



---

# Module de communication Ethernet **ETHM-1 Plus**



---

Version de programme 2.00

ethm1\_plus\_fr 07/14

SATEL sp. z o.o.  
ul. Budowlanych 66  
80-298 Gdańsk  
POLOGNE  
tél. +48 58 320 94 00  
[www.satel.eu](http://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.

FreeRTOS est utilisé dans ce dispositif ([www.freertos.org](http://www.freertos.org)).

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](http://www.satel.eu/ce)**

Les symboles suivants utilisés dans la présente notice :



- note ;



- avertissement.

## TABLE DE MATIERES

1	Introduction .....	2
2	Utilisations .....	2
3	Carte électronique .....	3
4	Réglage de l'adresse .....	3
4.1	Module connecté à la centrale INTEGRA / INTEGRA Plus .....	4
4.2	Module connecté à la centrale VERSA .....	4
5	Installation .....	4
6	Configuration .....	6
6.1	Paramètres et options du module .....	6
6.1.1	Module connecté à la centrale INTEGRA / INTEGRA Plus .....	6
6.1.2	Module connecté à la centrale VERSA .....	9
6.2	Clavier virtuel .....	10
6.2.1	Module connecté à la centrale INTEGRA / INTEGRA Plus .....	11
6.2.2	Module connecté à la centrale VERSA .....	12
6.3	Fonction utilisateur [INTEGRA / INTEGRA Plus] .....	12
6.4	Macro-commandes [INTEGRA / INTEGRA Plus] .....	12
6.4.1	Groupes .....	13
6.4.2	Définitions .....	14
6.4.3	Définir les macro-commandes .....	16
6.4.4	Export du fichier avec les macro-commandes .....	21
7	Programmation à distance et gestion de la centrale via Ethernet .....	21
7.1	Logiciel GuardX .....	21
7.1.1	Configuration du module ETHM-1 Plus .....	22
7.1.2	Configuration du logiciel GUARDX .....	22
7.1.3	Initialisation de la communication à partir du logiciel GUARDX .....	23
7.1.4	Initialisation de la communication à partir du clavier (par la centrale d'alarme) ..	23
7.2	Navigateur WWW .....	23
7.2.1	Configuration du module ETHM-1 Plus .....	23
7.2.2	Configuration de l'ordinateur .....	23
7.2.3	Etablissement de la communication .....	23
7.3	Téléphone mobile .....	24
7.3.1	Configuration du module ETHM-1 Plus .....	24
7.3.2	Configuration du téléphone mobile .....	25
7.3.3	Etablissement de la communication – MOBILEKPD .....	25
7.3.4	Etablissement de la communication – MOBILEKPD-2 / MOBILEKPD-2 PRO .....	25
8	Spécifications techniques .....	26

## 1 Introduction

---

Le module ETHM-1 Plus 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](http://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).
- Transmission des événements depuis la centrale d'alarme à la station de télésurveillance via réseau Ethernet, 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).
- Notification des événements dans le système d'alarme par des messages e-mail. Le contenu du message est automatiquement généré et correspond à la description dans le journal d'événements.  
Fonction disponible pour les centrales INTEGRA Plus (version du logiciel 1.13 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](http://www.satel.eu).*

### 3 Carte électronique

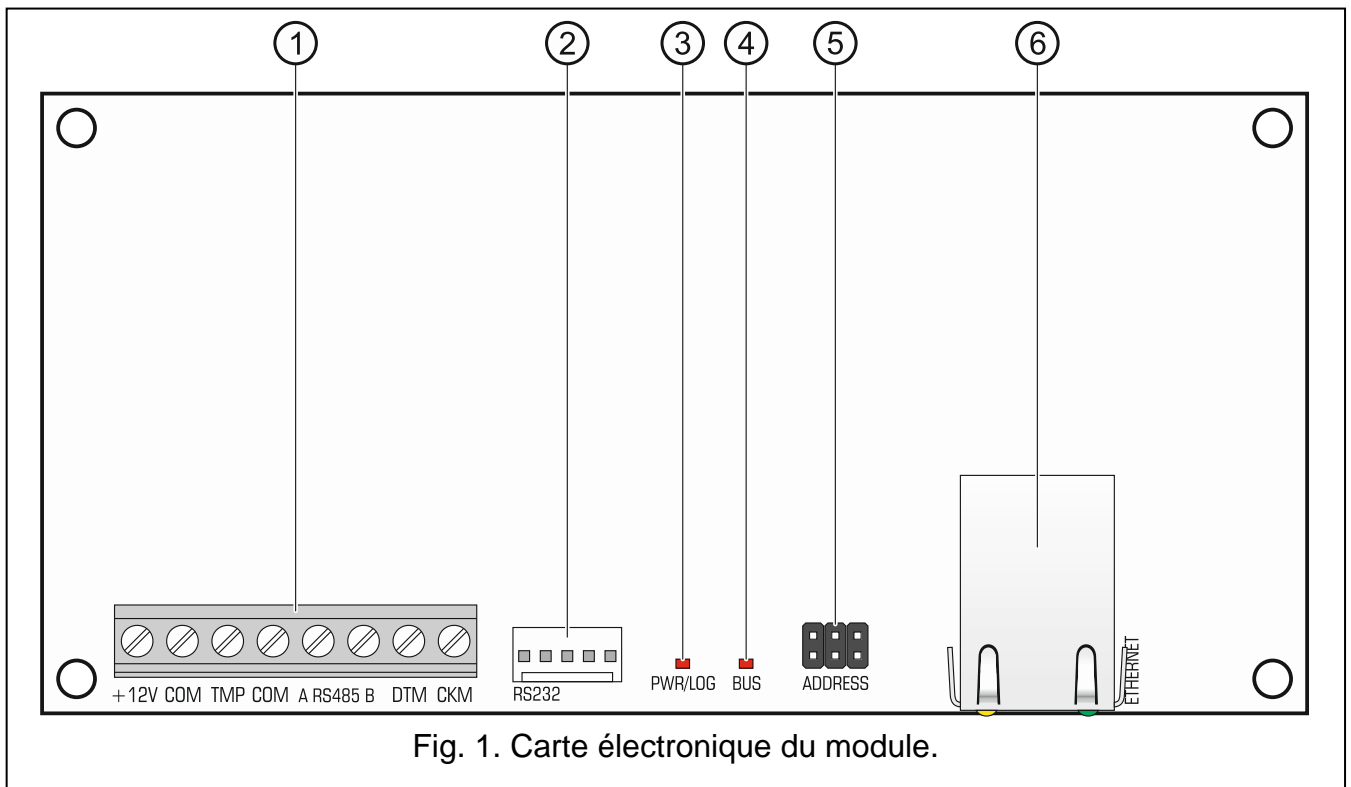


Fig. 1. Carte électronique du module.

- 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 prévues pour de futures utilisations (RS-485).
  - 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 clignote lorsque l'échange de données avec la centrale est en cours.
- ⑤ broches pour le réglage de l'adresse du module (voir : « Réglage de l'adresse »).
- ⑥ connecteur RJ-45 pour connecter le réseau Ethernet. Muni de deux voyants LED :
- vert – signale la connexion au réseau et la transmission des données,
  - jaune – indique la vitesse de transmission négociée (allumé : 100 Mb ; non allumé : 10 Mb).

### 4 Réglage de l'adresse

Régler l'adresse à l'aide des cavaliers en les plaçant sur les broches ADDRESS. Le tableau 1 représente comment placer les cavaliers pour régler l'adresse déterminée (■ - cavalier placé ; □ - cavalier enlevé).

Adresse	0	1	2	3	4	5	6	7
Etat des broches								

Tableau 1.

#### 4.1 Module connecté à la centrale INTEGRA / INTEGRA Plus

Régler l'adresse dans le module :

- de 0 à 3, s'il est connecté à la centrale INTEGRA 24 ou INTEGRA 32,
- de 0 à 7, s'il est connecté à une autre centrale INTEGRA ou INTEGRA Plus.

L'adresse doit être différente de celle dans d'autres dispositifs connectés au bus des claviers de la centrale d'alarme (la centrale ne gère pas les dispositifs aux adresses identiques).

#### 4.2 Module connecté à la centrale VERSA

Régler l'adresse 4 dans le module. Le clavier ayant l'adresse 4 ne peut pas être connecté à la centrale.

### 5 Installation



**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. Fixer la carte électronique du module dans le boîtier. Le module doit être installé dans le même boîtier que celui de la centrale d'alarme. Cela facilite de relier les ports RS-232 de la centrale et du module ce qui est nécessaire, si la centrale doit être configurée via réseau Ethernet à l'aide du logiciel DLOADX.
2. Régler l'adresse du module (voir : « Réglage de l'adresse »).
3. Raccorder les bornes +12V, COM, DTM et CKM du module aux bornes de la centrale d'alarme (fig. 2). Pour effectuer des raccordements, utiliser un câble non blindé droit. Si le câble de type « paire torsadée » est utilisé, ne pas oublier que les signaux CLM (horloge) et DTA (données) ne peuvent être envoyés par une paire de fils torsadés. Les fils doivent être conduits dans un câble.
4. Raccorder les fils du contact d'autoprotection aux bornes TMP et COM, si le module doit surveiller le contact d'autoprotection du boîtier. Sinon, raccorder les bornes TMP à la borne COM du module.
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. Remettre le système d'alarme sous tension.
7. Activer la fonction d'identification des dispositifs dans la centrale (voir : notice d'installation de la centrale correspondante). Le module sera identifié comme « ETHM-1 ».
8. Configurer le module (voir : « Configuration »).
9. 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 :  
INTEGRA avec la prise type PIN5 : **PIN5/PIN5** (fig. 3)

INTEGRA avec la prise type RJ / INTEGRA Plus : **RJ/PIN5** (fig. 4)

VERSA : **PIN5/RJ-TTL**

Les câbles mentionnés ci-dessus sont disponibles dans l'offre de la société SATEL.

