

6 - Menù Info

Menù Info: level 1 The Info menu contains information about the protection release settings, the protections and functions and the modules and accessories connected.

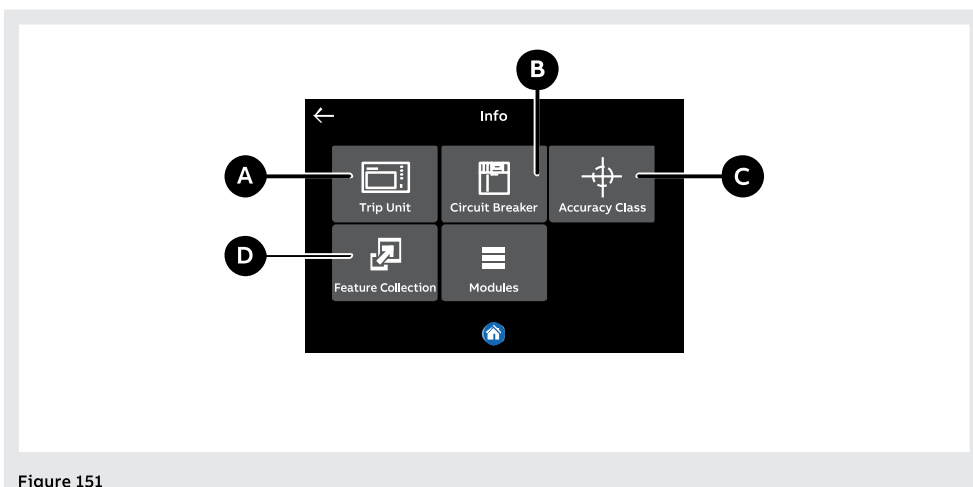


Figure 151

Pos.	Name	Description
A	Trip Unit	Information about the protection release
B	Circuit-breaker	Information about the CB
C	Accuracy Class	Information about the accuracy classes according to standard IEC61557-12
D	Feature Collection	List of protections available in protection release
E	Modules	List of modules detected by the protection release. The push-button is only visible when there are modules connected

Menù Info: Trip Unit Information about the protection release is given in the Trip Unit page.

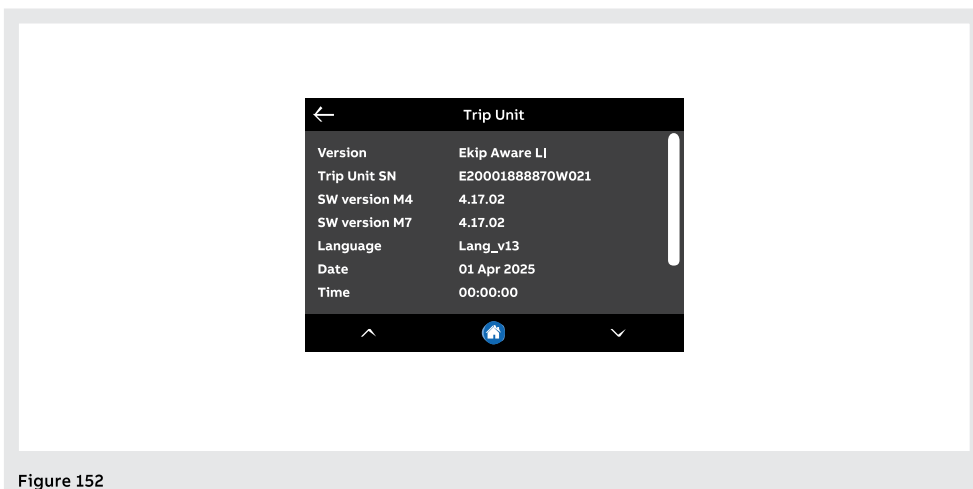


Figure 152

Name	Description
Version	Version of the Trip Unit
Trip Unit SN	Serial Number of the Trip Unit
SW version M4	Version M4 of firmware
SW version M7	Version M7 of firmware
Language	Language set
Date	Date set
Time	Hour set

Menù Info: Circuit Breaker Information about the circuit-breaker is given in the circuit-breaker page.

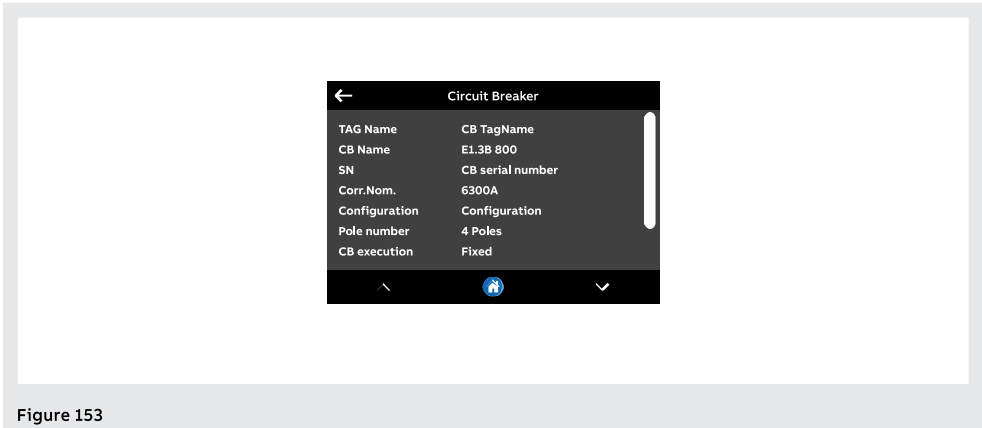


Figure 153

Name	Description
TAG Name	TAG name programmable by user
CB Name	CB Name
SN	Serial number of the CB
Corr.Nom.	Rated current setting
Configuration	Indication of 3-pole, 3P or 3P+N configuration
Number of poles	Number of poles
CB version	CB in fixed or withdrawable version
CB status	Status of the CB
CB Position	CB connected or disconnected
Total operations	Number of operations performed by CB
ReadyToClose	CB state, open or closed
Standard	Regulatory framework reference of circuit-breaker

Info menu: Accuracy Class The Accuracy Class page appears with the optional Class 0.5 and Class 1 functions.

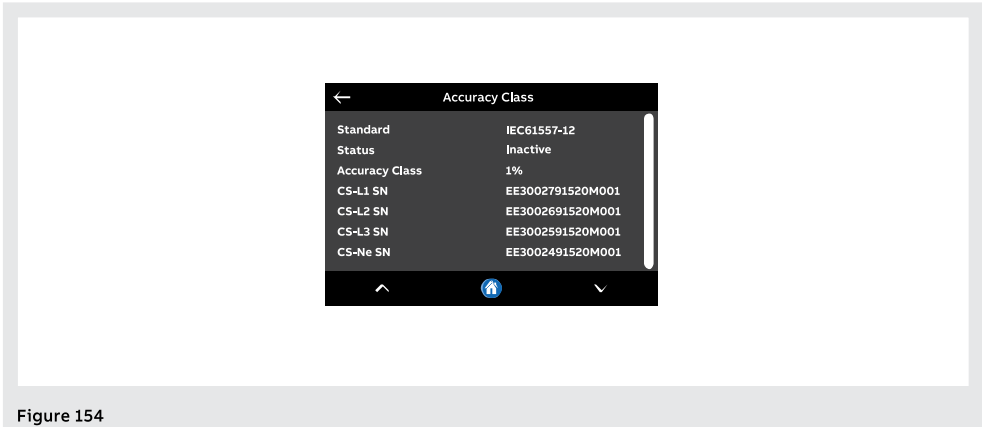


Figure 154

Name	Description
Standard	Name of Accuracy Class standard, IEC61557-12
State	Activation state of Class 0.5 and Class 1 functions
Accuracy Class	Indicates the accuracy class relating to the CB: 2%, 1% or 0,5%
CS-L1 SN	S/n of sensor on pole L1
CS-L2 SN	S/n of sensor on pole L2
CS-L3 SN	S/n of sensor on pole L3
CS-Ne SN	S/n of sensor on neutral pole

i **NOTE:** if CB model E6.3 is present, the first four s/n refer to sensors A on the half-poles; a second page with the s/n of sensors B of the other half-poles of each phase is also available.

Info menu: Modules The Modules page lists all the terminal block-mounted modules (plus Ekip Signalling 4K), if connected and detected by Ekip Aware.

Select each module to obtain useful information about the modules themselves, such as s/n, FW version, parameters and states.

These pages are only present if Ekip Aware detects the modules connected.

