

TERMINAUX TACTILES

## Guide de sécurité



Série HM

## Copyright et responsabilité

---

Copyright et responsabilité relatifs à cette documentation.

Copyright © 2024 Panasonic Industry Europe GmbH

Caroline-Herschel-Strasse 100, 85521 Ottobrunn, Allemagne

Dernière modification apportée le : 2024-07-23

Cette documentation et toutes les descriptions apparentées sont protégées par la législation sur la propriété intellectuelle. Aucune copie, même partielle n'est autorisée sans l'accord préalable écrit de Panasonic Industry Europe GmbH.

Panasonic Industry Europe poursuit une politique d'évolution constante du design et de la performance de ses produits. C'est la raison pour laquelle nous nous réservons le droit de modifier le contenu de la documentation/du produit sans notification préalable. Panasonic Industry Europe décline toute responsabilité en cas de dommages directs, particuliers, accidentels ou indirects résultant d'un défaut du produit ou d'une erreur dans sa documentation même si Panasonic Industry Europe en a été informée.

Si vous avez besoin d'une assistance technique, veuillez contacter l'[Assistance téléphonique Panasonic](#).

# Sommaire

---

<b>1 À propos de ce document.....</b>	<b>4</b>
<b>2 Politique de sécurité des produits Panasonic.....</b>	<b>5</b>
<b>3 Configuration par défaut du terminal tactile de la série HM.....</b>	<b>6</b>
<b>4 Scénarios de menaces potentielles.....</b>	<b>8</b>
<b>5 Mesures de sécurité générales.....</b>	<b>10</b>
<b>6 Bonnes pratique pour protéger votre terminal tactile.....</b>	<b>11</b>
6.1 Paramètres système.....	11
6.1.1 Protection par mot de passe.....	11
6.1.2 Paramètres pare-feu.....	11
6.1.3 Fichiers d'enregistrement et fonctionnalités de débogage SSH.....	12
<b>7 FAQ.....</b>	<b>13</b>
<b>8 Liste de vérification des configurations de sécurité.....</b>	<b>14</b>
<b>9 Assistance téléphonique Panasonic.....</b>	<b>16</b>
<b>10 Suivi des modifications.....</b>	<b>18</b>

# 1 À propos de ce document

---

Avec une numérisation croissante et une interconnectivité des réseaux en progression, les risques internes et externes en matière de cybersécurité évoluent.

Le BSI (Office fédéral allemand de la sécurité des technologies de l'information), par exemple, a publié un rapport avec les dix menaces les plus fréquentes et défini des règles et réglementations pour les produits en réseau dans des systèmes de contrôle industriels (ICS) :

- Infiltration d'un logiciel malveillant via un média amovible et un matériel externe
- Infection avec un logiciel malveillant via Internet et Intranet
- Erreur humaine et sabotage
- Compromission de composants d'extranet et du cloud
- Ingénierie sociale et hameçonnage (phishing)
- Attaques (D)DoS
- Composants de contrôle connectés à Internet
- Intrusion via un accès à distance
- Dysfonctionnement technique et force majeure
- Compromission de smartphones dans un environnement de fabrication

Source : <https://www.bsi.bund.de/ICS> 


Ce document contient des informations sur le dispositif, qui sont nécessaires à la gestion du réseau et qui vous aideront à protéger le terminal tactile de la série HM contre des risques en matière de sécurité.

---

## 2 Politique de sécurité des produits Panasonic

---

Les produits et services Panasonic sont améliorés continuellement. Nos produits sont développés en respectant des règles de sécurité strictes et sont soumis à des tests approfondis avant l'expédition. La politique de sécurité de Panasonic est basée sur les directives internationales spécifiées par les normes CEI 62443 et ISO/IEC 27001.

[Panasonic Product Security Incident Response Team](#)  (Panasonic PSIRT) est le centre de coordination en matière de vulnérabilités relatives aux produits Panasonic.