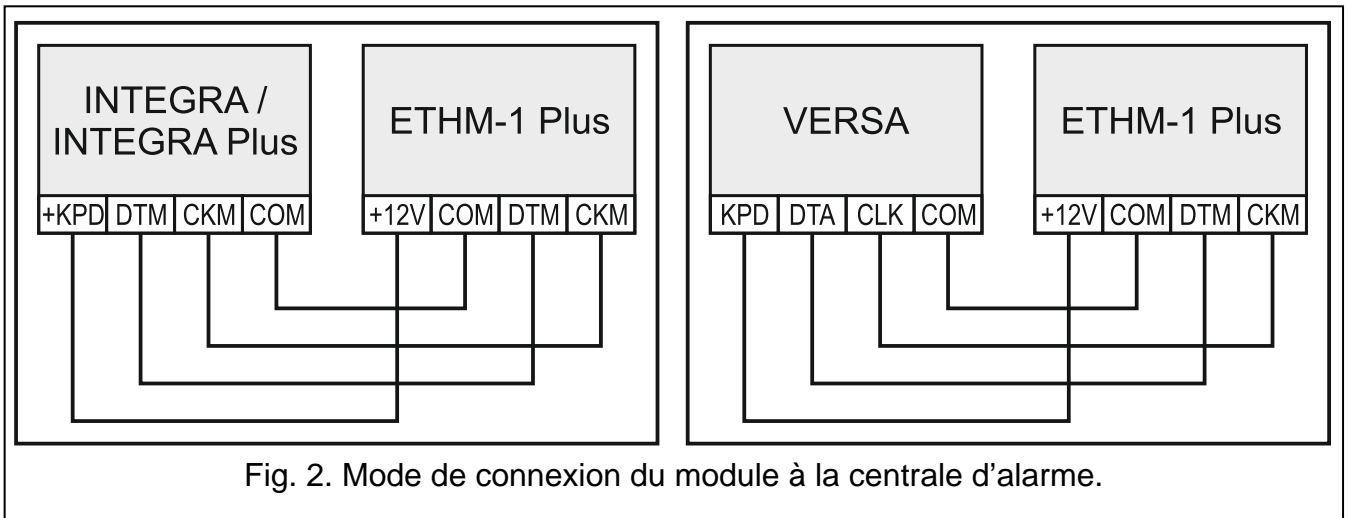


Fig. 2. Mode de connexion du module à la centrale d'alarme.

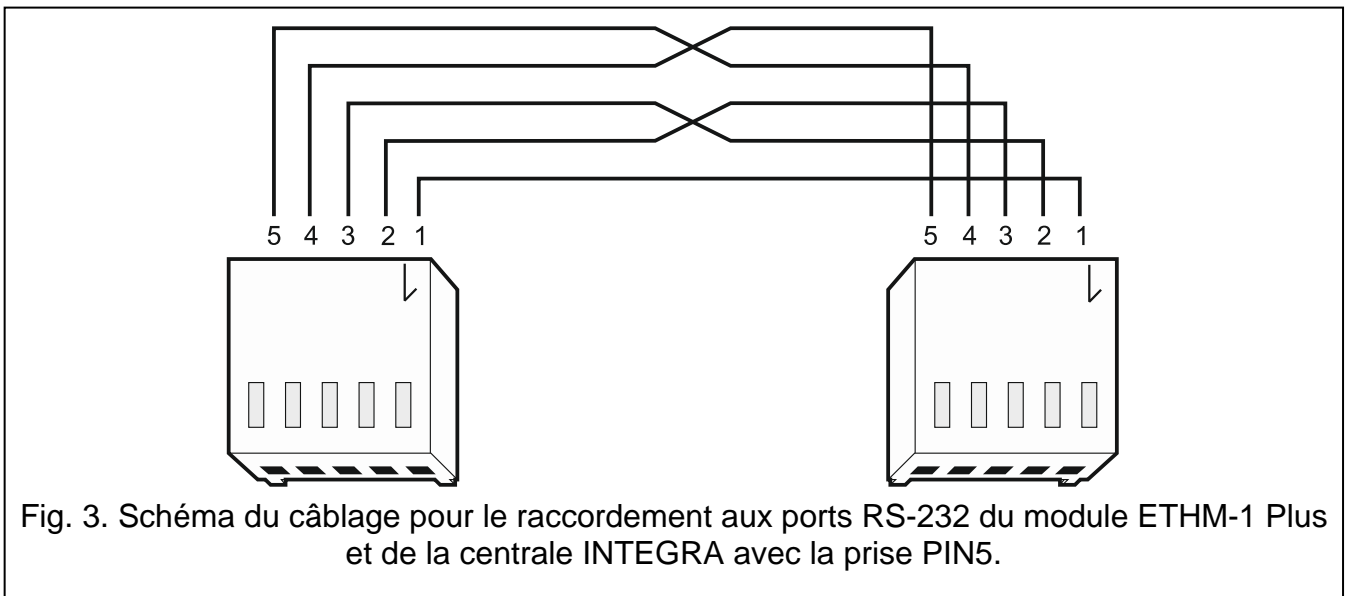


Fig. 3. Schéma du câblage pour le raccordement aux ports RS-232 du module ETHM-1 Plus et de la centrale INTEGRA avec la prise PIN5.

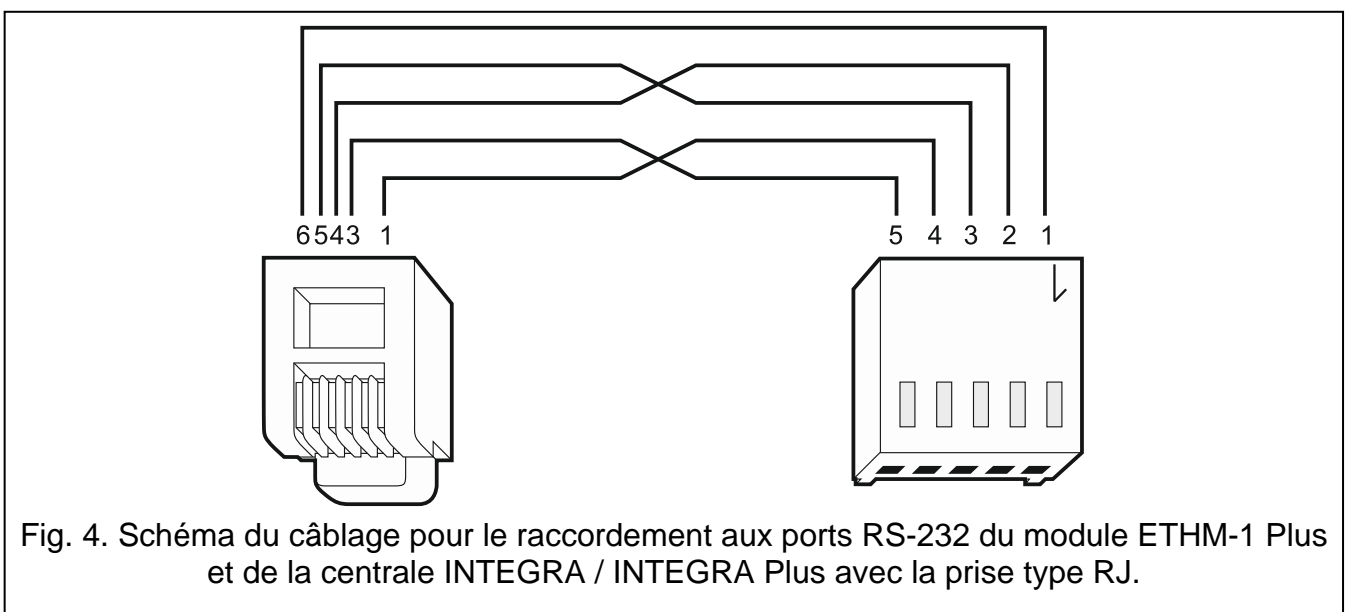


Fig. 4. Schéma du câblage pour le raccordement aux ports RS-232 du module ETHM-1 Plus et de la centrale INTEGRA / INTEGRA Plus avec la prise type RJ.

## 6 Configuration

Le module peut être configuré via la centrale d'alarme, à l'aide d'un clavier ou d'un ordinateur avec le logiciel DLOADX installé.

### 6.1 Paramètres et options du module

#### 6.1.1 Module connecté à la centrale INTEGRA / INTEGRA Plus

Les paramètres et les options du module peuvent être configurés à l'aide :

- du clavier : ►MODE SERVICE ►STRUCTURE ►MATÉRIEL ►CLAV. ET MOD. D'EXT. ►2. REGLAGES ►[nom du module],
- du logiciel DLOADX : →fenêtre « Structure » →onglet « Matériel » →branche « Claviers » →[nom du module] →onglet « ETHM-1 » (fig. 5).

Entre crochets sont présentés les noms des paramètres et des options affichés sur l'écran du clavier.

**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 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 DHCP (dans ce cas, ces paramètres ne sont pas programmables).



*L'adresse IP affectée au module peut être lue :*

- dans le clavier : à l'aide de la fonction utilisateur **IP/MAC ETHM-1** disponible au sous-menu **TESTS**. Pour les détails de la fonction, consulter le manuel utilisateur de la centrale d'alarme.
- dans le logiciel DLOADX : au-dessous des paramètres et options du module (fig. 5).

**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 AUTOMATIQUÉMENT L'ADRESSE IP (DHCP)** est activée.

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

#### 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]** – 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 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).*

