Guida alla sicurezza informatica

# hw+

## Interruttori automatici sentinel Energy

## HW1, HW2 e HW4

hager

# Sommario

Pagina

### Avvertenze e note

La presente documentazione contiene le istruzioni che è necessario rispettare per la propria sicurezza personale o per la prevenzione di danni alle proprietà.
Le istruzioni riferite alla sicurezza personale sono segnalate nella documentazione da un simbolo di allarme di sicurezza. Le istruzioni di sicurezza riferite a danni materiali sono segnalate dalla dicitura “AVVISO”.
I simboli di allarme di sicurezza e la dicitura sottostante sono classificati in base al grado di rischio.

**PERICOLO**

**PERICOLO** indica una situazione di pericolo imminente che, se non evitata, provocherà la morte o lesioni gravi.

**AVVERTIMENTO**

**AVVERTIMENTO** indica una situazione potenzialmente pericolosa che, se non evitata, può provocare lesioni gravi o addirittura la morte.

**ATTENZIONE**

**ATTENZIONE** indica una situazione potenzialmente pericolosa che, se non evitata, può provocare lesioni lievi o di moderata entità.

**AVVISO**

**AVVISO** indica un messaggio di allarme per danni materiali.
**AVVISO** indica anche importanti istruzioni per l’uso e soprattutto utili informazioni sul prodotto, alle quali prestare particolare attenzione per un uso efficace e sicuro.

### Personale qualificato

Il prodotto o l’impianto descritto nella presente documentazione deve essere installato, utilizzato e manutenuto solo da personale qualificato. Hager Electro declina qualsiasi responsabilità per le conseguenze dell’uso del presente materiale da parte di personale non qualificato.
Una persona qualificata ha le competenze e le conoscenze necessarie per la realizzazione e il funzionamento dell’impianto elettrico, e ha ricevuto una formazione che le consente di identificare ed evitare i relativi rischi.

### Uso corretto dei prodotti Hager

I prodotti Hager sono progettati per essere utilizzati solo per le applicazioni descritte nei cataloghi e nella relativa documentazione tecnica. Se vengono utilizzati prodotti e componenti di altri produttori, devono essere raccomandati o approvati da Hager.
La corretta gestione dei prodotti Hager durante il trasporto, lo stoccaggio, l’installazione, il montaggio, la messa in servizio, il funzionamento e la manutenzione è necessaria per garantire un funzionamento sicuro e senza problemi.
Devono essere rispettate le condizioni ambientali ammissibili. Devono essere rispettate le informazioni contenute nella documentazione tecnica.

### Responsabilità di pubblicazione

I contenuti della presente documentazione sono elaborati al fine di garantire l'attendibilità e la correttezza delle informazioni al momento della pubblicazione.
Hager si riserva il diritto di apportare le necessarie correzioni e modifiche nelle successive edizioni.

### Sicurezza informatica e connessione wireless

Il prodotto o il sistema descritto nella presente documentazione richiede l'implementazione di misure di protezione contro i rischi relativi a qualsiasi connessione e trasmissione wireless e i rischi relativi a qualsiasi connessione e trasmissione cablata.

**AVVERTIMENTO**

**Rischio di pirateria informatica da remoto in caso di connessione wireless**
- Mantenere la connessione Bluetooth Low Energy disattivata, se non si utilizza l'applicazione Hager Power touch.
- Evitare di attivare la connessione Bluetooth Low Energy, se non è possibile impedire l'accesso non autorizzato ai dispositivi installati.

La mancata osservanza di queste istruzioni può provocare il decesso, gravi lesioni personali o danni materiali.

**AVVERTIMENTO**

**Rischi che possono influire sulla disponibilità, integrità e riservatezza del sistema sentinel Energy**
- Modificare le password predefinite al primo utilizzo per evitare accessi non autorizzati alle impostazioni, ai controlli e alle informazioni dei dispositivi.
- Disattivare le porte e i servizi inutilizzati, nonché gli account predefiniti, per ridurre il rischio di attacchi dannosi.
- Proteggere i dispositivi in rete tramite diversi livelli di difesa informatica (firewall, segmentazione della rete, rilevamento delle intrusioni e protezione della rete).
- Rispettare le buone pratiche di sicurezza informatica (ad esempio, minimo privilegio, separazione dei compiti) per ridurre i rischi di intrusione, perdita o alterazione di dati e registri o interruzione dei servizi.

La mancata osservanza di queste istruzioni può provocare il decesso, gravi lesioni personali o danni materiali.

