Module de communication TCP/IP

ETHM-1

Version de programme 1.05

ethm1_fr 03/13

SATEL sp. z o.o.
ul. Schuberta 79
80-172 Gdańsk
POLOGNE
tél. +48 58 320 94 00
info@satel.pl
www.satel.eu

AVERTISSEMENT

Le système d'alarme doit être installé par un personnel qualifié.

Avant de procéder à l'installation, veuillez lire soigneusement la notice.

Toute modification de la construction des dispositifs et les réparations effectuées sans l'accord préalable du fabricant donnent lieu à la perte des droits de garantie.

La société SATEL a pour objectif d'améliorer continuellement la qualité de ses produits ce qui peut entraîner des modifications de leurs spécifications techniques et des logiciels. L'information actuelle sur les modifications apportées est disponible sur notre site.
Veuillez visiter notre site:
http://www.satel.eu

La déclaration de conformité peut être consultée sur le site www.satel.eu/ce

Les symboles suivants utilisés dans la présente notice :

 - note ;

 - avertissement.

1 Introduction

Le module ETHM-1 permet la communication via réseau Ethernet aux centrales d'alarme INTEGRA, INTEGRA Plus et VERSA. La transmission des données est codée à l'aide d'un algorithme avancé basé sur la clé de 192 bits.

Pour mettre à jour le logiciel du module, l'application correspondante est disponible sur le site www.satel.eu.

2 Utilisations

- Configuration de la centrale d'alarme à l'aide du logiciel DLOADX depuis un ordinateur disposant de l'accès à Internet.

  Fonction disponible pour les centrales : INTEGRA Plus et INTEGRA (version du logiciel 1.03 ou ultérieure) et VERSA (version du logiciel 1.01 ou ultérieure).

- Gestion du système d'alarme à l'aide du logiciel à l'aide du logiciel GUARDX depuis un ordinateur disposant de l'accès à Internet.

  Fonction disponible pour les centrales: INTEGRA Plus et INTEGRA (version du logiciel 1.03 ou ultérieure).

- Gestion et configuration de la centrale d'alarme à l'aide du navigateur Web utilisant les applications JAVA.

  Fonction disponible pour les centrales: INTEGRA Plus et INTEGRA (version du logiciel 1.03 ou ultérieure).

- Gestion et configuration de la centrale d'alarme à l'aide de l'application MOBILEKPD / MOBILEKPD2 depuis un téléphone mobile disposant de l'accès à Internet. L'appareil peut servir d'un clavier supplémentaire du système d'alarme.

  Fonction disponible pour les centrales: INTEGRA Plus et INTEGRA (version du logiciel 1.03 ou ultérieure).

L'application MOBILEKPD2 peut être installée sur différents dispositifs mobiles sous le système d'exploitation Android, iOS ou autre qui gère l'application Java.

- Transmission des événements depuis la centrale d'alarme à la station de télésurveillance via réseau Ethernet (TCP/IP), grâce à quoi, les coûts de télésurveillance peuvent être considérablement réduits.

  Fonction disponible pour les centrales : INTEGRA Plus, INTEGRA (version du logiciel 1.04 ou ultérieure) et VERSA (version du logiciel 1.01 ou ultérieure).

- Intégration de la centrale d'alarme avec d'autres systèmes grâce au protocole de communication basé sur open-source via le réseau Ethernet (TCP/IP). Cette application est dédiée aux sociétés traitant l'intégration des systèmes orientés objet et exige le développement de leur propre logiciel.

  Fonction disponible pour les centrales: INTEGRA Plus et INTEGRA (version du logiciel 1.06 ou ultérieure).

Pour plus d'informations sur le protocole de communication open-source, veuillez consulter le site www.satel.eu.

3 Carte électronique

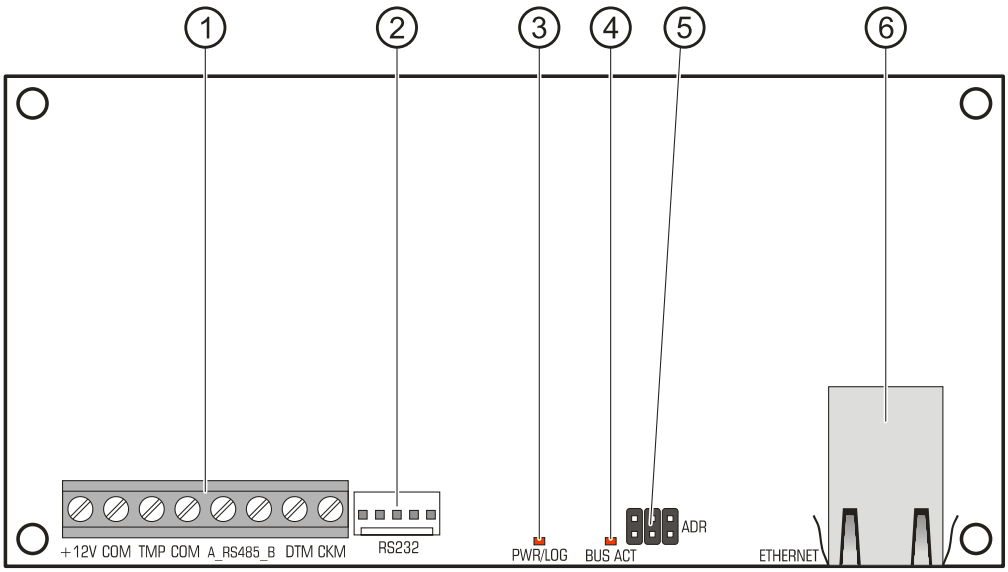

Fig. 1. Carte électronique du module.

(1) bornes :

+12V - entrée d'alimentation (+12 V DC).

COM - masse.

TMP - entrée du circuit d'autoprotection du module (NC). Si non utilisée, elle doit être court-circuitée à la masse.

A_RS485_B - bornes non utilisées.

DTM - données (bus de communication).

CKM - horloge (bus de communication).

(2) port RS-232.

(3) voyant LED PWR/LOG :

– allumé – alimentation en cours ;

– clignotant – la centrale est programmée ou exploitée au moyen du module.

(4) voyant LED BUS ACT clignote lorsque l'échange de données avec la centrale est en cours.

(5) broches ADR pour le réglage de l'adresse du module (voir : REGLAGE DE L'ADRESSE).

(6) prise pour connecter le module au réseau Ethernet (TCP/IP). La prise dispose de deux LED intégrés. Le vert indique la connexion au réseau et le transfert de données, et le jaune – la vitesse de transmission négociée (allumé : 100 Mb; éteint : 10 Mb).

4 Installation et démarrage

Mettre le système d'alarme hors tension avant d'effectuer tous raccordements électriques.

Le dispositif est conçu pour être utilisé dans les réseaux locaux (LAN). Il ne peut pas être connecté directement au réseau informatique public (MAN, WAN).

Le raccordement au réseau public ne peut être effectué que via un routeur ou un modem xDSL.

Le module est destiné à fonctionner dans les locaux fermés à une humidité normale d'air.

1. Régler l'adresse du module (voir : REGLAGE DE L'ADRESSE).
2. Installer le module dans le boitier. Si la centrale d'alarme est configurée via Ethernet (TCP/IP) à l'aide du logiciel DLOADX, utiliser le même boitier pour le module et la centrale.
3. Raccorder les bornes du module aux bornes de la centrale d'alarme selon le tableau 1 (pour alimenter le module, une autre sortie d'alimentation peut être utilisée). Pour effectuer des raccordements, utiliser un câble droit non blindé. Si le câble de type « paire torsadée » est utilisé, ne pas oublier que les signaux CK (horloge) et DT (données) ne peuvent être envoyés par une paire de fils torsadés.

ETHM-1	INTEGRA	VERSA
+12V	+KPD	KPD
COM	COM	COM
DTM	DTM	DTA
CKM	CKM	CLK

Tableau 1.

