




CONTROLLORE PROGRAMMABILE

## **Guida alla sicurezza**



FP-Industry 4.0 Communicator  
(FP-I4C)

## **Responsabilità e copyright**

---

Il presente manuale e il suo contenuto sono protetti da copyright. Non è permesso copiare il manuale, né per intero né in parte, senza il consenso scritto di Panasonic Electric Works Europe AG (PEWEU).

PEWEU segue una politica di continuo miglioramento del design e delle prestazioni dei suoi prodotti. Pertanto ci riserviamo il diritto di modificare il manuale/prodotto senza preavviso. In nessun caso PEWEU potrà essere ritenuta responsabile di eventuali danni diretti, speciali, accidentali o consequenziali derivanti da difetti del prodotto o della relativa documentazione, anche se a conoscenza della possibilità del verificarsi di tali danni.

Per eventuali domande di carattere tecnico e richieste di supporto rivolgetevi al rappresentante Panasonic locale.

### **Panasonic Electric Works Europe AG (PEWEU)**

Caroline-Herschel-Strasse 100

85521 Ottobrunn, Germania

Tel: +49 89 45 354-1000

## Contenuto

---

Liability and copyright .....	2
1 About this document .....	4
2 Panasonic product security policy .....	4
3 Default configuration of the FP-I4C unit .....	4
4 Potential threat scenarios .....	6
5 General security measures .....	7
6 Best practices to harden your FP-I4C unit .....	8
6.1 System settings .....	8
6.1.1 Password protection .....	8
6.1.2 Firewall settings .....	8
6.1.3 Log files and SSH debugging features .....	9
6.2 Application settings .....	9
7 FAQ .....	11
8 Security configuration check list .....	12
Panasonic hotline .....	13
Record of changes .....	14

## 1 Informazioni su questo documento

---

I rischi interni ed esterni per la cyber security continuano ad aumentare con il progredire della digitalizzazione e la crescente interconnettività dei network.

Il BSI (Ufficio Federale Tedesco per la Sicurezza Informatica), per esempio, ha pubblicato una relazione con le dieci principali minacce e ha definito regole e raccomandazioni per i prodotti impiegati in network nei sistemi di controllo industriale (ICS):

- Infiltrazione di malware tramite supporti rimovibili e hardware esterno
- Infezione malware via Internet e Intranet
- Errore umano e sabotaggio
- Compromissione di componenti extranet e cloud
- Ingegneria sociale e phishing
- Attacchi (D)Dos
- Componenti di controllo collegati a Internet
- Intrusione tramite accesso remoto
- Malfunzionamenti tecnici e forza maggiore
- Compromissione di smartphone nell'ambiente di produzione

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

Il presente documento contiene le informazioni sul dispositivo necessarie per la gestione del vostro network e vi aiuterà a proteggere l'unità FP-I4C dai rischi per la sicurezza.

## 2 Criteri di sicurezza per i prodotti Panasonic

---

I prodotti e servizi Panasonic sono continuamente migliorati. Lo sviluppo dei nostri prodotti segue rigorosamente le regole di sicurezza ed esegue test approfonditi prima della spedizione. La politica di sicurezza di Panasonic si basa sulle linee guida internazionali stabilite da IEC 62443 e ISO/IEC 27001.

Il [Panasonic Product Security Incident Response Team](#) (Panasonic PSIRT) è il centro di coordinamento in materia di vulnerabilità associata ai prodotti Panasonic.

## 3 Configurazione di default dell'unità FP-I4C

---

Le capacità di network integrate nell'unità FP-I4C costituiscono un potenziale di rischio per la sicurezza. Per eliminare o minimizzare tale rischio occorre customizzare le impostazioni di default.