### 3 Configuration par défaut du terminal tactile de la série HM

Les fonctions réseau intégrées du terminal tactile de la série HM représentent un risque potentiel en matière de sécurité. Veillez à modifier les paramètres par défaut pour éliminer ou minimiser ce risque.

- Pour les produits fabriqués à partir de mai 2024, il n'y a pas de mot de passe par défaut défini et lors de la première connexion au dispositif, vous devez entrer un mot de passe selon un minimum de règles prédéfinies. Pour les versions précédentes, un mot de passe par défaut a été défini et nous recommandons de changer ce mot de passe par défaut dès que possible.
- Les ports Ethernet sont configurés en tant que client DHCP.
- Par défaut, les ports suivants sont ouverts et en mode écoute :

N° du port	Protocole	Fonction
80, 8000, 443	TCP	Utilisé pour la configuration via le navigateur et pour les pages web utilisateur
53	TCP	Utilisé pour le service DNS
990-991	UDP	Utilisé pour la détection de dispositifs via broadcast
21 (BSP 1.0 avant 05/2024)	TCP	Ports des données FTP (mode FTP passif : 16384-17407/TCP)
18756-18759	TCP	Ports des données FTP, sécurisés
990 (à partir de BSP 1.3 05/2024)	TCP	Temps d'exécution et gestion de projets

- À l'exception de la fonction scripts d'exécution automatique, toutes les fonctionnalités et tous les services du terminal tactile de la série HM pouvant présenter un risque de vulnérabilité ont été désactivés départ usine. Les services sont répertoriés sous IP/machine\_config##/services.

Service	Risque en matière de sécurité
Scripts d'exécution automatique	Applications démarrées à partir d'une mémoire externe, par ex. une clé USB
Démon Avahi	Ouvre le port 5353 (pour collecter des informations et rechercher des fonctionnalités)
Service cloud	Par exemple, une configuration serveur OpenVPN utilisée précédemment
Serveur DHCP	Ouvre les ports 67, 68
Serveur SNMP	Ouvre les ports 161, 10161 (pour collecter des informations)
Serveur SSH	Ouvre le port 22 (connexion avec identifiants administrateur et exécution de commandes)
Serveur VNC	Ouvre le port 5900 (page web et contrôle de dispositifs)

- 
- Par défaut, le pare-feu implémenté dans le terminal tactile de la série HM (IP/machine\_config/#/services) est désactivé.
  - Le terminal tactile de la série HM écrit des données d'enregistrement et des informations relatives à un fonctionnement atypique du dispositif dans des fichiers d'enregistrement. Ces fichiers sont enregistrés dans le dispositif et peuvent être téléchargés avec des identifiants administrateur.

## AVIS

Utilisez le pare-feu pour fermer tous les ports qui ne sont pas utilisés mais veillez à ce que le port Ethernet 443 soit ouvert et entré dans la configuration du pare-feu (pour BSP 1.0, vous devez aussi ouvrir le port 80). Sinon, l'accès à la page paramètres système sera refusé en permanence.

## Thèmes apparentés

[Paramètres pare-feu](#) (page 11)

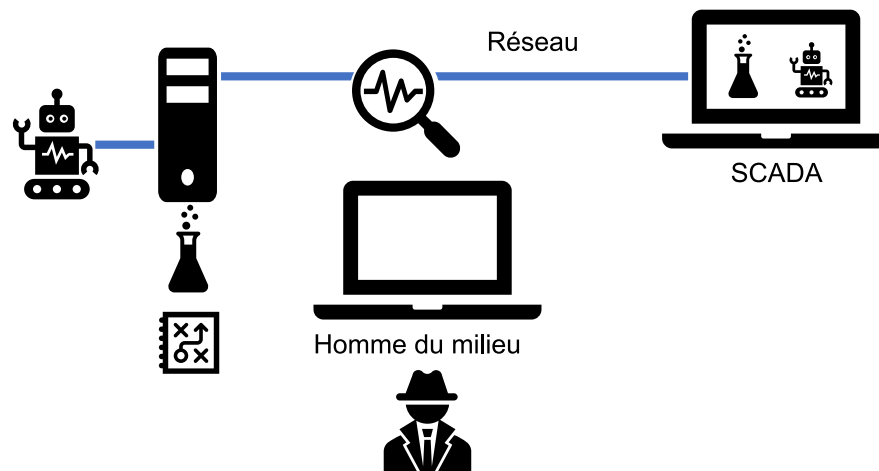
## 4 Scénarios de menaces potentielles

Voici quelques exemples de menaces cyber potentielles vous permettant de mieux comprendre et de mieux prendre conscience des risques en matière de cybersécurité.

