Cybersecurity Guide

System interface Gateway for bus System

Wireless and Modbus RTU/Ethernet Transceiver for Energy Management Systems

TMF100

:hager

EN

01 About this manual 5

01.01 Warnings and notes 5
01.02 Qualified personnel 5
01.03 Proper Use of Hager Products 6
01.04 Purpose of the Document 6
01.05 Scope 6
01.06 Documents to consult 6

02 Cybersecurity in Hager Products 7

03 Cybersecurity applied to TMF100 8

03.01 TMF100 : System Environment 8
03.02 Security Features 9

04 General Cybersecurity Recommendations 10

04.01 Deployment of operational technology 10
04.02 Password Policy 10
04.03 Instructions for users of the TMF100 device 10

05 Cybersecurity Recommendations for local access 12

05.01 Protecting access to the TMF100 device 12
05.02 Protecting access via Bluetooth communication 12
05.03 Using the Hager Pilot app 12
05.04 Protecting access via Wireless communication 13
05.05 Protecting access via Modbus RTU communication 13

06 Cybersecurity Recommendations for remote access 14

06.01 Remote access protection 14
06.02 Protecting access via Modbus-TCP 14

07 System Updates 16
07.01 Hager Pilot Software Update 16
07.02 TMF100 firmware update 16

08 Cybersecurity Recommendations for disposal 17

09 Cybersecurity Assistance 18

10 Glossary 19

01 About this manual

01.01 Warnings and notes

This documentation contains safety instructions that you must follow to ensure your personal safety and to prevent property damage.
Safety instructions relating to your personal safety are indicated in the documentation by a safety alert symbol.
Safety instructions relating to property damage are indicated by the word “NOTICE.”
The safety warning symbols and the notice below are classified according to the degree of risk.

DANGER !

indicates an imminent hazardous situation that, if not avoided, will result in death or serious injury.

WARNING !

indicates a potentially dangerous situation that, if it cannot be avoided, may result in serious injury or even death.

CAUTION !

indicates a cybersecurity risk, that may affect the availability, integrity or confidentiality.

NOTICE

indicates a warning about property damage.

also provides important operating instructions and, above all, useful information about the product, which should be given special attention to ensure safe and effective use.

01.02 Qualified personnel

The product or system described in this documentation must be installed, operated, and maintained by qualified personnel only. Hager Electro assumes no liability for the consequences of using this equipment by unqualified personnel.
A qualified person is one who possesses the skills and knowledge necessary for the construction and operation of electrical equipment installations, and who has received training enabling them to identify and avoid potential hazards.

01.03 Proper Use of Hager Products

Hager products are intended for use only in the applications described in the relevant catalogues and technical documentation. If products and components from other manufacturers are used, they must be recommended or approved by Hager.
Proper use of Hager products during transport, storage, installation, assembly, commissioning, operation, and maintenance is necessary to ensure safe and trouble-free operation.
Permissible ambient conditions must be observed. The information contained in the technical documentation must be followed.

01.04 Purpose of the Document

The purpose of this document is to provide electrical installers, system integrators, system designers, and end users with information about the cybersecurity features of the TMF100 device connected to energy management devices, in order to help them set up and maintain a secure operating environment for the product.

01.05 Scope

This document applies to TMF100 device connected to energy management devices.

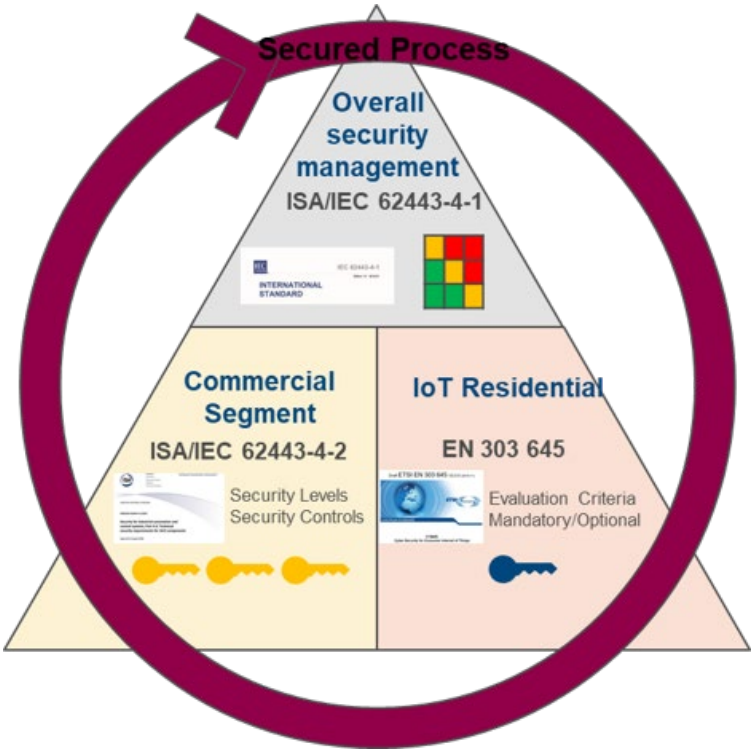
01.06 Documents to consult

Document	Reference
Installation Guide	6LE091061A

02 Cybersecurity in Hager Products

Hager pays particular attention to data protection and connection security issues for its connected products.
That is why we take every measure to achieve the highest quality standards in terms of data security for our products.