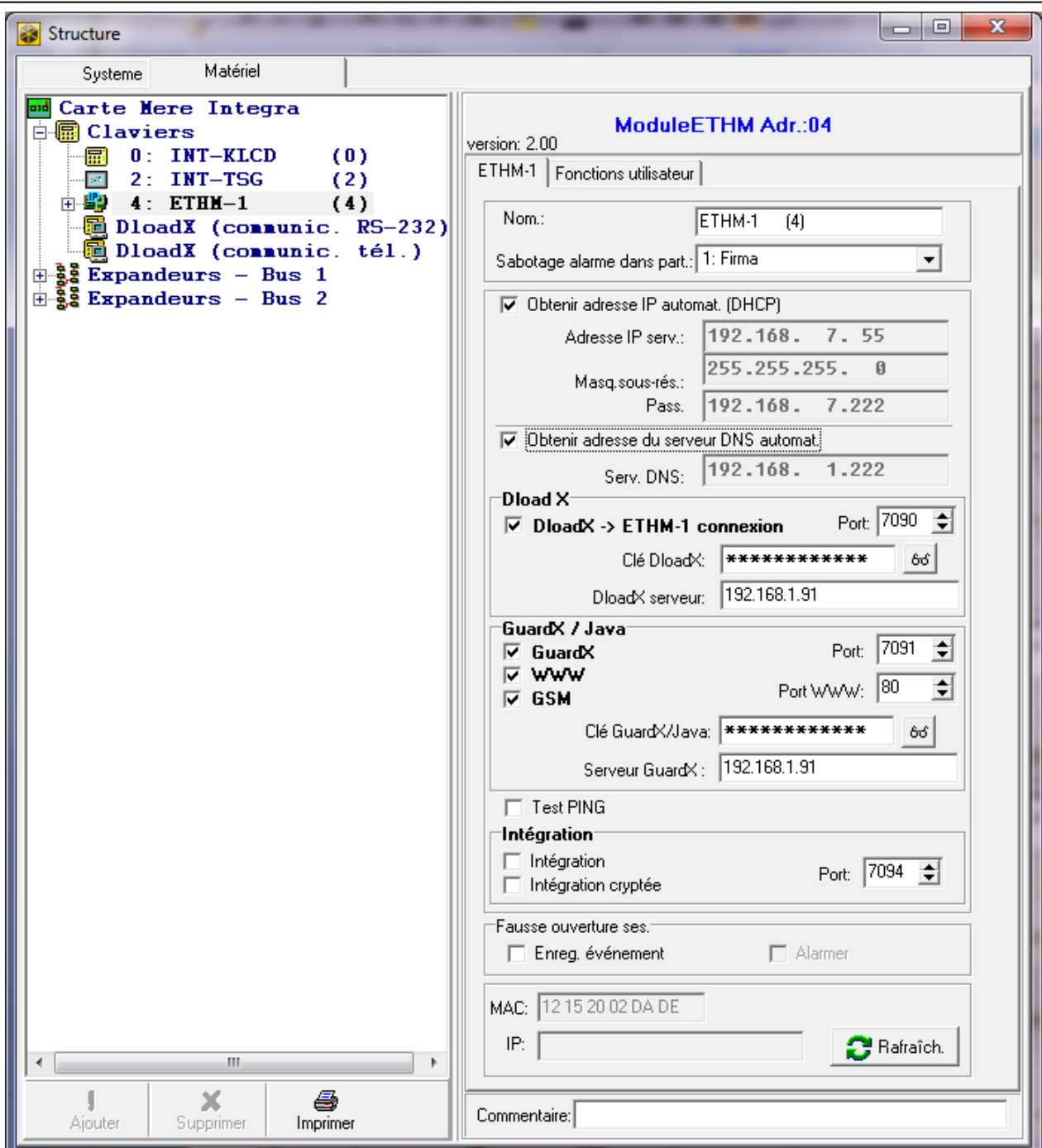


Fig. 5. Logiciel DLOADX : paramètres et options du module ETHM-1 Plus pour la centrale INTEGRA / INTEGRA Plus.

## GuardX / Java

**GuardX** [par GuardX] – si l'option est activée, la connexion avec la centrale d'alarme peut être lancée via le réseau Ethernet 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 Ethernet 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 Ethernet à l'aide de l'application MOBILEKPD / MOBILEKPD2 / MOBILEKPD-2 PRO.

**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 / MOBILEKPD-2 / MOBILEKPD-2 PRO dans le téléphone mobile.

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** – numéro du port TCP utilisé à la communication avec le navigateur. 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 / MOBILEKPD-2 / MOBILEKPD-2 PRO 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, 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. Les paramètres relatifs aux tests sont programmés dans la centrale d'alarme :

clavier : ►MODE SERVICE ►OPTIONS ►TEST PING,

logiciel DLOADX : →fenêtre « Structure » →onglet « Matériel » →branche « Claviers ».

## Serveur SATEL

**Connex.avec serveur SATEL** [Serveur SATEL] – si l'option est activée, la communication avec le module peut s'effectuer via le serveur SATEL. Pour la communication via le serveur SATEL, la configuration du périphérique réseau par lequel le module se connecte au réseau public n'est pas nécessaire.

## 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. La clé de cryptage est programmée dans la centrale d'alarme :

clavier : ►MODE SERVICE ►OPTIONS ►CLE INTEGRATION,

logiciel DLOADX : →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** [Efr. – 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.

### Informations

**MAC** – adresse matériel du module.

**ID** – identifiant attribué au module pour la communication via le serveur SATEL.

**IP** – adresse local / adresse publique du module.

### 6.1.2 Module connecté à la centrale VERSA

Les paramètres et les options du module peuvent être configurés à l'aide :

- du clavier : ►MODE SERVICE ►2. MATERIEL ►1. CLAV./MOD.EXT ►2. REGLAGES ►[nom du module],
- du logiciel DLOADX : →fenêtre « Versa – Structure » →onglet « Matériel » →branche « Module d'extension »→[nom du module] (fig. 6).

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 DHCP (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 **VER. MODULES** disponible dans le sous-menu **TESTS**. Pour les détails de la fonction, consulter le manuel utilisateur de la centrale d'alarme.*

**Adresse IP serv.** – l'adresse IP du module.

**Masq.sous-rés.** – le masque de sous-réseau dans laquelle le module fonctionne.

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

**Obtenir adresse IP automat.** [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 l'option OBTENIR ADRESSE IP AUTOMAT est désactivée.

### DloadX

**DloadX** -> **ETHM-1 connexion** [DloadX→ETHM-1] – si l'option est activée, la communication avec la centrale d'alarme peut être lancée via le réseau Ethernet depuis le logiciel DLOADX.

**Port** [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.

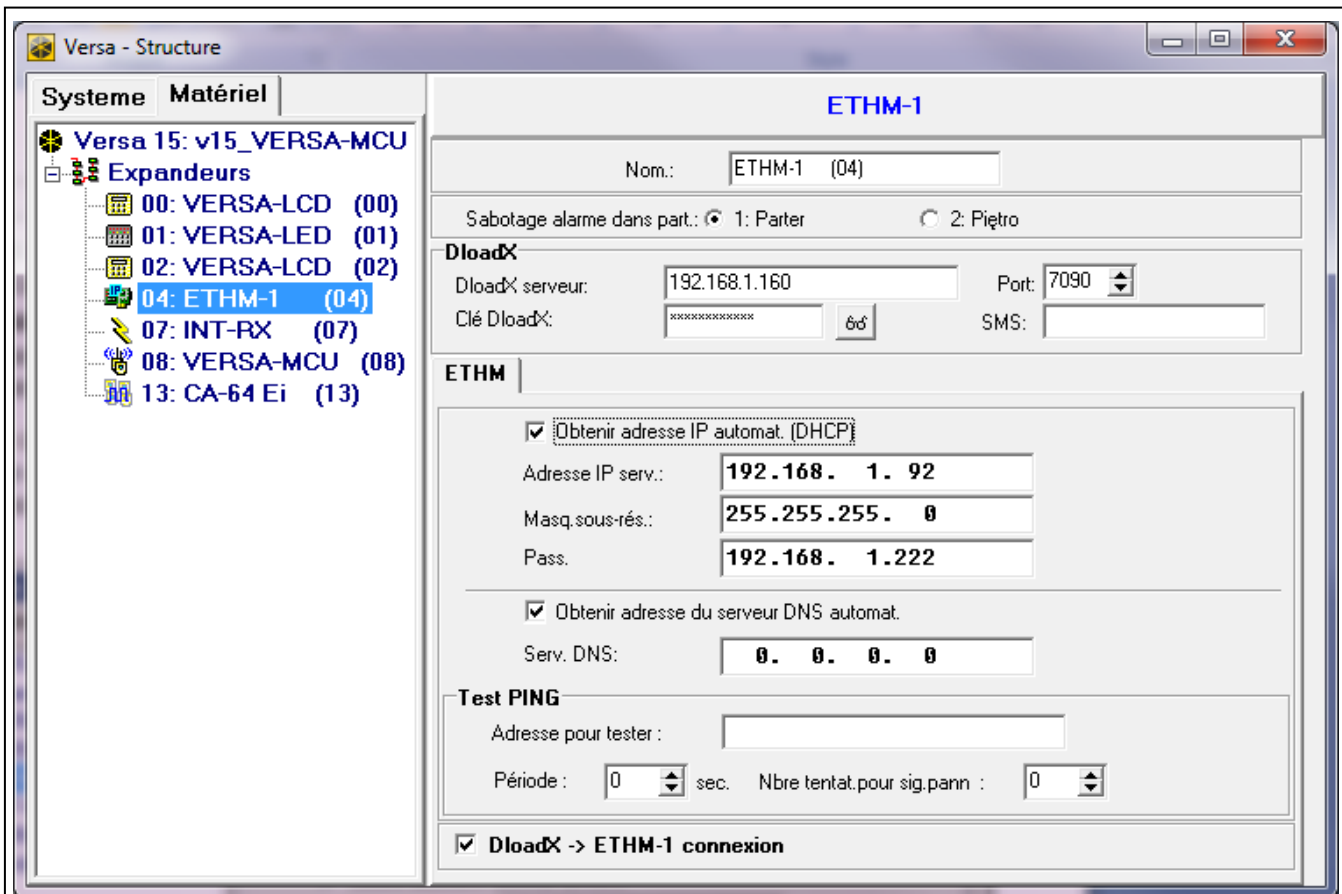


Fig. 6. Logiciel DLOADX : réglages du module ETHM-1 Plus connecté à la centrale VERSA.

**DLOADX serveur** [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.

**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.

### Test PING

**Adresse à tester** [PING] – 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.

**Nbre tentat.pour sig.pann** [Nbr.tentat.PING] – 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.

## 6.2 Clavier virtuel

Le clavier virtuel permet d'utiliser et de programmer le système d'alarme de la même manière que le clavier physique.

### 6.2.1 Module connecté à la centrale INTEGRA / INTEGRA Plus

Le clavier virtuel peut être utilisé dans les logiciels DLOADX et GUARDX, dans le navigateur WWW et le téléphone portable (après l'installation de l'application MOBILEKPD / MOBILEKPD-2 / MOBILEKPD-2 PRO).