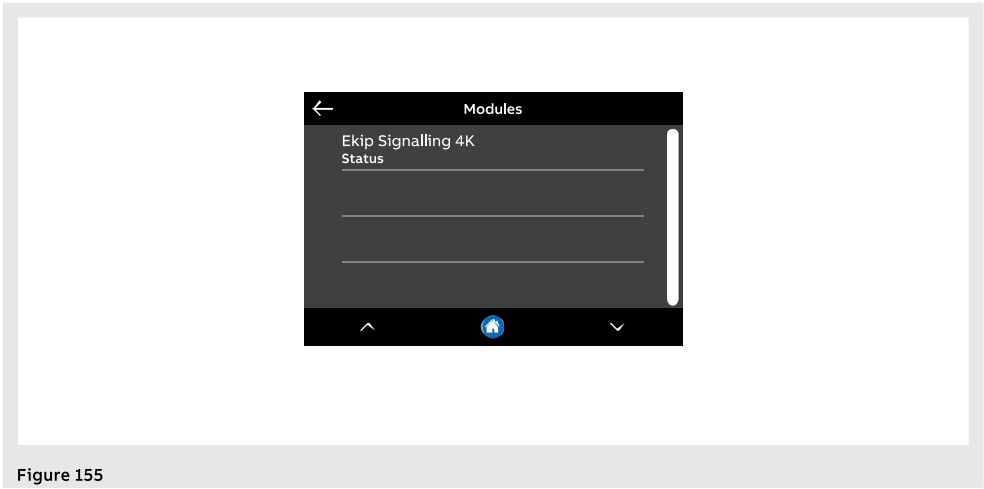


Figure 155

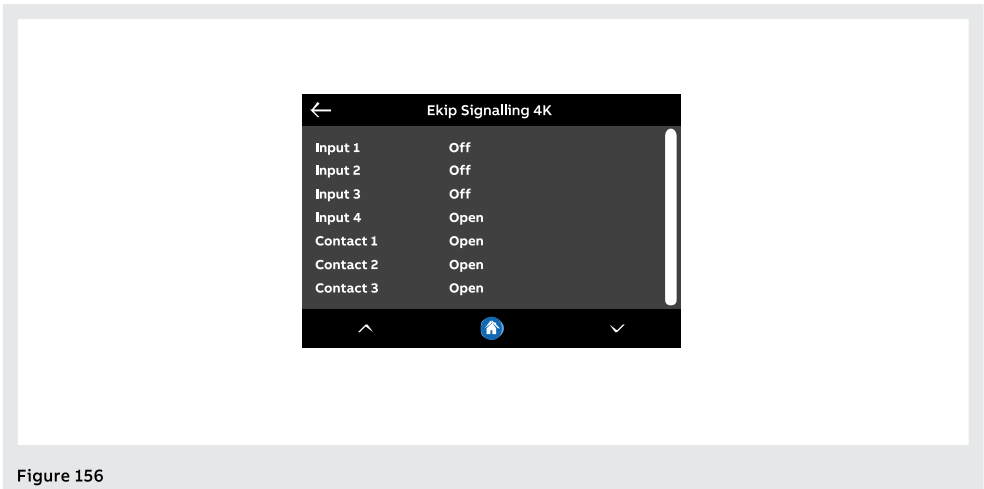


Figure 156

Menù Info: Feature Collection The Feature Collection page lists the protections and software packages present by default or acquired, available on the protection release.

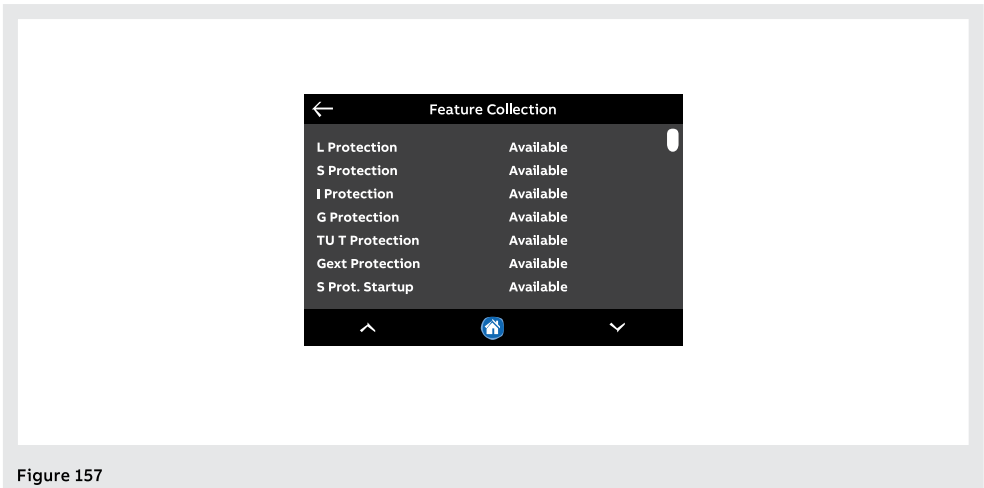


Figure 157

7 - Test Menu

Menù Test: level 1 The content of the Test menu depends on the protection release version and optional packages present.

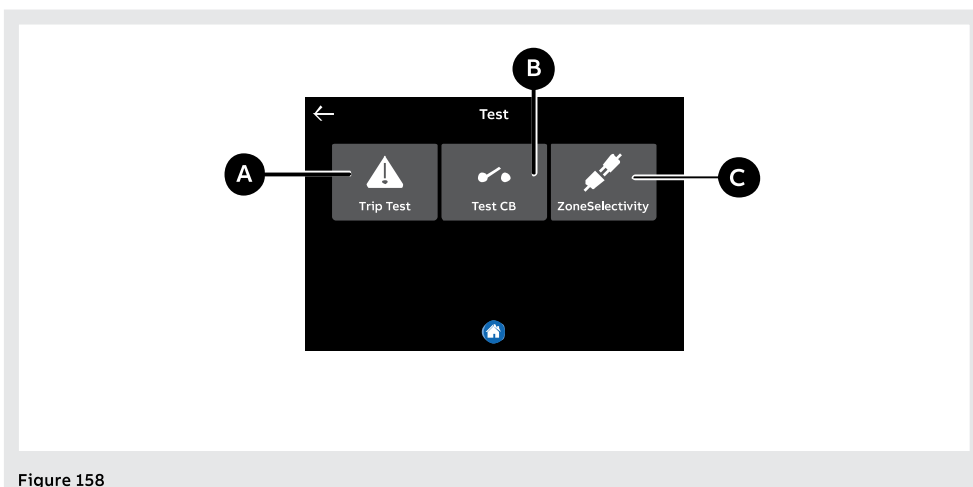


Figure 158

Pos.	Name	Description
A	Trip Test	CB opening test
B	Test CB	Tests of various types, coils (YO Sense and YC Sense) and displays
C	ZoneSelectivity	Test of hardware zone selectivity contacts

8 - Settings Menu

Menù Settings: level 1

The content of the Settings menu depends on the protection release version and optional packages present.

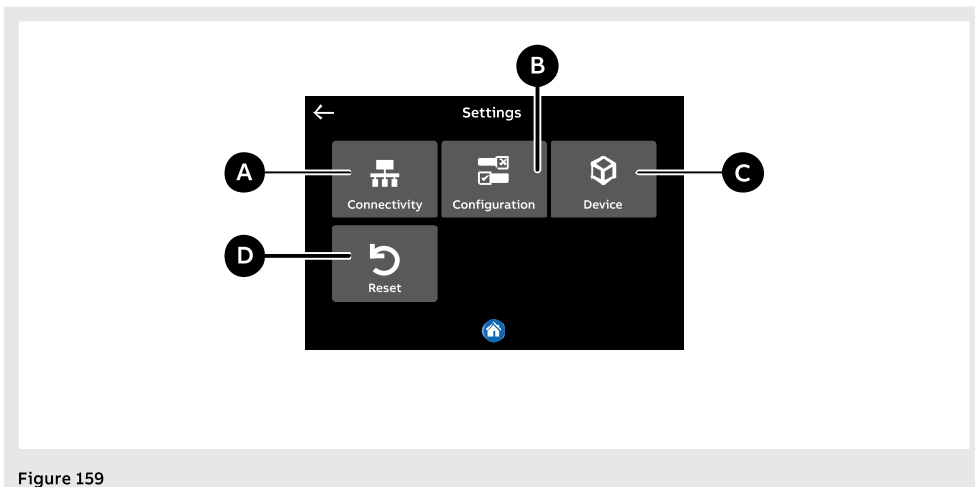


Figure 159

Pos.	Name	Description
A	Connectivity	Management of pairings with external devices
B	Configuration	Circuit-breaker parameter settings
C	Device	General parameters of protection release
D	Reset	Reset commands

9 - Changing parameters and commands

Changing parameters



IMPORTANT: parameters can be changed with protection release in the Local mode, in the absence of timing alarms and with the standard version protection release. If the Cybersecure software package is present, the only parameter that can be edited via display is BLE enabling.