- Per consentire la configurazione dell'unità FP-I4C è stata impostata una password di default. Raccomandiamo di sostituire al più presto possibile la password predefinita.
- Le due porte Ethernet ETH0 e ETH1 hanno configurazioni diverse: La ETH0 è configurata come una DHCP client e la ETH1 è configurata con l'indirizzo IP fisso 192.168.0.1.
- Le porte seguenti sono aperte e in modalità di ascolto per default:

Porta n.°	Protocollo	Funzione
80, 8081, 443	TCP	Utilizzata per la configurazione di browser e pagine web di utenti
53	TCP	Utilizzata per servizio DNS
990-991	UDP	Utilizzata per individuazione di dispositivi tramite broadcast
21	TCP	Runtime e gestione dei progetti (modalità FTP passiva: 16384-17407/TCP, 18756-18759/TCP)
16384-17407, 18756-18759	TCP	Modalità FTP passiva

- Tutte le funzioni e i servizi dell'unità FP-I4C che potrebbero costituire un rischio di vulnerabilità sono stati disabilitati dal produttore.  
I servizi sono elencati in IP/machine\_config/#!/services.

Servizio	Rischio per la sicurezza
Script di autorun	Applicazioni avviate da un dispositivo di memorizzazione esterno, ad esempio una chiavetta USB
Avahi daemon	Apri la porta 5353 (utilizzata per raccogliere informazioni e trovare funzioni)
Servizio cloud	Ad esempio una configurazione di server OpenVPN utilizzata precedentemente
Server DHCP	Apri le porte 67, 68
Server SNMP	Apri le porte 161, 10161 (utilizzate per raccogliere informazioni)
Server SSH	Apri la porta 22 (login con credenziali di amministratore ed esecuzione di comandi)
Server VNC	Apri la porta 5900 (sito web e controllo dispositivi)

- Il firewall applicato nell'unità FP-I4C (IP/machine\_config/#!/services) è disattivato per default.
- L'unità FP-I4C scrive dati di log e informazioni di utilizzo atipiche in file di log. Questi file sono archiviati nell'unità e possono essere scaricati con le credenziali di amministratore.

**Nota:**

Utilizzate il firewall per chiudere porte non utilizzate, ma fate attenzione che le porte Ethernet 80 e 443 siano aperte e comprese nella configurazione del firewall. Altrimenti l'accesso alla pagina di impostazione del sistema sarà permanentemente negato.

**Argomenti correlati**

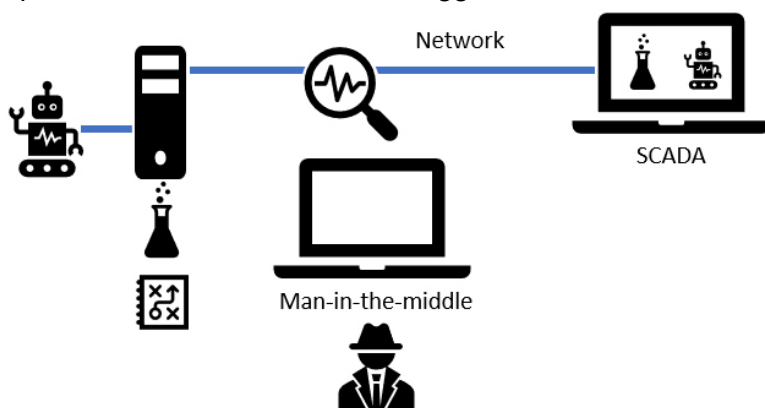
[Firewall settings](#)

## 4 Potenziali scenari di minaccia

Per aumentare la vostra consapevolezza degli scenari di minaccia e per una miglior comprensione, vi diamo alcuni esempi tipici di potenziali cyber minacce.

- **Cattura dei dati**

Per leggere il traffico di dati nel network, compresi nomi utente, password e altri dati sensibili, come ricette o dati di processo, sono disponibili numerosi strumenti. Soprattutto se il vostro traffico nella rete non è crittografato, è un facile bersaglio per spie alla ricerca di informazioni leggibili.