Hager uses the requirements of 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 automation systems (ICS) from design to management, including implementation.
The EN 303 645 standard defines high-level provisions for cybersecurity and data protection 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 altering your system configuration.

03 Cybersecurity applied to TMF100

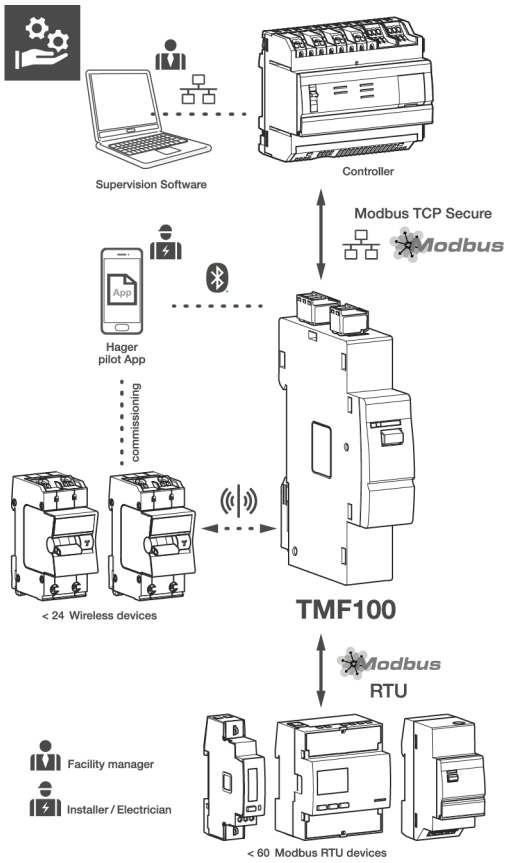
03.01 TMF100 : System Environment

The TMF100 provides communication between compatible Hager wireless devices, Modbus RTU devices and Modbus TCP systems.

Thanks to these communication functions, it provides access to real-time control and monitoring functions. This allows for greater efficiency and flexibility in managing your electrical installation.

The device transfers field data from compatible Hager wireless protection and energy devices (DPD) and Modbus RTU devices to controllers, supervision systems and Building Management Systems (BMS) and includes Cybersecurity features.

The following figure illustrates the communication environment in which the TMF100 is integrated:



The gateway can communicate with other products in one of the following ways:

- Wireless Bluetooth Low Energy (BLE) connection from a smartphone running the Hager Pilot configuration and commissioning application.
- Wireless connection for communication exclusively with compatible Hager devices.
- Connection to an RS 485 serial wired network using the Modbus-RTU protocol to communicate with Modbus products in the system.
- Connection to a wired Ethernet network using the Modbus-TCP protocol.

Each of these means of communication represents a vulnerability in your system if the appropriate security measures are not in place.
In particular, your system is exposed to the following risks if the appropriate security measures are not in place:

- Risk of system unavailability
- Risk of unauthorised persons modifying system settings
- Risk of unauthorised persons taking control of the system
- Risk of loss and theft of essential and sensitive data

This guide provides our recommendations for securing these means of communication and preventing intentional attacks or accidental misuse.

03.02 Security Features

The following security features have been incorporated into the design to mitigate the threats inherent in deploying the TMF100 device in a connected environment:

- Bluetooth communication is disabled by default and requires local activation.
- Bluetooth is automatically deactivated after 15 minutes without communication.
- Bluetooth communication is secured using the AES algorithm
- Settings modification and control/command actions accessible only after entering passwords in Hager Pilot
- After commissioning, configuration access is linked to the MyHager account used during the initial setup
- Encrypted IP communication with TLS1.2 certificates
- Modbus RTU is not encrypted/authenticated.
- Encrypted and authenticated Modbus TCP communication when TLS is enabled
- Graduated security level for write commands in Modbus registers, depending on the Modbus devices linked to the system
- Wireless communication is also secured using the AES algorithm. Moreover, a whitelist is defined allowing a restricted list of Hager devices to be enrolled in the system.