### Scopo del documento

Questo documento è concepito per fornire agli installatori elettrici, ai system integrator o ai progettisti di sistemi gli elementi di sicurezza informatica degli interruttori automatici hw+ dotati di sganciatori elettronici sentinel Energy. Lo scopo è quello di aiutare i progettisti e gli utilizzatori di questi sistemi a mettere in atto un ambiente operativosicuro del prodotto.

### Ambito di applicazione

Il presente documento si applica agli interruttori automatici hw+ dotati di sganciatori elettronici sentinel Energy.

### Revisioni

| Indice | Data |
|---|---|
| 6LE009858A | Luglio 2023 |

### Documenti da consultare

| Documento | Codice |
|---|---|
| Manuale di installazione HW1 | 6LE009862A |
| Manuale di installazione HW2 e HW4 | 6LE009847A |
| Manuale d'uso sganciatori elettronici sentinel Energy hw+ | 6LE009861A |
| Guida utente alla comunicazione Modbus sentinel Energy | 6LE009860A |

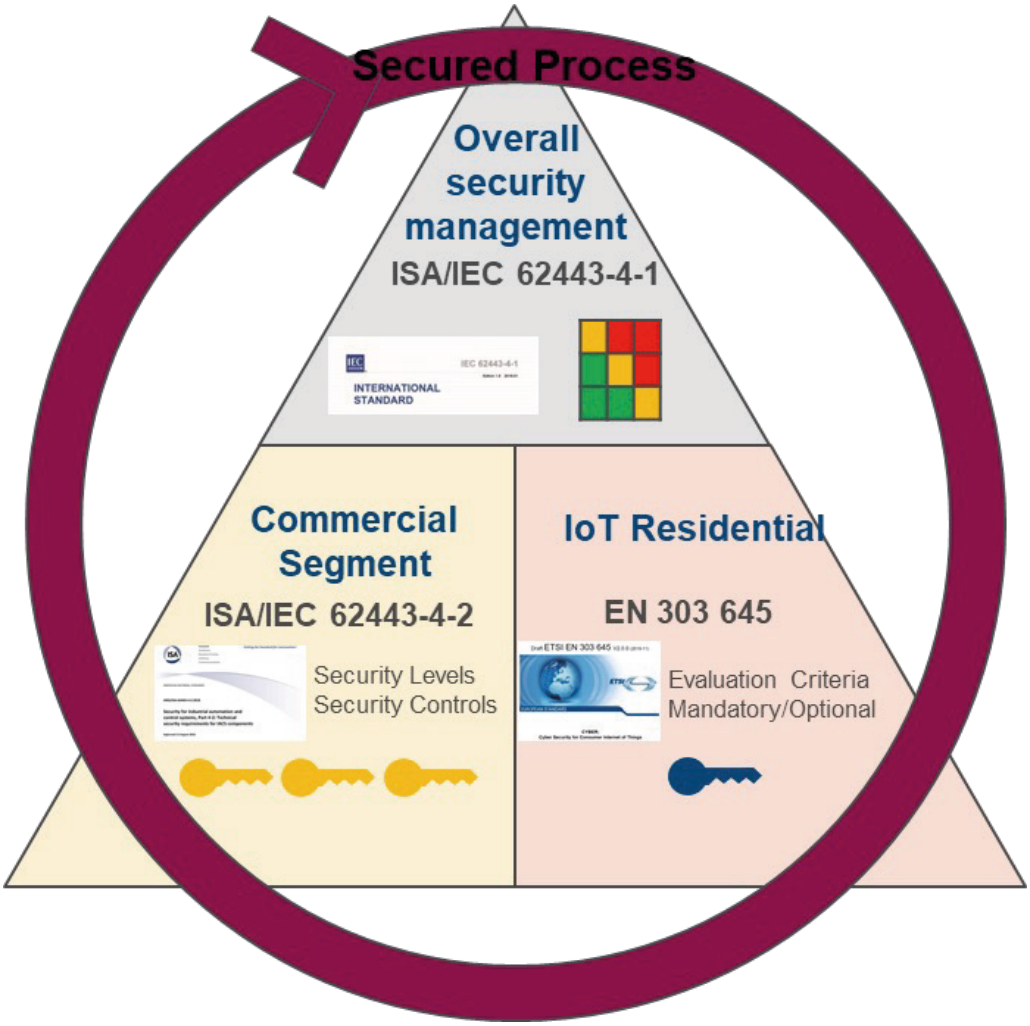
È possibile scaricare queste pubblicazioni e altre informazioni tecniche dal nostro sito Web all'indirizzo: www.hager-bocchiotti.com

### Contatto

| | |
|---|---|
| **Indirizzo** | Hager Bocchiotti S.p.A. 45 Via dei Valtorta, 20127 Milano Italia |
| **Telefono** | 02 7015 0511 |
| **Sito Internet** | www.hager-bocchiotti.com |

Hager presta particolare attenzione alle questioni riguardanti la protezione dei dati e la sicurezza della connessione dei suoi prodotti connessi.
Per questa ragione attuiamo tutte le disposizioni al fine di raggiungere i migliori standarddi qualità in termini di sicurezza dei dati trasmessi dai nostri prodotti.