4. Brancher le contact d'autoprotection du boitier aux bornes TMP et COM (ou court-circuiter la borne TMP à la borne COM).
5. Connecter le module au réseau. Utiliser un câble compatible avec le standard 100Base TX (identique à celui utilisé pour raccorder l'ordinateur au réseau).
6. Si la centrale d'alarme est configurée via Ethernet (TCP/IP) à l'aide du logiciel DLOADX, relier le port RS-232 du module avec le port RS-232 de la centrale. En fonction de la centrale d'alarme, la connexion doit être faite à l'aide des câbles suivants (offerts par la société SATEL) :

   INTEGRA avec la prise type PIN5 : **PIN5/PIN5** (voir : fig. 2)

   INTEGRA avec la prise type RJ / INTEGRA Plus : **RJ/PIN5** (voir : fig. 3)

   VERSA : **PIN5/RJ-TTL**

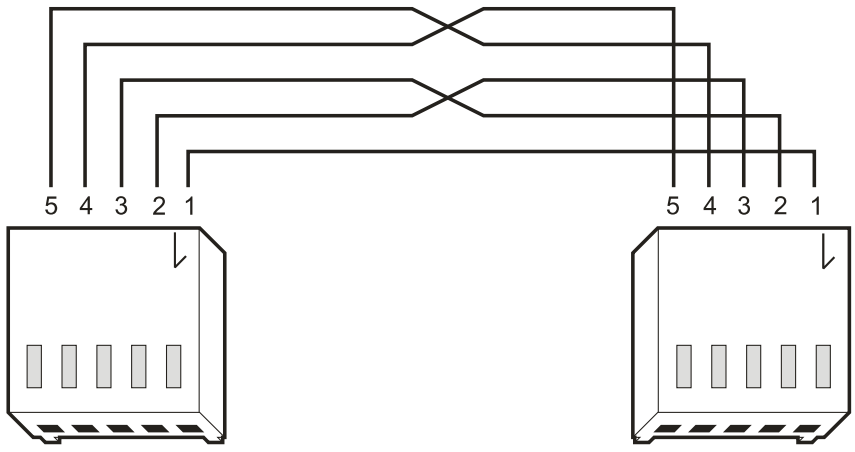

Fig. 2. Schéma du câblage pour le raccordement aux ports RS-232 du module ETHM-1 et de la centrale INTEGRA avec la prise PIN5.

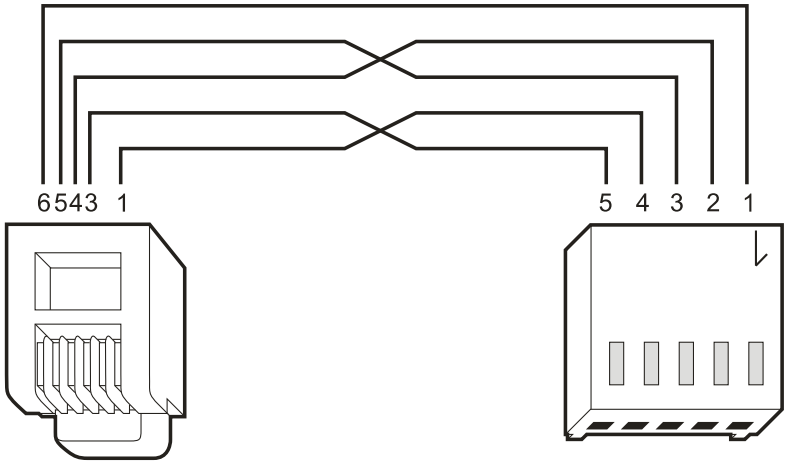

Fig. 3. Schéma du câblage pour le raccordement aux ports RS-232 du module ETHM-1 et de la centrale INTEGRA / INTEGRA Plus avec la prise type RJ.

7. Mettre le système sous tension.
8. Activer la fonction d'identification des dispositifs dans la centrale (voir : notice d'installation de la centrale correspondante).

4.1 Réglage de l'adresse

L'adresse est réglée à l'aide des cavaliers placés sur les broches ADR. Le tableau 2 représente le mode de placer des cavaliers pour le réglage de l'adresse (▮ - cavalier placé ; ⋮ - cavalier enlevé).

Adresse	0	1	2	3	4	5	6	7
Etat de broches	⋮⋮⋮	▮⋮⋮	⋮▮⋮	▮▮⋮	⋮⋮▮	▮⋮▮	⋮▮▮	▮▮▮

Tableau 2.

4.1.1 Fonctionnement avec la centrale INTEGRA / INTEGRA Plus

Régler l'adresse de 0 à 3 (INTEGRA 24 / INTEGRA 32) ou de 0 à 7 (INTEGRA 64 / INTEGRA 128 / INTEGRA 64 Plus / INTEGRA 128 Plus). L'adresse réglée doit être différente de celles d'autres dispositifs reliés au bus de claviers de la centrale d'alarme (les dispositifs possédant les adresses identiques ne sont pas gérés par la centrale).

4.1.2 Fonctionnement avec la centrale VERSA

L'adresse 4 doit être réglée dans le module. Le clavier à l'adresse 4 ne peut pas être connecté à la centrale.

5 Programmation

La programmation se fait via la centrale d'alarme à l'aide du clavier ou de l'ordinateur disposant le logiciel DLOADX installé.

5.1 Réglages du module

Les réglages du module peuvent être configurés comme suit :

- module connecté à la centrale INTEGRA / INTEGRA Plus :
  - clavier : ▶MODE SERVICE ▶STRUCTURE ▶MATERIEL ▶CLAVIERS ▶REGLAGES ▶[sélectionner le module dans la liste de dispositifs] ;
  - logiciel DLOADX : →fenêtre « Structure » →onglet « Matériel » →branche « Claviers » →[cliquer sur le modules dans la liste de dispositifs] (voir : fig. 4).
- module connecté à la centrale VERSA :
  - clavier : ▶MODE SERVICE ▶STRUCTURE ▶MATERIEL ▶CLAV. ET MOD. D'EXT. ▶2. REGLAGES ▶[sélectionner le module dans la liste de dispositifs] ;
  - logiciel DLOADX : →fenêtre « Versa – Structure » →onglet « Matériel » →[cliquer sur le modules dans la liste de dispositifs] (voir : fig. 5).

5.1.1 Paramètres et options

Les noms des paramètres et des options disponibles seulement en cas de connexion du module aux centrales INTEGRA ou INTEGRA Plus sont indiqués en blanc sur fond noir.

Entre crochets sont présentés les noms des paramètres et des options affichés sur l'écran du clavier du système d'alarme INTEGRA / INTEGRA Plus.

Nom – nom individuel du dispositif (jusqu'à 16 caractères).

Sabotage signalé dans la partition – la partition dans laquelle l'alarme se déclenche en cas de de sabotage du module.

Obtenir une adresse IP automatiquement (DHCP)] – si cette option est activée, le module va automatiquement télécharger les données relatives à l'adresse IP, du masque de sous-réseau et de la porte depuis le serveur DHPC (dans ce cas, ces paramètres ne sont pas programmables).

L'adresse IP attribuée au module peut être lue dans le clavier LCD à l'aide de la fonction utilisateur disponible dans le sous-menu TESTS :

*INTEGRA / INTEGRA Plus: **IP/MAC ETHM-1** ;*

*VERSA: **VER. MODULES** (Pour une description détaillée de la fonction, se référer à la notice utilisateur de la centrale d'alarme).*

Si le module est raccordé à la centrale INTEGRA / INTEGRA Plus, l'adresse IP peut être lue dans le logiciel DLOADX (elle est indiquée au-dessous des paramètres du module – voir : fig. 4).

Le module doit avoir une adresse publique permanente, si la communication avec la centrale d'alarme est possible à établir de l'extérieur du réseau local.

Adresse IP du serveur – l'adresse IP du module.

Masque de sous-réseau – le masque de sous-réseau dans laquelle le module fonctionne.

Porte – l'adresse IP du dispositif réseau à travers laquelle d'autres dispositifs du réseau local communiquent avec les dispositifs d'autres réseaux.

Obtenir automatiquement l'adresse du serveur DNS [Utiliser DHCP-DNS] – si cette option est activée, le module va automatiquement télécharger l'adresse IP depuis le serveur DNS. L'option est disponible, si l'option OBTENIR AUTOMATIQUEMENT L'ADRESSE IP (DHCP) est activée.

Serveur DNS – l'adresse IP du serveur DNS que le module va utiliser. Elle peut être programmée, si 'option OBTENIR AUTOMATIQUEMENT L'ADRESSE DNS est désactivée.