Comply with the following procedure to change one or more parameters:

1. Select parameter and enter PIN if required;
2. select the new value required from the central scale (A) or with the help of commands - and + (B);
3. select Ok (C) if present;

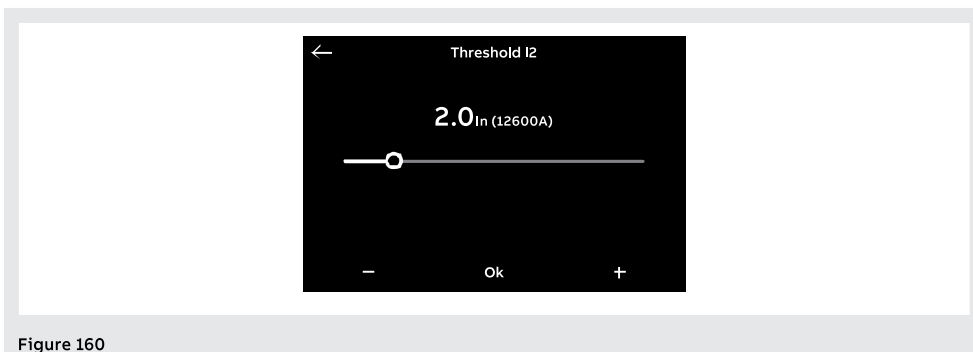


Figure 160

4. when the new value has been confirmed, you will automatically access the menu of the protection and the edited parameter will be highlighted by the edit symbol (Figure 161);

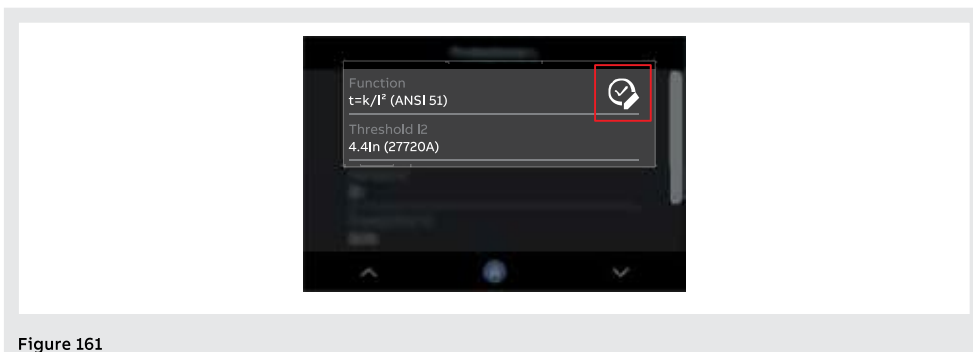


Figure 161

Now proceed by confirming the programming (Step 5) or access other parameters if further changes are required (Step 1).

5. select the arrow at the top left to access the top menu until the *Programming* page appears, or select HOME at the bottom of the page;
6. various commands are enabled in the Programming page:
 - Confirm to validate the new parameters and conclude the editing procedure;
 - Cancel to abort saving and return HOME;
 - Change to return to the menus and change the parameter or other.

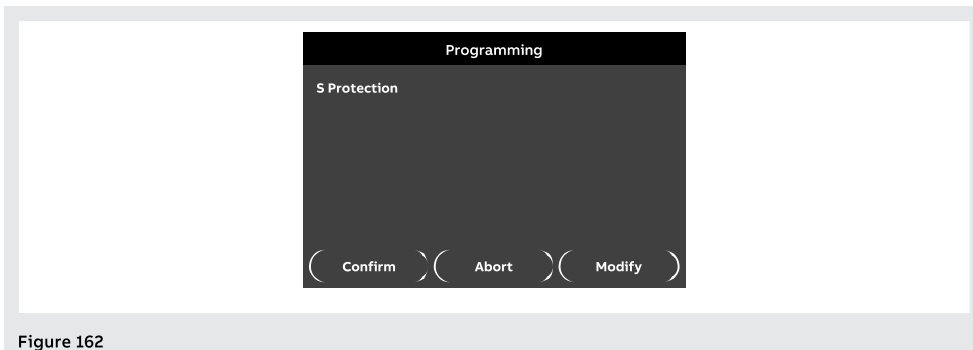


Figure 162

Modify the HOME page

The HOME page of the protection release displays the *Histograms* page of the *Measuring* menu.

The screen can be changed by choosing one of those available in the *Measuring* menu.

To change the HOME screen, navigate to the required page, press and hold the iTest button for a few seconds and confirm your choice when the following confirmation screen appears.

Commands

Selection of a command implies its immediate execution or opening of an intermediate confirm window.



CAUTION! Confirmation that the command has been sent can be viewed on the display. The user is responsible for checking the operation requested, regardless of the type of command: reset parameters, display management or open/close the contacts of the YO or YC coils.

Exceptions

In order to ascertain that there are no incorrect conditions or conflict, the protection release checks all its parameters before validating changes made to a parameter.



- If the protection release detects an incorrect condition, the relevant details appear on the display and parameter editing is annulled.

In addition, before executing a command, the protection release checks all its parameters to ascertain whether there are incorrect conditions or conflict.

- If the protection release detects an incorrect condition, the relevant details appear on the display and command execution is annulled.



IMPORTANT: aborting the programming affects all the parameters modified during the same session.

10 - PIN and security

Safety



WARNING! The user is responsible for security against unauthorized access and modification. The user must configure all protection release access points, including the display menu, Ekip Connect and the remote communication systems, using the access PIN and controlled and authorized connection systems.

Function

The PIN code enables access to certain screens and prevents unintentional setting errors from being entered via the display.

However, parameters can still be modified without having to enter the PIN via:

- BLE, with EPiC
- bus, in the presence of Ekip Com modules and with Trip unit configured as **Remote** (page 63).

To ensure your unit is in secure conditions, the Wizard window immediately asks you to change the PIN code on first power up; this is strongly recommended by ABB.

Description

The PIN code is a number formed by six digits, each of which can be given a value from 0 to 9; the default value is: **000001** and can be changed in the *Settings-Device[III]-New PIN* menu.

The PIN code must be entered to:

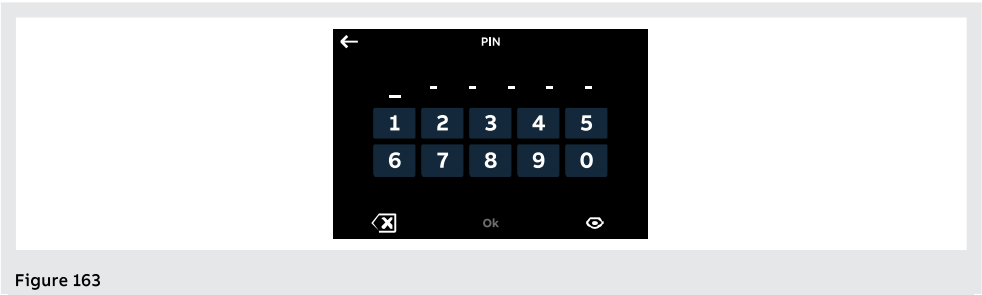
- change a parameter (including the PIN code itself);
- change settings of protection release
- access the Test menu.

Once the PIN code has been entered, all menus can be browsed for two minutes: once two minutes have elapsed, the PIN code must be entered again (depending on the case in question).



NOTE: the default PIN must be changed for security reasons. Ekip Aware periodically alerts users to the need to change the default PIN. The change message will no longer be displayed after the default PIN has been changed.

Entry The following page will appear when the PIN code is requested.



The position where the digit must be entered is indicated by the underscore dash.
The following keys are present and can be selected at the bottom of the display:

Icon	Description
	Always visible, deletes the last number entered.
	Visible once completed numbers have been entered, confirms the entered PIN code.
	Always visible, displays the numbers as they are entered.

- IMPORTANT:**
- if the user enters the wrong PIN code, Ekip Aware will display the “Incorrect PIN” message for the first three attempts while immediately allowing the user to enter the PIN again. After the fourth attempt, Ekip Aware activates a counter that inhibits entry of the PIN code for 30 seconds and increases the inhibition time at each new attempt. Entry of the correct PIN code resets the counters and restores the initial conditions at the next request for the PIN code.
 - there is no limit to the number of wrong PIN that can be entered

Disabling The PIN code can be disabled by entering 000000 as its value. In this case, the system only requests the PIN code for the purpose of changing the PIN itself in the Settings menu.

- IMPORTANT:** value 000000 cannot be entered for the purpose of disabling the PIN code if the protection release is in the Cybersecure mode.

Recovery Contact ABB directly if PIN code is lost.

Cybersecurity guidelines

1 - Disclaimer

This product is designed to be connected and to communicate information and data via a network interface. It is customer's sole responsibility to provide and continuously ensure a secure connection between the product and your network or any other network (as the case may be) and to establish and maintain any appropriate measures (such as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of anti-virus programs, etc.) to protect the product, the network, its system and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information.

ABB and its affiliates are not liable for damages and/or losses related to such security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information.

Although ABB provides functionality testing on the products and updates that we release, you should institute your own testing program for any product updates or other major system updates (to include but not limited to code changes, configuration file changes, third party software updates or patches, hardware change out, etc.) to ensure that the security measures that you have implemented have not been compromised and system functionality in your environment is as expected.

2 - Emax 3 product versions

Emax 3 products are available in two separate versions with increasing security characteristics:

- **Standard** version: provides security functions able to satisfy the majority of the customers' requirements.
- Version **IEC 62443**: Internationally recognized SL-C 2-certified device compliant with standard IEC 62443, which provides enhanced security for customers who need specific protection against security threats.

To implement a secure version of Emax 3, customers must always pair an Ekip Aware **IEC 62443** protection release with CAN **IEC 62443** accessory when using the unit in their system. All **IEC 62443** products have separate order codes. Standard products cannot be converted into **IEC 62443** products.

The main differences between the two versions are outlined in the table below and will be described more fully in the remaining part of this section.

Characteristic	Description of the characteristics	Version standard	Version IEC 62443
PIN	PIN required for write access to the settings via HMI and USB. Changing the PIN removes all the devices connected to BLE bonded.	Yes ⁽¹⁾	Yes ⁽²⁾
Secure upgrade of firmware	FW upgrade with digital signature and anti-rollback protection.	Yes	Yes
Secure storage	Anti-tampering of data and code of device.	Yes	Yes
Remote/local modes	Each communication module can be independently forced to local mode.	Yes	Yes
Secure modules	Set of dedicated modules to ensure that communications between Ekip Aware and the modules are authenticated.		Yes
Secure USB/BLE	Authenticated communication between Ekip Aware and Ekip Connect or EPiC.		Yes

⁽¹⁾ via HMI and USB only

⁽²⁾ via HMI only

3 - Defense in Depth

The Defense in Depth strategy employs many security defense levels. The strategy aims to provide redundancy if a security level fails or if someone exploits a vulnerability. Use of several security levels makes it more difficult to penetrate the system, steal digital assets or cause interruptions of service.