- Acquisition des données

De nombreux outils permettent de lire les données transmises dans un réseau, y compris les données d'utilisateur, mots de passe et autres données sensibles telles que les recettes et données du process.

Si les données du réseau transmises ne sont pas chiffrées, alors, elles sont une cible facile pour un espion à la recherche d'informations lisibles.

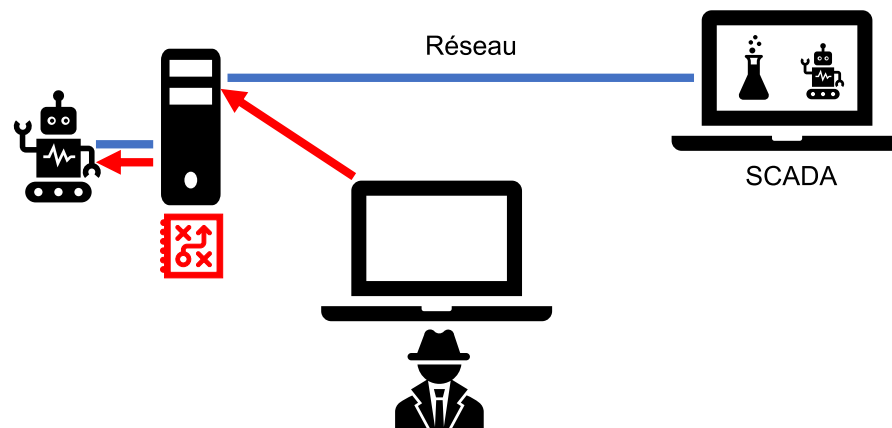


Mesures :

N'utilisez pas de protocole FTP ou Telnet en dehors d'un réseau encapsulé pour transmettre des données sensibles. Ces protocoles créent un risque élevé en matière de sécurité car les noms d'utilisateur et mots de passe sont transmis en texte clair.

- Accès aux systèmes de contrôle

Si les identifiants ou le protocole sont connus, des machines peuvent être endommagées et des dispositifs peuvent être détournés en botnets ou manipulés pour attaquer d'autres dispositifs.



