Cybersecurity guide

hw+

sentinel Energy circuit breakers
HW1, HW2 and HW4

hager

Contents

Page

Warnings and instructions

This documentation contains safety advice which must be respected for your own safety and to prevent property damage.
Safety advice relating to your own safety is identified by a safety warning symbol in the documentation. Safety advice relating to damage to property is identified by "ATTENTION".
The safety warning symbols and the wording below are classified according to the risk level.

⚠ DANGER

DANGER indicates an imminent dangerous situation which, if not avoided, will result in death or serious injuries.

⚠ WARNING

WARNING indicates a potentially dangerous situation which, if not avoided, may result in serious injuries or even death.

⚠ CAUTION

CAUTION indicates a potentially dangerous situation which, if not avoided, may result in minor or moderate injuries.

ATTENTION

ATTENTION indicates a warning message relating to equipment damage.
ATTENTION also indicates important instructions for use and particularly relevant information regarding the product, which must be respected to ensure effective and safe use.

Qualified personnel

The product or the system described in this documentation must be installed, operated and maintained by qualified personnel only. Hager Electro accepts no responsibility regarding the consequences of this equipment being used by unqualified personnel.
Qualified personnel are those people who have the necessary skills and knowledge for building, operating and installing electrical equipment, and who have received training enabling them to identify and avoid the risks incurred.

Appropriate use of Hager products

Hager products are designed to be used only for the applications described in the catalogues and in the technical documentation relating to them. If products and components from other manufacturers are used, they must be recommended or approved by Hager.
Appropriate use of Hager products during transport, storage, installation, assembly, commissioning, operation and maintenance is required to guarantee problem-free operation in complete safety.
The permissible ambient conditions must be respected. The information contained in the technical documentation must be respected.

Publication liability

The contents of this documentation have been reviewed in order to ensure that the information is correct at the time of publication.
Hager cannot, however, guarantee the accuracy of all the information contained in this documentation. Hager assumes no responsibility for printing errors and any damage they may cause.
Hager reserves the right to make the necessary corrections and modifications to subsequent versions.

Cybersecurity and wireless connection

The product or the system described in this documentation requires protective measures to be set up against the risks intrinsic to any wireless connection and transmission and the risks intrinsic to any cable-based connection and transmission.

⚠ WARNING

Risks of remote hacking through a wireless connection

- Keep the Bluetooth Low Energy connection deactivated, if you do not use the Hager Power touch application.
- Avoid activating the Bluetooth Low Energy connection if you are not able to prevent unauthorised access to the installed devices.

Failure to follow these instructions may result in death, serious injury or material damage.

⚠ WARNING

Risks that could affect the availability, integrity and confidentiality of the sentinel Energy system

- Change the default passwords during first use to prevent any unauthorised access to the device settings, controls and information.
- Disable unused ports and services, as well as default accounts, to reduce the risk of malicious attacks.
- Protect the devices in the network with several levels of cyberdefence (firewall, network segmentation, intrusion detection and network protection).
- Respect good cybersecurity practices (for example: least privilege principle, separation of tasks) to reduce the risks of intrusion, the loss or alteration of data and logs, or the interruption of services.

Failure to follow these instructions may result in death, serious injury or material damage.

Purpose of the document

This document is intended to provide electrical installers, system integrators or system designers with information about the cybersecurity of hw+ circuit breakers equipped with sentinel Energy electronic trip units. This is to help the designers and users of these systems implement a secure environment for operating the product.

Field of application

This document applies to hw+ circuit breakers equipped with sentinel Energy electronic trip units.