Hager utilizza le norme IEC 62443 e EN 303 645 nella progettazione e nello sviluppo dei propri prodotti connessi.
La serie di norme IEC 62443 si applica al funzionamento sicuro dei sistemi di automazione industriale (sistemi ICS), dalla progettazionealla gestione, passando per l'installazione.
La norma EN 303 645 definisce disposizioni di alto livello in materia di sicurezza informatica e protezione dei dati per i dispositivi IoT connessi destinati al grande pubblico.



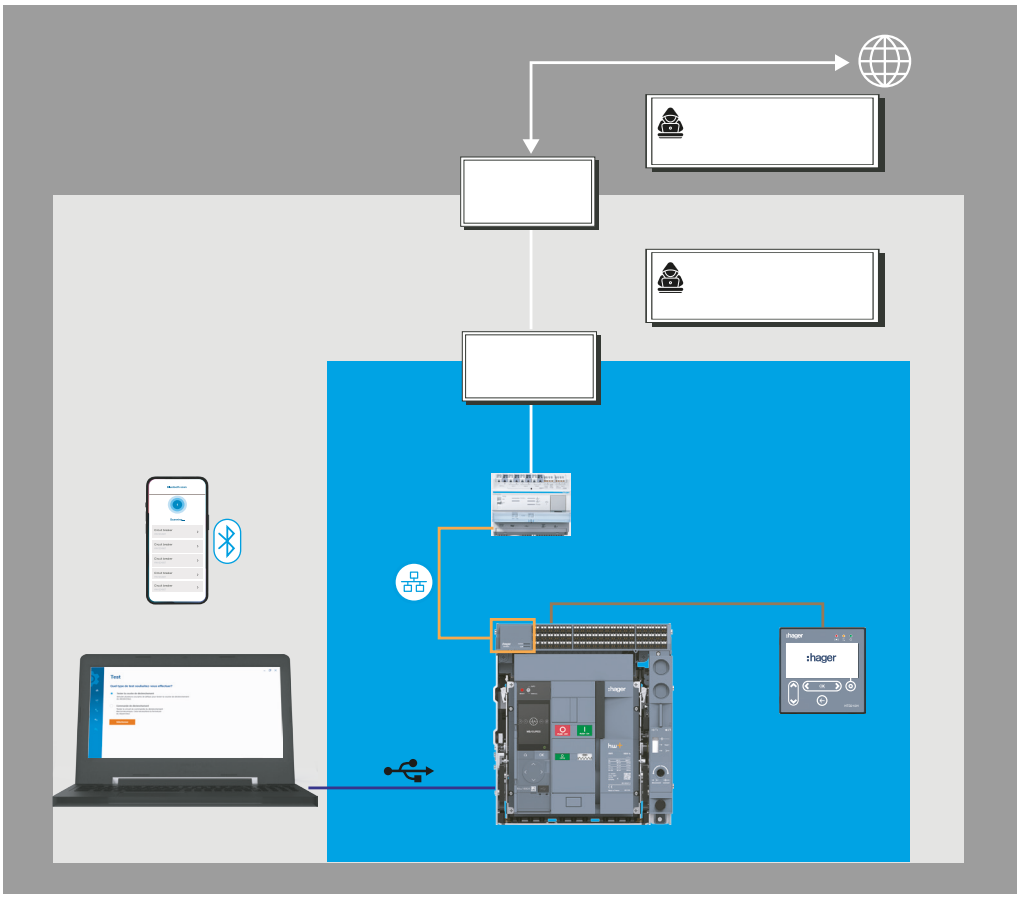

L'applicazione di un processo sicuro durante le fasi di progettazione, sviluppo e convalida previene anche gli attacchi volti a interrompere le produzioni dei clienti o a modificare la configurazione del loro sistema.

### 2.2.1 Ambiente del sistema sentinel Energy

L'interruttore automatico hw+ sentinel Energy è un elemento cruciale di una distribuzione o di un'apparecchiatura elettrica in quanto garantisce la protezione elettrica.