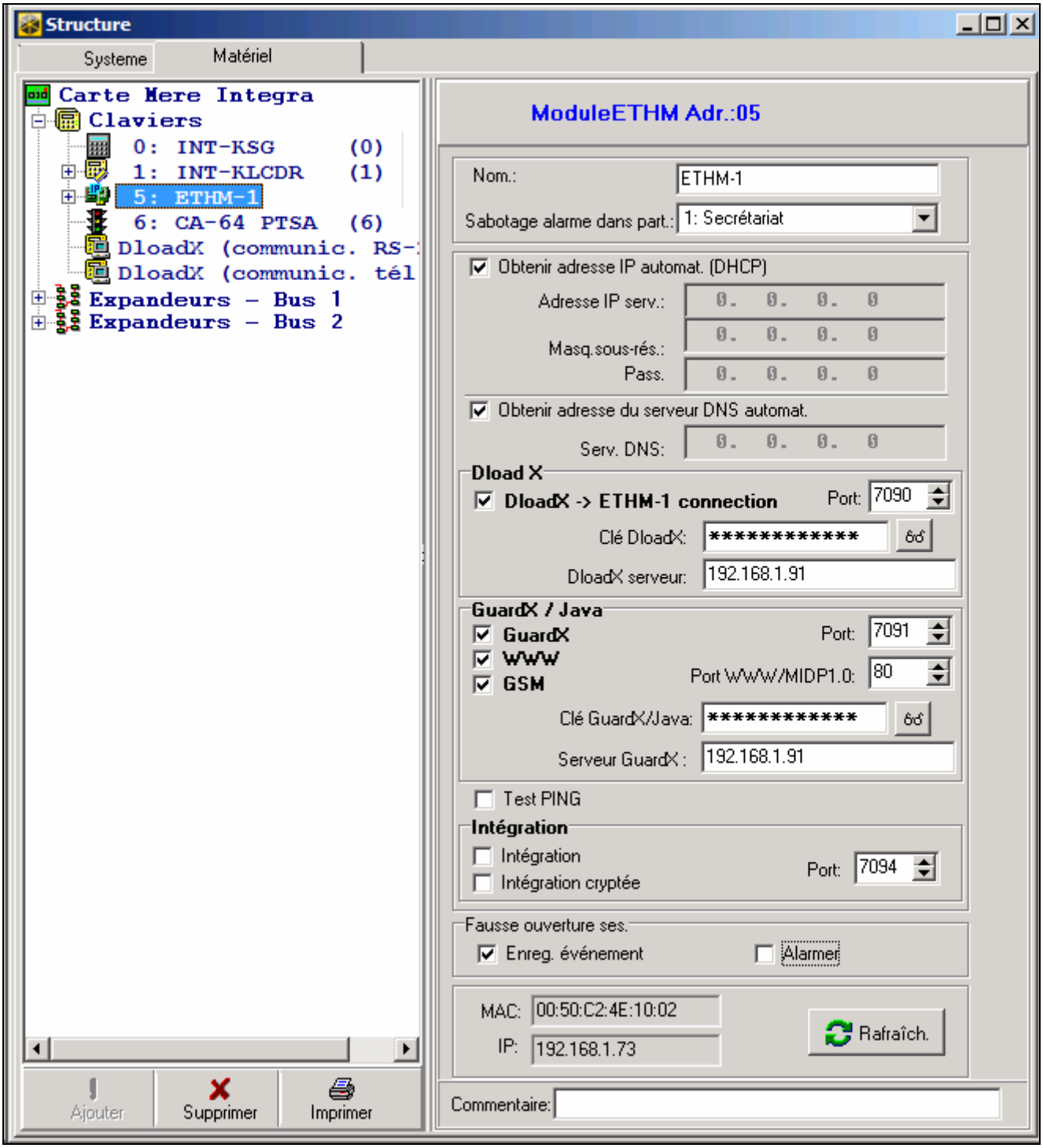

Fig. 4. Logiciel DLOADX : réglages du module ETHM-1 connecté à la centrale INTEGRA.

DLOADX

Communication DloadX->ETHM [Avec DloadX] – si l'option est activée, la communication avec la centrale d'alarme peut être lancée via le réseau TCP / IP depuis le logiciel DLOADX.

Port [Port DloadX] – **Port DLOADX** – le numéro du port utilisée pour la communication avec le logiciel DLOADX. Les valeurs de 1 à 65535 peuvent être saisies. La valeur doit être différente de celle indiquée pour les autres ports. Par défaut : 7090.

Clé DloadX – la séquence de 1 à 12 caractères alphanumériques (chiffres, lettres et caractères spéciaux) pour définir la clé servant à coder des données pendant la communication avec le logiciel DLOADX.

DLOADX serveur [Adresse DloadX] – l'adresse de l'ordinateur disposant du logiciel DLOADX. Cette adresse doit être une adresse publique à moins que l'ordinateur soit inclus dans le même réseau local. L'adresse IP ou le nom de domaine peuvent être entrés.

Dans le clavier du système INTEGRA / INTEGRA Plus, la fonction pour programmer l'adresse de l'ordinateur avec le logiciel DLOADX est incluse dans le menu utilisateur dans le sous-menu MODIFIER L'OPTION (accessible au service et aux administrateurs).

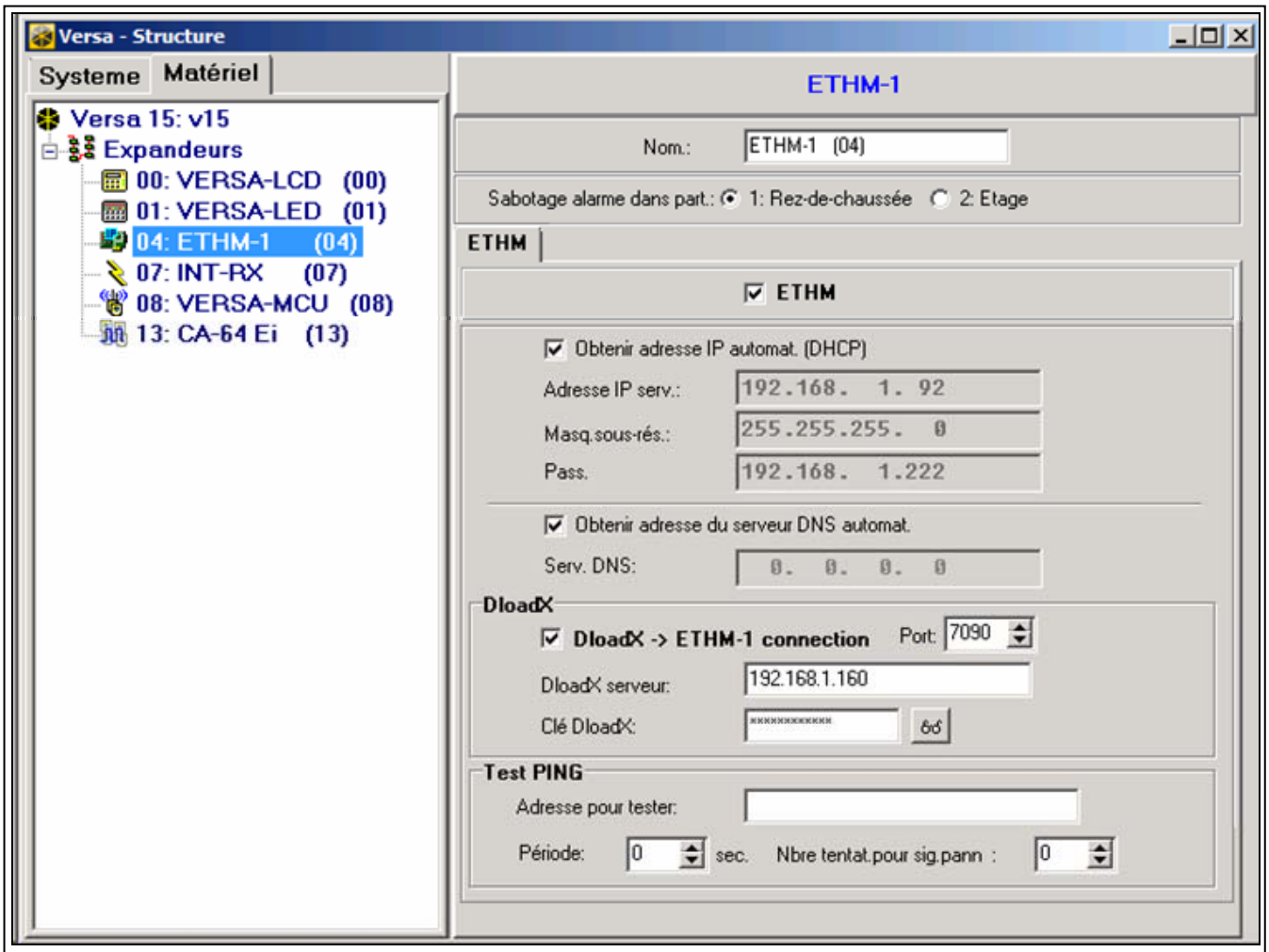

Fig. 5. Logiciel DLOADX : réglages du module ETHM-1 connecté à la centrale VERSA.

