre d'alarme non confirmée est sélectionné.
Zone technique Affichage	Sert à afficher l'ouverture de la zone sur l'afficheur du clavier. Le voyant LED d'alerte s'allume également. Quand des secteurs sont sélectionnés, l'ouverture est affichée seulement sur le clavier attribué au secteur comprenant la zone sélectionnée. L'alerte n'est affichée sur le clavier que si le secteur est désactivé (pas en mode MES partielle A, MES partielle B, ni MES totale).
Zone technique Audible	Permet d'activer le buzzer dans une zone activée. Le principe de fonctionnement est le même que pour Zone technique Affichage dans les différents modes de surveillance et sur des systèmes avec des secteurs.
Zone technique Délai	Indique qu'un délai programmable est appliqué à la zone. Ce délai est compris entre 0 et 9999 secondes (inclus) et s'applique à toutes les zones techniques. Le principe de fonctionnement est le même que pour le temporisateur Tempo défaut 230V : 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 déclenche pas avant la fin de la temporisation.
Transmis quand sous surveillance	Les ouvertures ne sont transmises que si le système est activé.
Pré-alarme incendie	Si cette option est activée et qu'une alarme incendie suit, la temporisation de pré-alarme incendie démarre et les sirènes intérieures et les buzzers sont activés. (Voir Temporisations [→ 245].) Si l'alarme n'est pas annulée avant la fin de la temporisation, l'alarme incendie est confirmée, les sirènes internes et externes sont déclenchées et un événement est signalé au CTS.

Confirmation incendie	Si activée, une temporisation de confirmation d'incendie est mise en œuvre ce qui allonge la durée de la pré-alarme incendie jusqu'à ce que une alarme d'incendie soit signalée pour la zone. Voir Temporisations [→ 245].
Test sismique/Test automatique du détecteur	Un type de zone sismique peut être testé manuellement ou automatiquement. Cet attribut permet l'activation du test automatique. Consultez la section sur les temporisations [→ 245] 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 est fixée à 7 jours.
Temporisée	L'attribut Temporisée différé sert à armer par clé les zones pour retarder la configuration d'un secteur. Le retard suit la temporisation de sortie du secteur auquel la clé de MES est associée.
Vérification	Sélectionnez la zone de vérification configurée à assigner à cette zone pour le déclenchement de la vérification 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 par types de zone

Le tableau ci-dessous indique les attributs applicables par type de zone :

Zone Type	Alarm	Entry/Exit	Exit Term	Fire	Fire Exit	Line	Panic	Holdup	Tamper	Tech	Medical	Keyarm	Unused	Shunt	X-Shunt	Detector Fault	Lock	Subexcision	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 conjonction avec la télémaintenance.

** 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 devrait 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. Cet erreur sera traité comme les autres erreurs du système.

Surveillance du RTC (SPCN110) et du GSM (SPCN310)

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 GSM 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	IB41-EM
PR500-EM	IB42-EM
SP500-EM	IB44-EM
PM500-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
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	Carte max n° 9999999999
COTAG	Non	Carte max n° 9999999999

Format Lecteur	Code du site disponible	Restrictions
Wiegand 26 bits	Oui	Code site max. 255 N° max. de cartes 65535
Wiegand 36 bits	Oui	Code site maxi 32767 Carte max n° 524287
HID Corporate 1000	Oui	Code site maxi 4095 Carte max n° 1048575
HID 37	Non	Carte max n° 34359738370
HID 37F	Oui	Code site max. 65535 Carte max n° 5242875
HID 37BCD	Non	Carte max n° 99999999
HID ICLASS MIFARE	Non	Carte max n° 4294967295
HID ICLASS DESFIRE	Non	Numéro de badge chiffré. Carte max n° 72×10^{16} . Ce numéro doit être reconnu par la centrale.
AR618 WIE BCD 52 BIT	Non	Carte max n° 4294967295
AR618 OMRON 80 BIT	Non	Carte max n° 99999999999999

23.21 Support SPC pour périphériques E-Bus

La passerelle E-Bus SPC (SPCG310) est un transpondeur X-BUS permettant la communication entre une centrale 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 ceci en compte, il peut s'avérer nécessaire d'effectuer un réadressage du périphérique E-BUS. Pour de plus amples informations, consultez la section MODE ADRESSAGE [→ 138].

!	AVIS
	Avant d'installer ce périphérique, Vanderbilt vous recommande de lire le document Sintony System Migration (Migration du système Sintony).

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
- Transpondeurs d'entrée Sintony
- Transpondeurs de sortie Sintony
- Sintony ALIM : SAP 8, SAP 14, SAP 20 et SAP 25

1. Dans le navigateur, aller à **Paramètres - X-BUS - Transpondeurs**.
⇒ La liste des **Transpondeurs configurés** s'affiche.
2. Sélectionner un **SPC E-Bus Gateway**.
3. Dans la fenêtre **Configuration Transpondeur**, saisir une **description** pour le **SPC E-Bus Gateway**. Pour un complément d'information à propos de la configuration des transpondeurs, voir la section Transpondeurs [→ 220].