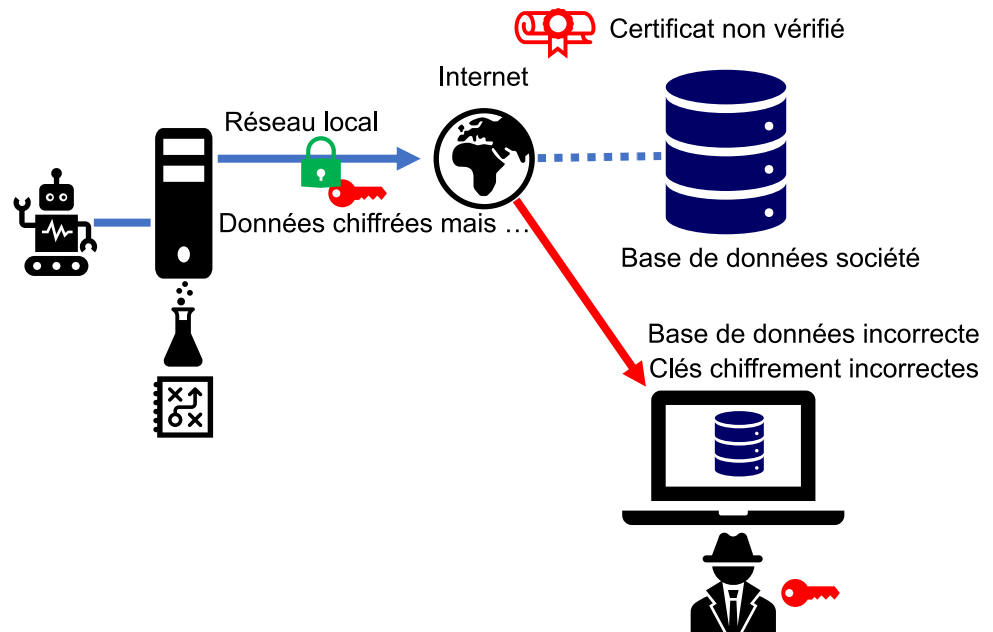


Mesures :

Ne permettez pas l'accès ou le contrôle à des ordinateurs tiers.

- Usurpation d'identité

Les connexions à des pages web qui ne sont pas vérifiées par une autorité de certification peuvent représenter un danger car elles facilitent l'usurpation d'identité et la redirection de la communication. Des attaquants peuvent ainsi acquérir des données sensibles (par exemple les noms d'utilisateur, mots de passe, données de process ou recettes) et endommager des machines en les manipulant.



Mesures :

Veillez à utiliser des certifications pour authentifier l'identité du serveur de destination.

## 5 Mesures de sécurité générales


---

Implémenter des mesures pour protéger votre réseau est essentiel pour garantir la sécurité de votre réseau et des données transmises.

Ce produit va être utilisé dans un réseau, il est donc important de prendre en compte les risques suivants en matière de sécurité.

- Fuite ou vol d'informations via ce produit
- Utilisation de ce produit à des fins illégales par des personnes ayant des intentions malveillantes
- Interférence ou arrêt de ce produit par des personnes ayant des intentions malveillantes
- Il est de la responsabilité de l'utilisateur de prendre les précautions telles que celles décrites ci-dessous pour protéger le réseau contre les risques en matière de sécurité.
- Si ce produit est connecté en réseau avec des ordinateurs, vérifiez que le système n'est pas contaminé par un virus ou autre entité malveillante (avec un logiciel antivirus ou anti-espion régulièrement mis à jour, etc.).
- Utilisez ce produit dans un environnement doté d'un réseau local (LAN), d'un réseau privé virtuel (VPN) ou d'une ligne spécialisée.
- Utilisez ce produit dans un environnement accessible uniquement avec des droits d'accès contrôlés.
- Utilisez ce produit et les autres dispositifs connectés au réseau tels qu'un ordinateur ou une tablette, uniquement si vous avez pris les mesures de protection garantissant la sécurité du système.
- N'installez pas ce produit dans des endroits où le produit ou les câbles peuvent être détruits ou endommagés par des personnes ayant des intentions malveillantes.

Notez qu'une connexion au LAN existant avec des paramètres incorrects peut entraîner un dysfonctionnement des dispositifs dans le réseau. Consultez votre administrateur réseau avant de vous connecter.

Vous trouverez des informations très utiles sur Internet : [MITRE ATT&CK®](#)  est une base de connaissances et un modèle organisés de comportement des cyber-adversaires.

## 6 Bonnes pratique pour protéger votre terminal tactile

---

Vous pouvez minimiser les risques en matière de sécurité en prenant des mesures préventives et en procédant correctement au paramétrage des applications et du système. Utilisez la liste de vérification livrée dans ce guide pour vous assurer que toutes les mesures nécessaires ont été prises pour protéger le terminal tactile de la série HM.

Thèmes apparentés

[Liste de vérification des configurations de sécurité](#) (page 14)

### 6.1 Paramètres système

---

Allez dans “Paramètres système” (IP/machine\_config) pour entrer les paramètres du pare-feu et le mot de passe, pour accéder aux fichiers d’enregistrement et pour utiliser les fonctionnalités de débogage SSH.

#### 6.1.1 Protection par mot de passe

---

Définissez un mot de passe fort avec des lettres capitales et minuscules, des nombres et des caractères spéciaux (sauf espaces).