Grazie alle sue funzioni di comunicazione, garantisce l'accesso alle funzioni di controllo in tempo reale e ai dati di monitoraggio della distribuzione elettrica. Ciò consente una efficienza e flessibilità superiori nella gestione del proprio impianto elettrico. Queste funzioni, tuttavia, espongono i clienti a potenziali attacchi informatici.

La figura riportata di seguito illustra l'ambiente di comunicazione in cui si inserisce l'interruttore automatico hw+ sentinel Energy.



Legenda:

| | |
|---|---|
| | Internet |
| | Intranet |
| | Quadro di distribuzione |
| | Comunicazione modbus |
| | USB-C |
| | Porta CIP per protocollo proprietario |
| | Bluetooth Low Energy |

(*) Rischio di attacchi o violazioni

Il sistema sentinel Energy consente di comunicare con l'interruttore automatico hw+ attraverso uno dei seguenti mezzi:
- interfaccia display/tastiera dello sganciatore sentinel Energy,
- connessione Bluetooth Low Energy (BLE) wireless da uno smartphone con l'applicazione Hager Power touch,
- connessione tramite porta USB-C al software Hager Power setup,
- connessione tramite collegamento seriale al protocollo proprietario CIP al display da quadro HTD210H,
- connessione a una rete di collegamento seriale RS 485 mediante il protocollo Modbus-RTU,
- connessione a una rete Ethernet mediante il protocollo Modbus-TCP.

Ciascuno di questi mezzi di comunicazione rappresenta una vulnerabilità nel sistema, se non vengono messe in atto le misure di sicurezza appropriate.
In questo caso, in particolare, il sistema è esposto ai seguenti rischi:
- rischio di indisponibilità del sistema,
- rischio di modifica dei parametri di sistema da parte di persone non autorizzate,
- rischio di acquisizione del controllo del sistema da parte di persone non autorizzate,
- rischio di perdita di dati essenziali e sensibili.

La presente guida fornisce le nostre raccomandazioni per proteggere questi mezzi di comunicazione ed evitare attacchi intenzionali o uso improprio accidentale.

### 2.2.2 Funzionalità di sicurezza

Durante la progettazione sono state integrate le seguenti funzionalità di sicurezza per mitigare le minacce inerenti all'implementazione del sistema Sentinel Energy in un ambiente connesso :

- messa in sicurezza della comunicazione Bluetooth utilizzando l'algoritmo AES,
- azioni di modifica delle impostazioni e azioni di controllo/comando accessibili solo dopo l'inserimento di password o codici personalizzati,
- comunicazione IP cifrata,
- abilitazione della crittografia eautenticazione della comunicazione Modbus,
- gradazione del livello di sicurezza durante i comandidi scrittura nei registri Modbus.

Queste funzionalità di sicurezza e il funzionamento del sistema Sentinel Energy sono stati verificati da organismi terzi esterni e indipendenti durante l'esecuzione di test di penetrazione (simulazione di attacchi di un utente malintenzionato o di un malware).

La tecnologia operativa (OT) si riferisce all'hardware e al software utilizzati per monitorare i dispositivi e i processi fisici all'interno di un'azienda. Durante la sua implementazione è importanteidentificare e proteggere le informazioni essenziali o sensibili alle operazioni di un'azienda.

Di seguito è riportato un elenco non esaustivo di informazioni sensibili :
- codici diaccesso delle apparecchiature o dei locali sotto chiave,
- architettura di sistema,
- indirizzi IP o MAC delle apparecchiature di comunicazione connesse,
- numeri di porta utilizzati per la comunicazione Ethernet,
- credenziali e password degli utilizzatori.

A questi si aggiungono le informazioni fornite dal sistema sentinel Energy.

| | **Display sentinel Energy** | **Display da quadro HTD210H** | **Bluetooth** | **USB-C** | **Modbus-RTU Modbus-TCP** |
|---|---|---|---|---|---|
| Modbus-TCP | | | | | |
| Monitoraggio dei dati | Lettura | Lettura | Lettura | Lettura | Lettura |
| Parametro di protezione dell'interruttore automatico | Lettura/ Scrittura | Lettura/ Scrittura | Lettura | Lettura/ Scrittura | Lettura/ Scrittura |
| Altri parametri-dell'interruttore automatico | Lettura/ Scrittura | Lettura/ Scrittura | Lettura | Lettura/ Scrittura | Lettura/ Scrittura |
| Comandi di apertura e chiusura | Sì | No | Sì | Sì | Sì |
| Reimpostazioni | Sì | Sì | No | Sì | Sì |

Uno dei punti chiave di una strategia di difesa dagli attacchi informatici è l'applicazione di un'efficace politica di password.