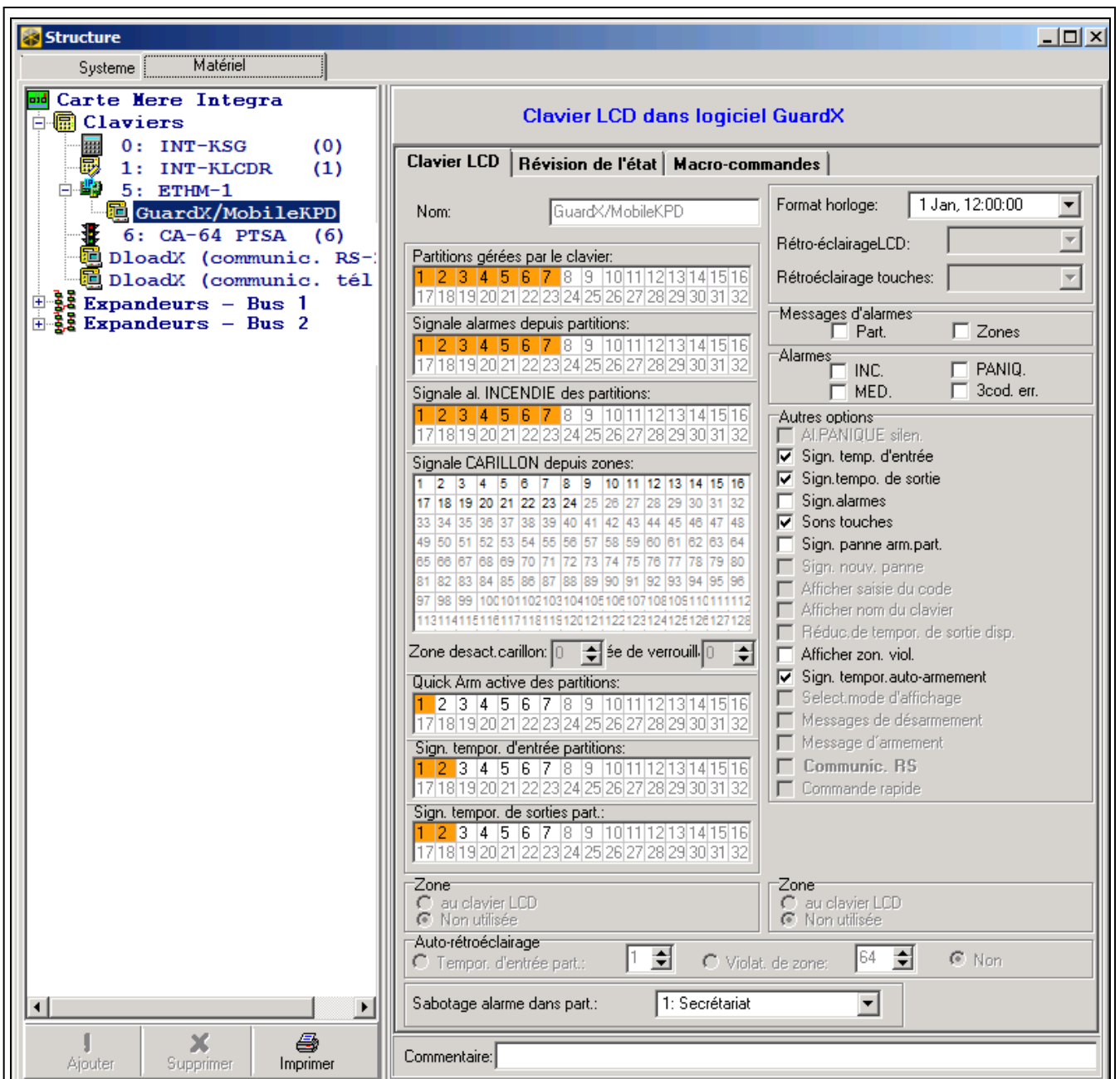


Fig. 7. Logiciel DLOADX : réglages du clavier virtuel accessible dans le logiciel GUARDX, le navigateur WWW ou le téléphone mobile.

Les paramètres et les options du clavier virtuel disponible dans le logiciel DLOADX sont programmés comme suit :

- clavier : ►MODE SERVICE ►STRUCTURE ►MATÉRIEL ►CLAVIERS ►REGLAGES ►DLOADX RS,
- logiciel DLOADX : →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 : ►MODE SERVICE ►STRUCTURE ►MATERIEL ►CLAVIERS ►REGLAGES ►GUARDX ADRESSE n (n = adresse du module),
- logiciel DLOADX : →fenêtre « Structure » →onglet « Matériel » →branche « Claviers » →[nom du module] →branche « GuardX/MobileKPD » (fig. 7).

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).

### 6.2.2 Module connecté à la centrale VERSA

Le clavier virtuel peut être utilisé dans le logiciel DLOADX. Les paramètres et les options du clavier virtuel ne peuvent pas être configurés.

## 6.3 Fonction utilisateur [INTEGRA / INTEGRA Plus]

Si l'application MOBILEKPD-2 / MOBILEKPD-2 PRO est utilisée dans le téléphone portable, le clavier virtuel permet de démarrer rapidement la fonction utilisateur après l'entrée du code et l'appui sur la touche fléchée. Les fonctions peuvent être attribuées aux touches à l'aide :

- du clavier : ►MODE SERVICE ►STRUCTURE ►MATERIEL ►CLAVIERS ►REGLAGES ►[nom du module] ►CODE+FLECHES,
- du logiciel DLOADX : →fenêtre « Structure » →onglet « Matériel » →branche « Claviers » → [nom du module] →onglet « Fonctions utilisateur » (fig. 8).

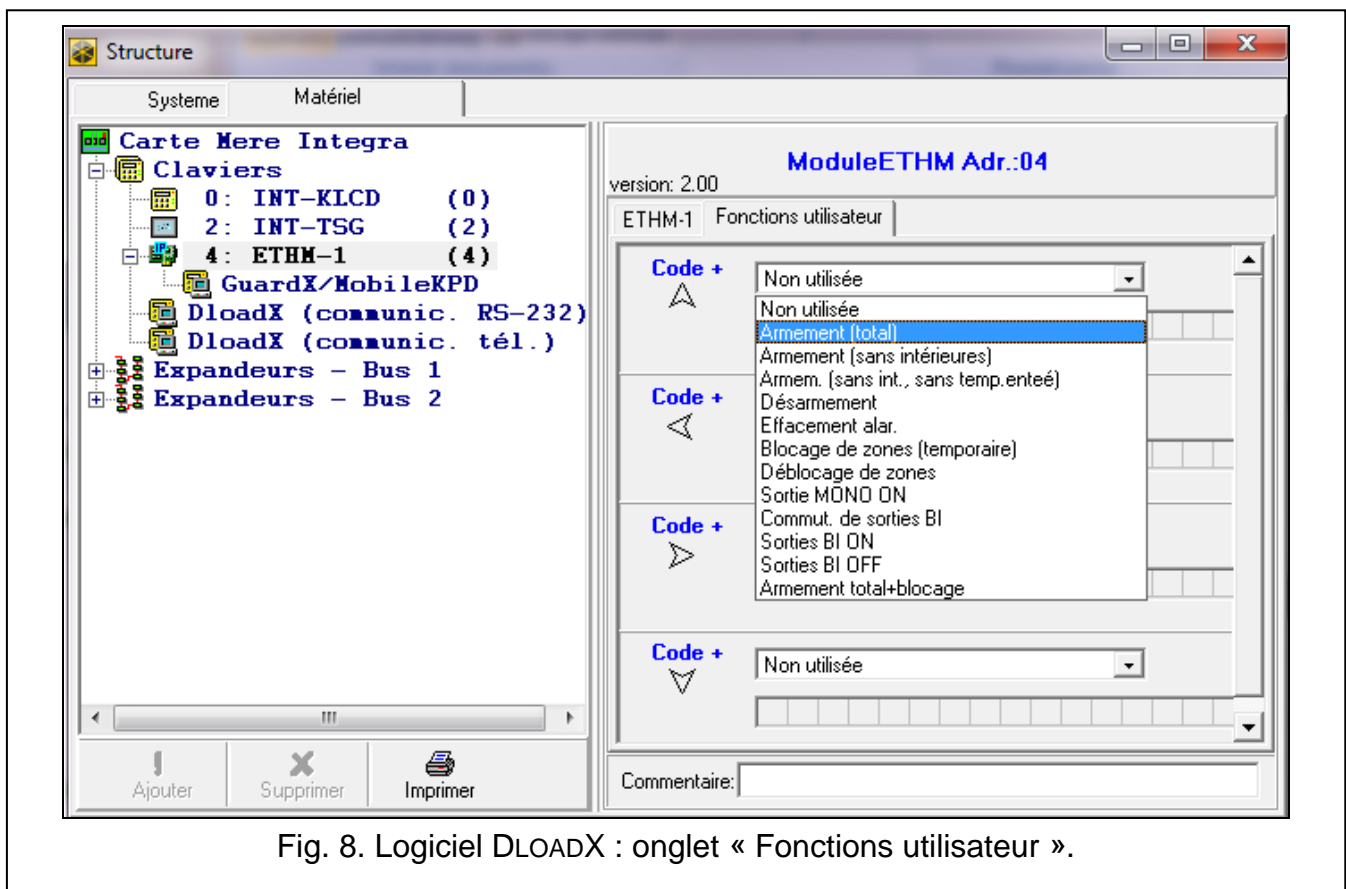


Fig. 8. Logiciel DLOADX : onglet « Fonctions utilisateur ».

## 6.4 Macro-commandes [INTEGRA / INTEGRA Plus]

L'application MOBILEKPD2 PRO permet de commander le système d'alarme 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 » →branche « Claviers » →branche [nom du module] →branche « GuardX/MobileKPD » →onglet « Macro-commandes »).

Les macro-commandes définies sont automatiquement téléchargées par l'application MOBILEKPD-2 PRO après l'établissement de la connexion avec le module ETHM-1 Plus.

Les macro-commandes peuvent être chargées dans l'application sans l'établissement de la connexion avec le module. Le fichier avec les macro-commandes peut être exporté et enregistré ensuite dans la mémoire du téléphone (pour transférer le fichier, utiliser une carte mémoire ou d'autres solutions disponibles pour l'appareil donné). Cette méthode permet à l'application MOBILEKPD-2 PRO d'utiliser les macro-commandes définies pour le clavier INT-KSG. Au lieu d'un fichier avec les macro-commandes définies pour le module ETHM-1 Plus, il est possible de charger un fichier avec les macro-commandes définies pour le clavier.



Les données relatives aux macro-commandes sont stockées dans la mémoire du module. Avant de commencer à définir les macro-commandes, cliquer sur le bouton « Lire » dans l'onglet « Macro-commandes » pour lire les données depuis le module. Après avoir défini les macro-commandes, cliquer sur le bouton « Enregistrer » dans l'onglet « Macro-commandes » pour enregistrer les données dans le module. Les données relatives aux macro-commandes ne sont pas lues / enregistrées, lorsque



l'on clique sur le bouton au menu principal du logiciel DLOADX.