Revisions

Version	Date
6LE009346A	December 2023

Documents to consult

Document	Reference
HW1 installation manual	6LE007893A
HW2 and HW4 installation manual	6LE009206A
User manual for sentinel Energy hw+ electronic trip units	6LE008147A
sentinel Energy Modbus communication user guide	6LE007964A

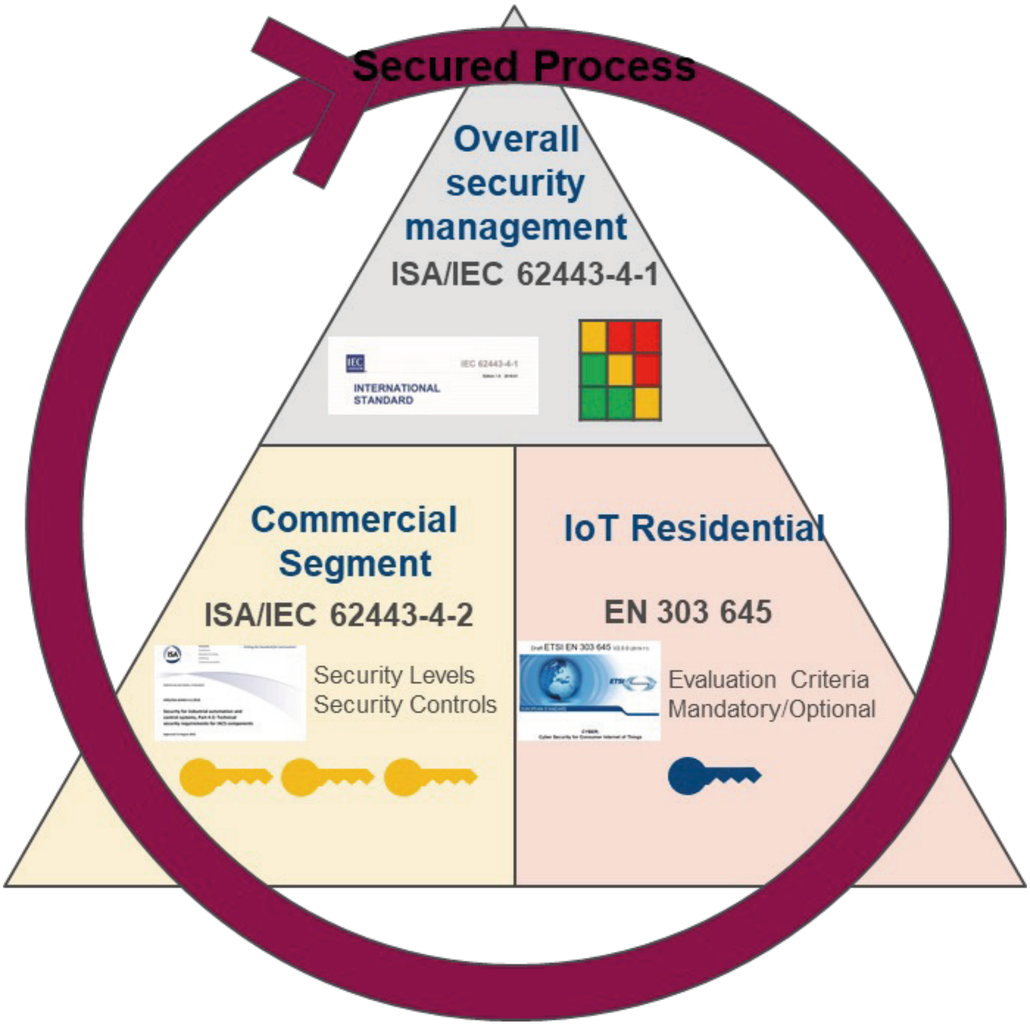
You can download these publications and other technical information from our website: www.hager.com

Contact

Address	Hager Electro SAS 132 Boulevard d’Europe 67215 Obernai France
Phone	+ 33 (0)3 88 49 50 50
Website	www.hager.com

Hager pays special attention to data protection and connection security issues related to its connected products.
For this reason we implement all regulations to reach the highest standards of quality in terms of the data security provided by our products.