4 - Secure operating environment

ABB advises customers to opt for the Defense in Depth approach, which uses multi-layered independent security levels to reduce the risk of a cyber-attack being successful. The Defense in Depth strategy requires the customer to create a perimeter that acts as the first line of defense.

There are certain things the customer must do to ensure that the Emax 3 devices function securely. The customer must:

- Physically and logistically segment the network of the control system (trusted network) and the network of the non-control system. By using VLANs, for example.
 - Keep the trusted network small and independent from the other networks.
 - Make sure that secure interconnections (such as a firewall or a firewall system, configured as “deny by default”) are used for the connection between trusted networks and the other networks.
 - Use virtual private networks (VPN) for secure remote access.
 - Make sure that physical access to Emax 3 is limited, by physical means, to authorized people only.
 - Make sure that the device is not connected directly to the Internet.
 - Constantly monitor the system in order to identify intrusion attempts.
-

5 - Recommendations concerning product security hardening

Security hardening in the context of Industrial Automation and Control Systems (IACS) involves implementing measures to enhance the security and resilience of these systems against cyber threats, by applying essential configurations and removing unnecessary services or applications that could be exploited. Hardening a system involves several steps to form layers of protection.

Hardening during installation and commissioning

The commissioning phase ensures that Emax 3 is installed securely and that it functions in an effective way. The user must implement the security measures recommended below in order to protect Emax 3 from unauthorized accesses and potential security threats.

- Make sure that the product is protected against unauthorized access.
- Make sure that the most recent firmware is installed in the product. This will help to protect against known vulnerabilities and exploits.
- Apply a strong password policy so that strong passwords are created and applied.
- Change the default password.
- Implement strong logic access controls to limit access to sensitive data.

Security control list

Use the control list below to make sure that Emax 3 has been installed securely into the control system.

What to do	Version standard	Version IEC 62443
Firewall configuration	X	X
Configuration of user accounts		X ⁽¹⁾
Change the default password	X	X
Protection of ports and services	X	X
Enabling of secure protocols	X ⁽²⁾	X ⁽²⁾
Last firmware upgrade	X	X
Installation of security certificate	X ⁽³⁾	X ⁽³⁾

⁽¹⁾ Account management is implemented on ABB Ekip Connect and EPiC Softwares.

⁽²⁾ The security protocols of the system depend on the communication module chosen. Check in the corresponding section of this user Manual to find out whether the selected communication module supports a secure protocol option.

⁽³⁾ The security certificate must be installed if the communication module needs certificates to support secure communication to the IACS system. Check in the corresponding section of the User manual to find out whether the communication module or modules used require this installation.

Hardening during operation and maintenance

After Emax 3 has been put into service in the control system the customer must proceed as follows to ensure that the product functions securely:

- Make sure that only authorized users can access (both physical & logical access) the product.
- Regularly check for the presence of upgrades and apply them as soon as they are available. This will help to protect against known vulnerabilities and exploits.
- Regularly examine and eliminate unused user accounts to reduce potential attack vectors to the minimum.
- Regularly analyze and examine the audit logs in order to detect any malicious activities.

Hardening during Decommissioning of the device

The decommissioning phase removes Emax 3 from active use in a secure way. You must eliminate all sensitive data, the user accounts and digital certificates, if present, to prevent unauthorized access and ensure that no information remains in the device.

In the IEC 62443 version, the **Factory Reset** command also resets the security log and is thus only available to Administrator and Owner roles.

In the standard version, the information that can be stored in the product does not contain sensitive data, user accounts or digital certificates so the **Factory Reset** command is available to all users both on Ekip Connect and on EPiC.

6 - Security capabilities of the product - Common characteristics

This section describes the security capabilities available in the **Standard** and **IEC 62443** versions of Emax 3 for enhanced security.

Default open ports and services

As a default setting, a minimum number of ports is opened to reduce the attack surface of the device to the minimum. Only those services required for initial configuration are opened, again as a default setting.

Ekip Aware protection trip unit

List of ports and services opened by default in the Ekip Aware device:

Port	Service	Purpose	Default
502	IEEE 1588	Synchronize time of device	Disabled

Ekip COM modules

The list of open ports is given for each communication module in the dedicated description in chapter External electronic accessories.

Secure storage of data at rest

The sensitive data that reside in the external memories of the various Emax 3 devices are encrypted to prevent this unauthorized exposure.

Emax 3 devices also disable access to the internal memories, thereby protecting sensitive data securely.

In addition, to provide authentication capabilities and data integrity, all the external memories are supported by cryptographic authentication codes.

Secure boot

The firmware running in Emax 3 devices is digitally signed to protect integrity and authenticity.

Secure Boot ensures that the device only launches firmware that ABB trusts.

Devices that load the code from an external memory support a secure boot that ensures that only authorized firmware is loaded and executed in the device itself.

Devices that execute the code from an internal memory validate and authenticate the code during secure upgrades of the firmware. This approach, along with secure storage of data at rest provides the same performance as Secure Boot.

Session timeout

A session timeout capability has been implemented to enhance the security of Emax 3 devices. This capability ensures the user sessions are automatically disconnected after 5 minutes of idle time, thereby reducing the risk of unauthorized access.

Secure firmware upgrades

This security capability guarantees the authenticity of the Emax 3 firmware upgrade. Each firmware image is digitally signed by ABB to guarantee its authenticity and each device installs only firmware with verified authenticity that has passed antirollback.

The firmware upgrades are handled by ABB Software (Ekip Connect and EPiC), which download the latest firmware image versions from the ABB library.

Audit logging

Emax 3 has a capability for recording events which creates a log of all the events involving device security, such as configuration changes, communication channel tampering events, etc.

To ensure data authenticity, a cryptographic authentication code is added to the log when stored.

7 - Communication available in Standard version

In the **Standard** version, communication between the Ekip Aware protection release and permanently connected accessories includes error detecting and correcting tools so as to maintain data **integrity** during transmission. Data integrity during transmission is also detected when Ekip Connect or EPiC are connected.

System communication with external systems

Emax 3 communication modules are used for connecting the Ekip Aware protection release to external systems and are described in a dedicated chapter of this user manual.

If a secure version of a protocol is available as well as the standard one, the product user is urged to use the secure version in his/her system.

Certificate management

Consult the specific section of this User manual for indications concerning secure communication protocols that require certificate management.

8 - Secure communication with the IEC 62443 Version

In the **IEC 62443** version, the cryptographic authentication codes maintain the integrity and authenticity of the data transmitted between the Ekip Aware protection release and the ABB accessories and Software. This solution protects the communications from tampering and forgery and guarantees that only original, verified ABB accessories and ABB Software with account management capability are included in the communication.

System communication with external systems

Emax 3 communication modules are used for connecting the Ekip Aware protection release to external systems and are described in chapter External electronic accessories.

If a secure version of a protocol is available as well as the standard one, the product user is urged to use the secure version in his/her system.

Certificate management

In the IEC 62443 version, a secure connection between client and server uses cryptographic authentication codes to protect data transmission. Cryptographic authentication codes safeguard sensitive information against tampering and forgery.

The IEC 62443 versions of the Emax 3 devices use signed certificates to protect communications via USB and BLE between ABB Software and the Ekip Aware protection release. Signed certificates also protect communications between CAN accessories and the Ekip Aware protection release.

The digital certificates are preloaded into IEC 62443 devices and ABB Software

Consult the specific section of this User manual for indications concerning secure communication protocols that require certificate management.

User account management

The ABB Ekip Connect and EPiC Software include integrated management of user accounts based on the Role Based Access Control (RBAC) concept. ABB Ekip Connect and EPiC Software enable roles with defined rights to be created. The roles must be assigned to newly created users based on the available access authorization. Follow the guidelines below to manage the user accounts in Emax3.

Principle of Least Privilege

- Limitation of access rights to the minimum required by the users to perform their tasks.
- Periodically review and adjust the authorizations to ensure they continue to be suitable.

Role-based access control (RBAC)

- Create roles on the basis of jobs and assign authorizations to those roles.
- Assign users to the roles rather than grant authorizations directly to the individual users.

Roles can be assigned to each user by making use of the ABB account management capability. A full description of the operations required to create user accounts and assign a specific role is given in documents [EKIP CONNECT](#) and [EPiC](#).

Continued on the next page

The next table provides an overview of the roles and their predefined rights.

Role	Description
Owner	The "Owner" role controls the protection settings and advanced functions of the circuit-breaker. The "Owner" role assigns roles to others and removes users. This role is exclusive for one individual only per circuit-breaker.
Admin	The "Admin" role supervises the protection settings and advanced functions of the circuit-breaker and has the authority to delegate roles to other users. The "Admin" role is crucial to maintaining the integrity of the system and to user access management.
Engineer	The "Engineer" role manages the protection settings of the circuit-breakers and uses the advanced functions in the Tools section. The "Engineer" role improves system efficiency and guarantees security by means of these settings and capabilities.
Operator	The "Operator" role controls the security measures of a circuit-breaker by performing basic operations and tests. "Operator" accesses and edits the basic characteristics of the circuit-breaker to guarantee efficiency and security.
Viewer	The "Viewer" role enables users to view all the settings and information in a system without being able to make changes. The "Viewer" enables the users to stay informed without being able to change the configurations or data.