GuardX / Java

GuardX [par GuardX] – si l'option est activée, la connexion avec la centrale d'alarme peut être lancée via le réseau TCP / IP depuis le logiciel GUARDX.

WWW [par Internet] – si l'option est activée, la connexion avec la centrale d'alarme peut être lancée via le réseau TCP / IP depuis le navigateur WWW.

GSM [par GSM] – si l'option est activée, la connexion avec la centrale d'alarme peut être lancée via le réseau TCP / IP à l'aide de l'application MOBILEKPD / MOBILEKPD2.

Port [Port autres] – numéro du port TCP utilisé à la communication avec :

- le logiciel GUARDX ;
- l'application JAVA dans le navigateur web ;
- l'application MOBILEKPD dans le téléphone mobile utilisant MIDP2.0 ;

– l'application MOBILEKPD2.

Les valeurs de 1 à 65535 peuvent être saisies. La valeur doit être différente de celle indiquée pour les autres ports. Par défaut: 7091.

Port WWW/MIDP1.0 [Port WWW] – le numéro du port TCP utilisé pour la communication avec :

– le navigateur web ;

– l'application MOBILEKPD dans le téléphone mobile gérant le standard MIDP1.0.

Les valeurs de 1 à 65535 peuvent être saisies. La valeur doit être différente de celle indiquée pour les autres ports. Par défaut : 80.

Clé GuardX/Java [Clé autres] – la séquence de 1 à 12 caractères alphanumériques (chiffres, lettres et caractères spéciaux) pour définir la clé servant à coder des données pendant la communication avec :

– le logiciel GUARDX ;

– l'application JAVA dans le navigateur web ;

– l'application MOBILEKPD / MOBILEKPD2 dans le téléphone mobile.

GuardX serveur [Adresse GuardX] – l'adresse de l'ordinateur disposant du logiciel GUARDX. Cette adresse doit être une adresse publique à moins que l'ordinateur soit inclus dans le même réseau local. L'adresse IP ou le nom de domaine peuvent être entrés.

Dans le clavier du système INTEGRA / INTEGRA Plus, la fonction pour programmer l'adresse de l'ordinateur avec le logiciel GUARDX est incluse dans le menu utilisateur dans le sous-menu MODIFIER L'OPTION (accessible au service et aux administrateurs).

Test PING

Test PING – si l'option est activée, le module peut tester la communication à l'aide de la commande envoyée au dispositif de réseau indiqué.

Adresse à tester [Adresse] – l'adresse du dispositif auquel une commande ping pour tester la communication doit être envoyée par le module. L'adresse IP ou le nom de domaine peuvent être entrés.

Période [Période du test] – l'intervalle de temps entre les tests de communication successifs à l'aide de la commande ping. La programmation de la valeur 0 désactive le test de communication.

Nombre d'essais avant la panne [Nombre d'essais] – le nombre de tests de communication échoués (le module n'a pas reçu de réponse à la commande ping envoyé) après lequel la panne sera signalée. La programmation de la valeur 0 désactive le test de communication.

Si le module est relié au panneau de contrôle de VERSA, le test à l'aide de la commande ping sera effectuée après l'entrée de l'adresse à tester, l'indication de la période du test (la valeur doit être différente de 0) et la définition des règles de signalisation de la panne (la valeur doit être différente de 0).

Si le module est relié au panneau de contrôle plus INTEGRA / INTEGRA, seule l'option de TEST PING est disponible dans les paramètres du module. Les autres paramètres sont globaux (ils s'appliquent à tous les modules ETHM-1 modules connectés à la centrale d'alarme) et peuvent être programmés :

– *clavier : à l'aide des fonctions disponibles au sous-menu TEST PING (▶MODE SERVICE ▶OPTIONS ▶TEST PING) ;*

– *logiciel DLOADX : cliquer sur le bus de claviers (→fenêtre « Structure » →onglet « Matériel » →branche « Claviers »).*

Intégration

Intégration – si l'option est activée, le module peut être utilisé pour l'intégration de la centrale d'alarme aux autres systèmes.

Intégration cryptée [Int. cryptée] – si l'option est activée, la communication avec d'autres systèmes est cryptée.

i *La clé de cryptage peut être programmée :*

- *clavier : à l'aide de la fonction CLE INTEGRATION. (▶MODE SERVICE ▶OPTIONS ▶CLE INTEGRATION) ;*
- *logiciel DLOADX : onglet « Service » (→fenêtre « Options » →onglet « Service »).*

Port [Port d'intégration] – numéro du port TCP utilisé pour l'intégration. Les valeurs de 1 à 65535 peuvent être saisies. La valeur doit être différente de celle indiquée pour les autres ports. Par défaut: 7094.

Connexion incorrecte

Enregistrer l'événement [Effr. – évén.] – si l'option est activée, chaque tentative non autorisée de se connecter est enregistrée dans le journal d'événements.

Alarmer [effr. – alarme] – si cette option est activée, toute tentative non autorisée de se connecter au module déclenche l'alarme anti-sabotage. L'option est disponible, si l'option ENREGISTRER L'EVENEMENT est activée.

5.2 Réglages du clavier virtuel

Lors de la communication avec la centrale d'alarme via le module ETHM-1, il est possible d'utiliser le clavier virtuel pour gérer et programmer le système d'alarme. En cas des centrales INTEGRA / INTEGRA Plus, les réglages du clavier virtuel peuvent être configurés. Les paramètres et les options du clavier virtuel disponible dans le logiciel DLOADX sont programmés comme suit :

- clavier : en utilisant les fonctions disponibles dans le sous-menu DLOADX RS (▶MODE SERVICE ▶STRUCTURE ▶MATERIEL ▶CLAVIERS ▶REGLAGES ▶DLOADX RS) ;
- logiciel DLOADX : cliquer sur la branche « DloadX (connexion RS-232) » (→fenêtre « Structure » →onglet « Matériel » →branche « Claviers » →branche « DloadX (connexion RS-232) ».

Les paramètres du clavier virtuel disponible dans le logiciel GUARDX, le navigateur WWW ou le téléphone mobile sont programmés comme suit :

- clavier : en utilisant les fonctions disponibles dans le sous-menu GUARDX ADRESSE (▶MODE SERVICE ▶STRUCTURE ▶MATERIEL ▶CLAVIERS ▶REGLAGES ▶GUARDX ADRESSE N (n = adresse du module] ;
- logiciel DLOADX : cliquer sur la branche « GuardX/MobileKPD » (→fenêtre « Structure » →onglet « Matériel » →branche « Claviers » →branche « GuardX/MobileKPD » – voir : fig. 6).

Pour les informations sur les paramètres et les options des claviers, veuillez consulter la notice de programmation de la centrales INTEGRA / INTEGRA Plus (seulement une partie de ces paramètres et options est disponible pour le clavier virtuel).