**⚠ AVVERTIMENTO**

**Rischi che possono influire sulla disponibilità, integrità e riservatezza del sistema sentinel Energy**
Modificare le password predefinite al primo utilizzo per evitare accessi non autorizzati alle impostazioni, ai controlli e alle informazioni dei dispositivi.
La mancata osservanza di queste istruzioni può provocare il decesso, gravi lesioni personali o danni materiali.

A questo scopo è necessario rispettare le seguenti best practice (elenco non esaustivo) :
- Modificare tutte le password predefinite.
- Impostare password complesse: le scelte banali come "1234" o "password" devono essere evitate.
- Non condividere le proprie password con persone non autorizzate o non abilitate.
- Cambiare regolarmente le password.
- Non riutilizzare le vecchie password.
- Conservare le password in un luogo sicuro (ad esempio una cassetta di sicurezza con combinazione).

Questa politica di password deve essere applicata a tutti i componenti del sistema sentinel Energy, ai server, ai computer, agli smartphone collegati al sistema e qualsiasi altro componente di rete.

La sicurezza informatica riguarda tutti i dipendenti dell'azienda. In particolare, tutti gli utilizzatori autorizzati ad accedere al sistema sentinel Energy e alla rete di comunicazione dell'impianto devono conoscere la strategia di protezione delle informazioni delladitta.

Devono inoltre aver seguito una formazione sui principi fondamentali della sicurezza informatica e sulle regole di esecuzione derivanti da tale strategia.

Periodicamente è necessario richiamare le seguenti buone pratiche (e non solo):
- seguire la strategia della password,
- non condividere password, codici di accesso e dati sensibili,
- accertarsi che tutti i computer collegati al sistema (messa in servizio, monitoraggio, controllo...) siano aggiornati e protetti da virus e malware,
- se i computer vengono utilizzati anche per l'invio di messaggi, gli utilizzatori devono essere formati per rilevare e-mail sospette,
- tutti gli smartphone utilizzati per accedere al sistema devono essere protettida PIN o riconoscimento facciale e devono essere protetti contro la pirateria su Internet e tramite Bluetooth,
- tutti gli smartphone devono mantenere la loro integrità di sistema e dei suoi componenti,
- tutti gli smartphone utilizzati per accedere al sistema devono sempre rimanere in possesso degli utilizzatori e non essere condivisi,
- le politiche di sicurezza in vigore non devono essere aggirate.

L'accesso in prossimità dello sganciatore sentinel Energy integrato nell'interruttore automatico hw+ consente di accedere a tutte le sue funzionalità, compresi i parametri di protezione e di controllo remoto.

È quindi importante limitarne l'accesso installando l'interruttore automatico in un locale sotto chiave o protetto da codice di accesso al fine di evitare:
- qualsiasi accesso non autorizzato al display sentinel Energy e alla relativa tastiera, evitando qualsiasi rischio di modifica dei parametri di impostazione e controllo,
- qualsiasi accesso non autorizzato alla comunicazione Bluetooth wireless, evitando il rischio di acquisire il controllo con l'applicazione Hager Power touch,
- qualsiasi connessione non autorizzata tramite porta USB-C per evitare il rischio di modificare i parametri dal software Hager Power setup.

In particolare, è necessario verificare che:
- il locale sia tenuto sempre sotto chiave,
- il locale sia dotato di un sistema di autenticazione e autorizzazione,
- solo il personale autorizzato disponga di una chiave o del codice di accesso,
- i cavi della rete di comunicazione che entrano nel locale e le porte di collegamento sulle apparecchiature di comunicazione al di fuori della sala siano protetti,
- tutte le apparecchiature (computer, smartphone e tablet) che hanno accesso allo sganciatore sentinel Energy beneficino di una protezione rafforzata in conformità con le istruzioni del fornitore più recenti.

Chiunque abbia accesso al quadro di distribuzione, in cui è installato l'interruttore automatico hw+, può accedere al display sentinel Energy, alla relativa tastiera e modificare in questo modo i parametri di regolazione dell'interruttore automatico.

Di seguito sono riportate le nostre raccomandazioni per proteggersi da qualsiasi atto doloso o involontario tramite accesso al display sentinel Energy e alla relativa tastiera:
- abilitare la protezione con password per la modifica di tutti i parametri (ad eccezione di quelli di impostazione del display),
- attivare il blocco della tastiera sentinel Energy,
- sigillare la finestra trasparente di protezione dello sganciatore,
- comunicare la password dello sganciatore sentinel Energy esclusivamente alle persone autorizzate,
- evitare di registrare questa password sullo smartphone in cui è installata l'applicazione Hager Power touch (sms, e-mail, note, ecc.).