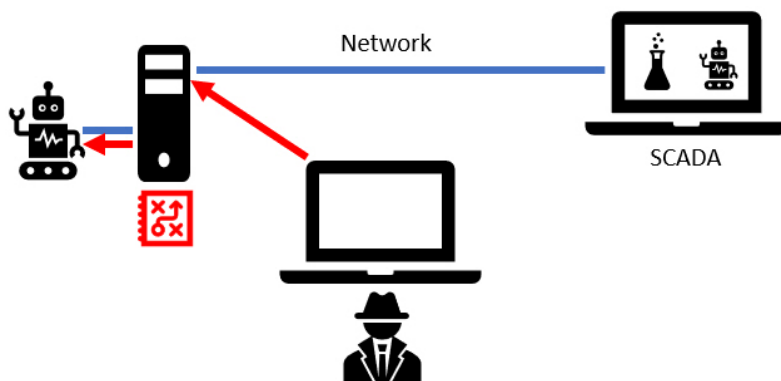


Contromisure:

Non utilizzate protocolli FTP o Telnet al di fuori di un network incapsulato per trasmettere dati sensibili. Questi protocolli rappresentano un alto rischio per la sicurezza perché i nomi utente e le password sono trasmessi in testi normali.

- **Ottenere l'accesso ai sistemi di controllo**

Se credenziali o il protocollo utilizzato sono noti, eventualmente possono essere causati guasti o danni alle macchine e i dispositivi possono essere dirottati in botnet o essere manipolati per attaccare altri dispositivi.

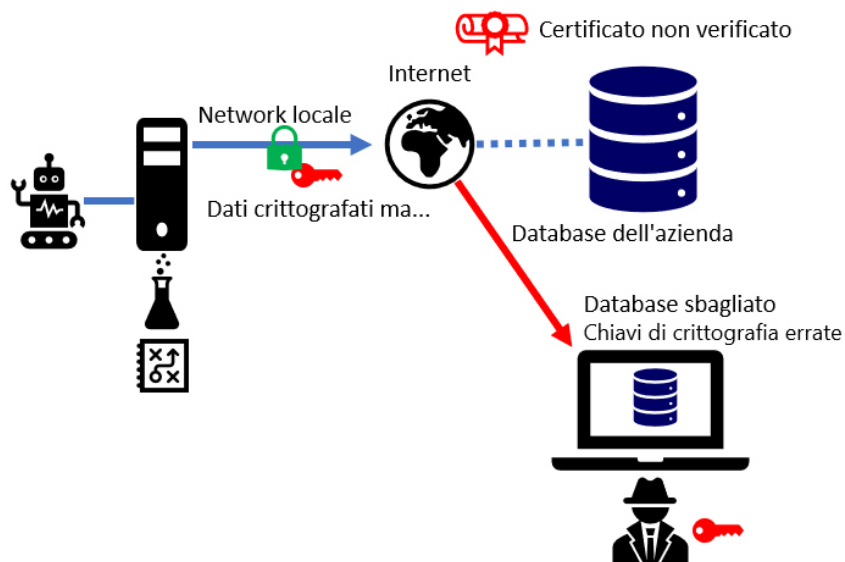


Contromisure:

Assicurarsi che computer di terzi non possano avere l'accesso o assumere il controllo.

- **Furto di identità**

Le connessioni a pagine web che non sono verificate da un'autorità di certificazione possono essere pericolose perché facilitano il furto di identità e il reindirizzamento di comunicazione. Questo consente ad aggressori di raccogliere informazioni sensibili (ad esempio nomi utente, password, dati di processo o ricette) e di causare danni manipolando macchine.



Contromisure:

Accertatevi che si faccia utilizzo di certificati per autenticare l'identità del server di destinazione.

## 5 Misure di sicurezza generali

Le misure protettive sono essenziali per la sicurezza e la protezione del network e del traffico.

Considerando che l'uso di questo prodotto richiede il collegamento a un network, è opportuno richiamare l'attenzione sui rischi per la sicurezza elencati di seguito.