Details about the roles and relevant access rights are given in the table below.

Action/item	Viewer	Operator	Engineer	Owner/Admin
User account management	-	-	-	X
Viewing of secure event logs	-	-	-	X
Displays product state	X	X	X	X
Operations and tests	-	X	X	X
Product settings	-	X	X	X
Firmware upgrade	-	-	X	X
Advanced features	-	-	X	X

Strong password policy

Comply with the indications below

- Change factory default password.
- Apply a strong password policy so that strong passwords are created and applied.
- Avoid sharing passwords if possible.

Continued on the next page

Characteristic	Location in Ekip Connect	Description	CB cybersecure roles			
			Viewer	Operator	Engineer	Owner/Admin
System Update	Instruments	System update of the circuit breaker			X	X
File manager	Instruments	Export/import of circuit breaker settings			X	X
Test area (LSIG test)	Instruments	Perform LSIG test		X	X	X
Test area Pro	Instruments	Perform advanced tests with Test Area Pro			X	X
Data logger	Instruments	Enable, set and download files from datalogger basic			X	X
Data logger Pro	Instruments	Enable, set and download files from datalogger Pro			X	X
Dataviewer	Instruments	Analyze datalogger files in dataviewer tool	X	X	X	X
Modules	Instruments	Ekip modules configuration (communication, signalling, temperature 4T)			X	X
CB Report	Instruments	Download a new circuit breaker report	X	X	X	X
Predictive maintenance	Service	Register and track maintenance operations, environmental conditions settings			X	X
Load Shedding	Instruments	Transfer the logic to a circuit breaker			X	X
Power Controller	Instruments	Transfer the logic to a circuit breaker			X	X
Networking	Instruments	Setting of communication network (TCP radial, daisy chain, link)			X	X
Custom Logics	Instruments	Transfer the logic to a circuit breaker			X	X
Classic view	Classic view	Transfer logic to a circuit breaker	x (Read mode only)	x (Read mode only)	X	X

9 - Vulnerability management

Use the ABB Cyber Security Portal to find information related to vulnerability management, including reporting of vulnerabilities or incidents, security advisories for ABB products, and ABB's vulnerability handling policy.

To receive email notifications about newly published advisories, we recommend you sign up for our email notification service.

Website: <https://www.abb.com/cybersecurity>

Ekip Aware - Connectivity

1 - Overview

Overview Besides direct access via display, other different channels can be used to communicate with the protection release:

- USB, for reading and writing parameters via Ekip Connect using a PC, or via EPiC using a Smartphone
- BLE, for reading and writing parameters via EPiC using a Smartphone and BLE connection. BLE is also useful for communicating with T-Sense modules
- Remote, for reading and writing parameters using different protocols and on remote networks
- NFC, for reading the main info, also when the protection release is off

A BLE MESH network can also be activated among different Ekip Aware and among Ekip Aware and T-Sense modules for automatic and independent exchange of certain data.

The ability to connect depends on the configuration of certain parameters (e.g. configuration of TestBus, BLE function, ...) or the presence of certain Packages (e.g. Cybersecure, Bluetooth deactivation), described in the following chapters.

When there are Ekip Com modules connected to Ekip Aware, these cannot be connected directly to the Internet. It is advisable to connect them solely to dedicated Ethernet networks with the same communication protocol as the module itself.

Apps and tools The ABB apps for data exchange with Ekip Aware are:

- Ekip Connect for use with a PC, with USB connection or remotely
- EPiC for use with smartphones/tablets and connection via BLE or USB, and MESH network configuration

Both are official ABB APPs compatible with the Cybersecure configuration.

Disclaimer - BLE Activation of communication via Bluetooth Low Energy means that Ekip Aware must be ready for wireless connection: security of data and the Bluetooth Low Energy connection between the protection release and your device is guaranteed thanks to the ABB EPiC application and the Pairing configuration described in the chapter dedicated to the BLE connection.

ABB recommends a few general configurations to strengthen the access of data into the Trip unit:

- configure the access PIN code with a different value from the default value
 - if parameters need not be written, configure the protection release only for parameter readout via bus (Test bus parameter = Off)
 - switch off the BLE (Bluetooth Low Energy-Enable parameter=Off) after use
-

2 - USB

Description The USB-C type port temporarily enables the protection release to be energized and to communicate with a PC via Ekip Connect or EPiC.
To energize and view / configure the main unit parameters, a power bank with USB port can be used for connection to the protection release even in the absence of other power sources.

Display When connection to the USB connector is present and there are no auxiliary power sources such as Ekip Supply or Ekip Busbar Supply, the icon of the USB symbol will appear on the display.



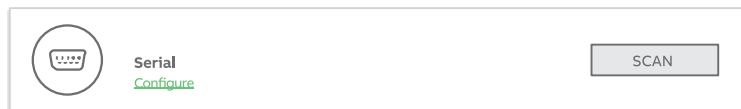
Connection and start of communication



IMPORTANT: make sure, in the Settings-Connectivity menu of the protection release, that the Test bus parameter = ON before launching Ekip Connect

To activate communication via USB:

1. Connect a USB cable to your PC
2. Connect the USB-C port to the front connector of the protection release
3. Launch Ekip Connect
4. Configure the parameters and then SCAN connection option: USB-C



Limitations Parameter writing via USB is not possible when the Testbus parameter = OFF.
In addition, even when communication is activated, parameters cannot be written via USB when Cybersecure is activated and the user is not enabled.

3 - BLE

- Description** Ekip Aware has BLE connection for communicating via EPiC with a smartphone using Bluetooth Low Energy protocol.
- BLE is available in all Ekip Aware with the exception of those ordered without (For details consult Limitations).
- BLE also supports the Beaconing function which, after a Trip, sends automatic alarm messages to all devices in the vicinity of the CB. The messages can be viewed in the EPiC App.

- Display** The Bluetooth icon appears at the top right of the display and indicates the state of the connection with an external device:

Icon	Description
-	No icon: BLE not available in Ekip Aware
	Grey icon, BLE available on Ekip Aware, but off
	White icon; BLE on but not connected to any device
	White with waves: pairing enabled, BLE available for pairing with new devices
	Light blue icon; BLE on and connected (or being connected) to a device

Certain information and commands are available in the menu. Consult the dedicated section on page 63.

- Pairing** To pair the protection release with its device:
1. Enable communication via display in the *Settings/Connectivity/Bluetooth Low Energy* menu
 2. Select the “Start Pairing” command, which enables BLE to be paired to new devices for 2 minutes. The command is available in HMI in the BLE enable menu or via Ekip Connect on the “Configure unit” page.
 3. Turn on the Bluetooth function in your device
 4. Open EPiC and find the device, select it and enter the pairing PIN that appears on the display of the protection release
 5. Confirm on your device and on the display of the protection release (“Confirm” command)



IMPORTANT: BLE communication functions with Ekip Aware on

- Connection and start of communication** To activate communication with EPiC:
1. Check the protection device to make sure that BLE is on and check your smartphone to make sure that Bluetooth is on
 2. Activate EPiC on your smartphone
 3. Select protection release ID

- Additional commands** You can configure the Start Pairing parameter in the “Configure unit” page of Ekip Connect; the protection release only enables and starts communication with devices that have been previously paired.

- Beaconing** The Beaconing function is activated in the following cases:
- In the case of Trip with Ekip Aware always on (auxiliary power supply present), the Beaconing function remains activated until Trip reset or removal of the auxiliary power supply.
 - In the case of Trip with Ekip Aware off (self-supply), the Beaconing function remains activated during the 30 minutes after shutdown. Once these 30 minutes have elapsed, data transmission via Beaconing can be reactivated by pressing the iTEST button, thereby resuming data transmission for a further 60 seconds.

In both cases, certain information about the Trip that has just occurred will appear automatically if your smartphone is near the CB. This information includes: CB TAG name, type of trip and current recorded.



NOTE: the function is always available when the BLE is on, even when no pairing has been made via Pairing

- Limitations** There can be no communication via BLE if the Bluetooth Low Energy parameter = Disable or when there are packages that disable its presence (Bluetooth removal ExCo, Bluetooth connection disabled E1.3.. E6.3).

In addition, even when BLE communication is activated, parameters cannot be written when Cybersecure is activated and user is not enabled.

4 - NFC

Description The NFC function enables certain information from the protection release to be read by means of the NFC function of your smartphone.

With the exception of those ordered without Bluetooth connection, NFC is available in all Ekip Aware with which it shares part of the communication circuit (For details consult Limitations).

Display The Bluetooth icon is available at the top right side of the display, useful for assessing the activation state of the NFC function:

Icon	Description
-	No icon: BLE and NFC not available in Ekip Aware
	Grey icon, BLE function off, thus NFC also off
	White icon, BLE function on, thus NFC also on and available
	White with waves: pairing enabled, BLE available for pairing with new devices
	Blue icon; BLE function on and connected, therefore also NFC on and connected

Activation and connection To activate NFC access from Ekip Aware just enable BLE communication on the display in the *Settings/Connectivity/Bluetooth Low Energy* menu.