Hager uses the IEC 62443 and EN 303 645 standards in the design and development of its connected products.
The IEC 62443 series of standards applies to the secure operation of Industrial Control Systems (ICS systems) from design to management and installation.
The EN 303 645 standard defines high-level cybersecurity and data protection provisions for connected consumer IoT devices.



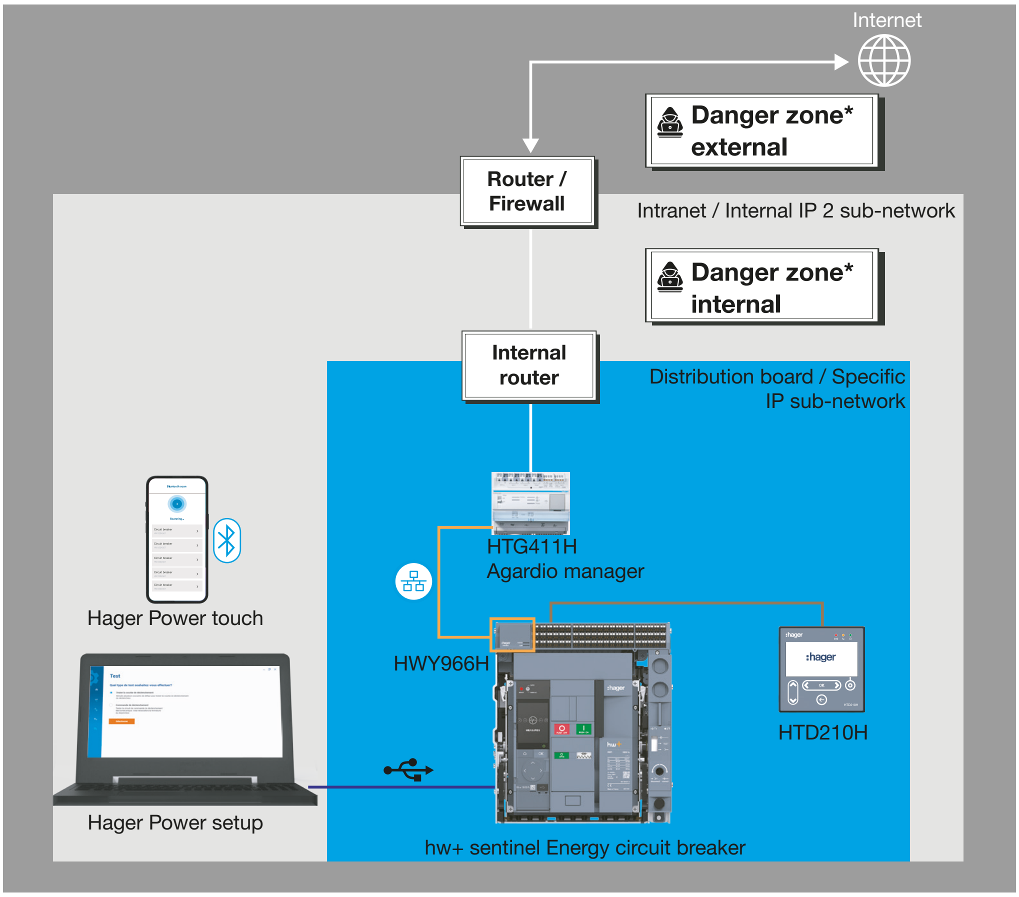
Applying a secure process during the design, development and validation phases also prevents attacks aimed at disrupting your products or modifying the configuration of your system.

2.2.1 Environment of the sentinel Energy system

The hw+ sentinel Energy circuit breaker is a crucial element in an electrical energy distribution or electrical equipment because it provides the electrical protection.

Thanks to its communication functions, it provides access to real-time control functions and data for monitoring electrical distribution. This allows more flexible and efficient management of your electrical installation. These functions do expose you to potential cyber attacks, however.

The following figure illustrates the communication environment in which the hw+ sentinel Energy circuit breaker is integrated.