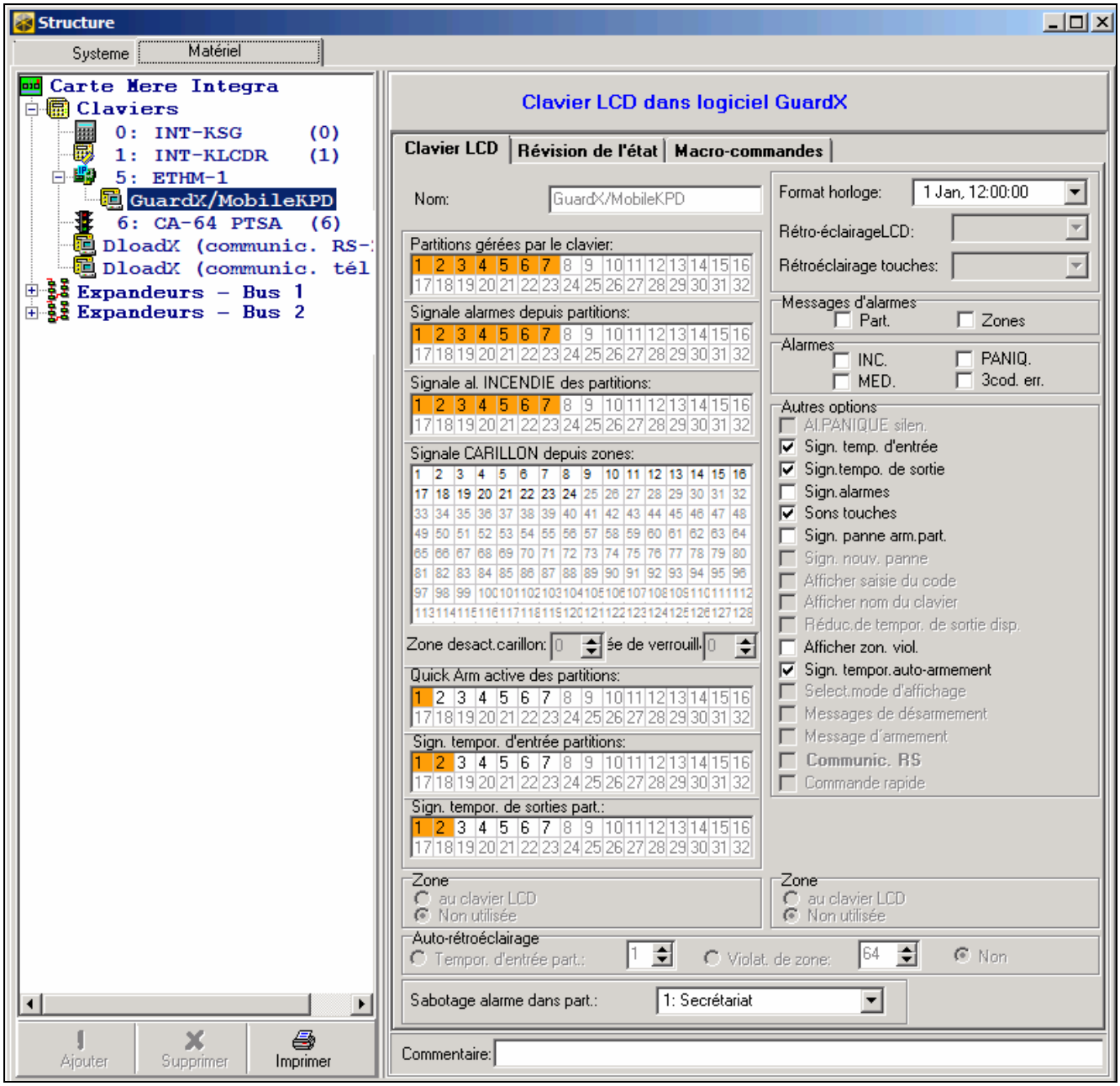

Fig. 6. Logiciel DLOADX : réglages du clavier virtuel accessible dans le logiciel GUARDX, le navigateur WWW ou le téléphone mobile.

5.3 Macro-commandes

L'application MOBILEKPD2 PRO permet de commander le système d'alarme INTEGRA / INTEGRA Plus à l'aide de macro-commandes ce qui permet d'activer facilement plusieurs différentes fonctions par l'appui de quelques touches seulement. Pour définir les macro-commandes, utiliser le logiciel DLOADX (→fenêtre « Structure » →onglet « Matériel » →bus de claviers →branche « GuardX/MobileKPD » →onglet « Macro-commandes ») et ensuite enregistrer dans la mémoire du téléphone mobile.

L'application MOBILEKPD2 PRO peut activer les mêmes macro-commandes qui sont définies pour le clavier INT-KSG. La programmation d'autres macro-commandes n'est pas nécessaire.

5.3.1 Paramètres et options

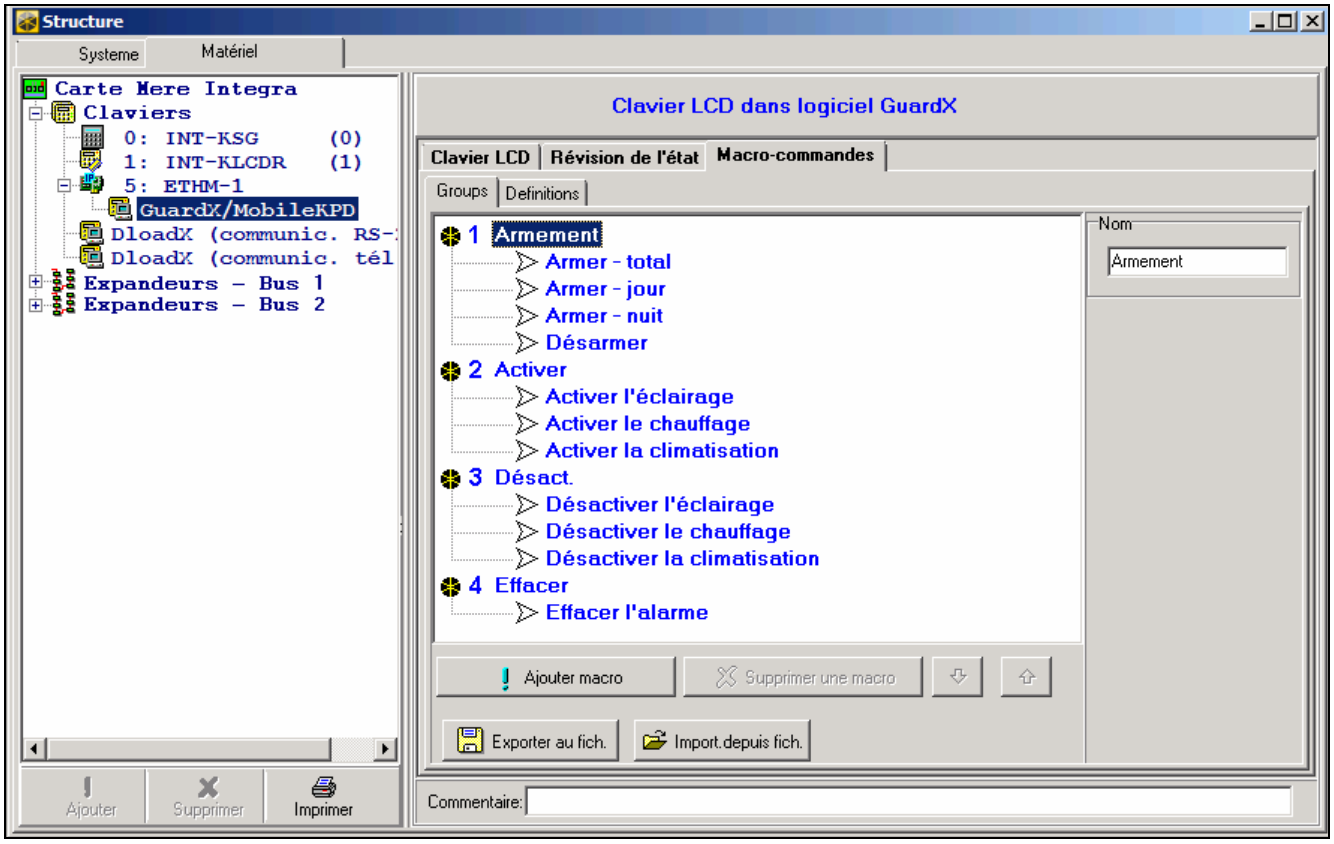

Fig. 7. Logiciel DLOADX : groupes de macro-commandes programmés pour l'application MOBILEKPD2 PRO.

Groupe de macro-commandes – liste de macro-commandes affichée si l'on appuie sur la touche macro. 4 groupes de macro-commandes sont possibles à définir.

Nom du groupes de macro-commandes – nom présenté sur la touche macro (jusqu'à 8 caractères).

Macro-commande – séquence d'opérations composée de commandes simples à exécuter par la centrale d'alarme après l'activation de la macro-commande.