These security features and the operation of the TMF100 system have been verified by external, independent third-party organisations during penetration testing (simulation of attacks by a malicious user or malware).

04 General Cybersecurity Recommendations

04.01 Deployment of operational technology

Operational technology (OT) refers to the hardware and software used to monitor physical devices and processes within a company. When deploying OT, it is important to identify and protect information that is essential or sensitive to a company's operations.

Here is a non-exhaustive list of sensitive information:

- Access codes for locked equipment or premises
- System architecture
- IP or MAC addresses of connected communication equipment
- Port numbers used for Ethernet communication
- User IDs and passwords

04.02 Password Policy

One of the key elements of a defence strategy against cyberattacks is to implement an effective password policy.

CAUTION !

Risks that may affect the availability, integrity and confidentiality of the TMF100 device and of the system.

Change the default passwords on first use to prevent unauthorised access to device settings, controls and information.

This involves 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 your passwords with unauthorised persons
- Change your passwords regularly
- Do not reuse old passwords

This password policy must be applied to all components of the system integrating the TMF100, servers, computers and smartphones connected to the system.

04.03 Instructions for users of the TMF100 device

Cybersecurity concerns all company employees. In particular, all users authorised to access the TMF100 device and the facility's communication network must be familiar with the company's information protection strategy.

They must also have undergone training in the fundamental principles of cybersecurity and the rules for implementing this strategy.

It is necessary to regularly remind users of the following best practices (among others):

- Follow the password strategy
- Do not share passwords, access codes, or sensitive data
- Ensure that all computers connected to the system (commissioning, monitoring, control, etc.) are up to date and protected against viruses and malware
- If computers are also used to send messages, users must be trained to detect suspicious emails.
- All smartphones used to access the system must be protected by a PIN code or biometric recognition and must be protected against hacking via the Internet and Bluetooth
- All smartphones used to access the system must always remain in the possession of users and must not be shared
- The security policies in place must not be circumvented

05 Cybersecurity Recommendations for local access

05.01 Protecting access to the TMF100 device

If the MyHager account associated with the TMF100 is compromised, local access allows the activation to all its features, including the configuration and the data access.

It is therefore important to restrict access by installing the device in a locked room or one protected by an access code to prevent:

- Unauthorised access to the TMF100 and connected products, avoiding any risk of modification of settings and control parameters
- Unauthorised access to wireless Bluetooth communication, avoiding the risk of takeover with the Hager Pilot application
- Unauthorised wireless connections, avoiding any risk of products being added or removed

In particular, you must verify that:

- the room is kept locked at all times
- the room is equipped with an authentication and authorisation system
- only authorised personnel have a key or access code
- the communication network cables entering the premises and the connection ports on communication equipment outside the room are protected
- all equipment (computers, smartphones and tablets) that has access to the Transceiver is protected in accordance with the latest instructions from the supplier

05.02 Protecting access via Bluetooth communication

The Bluetooth connection allows a smartphone running the Hager Pilot app to configure the TMF100 as well as Modbus and wireless devices. Bluetooth commissioning requires local physical access to the device to activate pairing mode. The communication is secured by default.

Here are our recommendations to protect against any malicious or unintentional acts via Bluetooth connection:

- Install the TMF100 and the products connected to it in a room that is kept locked or whose access is protected at all times
- Only authorised persons should have access to the room

05.03 Using the Hager Pilot app

The Hager Pilot app allows you to configure the transceiver, configure communications, and pair wireless Hager devices.

When you first connect, the transceiver is linked to the MyHager account that uses the Hager Pilot app. This prevents any other user from accessing the configuration data.

This user account is a key element of protection. It is therefore essential to protect it.

Here are our recommendations to protect this account:

- The password must comply with the password strategy.
- This account must not be shared.
- The password must be changed regularly, without using old passwords.
- Log out of the Hager Pilot app to prevent automatic reconnection without authentication.

05.04 Protecting access via Wireless communication

The wireless communication protocol is secured by default during commissioning and operation.
There are no specific security recommendations.

05.05 Protecting access via Modbus RTU communication

Modbus RTU communication does not provide encryption or authentication mechanisms.
Here are our recommendations to protect the Modbus RTU:

- The Modbus RTU network must be located only in a restricted and protected area with physical protection

06 Cybersecurity Recommendations for remote access

06.01 Remote access protection

The TMF100's Ethernet connectivity (Modbus over TCP/IP) allows remote control of all products connected to it. Some of these products may have security features.

It is essential to protect this Ethernet access point by following these recommendations:

- Do not redirect ports at the modem router level. This would expose your Modbus interface or configurator on the Internet.
- Protect devices with multiple levels of cyber defence (firewall, intrusion detection, etc.).
- Separate the company network from the operational technology (OT) network.