Key:

⬛	Internet
⬜	Intranet
🟦	Distribution board
━	Modbus communication
━	USB-C
━	CIP port for proprietary protocol
ᛒ	Bluetooth Low Energy

(*) Risk of attacks or compromise

The sentinel Energy system allows communication with the hw+ circuit breaker in the following ways:
- the display/keyboard interface of the sentinel Energy circuit breaker,
- the wireless Bluetooth Low Energy (BLE) connection from a smartphone with the Hager Power touch application,
- the Hager Power setup application connected via USB-C port,
- serial link connection using the proprietary CIP protocol to the HTD210H panel display,
- RS 485 serial link network connection using the Modbus-RTU protocol,
- Ethernet network connection using the Modbus-TCP protocol.

Each of these means of communication represents a vulnerability in your system, if appropriate security measures are not put in place.
If appropriate security measures are not put in place, your system is in particular exposed to the following risks:
- risk of system unavailability leading to a black-out,
- risk of system parameters being changed by unauthorised persons leading to malfunctions and a lack of electrical protection,
- risk of unauthorised persons taking control of the system, leading to a cyber-attack,
- risk of loss of essential and sensitive data via cyber-attack and blackmail.

This guide provides our recommendations to secure these means of communication and avoid intentional attacks or accidental improper use.

2.2.2 Security functions

The following safety functions have been integrated into the design in order to reduce the risks intrinsic to the deployment of the sentinel Energy system in a connected environment:

- securing Bluetooth communication using the AES algorithm,
- actions to change settings and control/command actions accessible only after entering passwords or PIN codes,
- encrypted IP communication,
- activation of encryption and authentication of the Modbus communication,
- graduated security level for write commands to Modbus registers.

These security functions as well as the operation of the sentinel Energy system have been verified by external and independent third-party organisations when running penetration tests (simulated attacks by hostile users or malicious software).

The operational technology (OT) designates the equipment and software used to monitor the devices and physical processes within a company. During deployment it is important to identify and protect information that is sensitive and essential to a company's operations.

Here is a non-exhaustive list of sensitive information:
- access codes to the equipment or locked premises,
- the system architecture,
- the IP or MAC addresses of the connected communication equipment,
- the port numbers used for Ethernet communication,
- user identifiers and passwords.

Information provided by the sentinel Energy system is also considered sensitive.

	sentinel Energy display	**HTD210H panel display**	**Bluetooth**	**USB-C**	**Modbus-RTU Modbus-TCP**
Modbus-TCP					
Data monitoring	Read	Read	Read	Read	Read
Circuit breaker protection parameter	Read/Write	Read/Write	Read	Read/Write	Read/Write
Other circuit breaker parameters	Read/Write	Read/Write	Read	Read/Write	Read/Write
Opening and closing commands	Yes	No	Yes	Yes	Yes
Resets	Yes	Yes	No	Yes	Yes

One of the key points in a defence strategy against cyber attacks is to apply an effective password policy.

⚠ WARNING

Risks that could affect the availability, integrity and confidentiality of the sentinel Energy system
Change the default passwords during first use to prevent any unauthorised access to the device settings, controls and information.
Failure to follow these instructions may result in death, serious injury or material damage.

This includes the following best practices (non-exhaustive list):

- Change all default passwords.
- Set strong passwords: trivial choices such as "1234" or "password" should be avoided.
- Do not share passwords with unauthorised or unapproved persons.
- Change your passwords regularly.
- Do not re-use old passwords.
- Store the passwords in a safe place (for example a passwords vault).

This password policy must be applied to all components of the sentinel Energy system, to the servers, computers, smartphones connected to the system and any other network component.

Cybersecurity involves all employees of the company. In particular, all users authorised to access the sentinel Energy system and the installation communication network must know the company's information protection strategy.

They must also have undergone training in the fundamental principles of cybersecurity and the implementation rules derived from this strategy.