Nom de la macro-commande – nom individuel de la macro-commande (jusqu'à 32 caractères).

Code – code utilisé pour l'autorisation lors de l'exécution des commandes contenues dans la macro-commande. Pour que la réalisation de ces commandes soit possible, un niveau d'autorisation adéquat doit être affecté au code.

Si, lors de l'exécution d'une macro-commande, il se révèle que le code est invalide (par exemple, il a été modifié), l'utilisateur peut saisir le code correct. Il sera automatiquement enregistré dans la mémoire du téléphone (et remplacera le code invalide).

Autorisation requise – si cette option est activée, la macro-commande ne sera exécutée qu'après l'autorisation de l'utilisateur au moyen d'un code. Le code entré dans le champ « Code » sera ignoré.

Désactivée si armée – si cette option est activée, la macro-commande ne sera pas disponible, lorsque l'une des partitions gérées par le clavier est armée.

Activer automatiquement – si cette option est activée et que le groupe ne contient qu'une macro-commande, la macro-commande sera immédiatement activée si l'on appuie sur

la touche macro (si l'option AUTORISATION REQUISE est activée, l'autorisation à l'aide du code est nécessaire).

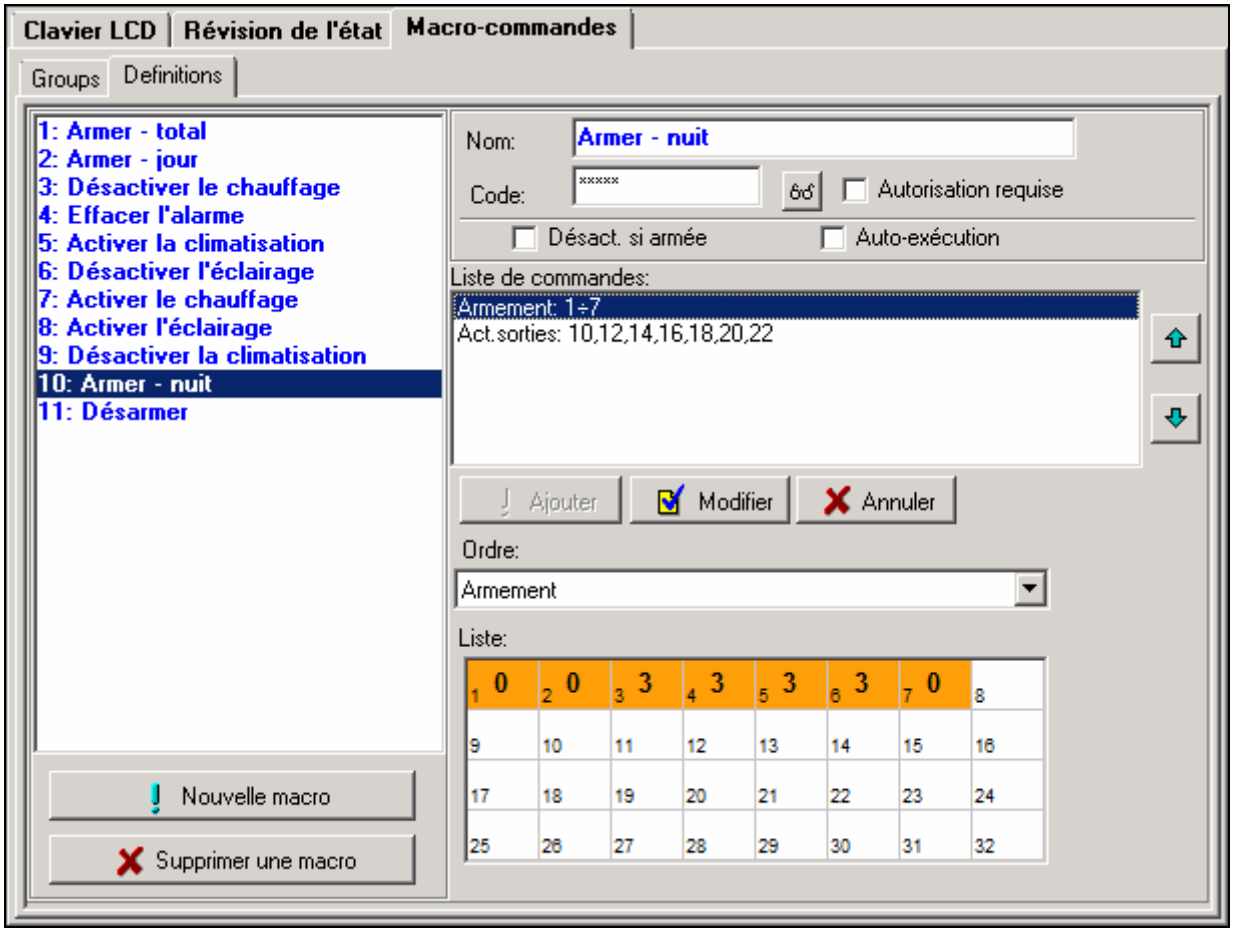

Fig. 8. Logiciel DLOADX: macro-commandes programmées pour l'application MOBILEKPD2 PRO.

Commande – fonction réalisée par la centrale qui peut être affectée à la macro-commande, par exemple :

- armement en mode défini dans les partitions sélectionnées ;
- désarmement dans les partitions sélectionnées ;
- effacement d'alarme dans les partitions sélectionnées ;
- blocage temporaire des zones sélectionnées ;
- déblocage des zones sélectionnées ;
- activation des sorties sélectionnées ;
- désactivation des sorties sélectionnées ;
- modification de l'état des sorties sélectionnées ;
- envoi du télégramme KNX ;
- envoi de la séquence des touches.

Les partitions doivent etre commnadees par le code de l'utilisateur.

L'option BLOCAGE DESACTIVE ne peut pas être activée dans les zones.

Les sorties doivent être de type 24. INTERRUPTEUR MONO, 25. INTERRUPTEUR BI, 105. VOLET EN HAUT, 106. VOLET EN BAS ou TRANSMETTEUR TELEPHONIQUE (ne doivent pas être affectées à un des groupes de sorties).

L'application MOBILEKPD2 PRO permet de commander le système KNX à condition que le module INT-KNX soit connecté à la centrale.

5.3.2 Définition de macro-commandes

1. Cliquer sur l'onglet « Définitions ».
2. Cliquer sur le bouton « Nouvelle macro-commande ». Une nouvelle macro-commande apparait dans la liste.
3. Entrer le nom de la nouvelle macro-commande.
4. Si la macro-commande doit être exécutée sans la saisie du code par l'utilisateur, entrer le code à un niveau approprié d'autorisation.
5. Si l'exécution de la macro-commande doit être chaque fois précédée de l'autorisation de l'utilisateur, activer l'option AUTORISATION REQUISE.
6. Si la macro-commande ne doit pas être disponible, lorsque l'une des partitions gérée par le clavier est armée, activer l'option DESACTIVEE SI ARMEE.
7. Si la macro-commande doit être exécutée immédiatement après l'appui de la touche macro, activer l'option ACTIVER AUTOMATIQUEMENT (dans ce cas, affecter une seule macro-commande au groupe).
8. Sélectionner dans la liste l'une des commandes que la macro-commande va exécuter.
9. Sélectionner les partitions (armement / désarmement, effacement d'alarme), les zones (blocage / déblocage) ou les sorties (activer / désactiver) contrôlés par la commande. Cliquer deux fois pour sélectionner / désélectionner le champ demandé.
10. Cliquer sur le bouton « Ajouter ». Une nouvelle commande apparaît dans la liste des commandes affectées à la macro-commande. Après avoir cliqué sur la commande, il est toujours faire une correction dans la liste de partitions / zones / sorties contrôlées par la commande. Après avoir effectué les modifications, cliquer sur le bouton « Modifier ».
11. Si nécessaire, répéter les étapes 8-10 pour ajouter d'autres commandes.
12. Cliquer sur l'onglet « Groupes ».
13. Cliquer sur le groupe à modifier.
14. Entrer le nom du groupe.
15. Cliquer sur le bouton « Ajouter macro ». Dans le menu déroulant, sélectionner la macro-commande à ajouter.