- Perdita o furto di informazioni per mezzo di questo prodotto
- Uso del prodotto per operazioni illecite da parte di malintenzionati
- Interferenza o interruzione del funzionamento dell'unità da parte di malintenzionati
- L'utente è responsabile di prendere le dovute precauzioni, di cui a seguire si riportano alcuni esempi, per proteggersi dai rischi per la sicurezza delle reti.
- Se questo prodotto è connesso a un network che include dei PC, accertarsi che il sistema non possa infettarsi con virus o altro malware (per mezzo di un antivirus aggiornato regolarmente, un programma anti-spyware ecc.).
- Usate questo prodotto in un ambiente dotato di una LAN, una VPN (rete privata virtuale) o una rete di linee affittate.
- Usate questo prodotto in un ambiente in cui possono entrare solo persone con diritti di accesso controllati.
- Usate questo prodotto e altri dispositivi collegati tramite network, come un PC o un tablet, solo se avete preso misure di protezione per garantire la sicurezza.
- Non installare questo prodotto in locali dove il prodotto o i cablaggi possono essere distrutti o danneggiati da malintenzionati.

È opportuno notare che un'impostazione scorretta alla rete LAN esistente può causare un malfunzionamento dei dispositivi connessi alla rete. Consultare il proprio amministratore di rete prima di effettuare la connessione.

## 6 Best practice per aumentare la protezione della vostra unità FP-I4C

Potete minimizzare i rischi per la sicurezza adottando misure preventive ed effettuando le impostazioni di sistema e di applicazioni giuste. Usate la lista di verifica fornita in questa guida per assicurarvi di prendere tutte le misure necessarie per proteggere l'unità FP-I4C.

### Argomenti correlati

[Security configuration check list](#)

### 6.1 Impostazioni di sistema

Andate a “System Settings” (Impostazioni di sistema, IP/machine\_config) per impostare password e firewall, per accedere a file di log e per utilizzare le funzioni di debug SSH.

#### 6.1.1 Password di protezione

La password predefinita dal produttore si usa per iniziare. Impostate una password forte che contenga lettere maiuscole e minuscole, numeri e caratteri speciali (tranne spazi vuoti).

Utilizzate password per FTP server diverse per HMWIN Studio e unità FP-I4C.

#### 6.1.2 Impostazione di firewall

Utilizzate il firewall (IP/machine\_config/#!/services) per chiudere tutte le porte non utilizzate.

Se attivate il “Firewall Service” (IP/machine\_config/#!/services), tutte le funzioni utilizzate sono attivate con le impostazioni e le porte indicate. Disattivate i servizi non utilizzati o negate l'accesso a interfacce dedicate (ETH0 o ETH1).

#### Nota:

Accertatevi che “Web Server – HTTP” e “Web Server – HTTPS” siano attivati e che le porte Ethernet 80 e 443 siano aperte. Altrimenti l'accesso alla pagina di impostazione del sistema sarà permanentemente negato.

Esempio di impostazioni di firewall:

Nome	Interfaccia source	Porta o range	Protocollo	Richiesto
Web-Server - HTTP (richiesto per la configurazione)	Qualsiasi	80	TCP	✓
Web-Server - HTTPS (richiesto per la configurazione)	Qualsiasi TCP	443	TCP	✓
Individuazione di dispositivo	Qualsiasi	990–991	UDP	✓
Porta di comando FTP, occorrente per il funzionamento di HMWIN Studio	Qualsiasi	21	TCP	
Modalità FTP passiva, occorrente per il funzionamento di HMWIN Studio	Qualsiasi	18756–18760	TCP	
Server SSH	Qualsiasi	22	TCP	
Server VNC	Qualsiasi	5900	TCP	
Server DHCP	Qualsiasi	67	UDP	
Server SNMP	Qualsiasi	161	UDP	



Nome	Interfaccia source	Porta o range	Protocollo	Richiesto
Interfacce PEW	Qualsiasi	9094–9097	TCP	

### 6.1.3 File di log e funzioni di debug SSH

Queste funzioni possono essere utilizzate per rilevare un utilizzo atipico. Possono essere utilizzate solo con credenziali di amministratore.