Regular reminders of good practices should be followed (including but not limited to the following):

- follow the password strategy,
- do not share passwords, access codes and sensitive data,
- ensure that all computers connected to the system (commissioning, monitoring, control...) have received the latest updates and have anti-virus and anti-malware protection,
- if the computers are also used to send messages, the users must be trained to detect suspicious emails,
- all smartphones used to access the system must be protected by a PIN code or facial recognition and must be protected against Internet and Bluetooth hacking,
- all smartphones must preserve their system integrity as well as their components,
- all smartphones used to access the system must always remain in the possession of the users and not be shared,
- the security policies in effect must not be bypassed.

Local access to the sentinel Energy trip unit included with the hw+ circuit breaker enables access to all of its functions, protection parameters and remote control in particular.

It is therefore important to restrict access to it by installing the circuit breaker in premises under lock and key or protected by access code in order to avoid:

- any unauthorised access to the sentinel Energy display and its keyboard, avoiding any risks of control and setting parameters being changed,
- any unauthorised access to the wireless Bluetooth communication, avoiding any risk of the Hager Power touch application being used to take control,
- any unauthorised connection via the USB-C port to avoid any risk of parameters being changed from the Hager Power setup software.

In particular, you must verify that:

- the premises are maintained under lock and key at all times,
- the premises are equipped with an authentication and authorisation system,
- only authorised personnel have a key or access code,
- the network communication cables that enter the premises and the connection ports on the communication equipment outside of the room are protected,
- all equipment (computer, smartphones and tablets) that have access to the sentinel Energy trip unit enjoy enhanced protection in accordance with the latest instructions from the supplier.

Any person with access to the distribution board where the hw+ circuit breaker is installed can access the sentinel Energy display and its keyboard and change the circuit breaker's parameter settings.

Here are our recommendations for protecting yourselves against malicious or involuntary acts resulting from access to the sentinel Energy display and its keyboard:

- activate password protection for changes to any parameters (other than screen display settings),
- activate locking of the sentinel Energy keyboard,
- seal the trip unit's transparent protection cover,
- communicate the sentinel Energy trip unit's password only to authorised persons,
- avoid storing this password on the smartphone where the Hager Power touch application is installed (sms, email, notes…).

Connection via Bluetooth communication allows a smartphone running the Hager Power touch application read access to information from the sentinel Energy trip unit and to initiate an opening or closing command on the hw+ circuit breaker.

Here are our recommendations for protecting yourself against malicious or involuntary acts resulting from access to the Bluetooth connection:

- install the hw+ circuit breaker in premises kept under lock and key, access to which is protected at all times,
- only authorised persons should have access to the premises,
- the password of the sentinel Energy trip unit must only be communicated to authorised persons.

Use of the Hager Power touch application

The Hager Power touch application allows monitoring of the information provided by the sentinel Energy trip unit, particularly the operational status of the circuit breaker and the metering values.
It also allows an opening or closing command to be carried out on the hw+ circuit breaker, if the appropriate accessories have been installed on the circuit breaker.

The first time the smartphone running the Hager Power touch application is paired with the circuit breaker, a physical action must be performed on the sentinel Energy trip unit. From the second connection, pairing is no longer required. A connection with the smartphone will be established automatically if Bluetooth communication is activated and the device is within range of the Bluetooth Low Energy transmission.
See the hw+ sentinel Energy electronic trip unit user manual for more information on this application.

It is therefore essential to avoid any risk of the Bluetooth communication being used for hacking with the Hager Power touch application.

⚠ **WARNING**

Risks of remote hacking through a wireless connection

- Keep the Bluetooth Low Energy connection of the trip unit deactivated, if the Hager Power touch application is not approved by your IT department.
- Deactivate the Bluetooth Low Energy connection on the trip unit if the Hager Power touch application is not used for an extended period.
- Delete the hw+ circuit breaker from your smartphone's known Bluetooth devices if the Hager Power touch application is not used for an extended period.
- Avoid activating the circuit breaker's Bluetooth Low Energy connection if you are not able to prevent unauthorised access to the installed devices.