La connessione tramite comunicazione Bluetooth consente a uno smartphone che esegue l'applicazione Hager Power touch di accedere in lettura alle informazioni dello sganciatore sentinel Energy e di avviare un comando di apertura o chiusura dell'interruttore automatico hw+.

Di seguito sono riportate le nostre raccomandazioni per proteggersi da qualsiasi atto doloso o involontario tramite accesso alla connessione Bluetooth:
- installare l'interruttore automatico hw+ in un locale tenuto sotto chiave o il cui accesso sia protetto in qualsiasi momento,
- unicamente le persone autorizzate devono avere accesso al locale,
- la password dello sganciatore sentinel Energy deve essere comunicata esclusivamente alle persone autorizzate.

**Utilizzo dell'applicazione Hager Power touch**
L'applicazione Hager Power touch consente di monitorare le informazioni fornite dallo sganciatore sentinel Energy, tra cui lo stato di funzionamento dell'interruttore automatico e i valori delle grandezze misurate.
Consente inoltre di eseguire un comando di apertura o chiusura dell'interruttore automatico hw+, se sull'interruttore automatico sono stati installati gli accessori appropriati.

Al primo collegamento, l'abbinamento dello smartphone che esegue l'applicazione Hager Power touch con l'interruttore automatico richiede un'impostazione sullo sganciatore sentinel Energy. A partire dal secondo collegamento, l'abbinamento non è più necessario. La connessione viene stabilita automaticamente con lo smartphone, se la comunicazione Bluetooth è attivata e se il dispositivo si trova nel raggio d'azione dell'emissione Bluetooth Low Energy.
Per ulteriori informazioni sul questa applicazione, fare riferimento al Manuale d'uso degli sganciatori elettronici sentinel Energy hw+.

È quindi indispensabile evitare qualsiasi rischio di hacking attraverso la comunicazione Bluetooth con l'applicazione Hager Power touch.

**⚠ AVVERTIMENTO**

**Rischio di pirateria informatica da remoto in caso di connessione wireless**
- Mantenere disattivata la connessione Bluetooth Low Energy dello sganciatore se l'applicazione Hager Power touch non è approvata dal reparto IT.
- In caso di mancato utilizzo prolungato dell'app Hager Power touch, disattivare la connessione Bluetooth Low Energy dello sganciatore.
- Rimuovere l'interruttore automatico hw+ dai dispositivi Bluetooth conosciuti dallo smartphone in caso di non utilizzo prolungato dell'applicazione Hager Power touch.
- Evitare di attivare la connessione Bluetooth Low Energy dello sganciatore se non è possibile impedire l'accesso non autorizzato ai dispositivi installati.

La mancata osservanza di queste istruzioni può provocare il decesso, gravi lesioni personali o danni materiali.

Il collegamento alla porta USB-C tramite il software Hager Power setup consente di accedere alle funzioni di protezione e di controllo dello sganciatore sentinel Energy.

**⚠ AVVERTIMENTO**

**Rischi che possono influire sulla disponibilità, sull'integrità e sul funzionamento dell'interruttore automatico hw+**
Sigillare la finestra trasparente di protezione dello sganciatore, se non è possibile impedire l'accesso non autorizzato all'interruttore automatico.
La mancata osservanza di queste istruzioni può provocare il decesso, gravi lesioni personali o danni materiali.

Per collegarsi alla porta USB-C è necessario soddisfare le seguenti condizioni:
- avere fisicamente accesso alla presa USB-C situata sullo sganciatore sentinel Energy,
- aver installato il software Hager Power setup su un computer portatile,
- connettere questo computer allo sganciatore utilizzando un adattatore USB-C.

Di seguito sono riportate le nostre raccomandazioni per l'utilizzo del software Hager Power setup:

Numerosi sono gli attacchi che sfruttano le falle del sistema operativo Microsoft Windows. Per questo motivo il computer su cui è installato Hager Power setup deve essere sicuro:
- il computer deve essere dotato di un antivirus installato, attivo e aggiornato,
- il computer deve essere configurato per il funzionamento a sessione (Identificativo + password),
- le policy relative alle password e all'utilizzo del computer devono essere rispettate,
- il software Hager Power setup deve beneficiare degli aggiornamenti più recenti.

Ildisplay da quadro HTD210H consente di accedere a diverse funzionalità dello sganciatore, compresi i suoi parametri di protezione.