Reading is possible with Ekip Aware on, off or turned off following a Trip. Besides information about the protection release, the Trip Active indication is provided if Ekip Aware is off, but not after a Trip: NO.

To read the information on your smartphone:

1. Make sure that NFC on your smartphone is on
2. Hold your smartphone near the left side of Ekip Aware and open EPiC
3. Information about the CB (model, size, TAG and s/n), information about the protection release (s/n, FW rev., miscellaneous) and details about the latest Trip (type, current values recorded, contact wear) will appear on the display of your smartphone.



IMPORTANT: when Ekip Aware is off, NFC can be momentarily activated using the internal battery and by pressing the iTest button, in a similar way to the procedure described in the Beacons chapter.

Limitations There can be no communication via NFC if the Bluetooth Low Energy parameter = Disable or when there are packages that disable the presence of BLE (Bluetooth removal ExCo, Bluetooth connection disabled E1.3..E6.3).

5 - Remote

Description When terminal block communication modules are present (Ekip Com in all versions), the protection release can be integrated into a communication network by various protocols.

Ekip Com modules are available in two versions:

- standard modules: configurable with protection release without Cybersecure package, do not guarantee the maximum security level for access to parameters between the two devices.
- secure modules: configurable when protection release is provided with Cybersecure package, guarantee the maximum security level for access to parameters between the two devices.



IMPORTANT: in hybrid configurations of protection releases and Ekip Com modules:

- **when the protection release is equipped with the Cybersecure package and the Ekip Com modules are standard, the Ekip Com modules are not detected.**
- **when the protection release is standard and the Ekip Com modules are secure, communication between the two devices is activated but not secure, the modules are interpreted as being standard modules.**

Display You can configure the Local Bus and Local/Remote parameters via display in the settings menu and check in the info menu to make sure the parameters of the modules are present.



When the *Local - Remote* parameter = Remote, the icon of the symbol of the same name (white) appears on the display.



IMPORTANT: In the absence of auxiliary power supply, communication between the protection release and modules is no longer activated and the parameter configures automatically as Local.

Connection and start of communication

Make sure that the following conditions are present when activating communication remotely:

1. the Ekip Com modules and Ekip Supply module (all versions) must be present in the terminal block
2. the protection release must have the Local Bus parameter = ON
3. auxiliary power supply must be present
4. check and configure the “Local/Remote” parameter to suit your requirements: if the setting is Local, only parameter reading is possible remotely; both parameter reading and writing are enabled if the setting is Remote.
5. check that the protection release detects both the presence and the parameters of the Ekip Com modules on the display of Ekip Aware (in the Info menu) or by means of other connection systems (USB or BLE)
6. your communication network must be configured and scanned.

Additional parameters

The “Local/Remote access” parameter of each Ekip Com module connected can be configured and assigned two values:

- General Setting: the Local or Remote mode of the module is the same as that of the “Local/Remote” parameter of the protection release
- Override to Local: sole reading of parameters is enabled for the specific Ekip com module, via its system bus

Limitations

Remote communication is not possible in the following cases:

- Local Bus configuration = OFF
- Protection release equipped with Cybersecure package connected to standard Ekip Com module

In addition, even when communication is activated, parameters cannot be written remotely if the *Local - Remote* parameter is set to Local

6 - BLE MESH

Description The BLE function on Ekip Aware enables communication via BLE-MESH protocol with other devices, by activating a data collection or an exchange:

- with other Ekip Aware (up to a total of six in the same network) for a two-way exchange of data
- With T-Sense Ambient and T-Sense Busbars (up to a maximum of 16 connected to the same protection release), for the purpose of transmitting temperature and humidity information to the protection release

BLE-MESH communication is available on all Ekip Aware protection trip units, except those that have been ordered without BLE (For details consult Limitations).

The BLE MESH network can be created using EPiC.

The exchanged information can be configured by connecting to each Ekip Aware protection release using EPiC or Ekip Connect (via USB)

Display The Bluetooth icon is available on the top right side of the display , useful for assessing the activation state of the BLE-MESH network:

Icon	Description
-	No icon: BLE and BLE MESH not available in Ekip Aware
	Grey icon; BLE function off, thus BLE-MESH is also off
	White icon; BLE function on, thus BLE-MESH also on and available
	White with waves: pairing enabled, BLE available for pairing with new devices
	Light blue icon; BLE on and connected, thus BLE-MESH also on and connected

Activation and configuration Activation and Provisioning / Configuration operations are required in order to prepare the protection release for a BLE MESH network.

Activation:

1. Enable communication via display in the “Settings-Connectivity-Bluetooth Low Energy” menu
2. Select the “Start Pairing” command, which enables BLE to be paired to new devices for 2 minutes. The command is available in HMI in the BLE enable menu or via Ekip Connect on the “Configure unit” page
3. Turn on the Bluetooth function in your device
4. Open EPiC and find the device, select it and enter the pairing PIN that appears on the display of the protection release
5. Confirm on your device and on the display of the protection release (“Confirm” command)

Provisioning / Configuration

6. Access the EPiC APP on your smartphone
7. Select “Product Commissioning” followed by “BLE Mesh Network”
8. Create your MESH network using the “+” command at bottom right and name it
9. The command with the “BT” symbol will appear at bottom right. Select it to launch an automatic search for devices that can be added to your MESH network



IMPORTANT: Devices that are already in other BLE-MESH networks will not be visible

Continued on the next page

10. Select the device you want to add to the BLE-MESH network you have created and confirm using the "Provision" command: an address will be automatically assigned to the device you have added



NOTE: *If Pairing has not already been executed, the operation will be proposed*

11. Repeat step 10 for all the devices you want to add to your network
12. Having terminated all the additions, proceed by configuring the role of each device by selecting the three dots alongside each: you can select Configure (to complete role assignment) or Delete (to delete the device from the network) in the window that appears



IMPORTANT: BLE-MESH communication functions with Ekip Aware on

Configuration for data exchange

Each unit must be programmed in a data exchange network between Ekip Aware in a BLE-MESH network; the steps using Ekip Connect are described below:

1. Connect Ekip Aware to your PC and activate communication using Ekip Connect
2. The assigned address and serial number must be entered for each protection release in the "BLE Mech Actors Configuration" page, with the aid of the list of devices created with EPiC
3. The following shared data are available in the Wireless Modules page for each protection release connected to the MESH network:

Parameter	Description
Network ID	Address of BLE-MESH network assigned to Trip unit
RSSI Signal	Power of BLE signal of specific Trip unit (in dBm)
Global Status Word 1	Register with values of CB statuses, see System Interface register 40
Programmable Status	Register with values of Programmable statuses, see System Interface register 67
PLC Programmable Status Word 1	Register with values of Custom Logic 1, see System Interface register 86
PLC Programmable Status Word 2	Register with values of Custom Logic 1, see System Interface register 87
Mesh connection lost	Trip unit disconnection alarm

Configuration for data collection with T-Sense

In a network for collecting data from T-Sense accessories in a BLE MESH network, the protection release must be programmed; the steps using Ekip Connect are described below:

1. Connect Ekip Aware to your PC and activate communication using Ekip Connect
2. The assigned address and serial number of each T-Sense module present must be entered in the "BLE WS Sensor Mech Actors Configuration" page, supported by the list of devices created with EPiC
3. The following shared data are available in the Wireless Modules page for each T-Sense accessory connected to the MESH network:

Parameter	Description
Network ID	Address of BLE-MESH network assigned to T-Sense
RSSI Signal	Power of BLE signal of specific Trip unit (in dBm)
Ambient Temperature	Probe contact temperature detected by T-Sense (in °C)
Humidity	Humidity detected by T-Sense (in %)
Mesh Sensor connection lost	T-Sense disconnection alarm
Battery low alarm	Only available for T-Sense Ambient. Warns that the battery is about to run out
Generic Alarm	Warns of a sensor fault
High temperature alarm	Warns that the temperature inside the accessory is over the permitted maximum operating limit



HAZARD! RISK OF ELECTRIC SHOCK! Make sure the busbars are not energized before working on the T-Sense Busbar accessories.



WARNING! the busbars must be disconnected from the power supply when the T-Sense Busbar accessories are configured. The modules must be energized via the USB-C port.



NOTE: press the button on the accessory to perform the configuration operations via EPiC. Once the button has been pressed you have 60 s to complete the configuration, after which the operation will be interrupted. Press the button again to resume the operation; the procedure will continue from the point at which it was interrupted. If the accessory fails to connect, move it closer to the CB.

Limitations

The BLE-MESH network cannot be activated if the Bluetooth Low Energy parameter = Disable or when there are packages that disable its presence (Bluetooth removal ExCo, Bluetooth connection disabled E1.3..E6.3).

In addition, the BLE-MESH network cannot be used if the Trip unit is off, even when BLE communication is activated.

Ekip Aware - Standard Protections

1 - Protections - Introduction

List of standard protections Ekip Aware is available in three versions which differ, depending on the standard protections present.