## 6.4.1 Groupes

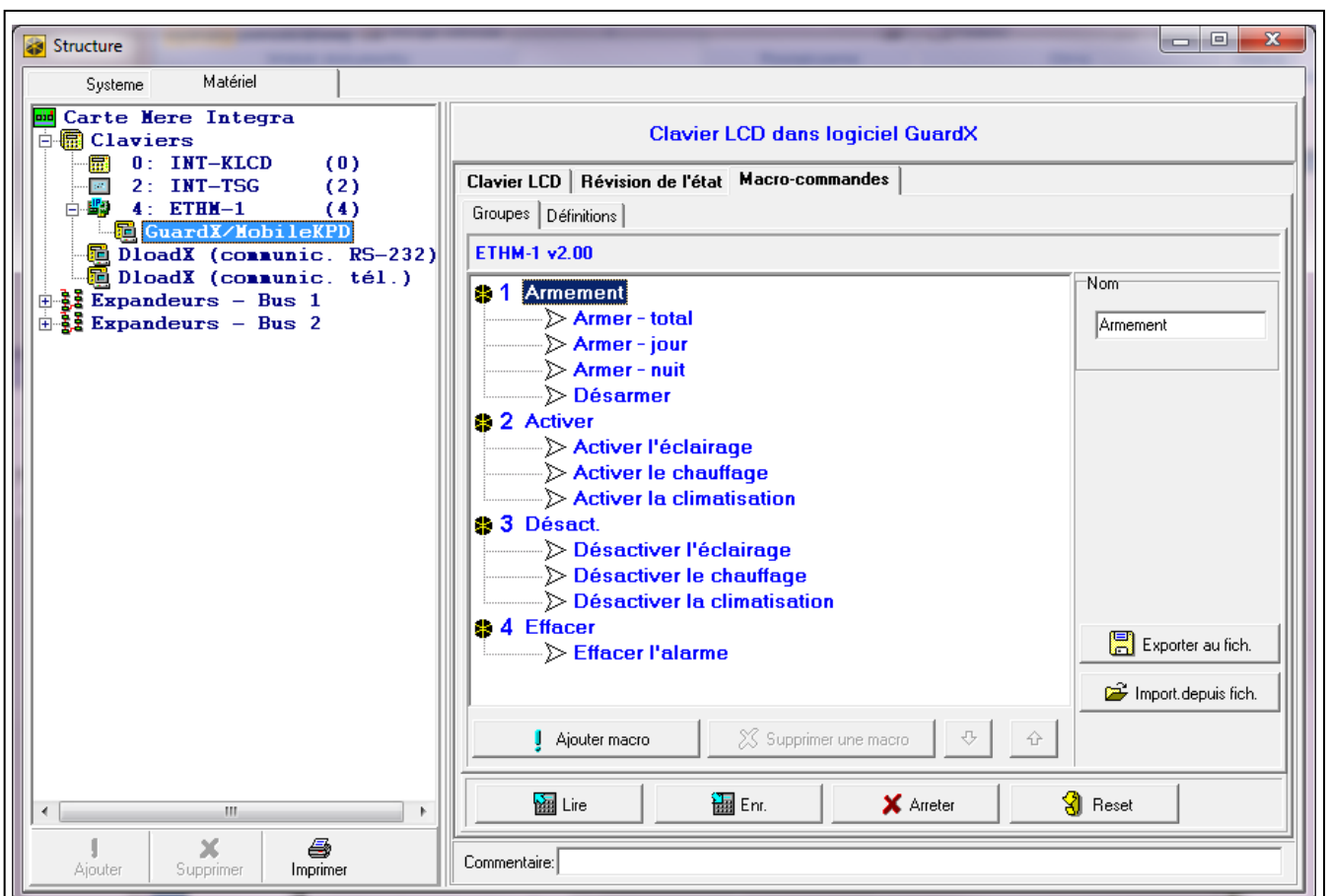


Fig. 9. Logiciel DLOADX : onglet « Groupes ».

Les macro-commandes devant être disponibles aux utilisateurs du clavier doivent être affectées à l'une de quatre groupes. 16 macro-commandes peuvent être attribuées à un groupe. Le logiciel DLOADX représente les groupes de macro-commandes et les macro-commandes qui y sont affectées sous forme de l'arborescence.

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

**Ajouter macro** – le bouton disponible après le clic sur le groupe de macro-commandes. Si l'on clique sur ce bouton, la liste des macro-commandes définies s'affiche. Pour ajouter une macro-commande au groupe, cliquer son nom.

**Supprimer une macro** – pour supprimer une macro-commande sélectionnée dans le groupe, cliquer sur ce bouton.



– cliquer sur le bouton pour déplacer une macro-commande sélectionnée du groupe en bas.



– cliquer sur le bouton pour déplacer une macro-commande sélectionnée du groupe en haut.

**Lire** – cliquer sur le bouton pour lire les données relatives aux macro-commandes du module.

**Enr.** – cliquer sur le bouton pour enregistrer les données relatives aux macro-commandes du module.

**Arrêter** – cliquer sur le bouton pour arrêter la lecture ou l'enregistrement des données relatives aux macro-commandes du module.

**Reset** – cliquer sur le bouton pour supprimer toutes les macro-commandes définies (restauration des paramètres d'usine).

**Exporter au fich.** – cliquer sur le bouton pour exporter les macro-commandes définies à un fichier. Le fichier avec les macro-commandes peut être chargé dans l'application MOBILEKPD-2 PRO ou importé à un autre module ETHM-1 Plus ou au clavier INT-KSG (les macro-commandes peuvent être copiées entre les dispositifs).

**Import.depuis fich.** – cliquer sur le bouton pour importer les macro-commandes depuis le fichier.

## 6.4.2 Définitions

Pour créer et configurer les macro-commandes, cliquer sur l'onglet « Définitions ». La macro-commande est une séquence d'opérations composée de commandes singulières qui sera exécutée par la centrale, une fois la macro-commande activée.

**Nouvelle macro** – cliquer sur le bouton pour créer une nouvelle macro-commande.

**Supprimer une macro** – cliquer sur le bouton pour supprimer la macro-commande sélectionnée.

**Nom** – 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 requisite** – 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.



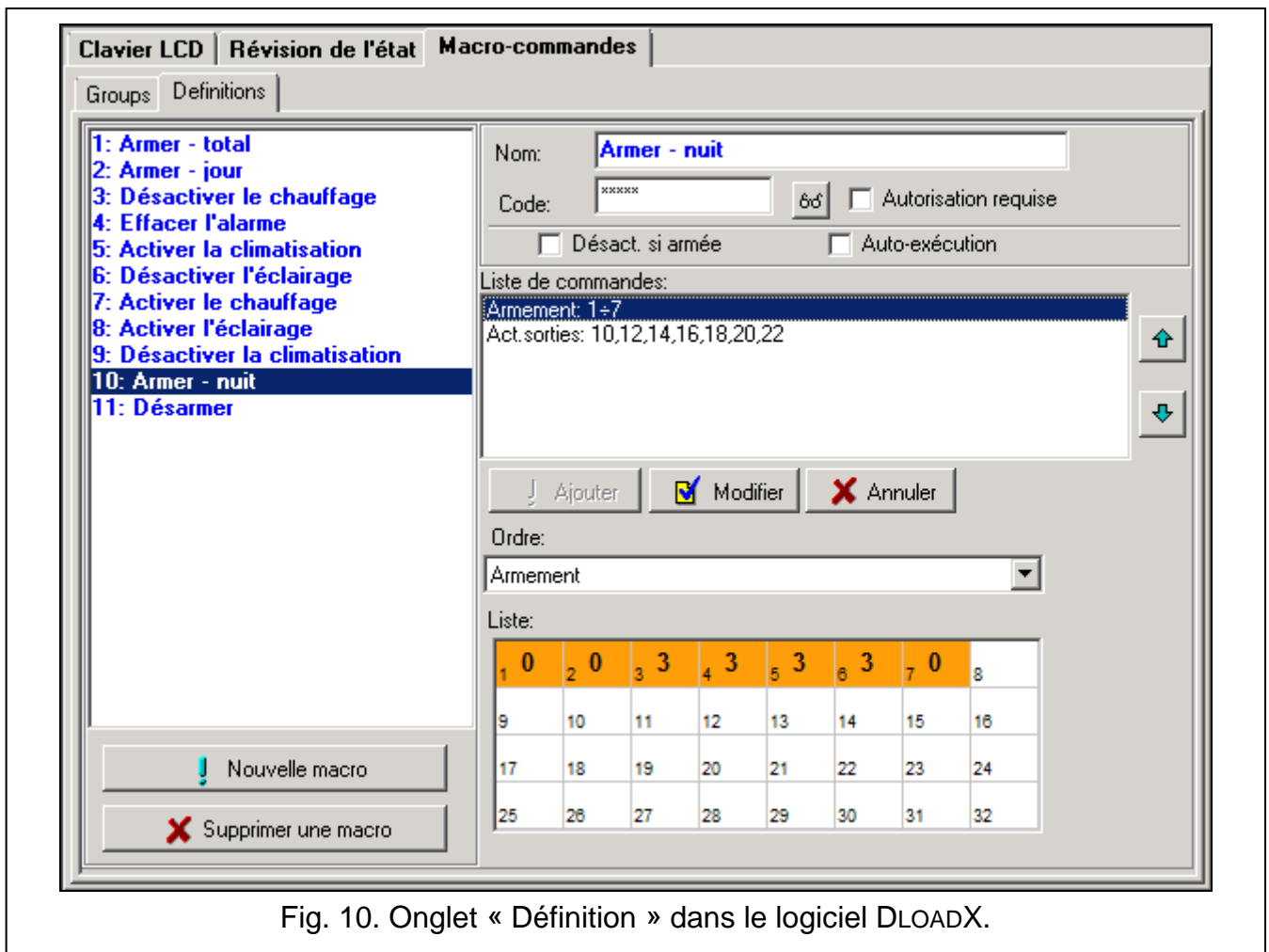




Fig. 10. Onglet « Définition » dans le logiciel DLOADX.

**Désact. 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.


**Auto-exécution** – 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).

**Liste de commandes** – les commandes affectées à la macro-commande actuellement sélectionnée. Les boutons  et  permettent le changement de l'ordre de commandes (déplacement de la commande sélectionnée en bas ou en haut).

**Ajouter** – cliquer sur le bouton pour ajouter une nouvelle commande sélectionnée dans le champ « Commande » à la liste de commandes.

**Modifier** – cliquer sur le bouton pour enregistrer les modifications dans les paramètres de la commande effectuées après l'ajout de la commande à la liste (sinon, les modifications apportées ne seront pas enregistrées).

**Annuler** – cliquer sur le bouton pour supprimer la commande sélectionnée.

**Ordre** – la fonction réalisée par la centrale qui peut être affectée à la macro-commande. Pour afficher la liste de toutes les fonctions disponibles, cliquer sur le bouton . Selon la fonction sélectionnée :

**Armement** – sélectionner les partitions à armer (double-cliquer sur le champ portant le numéro de la partition) et déterminer le type d'armement (clics suivants sur le champ portant le numéro de la partition ; le chiffre au milieu veut dire : 0 – armement total ;

1 - armement total + blocages ; 2 – armement sans intérieures ; 3 - armement sans intérieures et sans temporisation d'entrée).

**Désarmement** – sélectionner les partitions à désarmer (double-cliquer sur le champ portant le numéro de la partition).

**Effacement alar.** – sélectionner les partitions dans lesquelles l'alarme doit être effacée (double-cliquer sur le champ portant le numéro de la partition).

**Blocage zones** – sélectionner les zones à bloquer temporairement (double-cliquer sur le champ portant le numéro de la zone).

**Débloccage zones** – sélectionner les zones à débloquer (double-cliquer sur le champ portant le numéro de la zone).

**Act.sorties** – sélectionner les sorties à activer (double-cliquer sur le champ portant le numéro de la sortie).

**Sorties OFF** – sélectionner les sorties à désactiver (double-cliquer sur le champ portant le numéro de la sortie).

**Change outputs state** – sélectionner les sorties dont l'état doit changer (double-cliquer sur le champ portant le numéro de la sortie).