Failure to follow these instructions may result in death, serious injury or material damage.

The USB-C port connection using the Hager Power setup software allows access to the sentinel Energy trip unit's protection and control functions.

⚠ WARNING

Risks that could affect the availability, integrity and operation of the hw+ circuit breaker
Seal the trip unit's transparent protection cover if you are not able to prevent any unauthorised access to the circuit breaker.
Failure to follow these instructions may result in death, serious injury or material damage.

To connect to the USB-C port the following conditions must be fulfilled:
- to physically have access to the USB-C socket on the sentinel Energy trip unit,
- to have installed the Hager Power setup software on a laptop computer,
- to have connected this computer to the trip unit using a USB-C adapter.

Our recommendations for use of the Hager Power setup software are as follows:

Many attacks exploit weaknesses in the Microsoft Windows operating system. This is why the computer on which Hager Power setup is installed must be secure:
- the computer must have up-to-date anti-virus software installed and activated,
- the computer must be configured to operate on a per session basis (identifier + password),
- the password and computer use policies must be respected,
- the Hager Power setup software must be up-to-date.

4.4 Access protection for the HTD210H panel display

The HTD210H panel display offers access to several of the trip unit functions, including its protection parameters.

It is therefore important to restrict access to it by installing the circuit breaker in premises under lock and key or protected by access code in order to avoid:
- any unauthorised access to the sentinel Energy display and its keyboard, avoiding any risks of control and setting parameters being changed,
- any unauthorised access to the wireless Bluetooth communication, avoiding any risk of the Hager Power touch application being used to take control,
- any unauthorised connection via the USB-C port to avoid any risk of parameters being changed from the Hager Power setup software.

In particular, you must verify that:
- the premises are maintained under lock and key at all times,
- the premises are equipped with an authentication and authorisation system,
- only authorised personnel have a key or access code.

Here are our recommendations for protecting yourself against malicious or involuntary acts resulting from access to the HTD210H panel display:
- change the password of the HTD210H panel display the first time it is used,
- activate the display keyboard locking,
- seal the trip unit's transparent protection cover,
- communicate the display trip unit's password only to authorised persons.

The hw+ circuit breaker equipped with a sentinel Energy trip unit offers two remote access options:

- via an RS 485 serial link network using the Modbus RTU protocol with an HWY965H communication module,
- via an Ethernet network using the Modbus TCP/IP protocol with an HWY966H communication module.

This remote access makes all the functions of the sentinel Energy trip unit available, in particular the those related to the protection parameters and remote control.

It is therefore important to activate remote access locking, if write access to the trip unit parameters and access to the remote control functions is not required remotely.

Remote access locking is enabled from the sentinel Energy trip unit.
See the hw+ sentinel Energy electronic trip unit user manual for more information.

To secure the remote access, we recommend the following:

- do not do any port redirection in the router modem. This would expose your Modbus interface or configurator to the Internet,
- protect the devices with several levels of cyberdefence (firewall, intrusion detection, etc.),
- separate the company network from the operational technology (OT) network,
- set up a list of authorised addresses.

Modbus-TCP communication with the hw+ circuit breaker allows access to all status, indicator and measurement data, settings parameters and remote control functions.
The protocols used are:

- SNTP: synchronisation of date and time
- DHCP: assignment of IP network address
- DNS: domain name resolution
- HTTPS: for Ethernet access to the module configuration web page
- Modbus Messaging on TCP/IP: for the server's communication with the Modbus clients.

The Modbus-TCP communication module allows the hw+ circuit breaker server to connect to multiple clients or to connect a computer via Ethernet to configure the Modbus communication.

Here are our recommendations for protecting yourself against malicious or involuntary acts resulting from Modbus-TCP communication:

A computer connected to the Modbus-TCP module via Ethernet must have up-to-date anti-virus software installed and activated. It must be configured to work per session (identifier + password). The password and computer use policies must be respected.
This computer must be assigned only to approved and authorised persons.