Protection	Description	LI	LSI	LSIG	Page
L	Overload with inverse long-time delay	X	X	X	
I	Instantaneous short-circuit	X	X	X	
MCR	Instantaneous short-circuit on circuit-breaker closing	X	X	X	
RELT	Instantaneous short-circuit can be activated with programmable event	X	X	X	
Neutral	Different protection on neutral phase	X	X	X	
Iinst	Instantaneous short-circuit at high currents	X	X	X	
S ⁽¹⁾	Selective short-circuit	O	X	X	
G ⁽²⁾	Earth fault with adjustable delay	O	O	X	
Gext ⁽²⁾	Instantaneous short-circuit programmable	O	O	X	
MDGF ⁽²⁾	Current unbalance	O	O	X	

⁽¹⁾ can be purchased with S – Time-Delayed Overcurrent Protection digital upgrade, for the LI version

⁽²⁾ can be purchased with G – Earth Protections digital upgrade, for the LI and LSI versions

X = Available by default; O = Optional

Additional protections and functions not supplied upon purchase can be purchased later on in the form of packages, which will be described in the next chapters.

Operating principle Each Ekip Aware can be equipped with optional protection packages and functions, besides those present by default upon leaving the factory.

Each protection is associated with a different signal (current, voltages, frequencies, powers, etc) but the operating principle is the same:

1. If the signal measured exceeds the set **threshold**, the specific protection activates (prealarm and/or **alarm** condition).
2. The **alarm** appears on the display and, after a period of time (timing t_d), depending on the protection parameters set, can convert into a **trip command (TRIP)** transmitted to the internal Trip Coil of the CB.



IMPORTANT:

- Ekip Aware terminates the alarm and timing if it detects that the measured signal has dropped below the set threshold before the trip time has elapsed. Ekip Aware returns to the normal operating condition;
- all protections have a default configuration: check the parameters and change to suit the installation requirements before commissioning.

References Many of the protection thresholds are displayed in two different quantities: absolute value and relative value.

The relative value depends on the type of measurement:

Type of protection	Reference	Description
Current	In	Rated current of <i>Digital Rating plug</i>
Voltage	Un	Line-to-line voltage setting
Frequency	fn	Frequency setting
Power	Sn	$\sqrt{3} \times I_n \times U_n$

Access and configuration

Each protection on Ekip Aware can be configured using the official ABB Ekip Connect applications for access via PC and EPiC applications for access via smartphone.

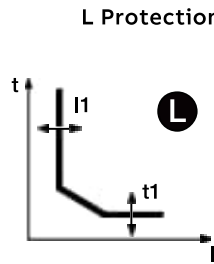
Access can be obtained via:

- the USB-C front port
- via Bluetooth Low Energy
- system bus using modules from the Ekip Com range. In this case, you can also access through your system or application by activating a communication network that complies with the rules described by Emax3 system interface.

Some protections, present in the Ekip Aware version or purchased as an optional package, have certain parameters that can also be edited or consulted in the menu of Ekip Aware. L, S, S2, I, G, D.

All the protections activated in the protection release can be checked in the Info menu.

2 - Standard Protections LI, LSI, LSIG



Function

If the current of one or more phases exceeds threshold I_1 , the protection trips and, after a time established by the value read and by the parameter settings, transmits the TRIP command.

To check and simulate the trip times in relation to all the parameters, please consult:

- the summary table of the protections with the calculation formulas (page 121)
- the graph with trip curve (from page 123)

Certain parameters can be configured and consulted in the Protections menu.

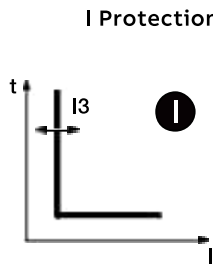
Parameters

Parameter	Description	Default
Curve	Establishes curve dynamics and trip time calculation: • $t = k / I^2$ according to IEC 60947-2 • IEC 60255-151 SI • IEC 60255-151 VI • IEC 60255-151 EI • $t = k / I^1$ according to 60255-151	$t = k/I^2$
Threshold I_1	Establishes the value that activates the protection and contributes towards calculating the trip time. The value is given as both absolute value (A) and relative value (I_n) and can be set within the range: $0.4 I_n$ to $1 I_n$, in $0.001 I_n$ steps	$1 I_n$
Time t_1	Contributes towards calculating the trip time. The value is given in seconds and can be set within the range: 3 s .. 144 s, in 1 s steps	144 s
Thermal memory	Activates/deactivates the thermal memory function (page 111) i NOTE: the function is available with curve $t = k / I^2$	OFF
Prealarm I_1	Warns that the measured current is near to protection activation threshold I_1 . The value is given in percentage of threshold I_1 and can be set within the range: $50\% I_1$ to $90\% I_1$, in 1% steps. i NOTA: the prealarm condition deactivates in two cases: • current lower than prealarm threshold I_1 • current higher than threshold I_1	$90\% I_1$

Limitations and additional functions

- threshold I_1 must be lower than threshold I_2 (if S protection is activated)
- L protection: the trip time of the protection is forcibly set at 1 s if the calculation results give a lower theoretical t_t value and/or if the current reading is more than $12 I_n$
- all the parameters described above are available via USB-C port, Bluetooth Low Energy and system bus, as are certain further ones:
 - L prealarm disable
 - Thermal Memory parameters (such as Algorithm, type of time, custom time)
 - L timing above threshold

The description is available in section List of additional protections and functions on page 110.



Function

If the current of one or more phases exceeds threshold I_3 , the protection trips and, after a non-programmable fixed time, transmits the TRIP command.

To check and simulate the trip times in relation to all the parameters, please consult:

- summary table of the protections with the operating characteristics (page 121);
- the graph with trip curve (page 126).

Certain parameters can be configured and consulted in the Protections menu.

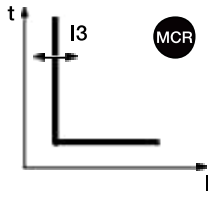
Parameters

Parameter	Description	Default
<i>Enable</i>	Activates/deactivates the protection and its availability in the parameters menu.	ON
<i>Threshold I_3</i>	Establishes the value that activates the protection. The value is given as both absolute value (A) and relative value (I_n) and can be set within the range: $1.5 I_n$ to $15 I_n$, in $0.1 I_n$ steps	$4 I_n$
<i>Zone Selectivity</i>	Activates/deactivates the function i NOTE: if at least two of the selectivity S, S2, I, RELT and MCR are enabled, the input and output are shared with the OR function; it is sufficient that even a selectivity is activated to stimulate inputs and outputs	OFF
<i>StartUp enable</i>	Activates/deactivates the function and availability of the associated parameters on the display (page 112)	OFF
<i>StartUp Threshold</i>	Protection threshold valid during Startup time, in the conditions in which the function is activated (page 112) The value is given as both absolute value (A) and relative value (I_n) and can be set within the range: $1.5 I_n$ to $15 I_n$, in $0.1 I_n$ steps	$1.5 I_n$
<i>StartUp Time</i>	This is the time for which the StartUp threshold remains activated, as calculated from the moment the activation Threshold is exceeded (page 112) The value is given in seconds and can be set within the range: 0.1 s to 30 s, in 0.01 s steps	0.1 s

Limitations and additional functions

- protection cannot be deactivated in “Non-defeatable instantaneous protection” version; consult catalog for further details ([1SDC220100D0201](#))
- threshold I_3 must be higher than threshold I_2 (if S and I protections are activated)
- I protection can be activated with MCR protection disabled
- all the parameters described above are available via USB-C port, Bluetooth Low Energy and system bus, as are the following further ones: block and selectivity type functions.
The description is available in section List of additional protections and functions on page 110.

Protection MCR Function



The protection functions for a time window calculated from the change of state of the CB from open to closed. After this, the protection shuts down.

During this interval, if the current of one or more phases exceeds threshold I_3 , the protection system sends the TRIP command after a non-programmable fixed time.

The MCR protection only functions with Vaux or with supply via the *Measurement Enabler with voltage socket* module.

To check and simulate the trip times in relation to all the parameters, please consult:

- summary table of the protections with the operating characteristics (page 121)
- the graph with trip curve (page 126)



NOTE: to activate MCR, protection I must be disabled

Parameter	Description	Default
<i>Enable</i>	Activates/deactivates the protection and its availability in the parameters menu.	OFF
<i>Threshold I3</i>	Establishes the value that activates the protection. The value is given as both absolute value (A) and relative value (I_n) and can be set within the range: $1.5 I_n$ to $15 I_n$, in $0.1 I_n$ steps	$6 I_n$
<i>Monitor Time</i>	Defines the time interval in which the MCR protection remains activated, as calculated from the open - closed change of status The value is given in seconds and can be set within the range: 0.04 s to 0.5 s, in 0.01 s steps	0,04 s
<i>Zone Selectivity</i>	Activates/deactivates the function  NOTE: if at least two of the selectivity S, S2, I, RELT and MCR are enabled, the input and output are shared with the OR function; it is sufficient that even a selectivity is activated to stimulate inputs and outputs	OFF

Limitations and additional functions

The protection parameters can be configured and consulted via USB-C port, Bluetooth Low Energy and system bus.

Further protection parameters and functions (block functions) are described in section List of additional protections and functions on page 110.

RELT protection Overview

The protection protects against short-circuit currents and differs from other protections of the same type owing to the presence of an activation event, programmable by the user.

Function configuration can be checked via all remote connection systems.

In addition, a dedicated menu can be activated, via display, in the Protections menu and the presence of the package can be checked in the Info menu.

Function

If the current of one or more phases exceeds threshold I₃₁ and a trip event is present, the protection transmits the TRIP command after a non-programmable fixed time.