**Télégramme KNX** – programmer les paramètres suivants du télégramme KNX :

**Module INT-KNX** – le module INT-KNX qui va envoyer le télégramme.

**Adresse du groupe** – l'adresse du groupe qui sera insérée dans le télégramme.

**Type** – le type du télégramme.

**Valeur** – la valeur qui sera insérée dans le télégramme (paramètre disponible pour certains types du télégramme).

**Priorité** – la priorité du télégramme (si deux éléments du bus commencent à émettre en même temps, le télégramme avec la priorité plus élevée sera envoyé comme premier).

**Réduc. temp. sortie** (aucun paramètre supplémentaire à configurer).

**Armement rapide** – sélectionner le type de l'armement à activer.



*Les partitions doivent être commandées par le code de l'utilisateur.*

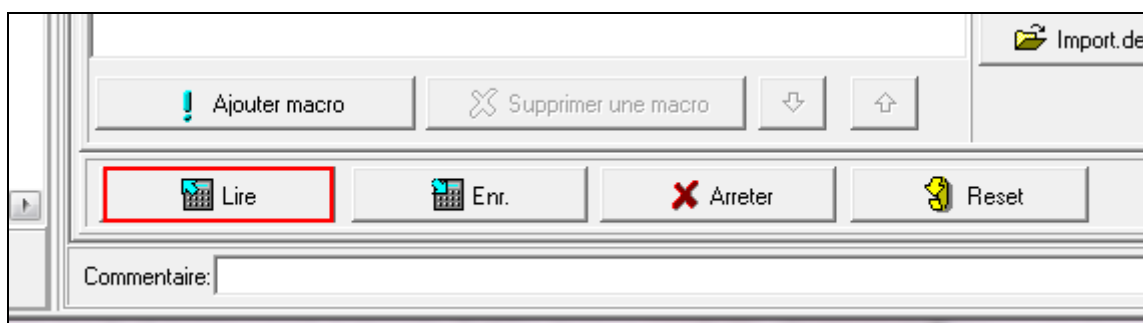
*L'option BLOCAGE INDISPONIBLE ne peut pas être activée dans les zones.*

*Les sorties doivent être de type 24. COMMUTAT. MONO, 25. COMMUTAT. BI, 105. VOLET EN HAUT, 106. VOLET EN BAS OU RELAIS TELEPH. (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.*

### 6.4.3 Définir les macro-commandes

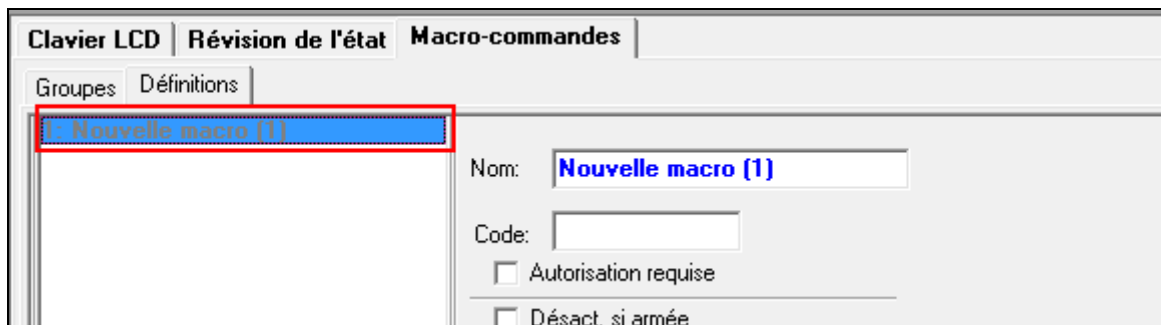
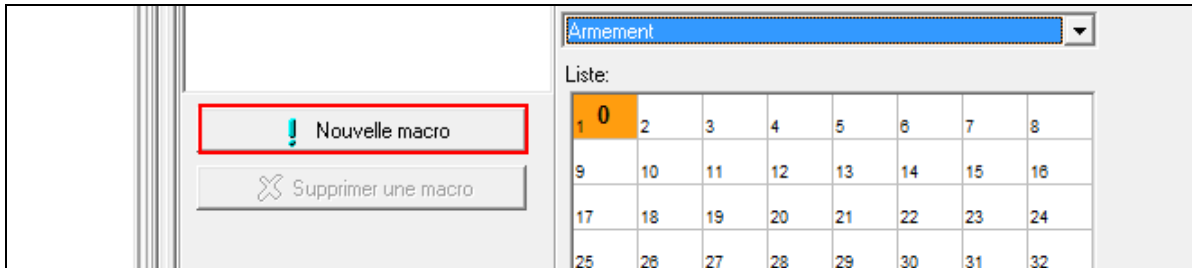
1. Cliquer sur le bouton « Lire » pour lire les données relatives aux macro-commandes depuis le module.



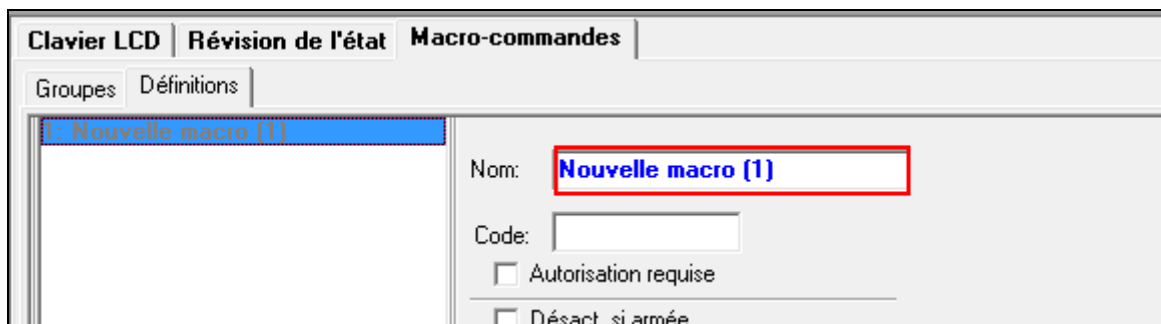
2. Cliquer sur l'onglet « Définitions ».



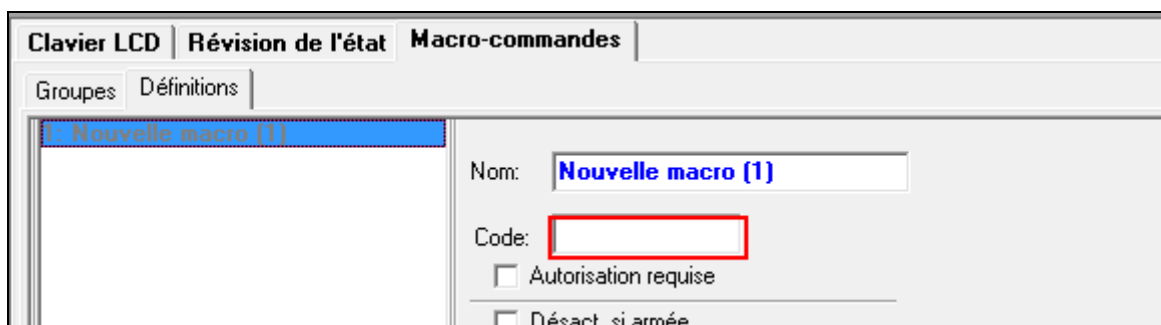
3. Cliquer sur le bouton « Nouvelle macro ». Une nouvelle macro-commande apparaît dans la liste.



4. Entrer le nom de la nouvelle macro-commande.



5. Si la macro-commande peut être activée sans le code saisi par l'utilisateur, entrer le code ayant des autorisations appropriées.



6. Si l'activation de la macro-commande doit être chaque fois précédée de l'autorisation de l'utilisateur, activer l'option AUTORISATION REQUISE.

Clavier LCD | Révision de l'état | **Macro-commandes**

Groupes | Définitions

Nouvelle macro (1)

Nom: Nouvelle macro (1)

Code:

Autorisation requise

Désact. si armée

7. Si la macro-commande doit être indisponible lorsque l'une des partitions gérées par le clavier est armée, activer l'option DESACTIVEE SI ARMEE.

Code:

Autorisation requise

Désact. si armée

Auto-exécution

Liste de commandes:

8. Si la macro-commande doit être activée immédiatement après la pression de la touche macro, activer l'option AUTO-EXECUTION (dans ce cas, il est possible d'affecter une seule macro-commande au groupe).


Code:


Autorisation requise

Désact. si armée

Auto-exécution

Liste de commandes:

9. Cliquer sur le bouton  et sélectionner la fonction qui va activer la nouvelle macro-commande.

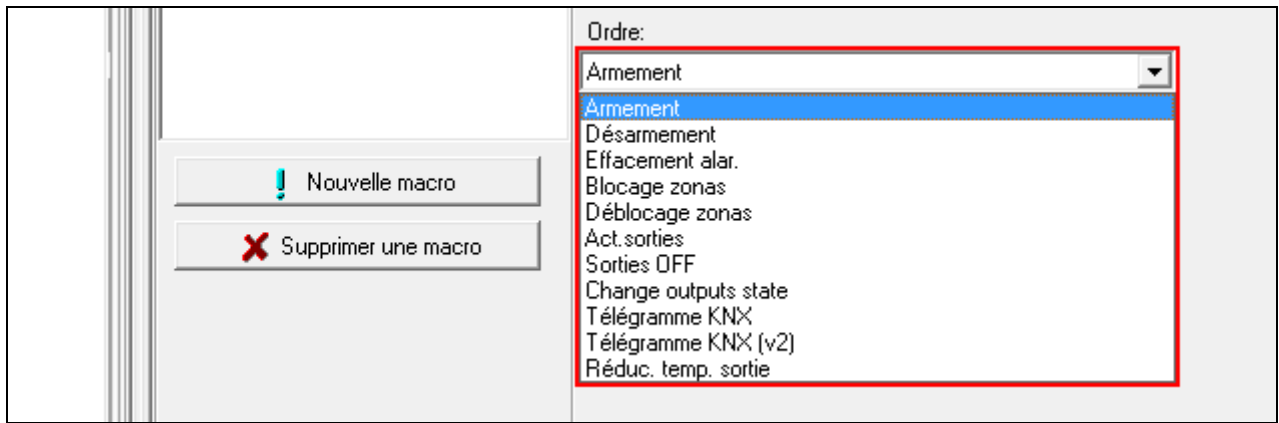
Ordre: Arment 

Liste:

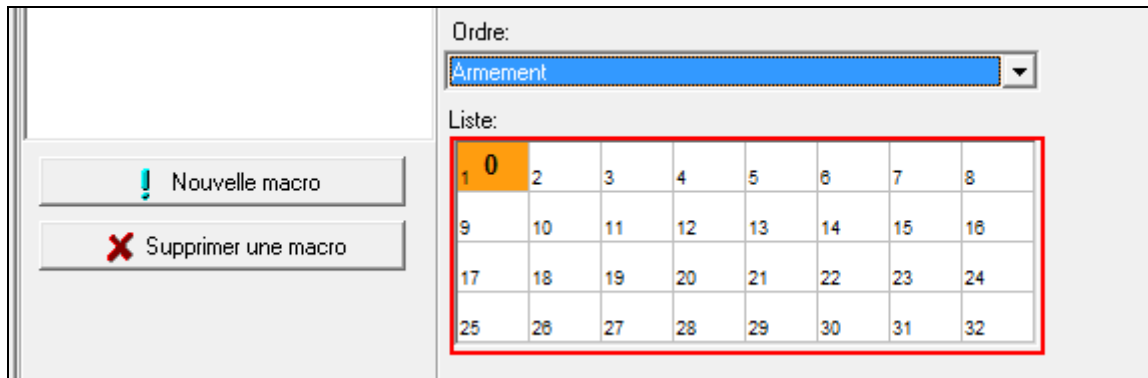
1	0	2	0	3	0	4	0	5	0	6	0	7	0	8
9	10	11	12	13	14	15	16							
17	18	19	20	21	22	23	24							

Nouvelle macro

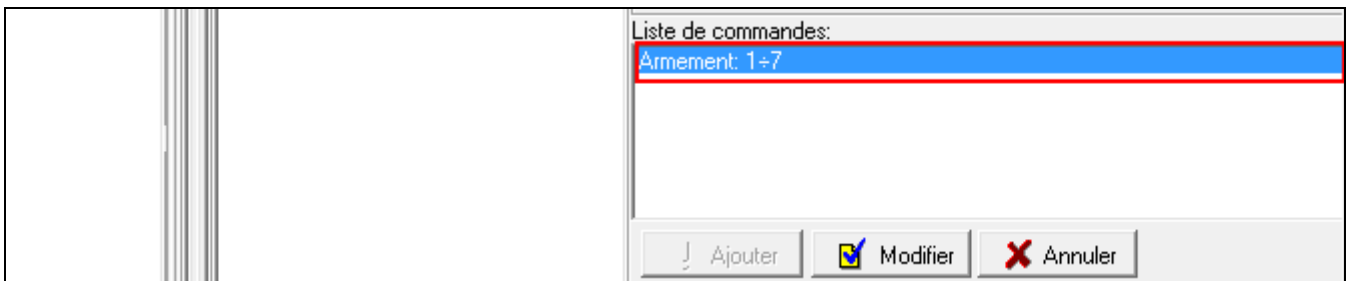
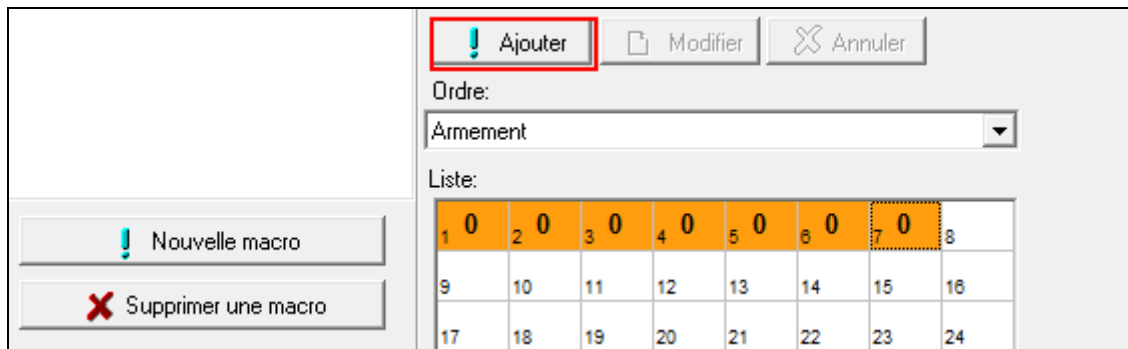
Supprimer une macro



10. Configurer les paramètres de la commande.



11. Cliquer sur le bouton « Ajouter ». Une nouvelle commande apparait dans la liste de commandes affectées à la macro-commande. Pour modifier ses paramètres, cliquer sur la commande (après avoir apporté des changements, cliquer sur le bouton « Modifier »).



12. Répéter les opérations des points 9-11 pour ajouter d'autres commandes.

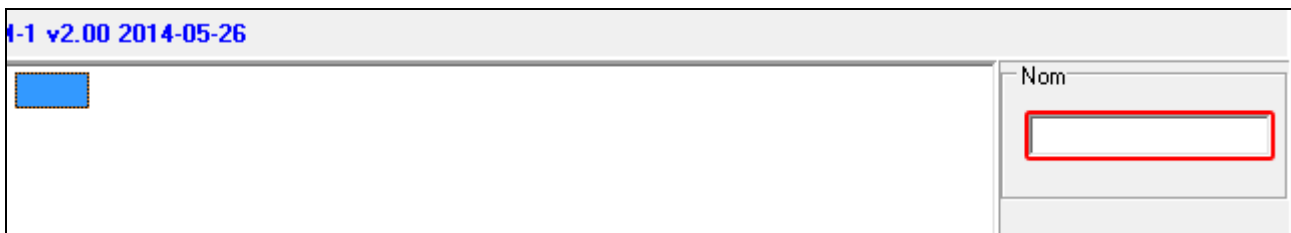
13. Cliquer sur l'onglet « Groupes ».



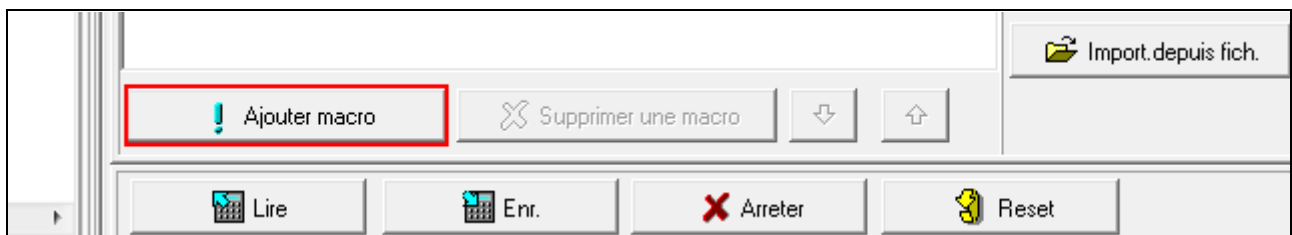
14. Cliquer sur le groupe à éditer.



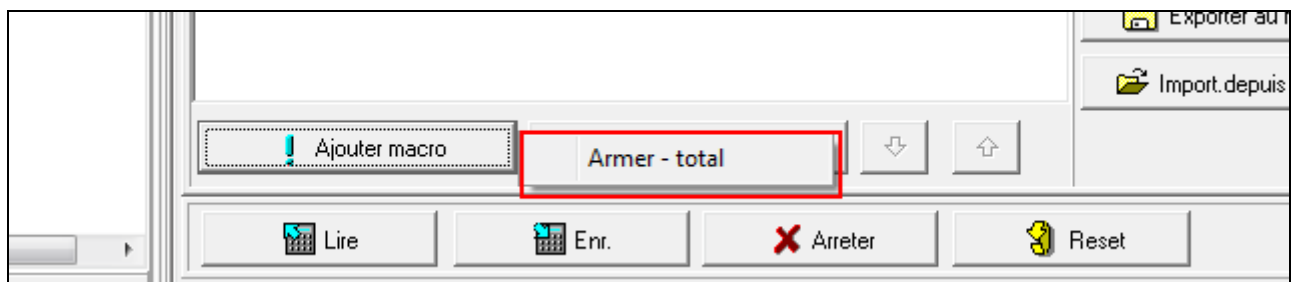
15. Entrer le nom du groupe.

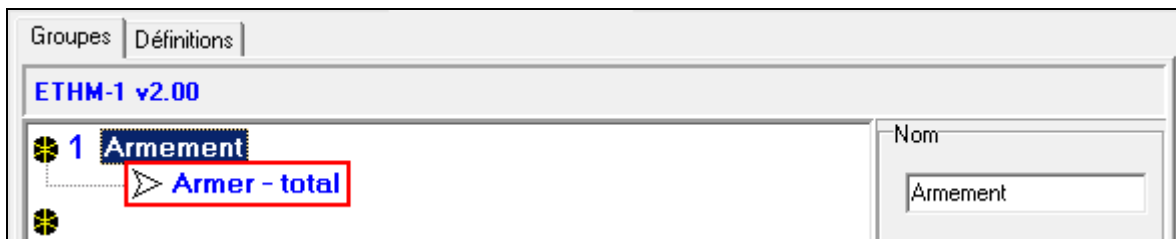


16. Cliquer sur le bouton « Ajouter macro ». La liste de toutes les macro-commandes définies s'affiche.

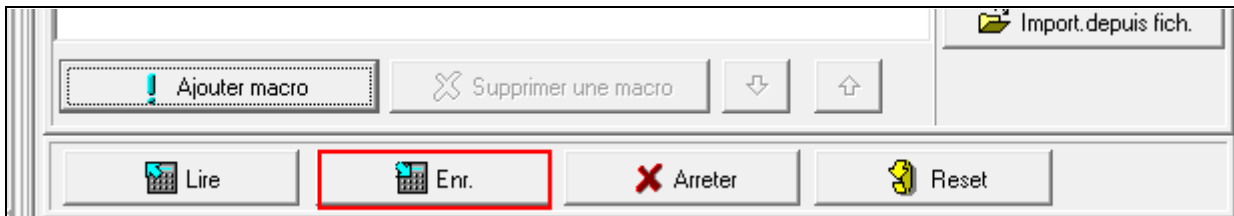


17. Cliquer sur la macro-commande pour l'ajouter au groupe. La macro-commande apparaît dans l'arborescence sous le groupe.





18. Cliquer sur le bouton « Enregistrer » pour enregistrer les données relatives aux macro-commandes au module.



#### 6.4.4 Export du fichier avec les macro-commandes



*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.

## 7 Programmation à distance et gestion de la centrale via Ethernet



*Pour la communication avec la centrale d'alarme en dehors du réseau local, le module doit avoir une adresse publique fixe.*

*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, veuillez vous référer au manuel de programmation de la centrale d'alarme.

### 7.1 Logiciel GuardX

La communication entre le logiciel GUARDX et la centrale d'alarme via le module ETHM-1 Plus 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.

- Initialiser la communication depuis le clavier (par la centrale d'alarme). Le système d'alarme peut être géré à distance uniquement au su de l'utilisateur depuis l'adresse programmée dans 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).

### 7.1.1 Configuration du module ETHM-1 Plus

- 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 différent de 7091.