Les mots de passe pour le serveur FTP doivent être différents pour les applications HMWIN Studio et les paramètres principaux du terminal tactile de la série HM. Lorsqu’un terminal tactile est mis sous tension la première fois, vous devez entrer un mot de passe sûr. Vous pouvez le faire directement sur l’écran ou via un navigateur connecté au dispositif via son adresse IP (IP/machine\_config).

#### 6.1.2 Paramètres pare-feu

---

Utilisez le pare-feu (IP/machine\_config/#!/services) pour fermer tous les ports non utilisés.

Lorsque vous activez “Firewall Service” (IP/machine\_config/#!/services), toutes les fonctionnalités utilisées sont activées avec les paramètres et ports spécifiés. Désactivez tous les services et ports non utilisés ou refusez l’accès aux interfaces dédiées (ETH0, ETH1 et ETH2).

AVIS

“Web Server – HTTP” et “Web Server – HTTPS” doivent être activés et le port Ethernet 443 doit être ouvert (le port 80 pour BSP 1.0 aussi). Sinon, l’accès à la page paramètres système sera refusé en permanence.

Exemple de paramètres pare-feu :

Nom	Interface source	Port ou plage	Protocole	Requis
Web server - HTTP (nécessaire à la configuration)	N'importe laquelle	80	TCP	✓ (BSP 1.0)
Web server - HTTPS (nécessaire à la configuration)	N'importe laquelle	443	TCP	✓
Détection de dispositifs	N'importe laquelle	990–991	UDP	✓
Port commande FTP, pour HMWIN Studio	N'importe laquelle	21	TCP	✓ (BSP 1.0)
Mode FTP passif, pour HMWIN Studio	N'importe laquelle	18756–18759	TCP	
Serveur SSH	N'importe laquelle	22	TCP	
Serveur VNC	N'importe laquelle	5900	TCP	
Serveur DHCP	N'importe laquelle	67	UDP	
Serveur SNMP	N'importe laquelle	161	UDP	
Ports de connexion API	N'importe laquelle	9094–9097	TCP	
Opérations HMWIN Studio	N'importe laquelle	990	TCP	

### 6.1.3 Fichiers d'enregistrement et fonctionnalités de débogage SSH

Ces fonctionnalités peuvent être utilisées pour détecter un fonctionnement inhabituel. Elles ne peuvent être utilisées qu'avec des identifiants administrateur.

## 7 FAQ

---

1. Est-ce que je peux avoir des correctifs du logiciel et des mises à jour du firmware ?  
Les téléchargements des dernières versions sont disponibles gratuitement sur le site internet de : [Panasonic à la page Téléchargements](#) ou dans l'[InfoHub](#)
2. Une porte dérobée (backdoor) est-elle installée sur le dispositif ?  
Il n'y a pas de porte dérobée (backdoor) installée sur le dispositif. Si vous perdez votre mot de passe, vos paramètres ne peuvent plus être rétablis.
3. Est-ce que le dispositif appelle un serveur Panasonic ?  
Avec les paramètres par défaut, aucun processus n'appelle automatiquement un serveur Panasonic.
4. Où signaler une nouvelle vulnérabilité ?  
Veuillez contacter [Panasonic Product Security Incident Response Team](#) (Panasonic PSIRT), le centre de coordination en matière de vulnérabilités relatives aux produits Panasonic.

## 8 Liste de vérification des configurations de sécurité

Utilisez cette liste de vérification pour vous assurer que toutes les mesures nécessaires ont été prises pour protéger le terminal tactile de la série HM. Cochez tous les éléments qui ont été mis en place. À la fin de la liste, il y a de l'espace pour des éléments supplémentaires.