## 6.2 Impostazioni applicazione

Andate a "Application Settings" (Impostazioni applicazione, IP/fp\_config) per fare le impostazioni di sicurezza specifiche dell'applicazione nella pagina di configurazione corrispondente.

- Configurazione delle porte

Le porte TCP in ascolto possono essere configurate nella pagina "Port" dell'interfaccia Web di FP-I4C. Poiché la maggior parte dei protocolli di comunicazione industriale non forniscono protezione accesso, utilizzate queste porte solo per comunicazioni interne in un network incapsulato.

Adottate le seguenti misure supplementari per ridurre al minimo il rischio che un aggressore ottenga il controllo non autorizzato del PLC collegato:

- Eliminare tutte le impostazioni delle porte inutilizzate.
- Se possibile, permettete l'accesso in lettura solo ai vostri dati.
- Bloccate la trasmissione di dati per tutti i dati del PLC che sono usati solo internamente.
- Riducete al minimo soprattutto il numero di registri di controllo (come valore target o comandi) necessari per operazioni di scrittura.
- Stabilite gli indirizzi IP autorizzati a comunicare. Per la comunicazione interna del dispositivo (ad esempio l'accesso tramite pagina web), assegnate l'indirizzo IP 127.0.0.1 (local host).
- Ogni PLC collegato dovrebbe avere la propria protezione accesso in modo che il programma PLC in esecuzione non possa essere modificato.

- Servizio data logger

Il data logger non apre nessuna porta di ascolto. Invece, i dati sono raccolti attraverso RS232, RS485, USB e connessioni client Ethernet TCP. Nessuno protocollo supportato utilizza la crittografia.

Quando si raccolgono dati attraverso network pubblici, si deve utilizzare una soluzione VPN.

- Servizio MQTT

Il protocollo IoT (Internet of Things) supporta la comunicazione in chiaro e crittografata oltre che il controllo dell'accesso supplementare.

- Quando trasmettete dati attraverso network pubblici, utilizzate certificati di radice per verificare l'identità del broker/server.
- Utilizzate connessioni crittografate tra l'unità FP-I4C e il broker.

I dati sensibili non sono crittografati all'interno del broker e possono essere inoltrati tramite connessioni non crittografate. Il broker deve essere protetto da accessi non autorizzati mediante un controllo degli accessi basato sui ruoli.

- Servizio client FTP

La funzione client FTP stabilisce connessioni con server FTP per la trasmissione di file. I login degli utenti non sono crittografati con le trasmissioni FTP standard. Vi raccomandiamo di usare solo trasmissioni FTPS sicure. Quando trasmettete dati attraverso network pubblici, usate inoltre certificati di radice.

Se il server FTP rifiuta la connessione crittografata, l'handshake fallisce e la trasmissione viene terminata.

- Servizio script

La funzione script applicata è un interprete incapsulato molto piccolo con caratteristiche limitate, creato per fornire informazioni sul dispositivo ad un PLC collegato.

- La modifica dello script richiede credenziali di amministratore.
- Nessuna funzione script è stata applicata per aprire porte di ascolto.
- È stata applicata solo una funzione per la trasmissione di dati come client TCP.

- Servizio client SQL

La funzione client SQL consente la comunicazione con i database. Generalmente, i database usano la propria autenticazione crittografata. Poiché i database possono contenere dati sensibili, dovete proteggere la vostra infrastruttura di database.

Usate il client SQL solo per connettervi a parti non sensibili dell'infrastruttura del database.

- Servizio IEC60870

Il protocollo di telecontrollo IEC60870 usa una porta di ascolto senza alcuna protezione dell'accesso utente. Usate questo protocollo solo in network incapsulati.