4. Pour adresser un périphérique E-Bus, sélectionner une adresse dans la liste déroulante décrit 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. » affiché en haut de l'écran.
 - ⇒ 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. Aller à **Paramètres - X-BUS - Transpondeurs**.
8. Cliquer sur le bouton **Reconfigurer**.
 - ⇒ Le message « Reconfiguration terminée » s'affiche en haut de l'écran. 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 configuré**.
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**, consulter les Transpondeurs d'adressage pour SAP 8, SAP 14 et SAP 20 [→ 379].
10. Si le X-Bus a des conflits d'adressage, le message d'avertissement **ID Invalide ou déjà utilisée comme IDx Transpondeur** s'affiche. Répéter les étapes précédentes jusqu'à l'élimination des conflits d'adressage.

Périphérique E-Bus : Menu déroulant	Description	Format d'adresse	Adressage
Clavier	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	Adresse E-BUS (ID X-BUS)	Maintenir enfoncé le

	transpondeurs d'entrée Sintony		bouton d'adressage pendant 5 secondes et le relâcher pour entendre le bip continu.
Sortie	ID à assigner aux transpondeurs de sortie Sintony	Adresse E-BUS (ID X-BUS)	Maintenir enfoncé le bouton d'adressage pendant 5 secondes et le relâcher pour entendre le Gateway E-BUS pour SPC émettre un bip continu.
ALIM	ID assignables aux périphériques ALIM Sintony SAP 8, SAP 14, SAP 20 et SAP 25	E-BUS ID (X-BUS ID des transpondeurs associés)	Maintenir enfoncé le bouton d'adressage jusqu'à entendre le Gateway E-BUS pour SPC émettre un bip continu.

Voir aussi

 MODE ADRESSAGE [→ 138]

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 [→ 377], pour assigner un transpondeur d'entrée à l'ALIM. Cela simule une communication avec la centrale SPC via transpondeur.

1. Sur la liste **Transpondeurs configurés**, sélectionner le **Gateway E-BUS pour SPC**.
⇒ La fenêtre **Configuration Transpondeur** s'affiche.
2. Consulter la nouvelle adresse ALIM dans la liste déroulante.
⇒ Un point d'exclamation précède l'adresse ALIM que vous avez assigné au périphérique. Cela indique qu'un transpondeur d'entrée est disponible pour être assigné à l'ALIM.
3. Prendre note du 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. Aller à **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 à la section Configuration et adressage des périphériques E-Bus [→ 377]. 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.

!	AVIS
	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	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 (exposition automatique) 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	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	ATE - Équipement de Transmission d'Alarme Terme collectif désignant l'ATE, le MCT (Monitoring Centre Transceiver) et le frontal de réception des alarmes.	-
ATP	ATP - Chemin de transmission d'alarmes 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)	Un chemin défini entre la centrale SPC et le SPC Com XT. C'est à dire qu'un système utilisant Ethernet comme chemin principal et GPRS comme chemin de secours aura deux ATP différents au sein de l'ATS.

	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.	
ATS	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'alarmes (AS) vers un ou plusieurs récepteurs d'alarme (AE). 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 Frontal de réception d'alarme (ATE) relié à un ou plusieurs postes opérateurs (AE) via une serveur d'alarme et relié à un ou plusieurs réseau 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 réseau 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 sur le réseau téléphonique, c'est à dire 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
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
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
Fichier de Commandes	Met à jour le firmware de la centrale
	Met à jour le firmware des périphériques
	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 des ATS décrits dans la norme EN50136-1 et précise comment FlexC respecte ces dispositions dans les catégories SP1-SP6 et DP1-DP4.

		Tempos requis par EN50136-1				FlexC - Implémentation des tempos pour les différentes catégories d'ATS			
Catégorie 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	-	-
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 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. C'est-à-dire que les interrogations Cat 3 [Modem] interviennent toutes les 25 mn, puis toutes les 60 s pendant 5 mn pendant un maximum de 30 mn. Pour une vue d'ensemble de l'intervalle de polling configuré, allez à **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**.

<i>Catégories de sécurité - Ethernet</i>		Polling quand le chemin est actif			Polling quand le Chemin est inactif			Polling quand le Chemin est tombé	
Catégorie du Chemin	Événement Timeout	Intervalles des pollings	Intervalle de tentative	Timeout des pollings	Intervalles des pollings	Intervalle de tentative	Timeout des pollings	Polling Intervalle	Timeout
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
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
<i>Catégorie de sécurité - Modem</i>									
Cat 5 [Modem]	30 s	10 s	30 s	90 s	4 h	2 mn	4 h 10	10 mn	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 mn	25 h	30 Jours	10 mn	30 jours 1 h	7 jours	90 s

Edité par
Vanderbilt

Clonshaugh Business and Technology Park
Clonshaugh
Dublin
D17 KV84
www.service.vanderbiltindustries.com

© 2016 Copyright Vanderbilt
Sous réserve de disponibilité et de modifications techniques.