5.3.3 Préparation du fichier avec macro-commandes pour l'application MOBILEKPD2 PRO

Si l'application MOBILEKPD2 PRO doit exécuter les mêmes macro- commandes qui ont été définis pour le clavier INT-KSG, les opérations décrites ci-dessous peuvent être effectuées dans l'onglet « Macro-commandes » pour le clavier INT-KSG.

1. Cliquer sur l'onglet « Groupes ».
2. Cliquer sur le bouton « Exporter vers le fichier ».
3. Dans la fenêtre qui s'affiche, entrer le nom du fichier, puis cliquer sur le bouton « Enregistrer ». Si le fichier doit être enregistré dans un autre emplacement que celui par défaut, indiquer le dossier approprié avant de cliquer sur le bouton « Enregistrer ».
4. Une fenêtre s'ouvrira où il faut entrer le code de cryptage de fichier (jusqu'à 24 caractères alphanumériques), puis cliquer sur le bouton « OK ». Le code de cryptage de fichier sera requis lors du chargement des macro-commandes par l'application MOBILEKPD2 PRO.
5. Une fenêtre avec les informations que le fichier a été enregistré s'affichera.

6 Programmation à distance et gestion de la centrale via Ethernet

Après trois tentatives consécutives pour établir la communication avec le module à l'aide d'une clé incorrecte, le module ne répondra pas pendant environ 20 minutes à toute tentative visant à établir la communication à partir de l'adresse IP donnée.

Pour plus d'informations sur la configuration de la centrale d'alarme à l'aide du logiciel DLOADX via le réseau Ethernet (TCP/IP), veuillez vous référer au manuel de programmation de la centrale d'alarme.

6.1 Logiciel GuardX

La communication entre le logiciel GUARDX et la centrale d'alarme via le module ETHM-1 peut être établie de deux façons :

1. Initialiser la communication depuis le logiciel GUARDX. Cette méthode permet d'établir la communication avec la centrale d'alarme à partir de n'importe quel emplacement.
2. Initialiser la communication depuis le clavier (par la centrale d'alarme). Le système d'alarme ne peut être géré à distance que depuis un emplacement déterminé à la connaissance de l'utilisateur de la centrale.

La communication entre la centrale et le logiciel GUARDX peut être établie, si les identifiants dans le logiciel et dans la centrale sont identiques (IDENTIFIANT INTEGRA et IDENTIFIANT GUARDX).

6.1.1 Configuration du module ETHM-1

Pour configurer, procéder comme suit :

- programmer la clé qui servira à coder les données lors de la communication avec le logiciel GUARDX (CLE GUARDX/JAVA) ;
- activer l'option GUARDX, si la communication doit être initialisée depuis le logiciel GUARDX ;
- programmer l'adresse de l'ordinateur avec le logiciel GUARDX (GUARDX SERVEUR), si la communication doit être initialisée depuis le clavier (par la centrale d'alarme) ;
- programmer le numéro du port TCP qui sera utilisée pour la communication avec le logiciel GUARDX, s'il doit être diffèrent de 7091.

6.1.2 Configuration du logiciel GUARDX

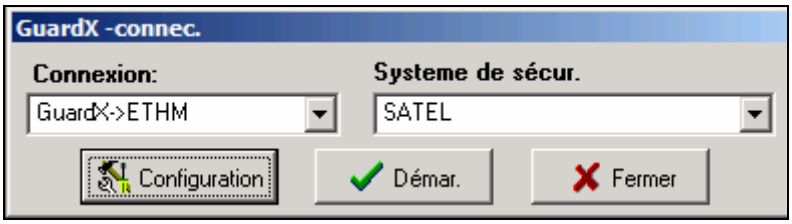

Fig. 9. Logiciel GUARDX: fenêtre de démarrage.

Dans la fenêtre de démarrage du logiciel GUARDX (voir: fig. 9), cliquer sur le bouton « Configuration ». Dans la fenêtre qui s'affiche, dans l'onglet « TCP/IP » (voir: fig. 10), programmer :

- numéro du port TCP (port – identique à celui programmé dans le module pour la communication avec le logiciel GUARDX – sauf la situation où la communication se fait lieu via le dispositif réseau sur lequel la redirection vers un autre port a lieu) ;

- clé servant à coder des données (identique à celui programmé dans le module pour la communication avec le logiciel GUARDX) ;
- adresse du module ETHM-1, si la communication doit être initialisée à partir du logiciel GUARDX.

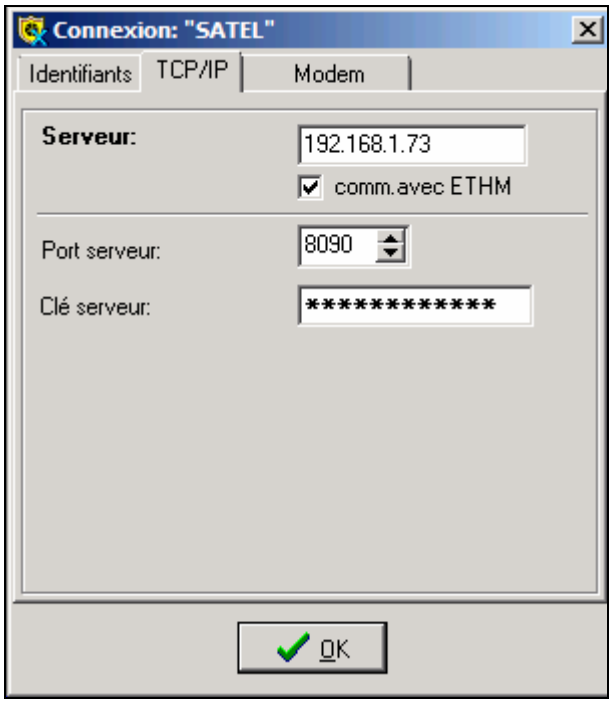

Fig. 10. Logiciel GUARDX: réglages de la communication via le réseau Ethernet (TCP/IP).

6.1.3 Initialisation de la communication à partir du logiciel GUARDX

1. Dans la fenêtre de démarrage, dans le champ « Connexion », sélectionner « GuardX -> ETHM » (voir : fig. 9), ensuite cliquer sur le bouton « Démarrer ».
2. Une fois la communication établie, dans la fenêtre qui apparait entrer le code de l'administrateur / utilisateur de la centrale.

6.1.4 Initialisation de la communication à partir du clavier (par la centrale d'alarme)

1. Dans la fenêtre de démarrage, dans le champ « Connexion », sélectionner « GuardX <- ETHM », ensuite cliquer sur le bouton « Démarrer ».
2. Sur le clavier, activer la fonction ETHM-1 – GUARDX ([*code*]✱ ▶DOWNLOADING ▶ETHM-1 – GUARDX). La fonction est disponible au service, à l'administrateur et à l'utilisateur autorisés à ACTIVER LA FONCTION DOWNLOAD.
3. Une fois la communication établie, dans la fenêtre qui apparait entrer le mot de passe de l'administrateur / utilisateur de la centrale.

6.2 Navigateur WWW

6.2.1 Configuration du module ETHM-1

Dans le module ETHM-1, il faut :

- activer l'option WWW ;
- programmer la clé servant à coder des données lors de la communication avec l'application JAVA dans le navigateur web (CLE GUARDX/JAVA) ;

- programmer le numéro du port TCP qui sera utilisé pour la communication avec le navigateur web, si ce port doit être différent de 80 (PORT WWW/MIDP1.0) ;
- programmer le numéro du port TCP qui sera utilisé pour la communication avec l'application JAVA dans le navigateur, si ce numéro doit être différent de 7091.

6.2.2 Configuration de l'ordinateur

La Machine Virtuelle JAVA doit être installée sur l'ordinateur (Java Virtual Machine).