La possibilità di controllare il PLC, la macchina o la sottostazione collegati costituisce un ulteriore rischio. Per ridurre al minimo tale rischio, raccomandiamo le seguenti misure:

- Stabilite gli indirizzi IP partner consentiti.
- Utilizzare tunnel VPN crittografati.
- Tutti i valori target e i comandi sono gestiti nel PLC. I telegrammi in arrivo vengono elaborati prima nell'unità FP-I4C e poi nel PLC. Applicate una procedura PLC per identificare comandi non ammessi.
- Usate timbri data/ora con tutti i comandi per il controllo di macchine.
- Tutti i PLC collegati dovrebbero avere la propria protezione accesso in modo che il programma del PLC in esecuzione non possa essere modificato.

- Servizio client HTTP

Il client HTTP funziona come un browser per ottenere o inviare informazioni a un server HTTP (server cloud).

- Quando trasmettete dati attraverso network pubblici, utilizzate certificati di radice per verificare che l'unità FP-I4C sia connessa al server HTTP corretto.
- Usate connessioni crittografate tra l'unità FP-I4C e il server HTTP.

- Servizio client di e-mail

Il client di e-mail comunica con un server di e-mail. Questo server dovrebbe essere preparato per una comunicazione sicura e crittografata e i diritti di accesso degli utenti dovrebbero essere definiti. Il client di e-mail può trasmettere messaggi con o senza allegati, ma non file eseguibili.

- Quando si trasmettono dati attraverso network pubblici, usate certificati di radice per verificare che l'unità FP-I4C sia connessa al server di e-mail corretto.
- Utilizzate connessioni crittografate fra l'unità FP-I4C e il server di e-mail per la

procedura di login.

- Servizio REST API

Il REST API funziona come un server HTTP per fornire informazioni sul PLC collegato e per controllare il PLC.

Per ridurre al minimo i rischi per la sicurezza, fare le seguenti impostazioni nella pagina "Port":

- Se possibile, permettete l'accesso in lettura solo ai vostri dati.
- Bloccate la trasmissione di dati per tutti i dati del PLC che sono usati solo internamente.
- Riducete al minimo soprattutto il numero di registri di controllo (come valore target o comandi) necessari per operazioni di scrittura.
- Stabilite gli indirizzi IP autorizzati a comunicare.
- Utilizzate connessioni crittografate fra l'unità FP-I4C (come server HTTPS) e il client.

## 7 FAQ

---

1. Posso ottenere patch software e aggiornamenti del firmware?

I download gratuiti delle versioni più recenti sono disponibili sul sito web Panasonic:

[Downloads | Panasonic Industry Europe GmbH](#)

2. C'è qualche backdoor installata sul dispositivo?

Non c'è nessuna backdoor installata sul dispositivo. Se perdete la password, non c'è modo di ripristinare le impostazioni.

3. Il dispositivo chiama qualche server Panasonic?

Con le impostazioni del produttore nessun processo chiama automaticamente un server Panasonic.

## 8 Lista di verifica della configurazione di sicurezza

Usate questa lista di verifica per assicurarvi di aver attuato tutte le misure necessarie per proteggere l'unità FP-I4C. Spuntate tutte le voci che avete completato. Alla fine della lista, c'è spazio per voci aggiuntive.