Vérifié	Risque <sup>1)</sup>	Zone	Page de configuration	À faire
	Élevé	Mots de passe (admin., utilisateur)	IP/machine_config/##/authentication	Modifier pour des mots de passe administrateur et utilisateur sécurisés
	Élevé	Service : Scripts d'exécution automatique	IP/machine_config/##/services	Désactiver
	Élevé	Service : Serveur SSH	IP/machine_config/##/services	Désactiver, si non nécessaire
	Faible	Démon Avahi	IP/machine_config/##/services	Désactiver, si non nécessaire
	Faible	Service cloud	IP/machine_config/##/services	Désactiver, si non nécessaire
	Faible	Serveur DHCP	IP/machine_config/##/services	Désactiver, si non nécessaire
	Faible	Service VNC	IP/machine_config/##/services	Désactiver, si non nécessaire
	Faible	Pare-feu	IP/machine_config/##/services	Activer et adapter les paramètres
	Élevé	Mots de passe HMWIN (au moins admin., utilisateur, log)	HMWIN Studio Project/Configuration/Security	Changer les mots de passe administrateur et utilisateur par défaut
	Élevé	Configuration des protocoles	HMWIN Studio Project/Configuration/ Protocols	Désactiver les fonctionnalités passthrough (mode transparent) et les protocoles serveurs si non nécessaires Sélectionner les variantes chiffrées des protocoles bus de terrain utilisés
	Moyen	Fonctionnalité HMWIN OPC UA	HMWIN Studio Project/Configuration/Interface	Vérifier l'accès au serveur
	Moyen	Fonctionnalité MQTT HMWIN	HMWIN Studio Project/Configuration/Interface	Utiliser chiffrement et certificats

Vérifié	Risque <sup>1)</sup>	Zone	Page de configuration	À faire
	Moyen	Fonctionnalités Javascript SMTP et FTP	HMWIN Studio Vérifier les événements configurés (par ex. e-mail, FTP, caméra web ...)	Utiliser chiffrement et certificats

1) Le niveau de risque dépend de votre application.


## 9 Assistance téléphonique Panasonic


---

Si vous avez des questions auxquelles les manuels ou l'aide en ligne ne peuvent pas répondre, veuillez contacter une de nos succursales locales.

En disposant des informations suivantes, vous nous aiderez à répondre au mieux à vos questions :

- Le numéro de série et/ou le numéro de version de votre produit.
- Les numéros de version et Service Pack de Microsoft Windows installés sur votre ordinateur.
- Le type de matériel que vous utilisez.
- Le message exact qui apparaît sur votre écran.
- Que s'est-il passé et que faisiez-vous lorsque le problème est apparu ?
- Qu'avez-vous fait pour essayer de résoudre le problème ?

Composez un des numéros de l'assistance téléphonique ou utilisez notre [formulaire de contact](#)  pour nous envoyer votre demande de renseignements.

Pour contacter l'assistance technique en dehors de l'Europe, veuillez consulter notre [site Internet global](#) .

### Panasonic Industry Europe GmbH

- Allemagne et pays européens non répertoriés sur cette page :  
+49 89 45354-2748 (automates, FP-I4C, écrans tactiles)  
+49 89 45354-2737 (capteurs)  
+49 89 45354-2750 (servosystèmes)
- France :  
+33 160 135757

### Panasonic Industry Austria GmbH

Autriche, Bosnie-Herzégovine, Bulgarie, Croatie, Monténégro, Serbie, Slovénie, Suisse :  
+43 2236 26846

### Panasonic Industry Benelux B.V.

Belgique, Danemark, Luxembourg, Norvège, Pays-Bas, Suède :  
+31 499 372727

### Panasonic Industry Italia srl

Italie :



+39 045 6752711, [support.piit@eu.panasonic.com](mailto:support.piit@eu.panasonic.com)

**Panasonic Industry Poland sp. z o.o.**

Finlande, Hongrie, Pays baltes, Pologne, République Tchèque, Roumanie, Slovaquie :

+48 42 2309633

**Panasonic Industry Iberia S.A.**

Portugal, Espagne :

+34 91 3293875

**Panasonic Industry UK Ltd.**

Royaume-Uni de Grande-Bretagne et d'Irlande :

+44 1908 231555

## 10 Suivi des modifications

---

Guide de sécurité Version 1.0, 07.2024

Première édition