È quindi importante limitarne l'accesso installando l'interruttore automatico in un locale sotto chiave o protetto da codice di accesso al fine di evitare:
- qualsiasi accesso non autorizzato al display sentinel Energy e alla relativa tastiera, evitando qualsiasi rischio di modifica dei parametri di impostazione e controllo,
- qualsiasi accesso non autorizzato alla comunicazione Bluetooth wireless, evitando il rischio di acquisire il controllo con l'applicazione Hager Power touch,
- qualsiasi connessione non autorizzata tramite porta USB-C per evitare il rischio di modificare i parametri dal software Hager Power setup.

In particolare, è necessario verificare che:
- il locale sia tenuto sempre sotto chiave,
- il locale sia dotato diun sistema di autenticazione e autorizzazione,
- solo il personale autorizzato disponga di una chiave o diaccesso.

Di seguito sono riportate le nostre raccomandazioni per proteggersi da qualsiasi atto doloso o involontario tramite accesso al display da quadro HTD210H :
- modificare la password del display HTD210H al primo utilizzo,
- attivare il blocco della tastiera del display,
- sigillare la finestra trasparente di protezione dello sganciatore,
- comunicare la password del display esclusivamente alle persone autorizzate.

L'interruttore automatico hw+ dotato di uno sganciatore sentinel Energy offre due possibilità di accesso remoto:
- tramite una rete di collegamento seriale RS 485 utilizzando il protocollo Modbus RTU nel caso del modulo di comunicazione HWY965H,
- tramite una rete Ethernet utilizzando il protocollo Modbus TCP/IP nel caso del modulo di comunicazione HWY966H.

Questo accesso remoto consente di accedere a tutte le funzionalità dello sganciatore sentinel Energy, comprese le impostazioni di protezione e di controllo remoto.

È quindi importante abilitare il blocco dell'accesso remoto, se non sono richiesti l'accesso in scrittura ai parametri dello sganciatore e l'accesso alle funzioni di controllo remoto.

Il blocco dell'accesso remoto viene eseguito dallo sganciatore sentinel Energy.
Per informazioni, fare riferimento al Manuale d'uso sganciatori elettronici sentinel Energy hw+.

Al fine di proteggere l'accesso remoto, raccomandiamo quanto segue:
- non reindirizzare le porte al modem router. per evitare di esporre l'interfaccia Modbus o il configuratore su Internet,
- proteggere i dispositivi da diversi livelli di difesa informatica (firewall, rilevamento delle intrusioni...),
- separare la rete aziendale dalla rete di tecnologia operativa (OT),
- creare un elenco di indirizzi autorizzati.

L'accesso all'interruttore automatico hw+ tramite comunicazione Modbus-TCP permette di accedere a tutti i suoi dati di stato, indicatori, misure, parametri di regolazione e funzioni di controllo a distanza.
I protocolli utilizzati sono:
- SNTP: sincronizzazione di data e ora
- DHCP: assegnazione dell'indirizzo di rete IP
- DNS: risoluzioni dei nomi di dominio
- HTTPS: per l'accesso via Ethernet alle pagine web di configurazione del modulo
- Modbus Messaging on TCP/IP: per la comunicazione del server con i client Modbus.

Il modulo di comunicazione Modbus-TCP consente di collegare il server interruttore automatico hw+ a più client o di collegare un computer tramite Ethernet per impostare la comunicazione modbus.

Di seguito sono riportate le nostre raccomandazioni per proteggersi da qualsiasi atto doloso o involontario tramite comunicazione Modbus-TCP:

Per quanto riguarda un computer collegato via Ethernet al modulo Modbus-TCP, quest' ultimo deve essere dotato di un antivirus installato, attivo e aggiornato. Deve essere configurato per il funzionamento a sessione (Identificativo + password). Le policy relative alle password e all'utilizzo del computer devono essere rispettate.
Questo computer deve essere assegnato unicamente a persone qualificate e autorizzate.

Per quanto riguarda la comunicazione con un client Modbus, se questo e il sistema di comunicazione implementato lo consentono, si consiglia di attivare il modbus protetto da TLS sul modulo di comunicazione Modbus-TCP.
Per impostazione predefinita, il protocollo Modbus-TCP non è sicuro, alcuni messaggi possono essere decifrati facilmente.

Il modulo Modbus-TCP consente di attivare il protocollo modbus sicuro con TLS non autenticato oppure il protocollo Modbus sicuro con TLS e autenticazione reciproca.

La connessione di un computer tramite Ethernet al modulo di comunicazione consente di accedere tramite HTTPS alle pagine Web del modulo per configurare la strategia di allocazione dell'indirizzo IP e la gestione dei certificati X.509 di autenticazione del server Modbus e dei suoi client.

Per maggiori informazioni sul modbus sicuro tramite TLS e la connessione tramite HTTPS, fare riferimento alla Guida utente alla comunicazione Modbus sentinel Energy.