Verificato	Rischio <sup>1)</sup>	Area	Pagina di configurazione	Da fare
	Alto	Password (admin, user)	Autenticazione IP/machine_config/#/	Cambiare password di default per amministratore e utente
	Alto	Servizio: Script di autorun	IP/machine_config/#/ services	Disattivare
	Alto	Servizio: Server SSH	IP/machine_config/#/ services	Disattivare se non necessario
	Basso	Avahi daemon	IP/machine_config/#/ services	Disattivare se non necessario
	Basso	Servizio cloud	IP/machine_config/#/ services	Disattivare se non necessario
	Basso	Server DHCP	IP/machine_config/#/ services	Disattivare se non necessario
	Basso	Servizio VNC	IP/machine_config/#/ services	Disattivare se non necessario
	Basso	Firewall	IP/machine_config/#/ services	Attivare e customizzare le impostazioni
	Alto	Password HMWIN (almeno amministratore, utente, log) <sup>2)</sup>	HMWIN Studio Project/Configuration/ Security	Cambiare password di default per amministratore e utente
	Medio	Funzione HMWIN OPC UA <sup>2)</sup>	HMWIN Studio Project/Configuration/ Security	Verificare l'accesso a server
	Alto	Configurazione delle porte	IP/fp_config → "Port"	Configurare l'accesso ad area dati (lettura, scrittura o blocco)
	Medio	Servizio MQTT	IP/fp_config → "MQTT"	Utilizzare crittografia e certificati
	Medio	Servizio client FTP	IP/fp_config → "FTP Client"	Utilizzare crittografia e certificati
	Medio	Servizio client HTTP	IP/fp_config → "HTTP Client"	Utilizzare crittografia e certificati
	Medio	Servizio client di e-mail	IP/fp_config → "Email Client"	Utilizzare crittografia, certificati e password
	Medio	Servizio REST API	IP/fp_config → "REST API"	Disattivare "Accept external requests" (Accettare richieste esterne) se non necessario
			IP/fp_config → "Port"	Configurare l'accesso ad area dati (lettura, o scrittura)

<sup>1)</sup> Il livello di rischio dipende dalla vostra applicazione.

<sup>2)</sup> Se installato

## Linea assistenza Panasonic

---

In caso di domande che non trovano risposte all'interno dei manuali o dell'help online, contattate il servizio vendite.

### Europa

**Austria:** 02236 / 2 68 46, [info.pewat@eu.panasonic.com](mailto:info.pewat@eu.panasonic.com)

**Benelux:** 0499 / 37 27 27, [info.pewswe@eu.panasonic.com](mailto:info.pewswe@eu.panasonic.com)

**Francia:** 01 / 60 13 57 57, [info.pewswef@eu.panasonic.com](mailto:info.pewswef@eu.panasonic.com)

**Germania:** 089 / 45 354 2748, [plc.peweu@eu.panasonic.com](mailto:plc.peweu@eu.panasonic.com)

**Irlanda:** 01 / 4 60 09 69, [info.pewuk@eu.panasonic.com](mailto:info.pewuk@eu.panasonic.com)

**Italia:** 045 / 67 52 711, [info.pewit@eu.panasonic.com](mailto:info.pewit@eu.panasonic.com)

**Scandinavia:** 46 / 8 59 47 66 80, [info.pewns@eu.panasonic.com](mailto:info.pewns@eu.panasonic.com)

**Spagna:** 91 / 3 29 38 75, [info.pewes@eu.panasonic.com](mailto:info.pewes@eu.panasonic.com)

**Svizzera:** 041 / 799 70 50, [info.pewch@eu.panasonic.com](mailto:info.pewch@eu.panasonic.com)

**Regno Unito:** 01908 / 23 15 55, [info.pewuk@eu.panasonic.com](mailto:info.pewuk@eu.panasonic.com)

### America del Nord e del Sud

**USA:** 1 877 / 624 7872, [iasupport@us.panasonic.com](mailto:iasupport@us.panasonic.com)

### Asia

**Cina:** 400-920-9200, <https://industrial.panasonic.cn/ea/>

**Corea:** +82-2-2052-1050, <http://pidskr.panasonic.co.kr/>

**Taiwan:** +886-2-2757-1900, <https://industrial.panasonic.com/>

**Hong Kong:** +852-2306-3128, <https://industrial.panasonic.com/>

**Giappone:** 0120-394-205, <https://industrial.panasonic.com/>

**Singapore:** +65 / 635 92128, [pewapfa@sg.pewg.panasonic.com](mailto:pewapfa@sg.pewg.panasonic.com)

## Registrazione di modifiche

---

Data	Descrizione
2021.11, versione 1.1	Aggiunto il capitolo 2, cambiata la denominazione per accesso in lettura nel capitolo 6.2
2021.08, versione 1.0	Prima edizione