For communication with a Modbus client, if possible on the latter and the communication system deployed, it is recommended that TLS Modbus security be activated on the Modbus TCP communication module.
By default, the Modbus-TCP protocol is not secure; some messages can be decrypted easily.

The Modbus TCP module allows activation of the secure Modbus protocol with TLS and no authentication or the secure Modbus protocol with TLS and mutual authentication.

The connection of a computer via Ethernet to the communication module allows HTTPS access to the module's web pages to configure the IP address assignment strategy and the management of X.509 certificates to authenticate the Modbus server and its clients.

See the sentinel Energy Modbus communication user guide for more information about secure Modbus via TLS and the HTTPS connection.

Modbus-RTU communication with the hw+ circuit breaker allows access to all its status, indicator and measurement data, settings parameters and remote control functions.

Here are our recommendations for protecting yourself against malicious or involuntary acts resulting from Modbus-RTU communication:

- antivirus software must be installed on the computer with access to the network connected to the Modbus-RTU communication,
- this antivirus software must be active and up-to-date,
- the computer must be configured to operate on a per session basis (identifier + password),
- the password and computer use policies must be respected,
- this computer must be assigned only to approved and authorised persons. .

See the sentinel Energy Modbus communication user guide for more information about the use of Modbus-RTU.

Update of the Hager Power setup software and the Hager Power touch application
It is important to always have the latest software versions. In addition to functional bug-fixes and developments, these also include security updates because cyberattack and cyberdefence techniques are in a state of constant evolution.

The following can be updated as indicated:

- Hager Power setup software: to be notified whenever an update is available, the computer running the software must be connected to the Internet,
- Hager Power touch application: as with all mobile phone applications, updates are made available on the Apple store and Google Play.

Firmware updates
For updates to the firmware of the sentinel Energy trip unit, the communication modules and the panel display, if an update is necessary, it will be performed by a Hager technician.

Cybersecurity assistance
Hager has put in place a vulnerability management policy in order to respond rapidly to cybersecurity failure incidents in its connected services and products.

You can declare a cybersecurity incident or vulnerability in one of the following ways:
a) For an optimum response time, send an email to our Product Security Team with a precise description of the problem and the product models concerned. Email: productsecurity@hagergroup.com
b) Contact your Hager representative or local Hager technical support (contact details on the Hager website for your country), making clear that the issue relates to cybersecurity and giving a precise description of the problem as well as the products concerned.

The declaration of a cybersecurity incident allows the Product Security Team to evaluate the risks, propose counter-measures and develop the software and equipment by making the corrections required.

AES
Advanced Encryption Standard

DHCP
Dynamic Host Configuration Protocol. Dynamic Host Configuration Protocol used to manage IP addresses.

DNS
Domain Name System. DNS allows a comprehensible name to be associated with an IP address.

CIP
Communication Interface Port. Also used to refer to the proprietary protocol that enables interfacing with components of the sentinel Energy system.

ICS
Industrial Control System. An industrial control system designates physical and digital objects that regulate and manage the behaviour of machines and machine processes in industrial installations.

MAC
The MAC (Media Access Control) address is the physical address of a network peripheral. Each MAC address is unique, allowing electronic devices to be identified.

OT
The operational technology consists of the hardware and software that monitor and control the processes and physical industrial devices.

RTU
Modbus RTU (Remote Terminal Unit), is an Open Source serial protocol based on the master / slave design initially created by Modicon (currently Schneider Electric).

SNTP
Simple Network Time Protocol. Used by a server managing the date and time of the communication network.

TCP
Transmission Control Protocol. TCP/IP is a set of standardised rules allowing computers to communicate on a network such as the Internet.

TLS
Transport Layer Security.

Hager Electro SAS
132 Boulevard d’Europe
BP3
67210 OBERNAI CEDEX

www.hager.com

2024-04