L'accesso all'interruttore automatico hw+ tramite comunicazione Modbus-RTU permette di accedere a tutti i suoi dati di stato, indicatori, misure, parametri di regolazione e funzioni di controllo a distanza.

Di seguito sono riportate le nostre raccomandazioni per proteggersi da qualsiasi atto doloso o involontario tramite comunicazione Modbus-RTU:
Per quanto riguarda un computer in rete con accesso alla comunicazione Modbus-RTU, quest'ultimo deve essere dotato di un antivirus installato, attivo e aggiornato. Deve essere configurato per il funzionamento a sessione (Identificativo + password). Le policy relative alle password e all'utilizzo del computer devono essere rispettate.
Questo computer deve essere assegnato unicamente a persone qualificate e autorizzate.

Per maggiori informazioni sull'utilizzo del modbus-RTU, fare riferimento alla Guida utente Comunicazione Modbus sentinel Energy.

**Aggiornamento del software Hager Power setup e dell'applicazione Hager Power touch**
È importante disporre sempre delle versioni software più recenti. Infatti, oltre a contenere evoluzioni e correzioni funzionali, queste includono anche aggiornamenti di sicurezza perché le tecniche di attacco e difesa informatica sono in continua mutazione.

**Di seguito è riportato un elenco di elementi con i relativi metodi di aggiornamento:**
- software Hager Power setup: per essere informato di un aggiornamento disponibile, il computer che esegue il software deve essere connesso a Internet,
- applicazione Hager Power touch: come tutte le applicazioni per cellulari, gli aggiornamenti sono disponibili su Apple store e su Google Play.

**Aggiornamento dei firmware**
Per l'eventuale aggiornamento del firmware dello sganciatore sentinel Energy, dei moduli di comunicazione e del display da quadro, sarà necessario rivolgersi a un operatore Hager Bocchiotti.

**Assistenza alla sicurezza informatica**
Hager implementa una politica di gestione delle vulnerabilità per rispondere rapidamente agli incidenti di falla di sicurezza informatica sui propri prodotti e servizi connessi.

Per segnalare un incidente o una vulnerabilità di sicurezza informatica è possibile applicare uno dei seguenti metodi :
a) Per una migliore reattività, è preferibile inviare una mail al nostro Product Security Team specificando la descrizione del problema e i codici dei prodotti interessati. E-mail da inviare a : productsecurity@hagergroup.com
b) Contattare il proprio rappresentante Hager Bocchiotti o l'Assistenza tecnica locale Hager (informazioni di contatto sul sito Internet Hager del proprio Paese) specificando che si tratta di un problema di sicurezza informatica, la descrizione del problema e i codici dei prodotti interessati.

La segnalazione di un incidente di sicurezza informatica consente al Product Security Team di valutare i rischi, proporre contromisure e far evolvere software e hardware apportando le necessarie correzioni.

**AES**
Advanced Encryption Standard

**DHCP**
Dynamic Host Configuration Protocol. Protocollo di configurazione dinamica host utilizzato per la gestione degli indirizzi IP.

**DNS**
Domaine Name System. Il DNS consente di associare un nome comprensibile a un indirizzo IP.

**CIP**
Communication Interface Port. Espressione equivalente al protocollo proprietario che permette di interfacciare i componenti del sistema sentinel Energy.

**ICS**
Industrial Control System. Un sistema di controllo industriale si riferisce agli oggetti fisici e digitali, che regolano e gestiscono il comportamento delle macchine e dei processi delle macchine negli impianti industriali.

**MAC**
L'indirizzo MAC (Media Access Control) è l'indirizzo fisico di un dispositivo di rete. Ciascun indirizzo MAC è univoco e consente quindi di identificare i dispositivi elettronici.

**OT**
La tecnologia operativa (Operational Technology in inglese) è costituita da hardware e software, che monitorano, controllano processi e dispositivi fisici industriali.

**RTU**
Modbus RTU (Remote Terminal Unit), è un protocollo seriale Open Source nato dal paradigma master/slave inizialmente creato da Modicon.

**SNTP**
Simple Network Time Protocol. Espressione riferita a un server adibito alla gestione della data e dell'ora della rete di comunicazione.

**TCP**
Transmission Control Protocol. Il protocollo TCP/IP è un insieme di regole standardizzate che consentono ai computer di comunicare su una rete come Internet.

**TLS**
Transport Layer Security.

**Hager Bocchiotti S.p.A.**
Via dei Valtorta, 45

20127 MILANO

**www.hager-bocchiotti.com**

2023-07

6LE009858A