06.02 Protecting access via Modbus-TCP

Access via Modbus-TCP communication to the transceiver allows access to status data, indicators, measurements, setting parameters and remote control functions.
The protocols used are:

- SNTP: date and time synchronisation
- DHCP: IP network address assignment. It can be disabled with fixed IP addresses.
  DHCP is recommended during commissioning to simplify network integration. If no DHCP server is available, manual IP configuration using the default IP settings is possible
- DNS: domain name resolution
- HTTPS: Hypertext Transfer Protocol Secure
- Modbus Messaging on TCP/IP: for server communication with Modbus clients.

Modbus-TCP communication allows the transceiver to be connected to multiple clients or to connect a computer via Ethernet to configure Modbus communication. The TMF100 does not provide a default register model for third-party Modbus devices. Register mapping, polling strategy and data interpretation are configured in the controller/BMS.

We recommend the following measures to protect against malicious or unintentional actions via Modbus-TCP communication:

For a computer connected via Ethernet to the Modbus-TCP module:

- It must have antivirus software installed, active and up to date.
- It must be configured to operate by session (username + password).
- Password and computer usage policies must be followed.
- Only authorised persons should have access to this computer.

For communication with a TCP Modbus client: By default, TLS certificates are active in the transceiver in one-way, unauthenticated mode. These certificates are generated by Hager and can be replaced by proprietary certificates.

- If a new certificate is used, the expiry date must be short and therefore renewed regularly.
- If the products allow it, enable TLS security with mutual authentication.

CAUTION !
Disabling the TLS certificates

In some particular cases, some TCP/Modbus clients do not support the TLS configuration, it is possible to remove the certificates. If so, all messages will appear in clear text and can be easily understood and replayed. If so, this network must be isolated and secured to avoid data leakage.

07 System Updates

07.01 Hager Pilot Software Update

It is important to always have the latest software version. In addition to containing functional improvements and corrections, it also includes security updates, as cyberattack and cyberdefence techniques are constantly evolving.

Here is how to update the application:

- As with all mobile phone applications, updates are available on the Apple Store and Google Play.

07.02 TMF100 firmware update

Here is how to update the firmware of the device:

- Firmware updates are deployed via the Hager Pilot application during maintenance operations.

08 Cybersecurity Recommendations for disposal

Depending on the state of the TMF100 device (not broken and still accessible), here are the recommendations before product disposal :

- remove account association
- remove certificates
- factory reset
- delete network credentials

09 Cybersecurity Assistance

Hager has implemented a vulnerability management policy to respond quickly to cybersecurity incidents and vulnerabilities affecting its connected products and services.

To report a cybersecurity incident or vulnerability, you may use one of the following methods:
a) For the fastest response, fill the form “Report a vulnerability” accessible in the footer of the Hager website for your country.
b) Or, send an email to our Product Security Team, including a description of the issue and the model numbers of the affected products. Email address: productsecurity@hagergroup.com
c) Or contact your Hager representative or local Hager technical support (contact information available on the Hager website for your country), specifying that it is a cybersecurity issue, providing a description of the problem, and including the product references of the affected products.

Reporting a cybersecurity incident allows the Product Security Team to assess the risks, propose countermeasures, and update the software and hardware by applying the necessary fixes.

10 Glossary

AES
Advanced Encryption Standard.

BLE
Bluetooth Low Energy.

BMS
Building Management System.

DHCP
Dynamic Host Configuration Protocol. Dynamic Host Configuration Protocol used for managing IP addresses.

DNS
Domain Name System. DNS allows you to associate a human-readable name with an IP address.

ICS
Industrial Control System. An industrial control system refers to the physical and digital components that regulate and manage the behaviour of machines and machine processes in industrial facilities.

MAC
Media Access Control. A MAC address is the physical address of a network device. Each MAC address is unique, allowing electronic devices to be identified.

OT
Operational Technology. Operational technology refers to the hardware and software that monitor and control industrial processes and physical devices.

RTU
Remote Terminal Unit. Modbus RTU is an open-source serial protocol based on the master/slave architecture originally developed by Modicon (now Schneider Electric).

SNTP
Simple Network Time Protocol. Refers to a server responsible for managing the date and time of a communications network.

TCP
Transmission Control Protocol. TCP/IP is a set of standardized rules that allow computers to communicate over a network such as the Internet.

TLS
Transport Layer Security. A protocol used to encrypt and authenticate network communication.

Hager Controls S.A.S
B.P. 10140
Saverne Cedex
France

Tel.: +33 (0) 3 88 02 87 00
info@hager.com

hager.com

2026-08

6LE010014A