### 7.1.2 Configuration du logiciel GUARDX

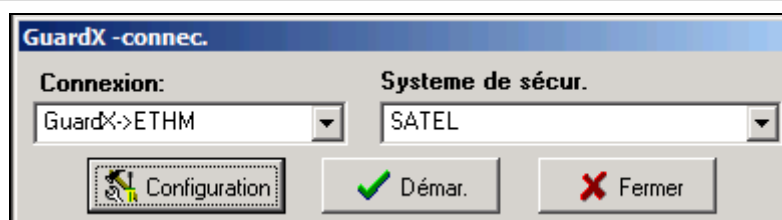


Fig. 11. Logiciel GUARDX : fenêtre de démarrage.

Dans la fenêtre de démarrage du logiciel GUARDX (fig. 11) cliquer sur le bouton « Configuration ». Dans la fenêtre qui s'affiche, dans l'onglet « TCP/IP » (fig. 12) programmer :

- adresse du module ETHM-1 Plus pour initialiser la communication depuis le logiciel GUARDX,
- 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 (CLE GUARDX/JAVA).

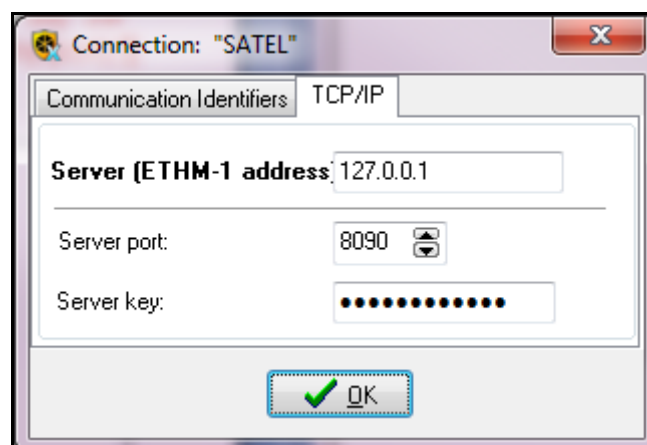


Fig. 12. Logiciel GUARDX : réglages de la communication via le réseau Ethernet.



### 7.1.3 Initialisation de la communication à partir du logiciel GUARDX

1. Dans la fenêtre de démarrage, dans le champ « Connexion », sélectionner « GuardX -> ETHM » (fig. 11), ensuite cliquer sur le bouton « Démarrer ».
2. Une fois la communication établie, dans la fenêtre qui apparaît entrer le code de l'administrateur / utilisateur de la centrale.

### 7.1.4 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]\* ► DOWNLOAD ► 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 apparaît entrer le mot de passe de l'administrateur / utilisateur de la centrale.

## 7.2 Navigateur WWW

---

### 7.2.1 Configuration du module ETHM-1 Plus

- 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).
- 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.

### 7.2.2 Configuration de l'ordinateur

La Machine Virtuelle JAVA doit être installée sur l'ordinateur (Java Virtual Machine).  
A télécharger sur [www.java.com](http://www.java.com)

### 7.2.3 Etablissement de la communication

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 (fig. 13) qui apparaîtra dans le navigateur :
  - clé de cryptage de données (CLE GUARDX/JAVA),
  - 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).

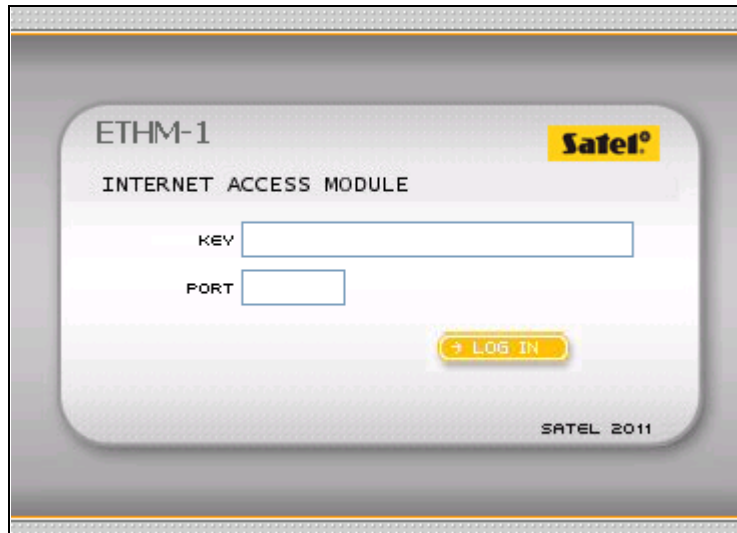


Fig. 13. Navigateur WWW : page de connexion.

4. Cliquer sur le bouton « Log in ».
5. Le clavier virtuel s'affiche dans le navigateur (fig. 14).

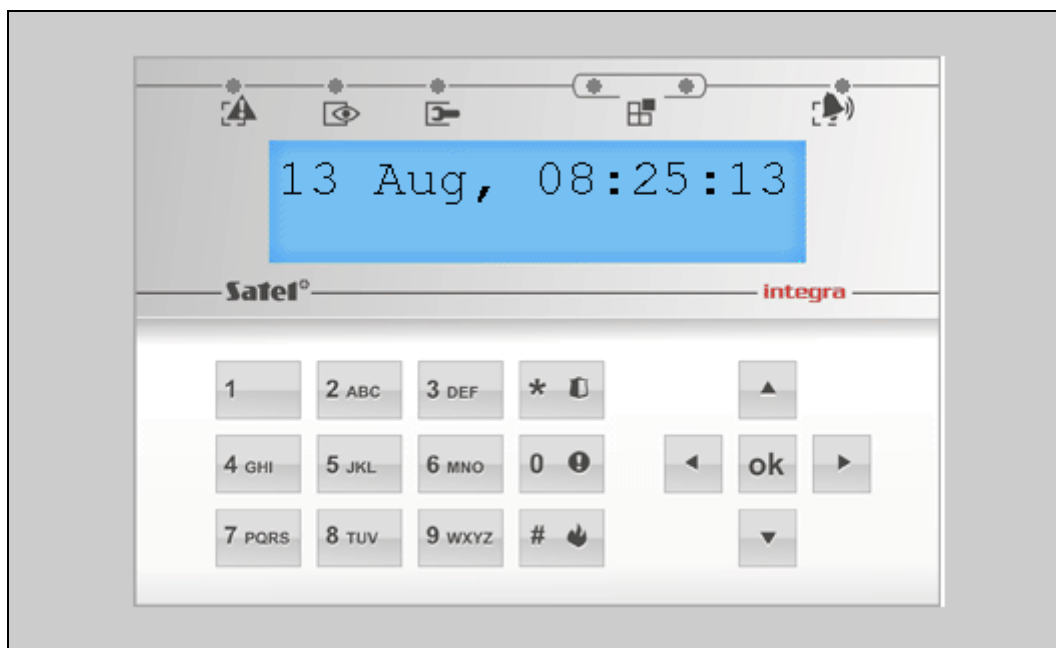


Fig. 14. Navigateur WWW : clavier virtuel.

## 7.3 Téléphone mobile

### 7.3.1 Configuration du module ETHM-1 Plus

- Activer l'option GSM.
- Programmer la clé servant à coder des données lors de la communication avec l'application MOBILEKPD / MOBILEKPD-2 / MOBILEKPD-2 PRO dans le téléphone mobile (CLE GUARDX/JAVA).
- Programmer le numéro du port TCP qui sera utilisé pour la communication avec l'application MOBILEKPD / MOBILEKPD-2 / MOBILEKPD-2 PRO dans le téléphone mobile, s'il doit être différent que 7091.

### 7.3.2 Configuration du téléphone mobile

Installer l'application MOBILEKPD / MOBILEKPD-2 / MOBILEKPD-2 PRO. dans le téléphone mobile. Il est possible de la télécharger sur le site [www.satel.pl](http://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 Plus ;
- le numéro du port TCP (identique à celui programmé dans le module pour la communication avec l'application MOBILEKPD / MOBILEKPD-2 / MOBILEKPD-2 PRO – sauf la situation où la communication se fait lieu via le dispositif réseau sur lequel la redirection vers un autre port a lieu) ;
- clé de cryptage de données (CLE GUARDX/JAVA).

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 – MOBILEKPD-2 PRO

Pour l'application MOBILEKPD-2 PRO, lors de la configuration des paramètres requis pour établir la communication avec le système d'alarme, les macro-commandes peuvent être chargées depuis le fichier. Indiquer le fichier comportant les macro-commandes et ensuite saisir le code de cryptage du fichier.

### 7.3.3 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.

### 7.3.4 Etablissement de la communication – MOBILEKPD-2 / MOBILEKPD-2 PRO

Toucher le nom du système d'alarme. Le clavier virtuel apparaît sur l'afficheur.



*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 apparaît immédiatement.*

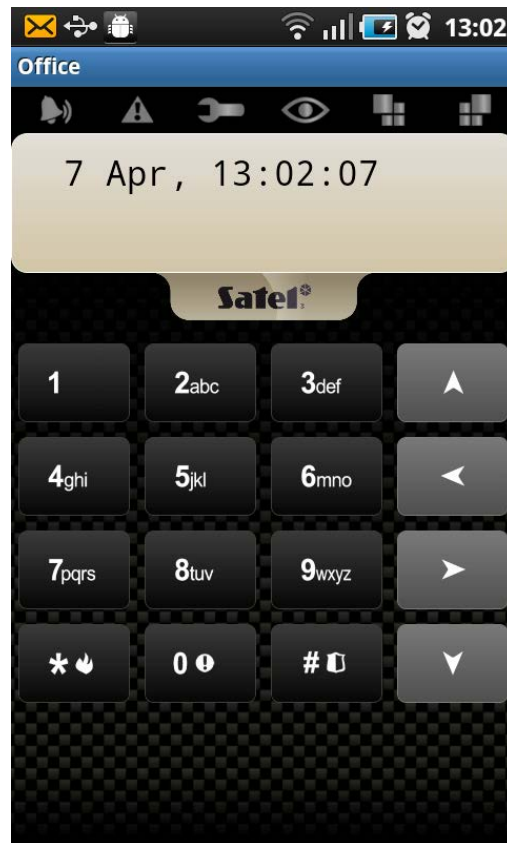


Fig. 15. Application MOBILEKPD-2 (téléphone avec le système Androïde) : clavier virtuel.

## 8 Spécifications techniques

Tension d'alimentation .....	12 V DC $\pm 15\%$
Consommation de courant en veille .....	70 mA
Consommation maximale de courant.....	80 mA
Classe environnementale selon EN50130-5 .....	II
Températures de fonctionnement .....	-10...+55 °C
Humidité maximale .....	93 $\pm$ 3%
Dimension .....	68 x 140 mm
Masse .....	64 g