6.2.3 Etablissement de la communication

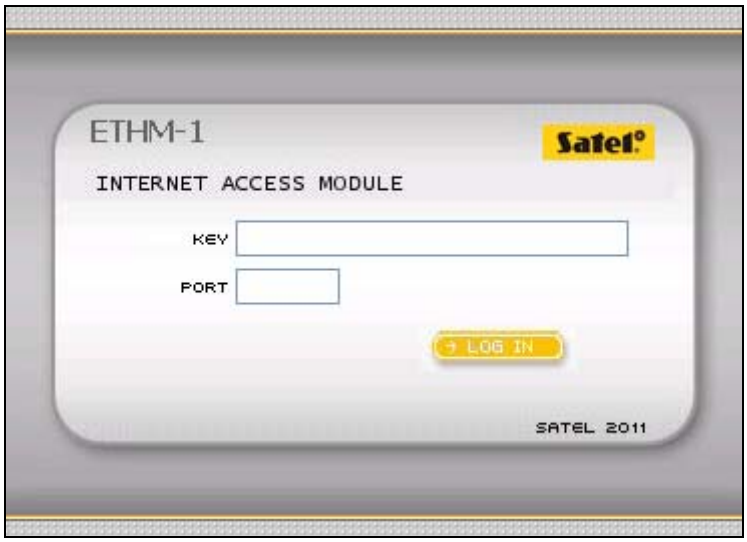

Fig. 11. Page de connexion affichée dans le navigateur web.

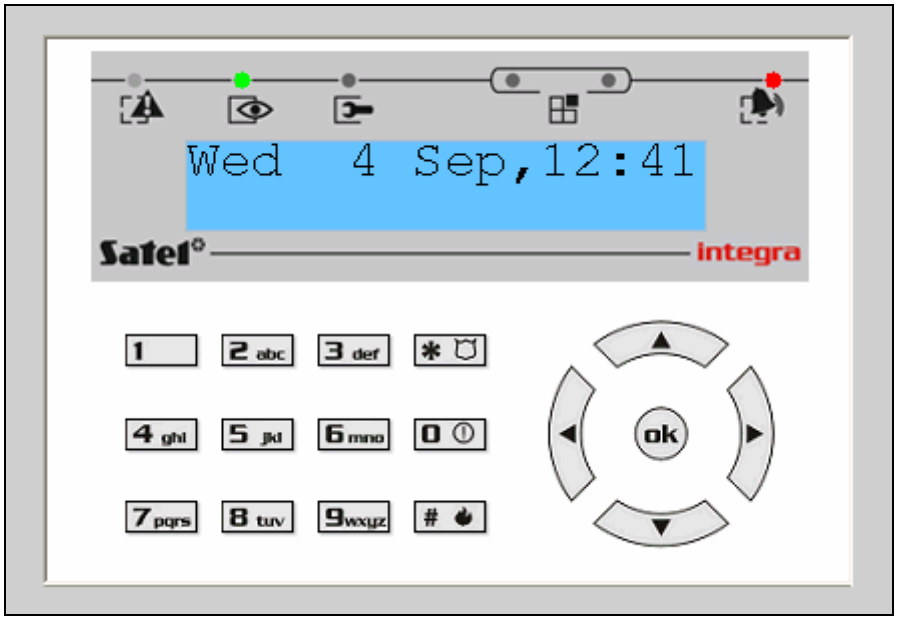

Fig. 12. Clavier virtuel disponible dans le navigateur web.

1. Démarrer le navigateur WWW.
2. Saisir l'adresse IP du module ETHM-1 dans le champ adresse, et appuyer sur le bouton ENTER.

Si dans les paramètres du module, le port différent de 80 est programmé pour la communication avec le navigateur web, une fois l'adresse est saisie, indiquer le numéro du port après deux points.

3. Entrer des informations suivantes dans les champs correspondants sur la page de connexion qui apparaitra dans le navigateur :
   - clé servant à coder des données (identique à celui programmé dans le module pour la communication avec l'application JAVA dans le navigateur web) ;
   - numéro du port (identique à celui programmé dans le module pour la communication avec l'application JAVA dans le navigateur web - sauf la situation où la communication se fait lieu via le dispositif réseau sur lequel la redirection vers un autre port a lieu).
4. Clique sur le bouton « Connecter ».
5. Dans le navigateur, un clavier virtuel apparaitra et il permettra de faire fonctionner et programmer le système d'alarme.

6.3 Téléphone mobile

6.3.1 Configuration du module ETHM-1

Dans le module ETHM-1, il faut :

- activer l'option :
- programmer la clé servant à coder des données lors de la communication avec l'application MOBILEKPD / MOBILEKPD2 dans le téléphone mobile (CLE GUARDX/JAVA) ;
- programmer le numéro du port TCP qui sera utilisé pour la communication avec l'application MOBILEKPD / MOBILEKPD2 dans le téléphone mobile, s'il doit être différent de celui d'usine.

6.3.2 Configuration du téléphone mobile

Installer l'application MOBILEKPD / MOBILEKPD2 dans le téléphone mobile. Il est possible de la télécharger sur le site www.satel.pl (sélectionner l'application en fonction du téléphone possédé), sur « Google play » (dispositifs avec le système Android) ou « App Store » (dispositifs avec le système iOS).

Après avoir installé l'application, entrer :

- le nom du système d'alarme ;
- l'adresse du module ETHM-1 ;
- le numéro du port TCP (identique à celui programmé dans le module pour la communication avec l'application MOBILEKPD / MOBILEKPD2 - sauf la situation où la communication se fait lieu via le dispositif réseau sur lequel la redirection vers un autre port a lieu) ;
- la clé servant à coder des données (identique à celui programmé dans le module pour la communication avec l'application MOBILEKPD / MOBILEKPD2).

Lorsque toutes les données mentionnées ci-dessous sont enregistrées dans la mémoire du téléphone, la liste des systèmes d'alarme sera affichée.

Lecture du fichier avec macro-commandes – MOBILE KPD2 PRO

Pour l'application MOBILEKPD2 PRO, lors de la configuration des paramètres requis à l'établissement de la communication avec le système d'alarme, la lecture des macro-commandes est possible à condition que le fichier soit préalablement enregistré dans la mémoire du téléphone. Après avoir indiqué le fichier contenant des macro-commandes, entrer le code de cryptage du fichier.

6.3.3 Etablissement de la communication – MOBILEKPD

1. A l'aide des touches du téléphone, sélectionner le système d'alarme dans la liste.
2. Sélectionner : → « Options » → « Démarrage ».

3. Les éléments du clavier virtuel apparaissent sur l'afficheur. Le téléphone mobile permet de programmer er de gérer le système d'alarme.

6.3.4 Etablissement de la communication – MOBILEKPD2

Toucher le nom du système d'alarme. Le clavier virtuel apparait sur l'afficheur. Il permet de programmer er de gérer le système d'alarme.

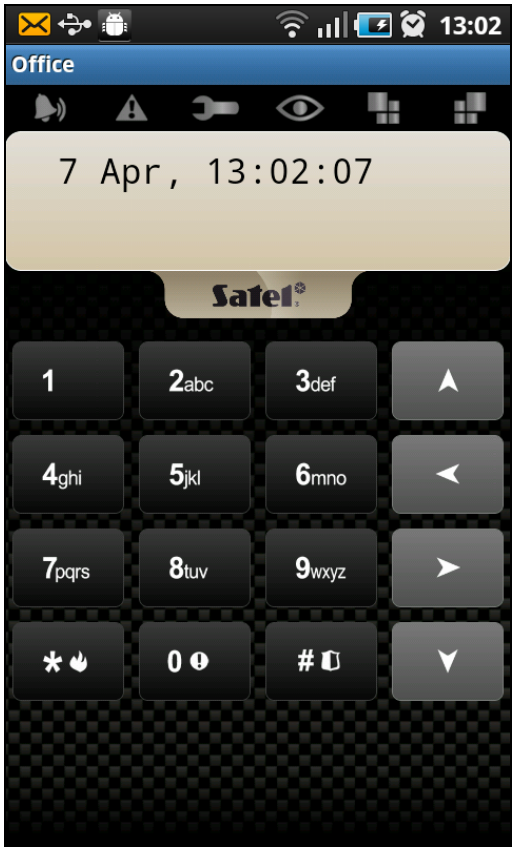

Fig. 13. Clavier virtuel accessible dans l'application MOBILEKPD2 (téléphone avec le système Android).

Si les paramètres sont programmés seulement pour un système d'alarme, après le redémarrage de l'application, l'écran avec la liste de systèmes ne s'affiche pas – c'est le clavier virtuel qui apparait immédiatement.

7 Spécifications techniques

Tension d'alimentation	12 V DC ±15%
Consommation de courant en veille	120 mA
Consommation maximale de courant	120 mA
Classe environnementale selon EN50130-5	II
Températures de fonctionnement	-10...+55 °C
Humidité maximale	93±3%
Dimension	68 x 140 mm
Masse	64 g