To check and simulate the trip times in relation to all the parameters, please consult:

- summary table of the protections with the operating characteristics (page 121)
- the graph with trip curve (page 126)

Parameters

Taking Ekip Connect as a reference, you can access the protection parameters in the “A Parameters” section (or “B Parameters” and “C Parameters” if the Dual or Triple Setting digital upgrades are installed) of the “Protection parameters” page

Parameter	Description	Default
<i>Enable</i>	Activates/deactivates the protection and its availability in the parameters menu.	OFF
<i>RELT Mode</i>	Two alternative modes are available: • Dependent function: the protection is activated if the programmed activation event is present; this configuration makes the function and delay parameters available • Manual: the protection is always activated i NOTE: the Manual mode can be configured via BLE if the Ekip RELT module is present	Dependent function
<i>Function</i>	The activation event can be chosen from among: input contacts of Ekip RELT, Ekip Signalling 2K or Ekip Signalling 4K, states of the CB (open/closed) and the Custom mode. i NOTE: Custom enables up to eight states in AND or OR logic to be programmed	Disabled
<i>Threshold I₃₁</i>	Establishes the value that activates the protection. The value is given as both absolute value (A) and relative value (In) and can be set within the range: 1.5 In to 15 In, in 0.1 In steps.	1,5 In
<i>Delay ON</i>	Protection activation delay calculated from the presence of the activation event: the protection activates if the event is present for longer than the set delay. The value is given in seconds and can be set within range: 0 s to 100 s, in 0.01 s steps	0 s
<i>Delay OFF</i>	Protection deactivation delay calculated from the disappearance of the activation event: the protection deactivates if the event is absent for longer than the set delay. The value is given in seconds and can be set within range: 0 s to 100 s, in 0.01 s steps	15 s
<i>Zone Selectivity</i>	Activates/deactivates the function i NOTE: if at least two of the selectivity S, S2, I, RELT and MCR are enabled, the input and output are shared with the OR function; it is sufficient that even a selectivity is activated to stimulate inputs and outputs	OFF
<i>Zone Selectivity Type</i>	Selection between Logic and Hardware Selectivity (both via cabling and through communication via Link Bus) and Solely Logic (only via Link Bus). Further details are available in the chapter that describes zone selectivity	Hardware and Logic

Continued on the next page

Display

If RELT protection is enabled and active (on the basis of the RELT Mode parameter), certain information appears and changes on the display:

- Activation of a blue coloured information Pop-up giving the state of the protection ("RELT Enabled"). Press the Home icon to remove the pop-up or press the iTEST button to make it appear again. When the activation event disappears, a countdown lasting for as long as the Delay OFF value appears in the window.



NOTE: When the RELT Mode parameter= Manual, the pop-up also has a Disable command for rapid and automatic disabling (Enable= OFF) of the protection

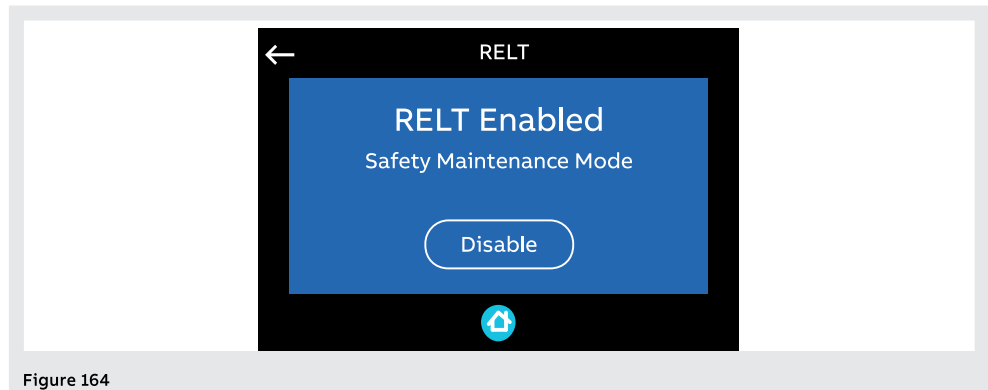


Figure 164

- The first line at the top of all display menus is always BLUE
- In HOME, diagnostic bar, presence of "RELT activated" message
- Warning LED on and steady

Ekip RELT module

If the Ekip RELT module is present, a new command (RELT Wizard) becomes available in the Protections - RELT menu.

The command automatically programs the protection parameters and module according to a pre-defined configuration.

Details are available in the chapter dedicated to the Ekip RELT module, on page 314.



NOTE: if more than one protections SET (Dual and Triple Settings) is present, the RELT Wizard command programs the same parameters for all the sets

Commands by remote control

If, besides the RELT package, communication with an external network (communication with Ekip Com modules) is activated, the RELT protection will have two activation/deactivation commands:

- RELT Mode OFF: deactivates the protection by changing the RELT Mode = Manual parameter
- RELT Mode OFF: deactivates the protection by changing the RELT Mode = Function dependent parameter



IMPORTANT: the commands are valid if the protection is enabled (Enable= ON).

For further details consult the document [1SDH002310A1524](#) or, taking Ekip Connect as a reference, the commands are available in the "Protection parameters" page in the "A Parameters" section (and "B Parameters" and "C Parameters" sections if the Dual or Triple Setting digital upgrade are installed), "RELT Mode" group.

Neutral Protection Function

Neutral protection characterizes protections L, S and I differently on the neutral phase by introducing a different control factor from the other phases.

The protection is available with the 4P and 3P + N configuration; the configuration parameters can be accessed via the Settings menu (page 75).

Parameters

Parameter	Description	Default
<i>Enable</i>	Activates/deactivates the protection	ON
<i>Neutral threshold</i>	Defines the multiplicative factor applied to the trip thresholds and curves of the protections for the current read on phase Ne: • 50 %: lowest trip thresholds for the neutral current • 100 %: same trip thresholds for all phases • 150 %: highest trip thresholds for the neutral current • 200 %: highest trip thresholds for the neutral current	50 %

Limitations and additional functions

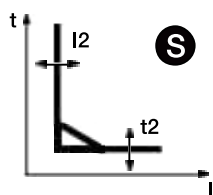
Ekip Aware rejects modification of thresholds I_1 and I_{nN} in the absence of the following limitation: $(I_1 \times I_{nN}) \leq I_u$

- I_1 is the threshold of L protection in amperes (example: $I_n = 800$ A and $I_1 = 0.6$ becomes $I_1 = 480$ A)
- I_{nN} is the neutral threshold expressed as multiplicative factor (example: $I_{nN} = 200\%$ becomes $I_{nN} = 2$)
- I_u is the size of the CB



IMPORTANT: With 150% and 200% threshold; if the measured neutral current exceeds $16I_n$, the Trip unit resets the protection to 100% by itself

Inst The protection preserves the integrity of the circuit-breaker and installation during high current values. High current values require shorter reaction times than the instantaneous short-circuit protection. ABB defines the threshold and trip time of the protection. The protection cannot be disabled.

S Protection Function

If the current of one or more phases exceeds threshold I_2 , the protection trips and, after a time established by the value read and by the parameter settings, transmits the TRIP command.

To check and simulate the trip times in relation to all the parameters, please consult:

- the summary table of the protections with the calculation formulas (page 121);
- the graph with trip curve (page 127).

Certain parameters can be configured and consulted in the Protections menu.

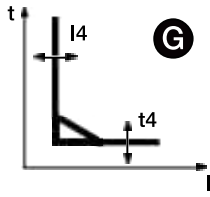
Parameters

Parameter	Description	Default
<i>Enable</i>	Activates/deactivates the protection and its availability in the parameters menu.	OFF
<i>Trip Enable</i>	Activates/deactivates transmission of the open command. If disabled, the alarm and exceedance of protection time are only managed as information.	ON
<i>Curve</i>	Establishes curve dynamics and the threshold or trip time calculation: • $t = k$: fixed time trip • $t = k/I^2$: inverse time-delay dynamic trip	$t = k$
<i>Threshold I_2</i>	Establishes the value that activates the protection and contributes towards calculating the trip time. The value is given as both absolute value (A) and relative value (I_n) and can be set within the range: $0.6 I_n$ to $10 I_n$, in $0.1 I_n$ steps	$2 I_n$
<i>Time t_2</i>	It is the trip time or contributes towards timing calculation, depending on the type of curve selected. The value is given in seconds and can be set within the range: 0.05 s to 0.8 s, in 0.01 s steps	0.1 s
<i>Thermal memory</i>	Activates/deactivates the thermal memory function (page 111) i NOTE: the function is only available with curve $t=k/I^2$	OFF
<i>Zone Selectivity</i>	Activates/deactivates the function and selectivity time availability on the display (page 111) i NOTE: the function is only available with curve $t=k$	OFF
<i>Selectivity time</i>	This is the trip time of the protection with the zone selectivity function activated and selectivity input not present The value is given in seconds and can be set within the range: 0.04 s to 0.2 s, in 0.01 s steps	0,04 s
<i>StartUp enable</i>	Activates/deactivates the function and availability of the associated parameters on the display (page 113) i NOTE: the function is only available with curve $t=k$	OFF
<i>StartUp Threshold</i>	Protection threshold valid during Startup time, in the conditions in which the function is activated (page 113) The value is given as both absolute value (A) and relative value (I_n) and can be set within the range: $0.6 I_n$ to $10 I_n$, in $0.1 I_n$ steps	$0,6 I_n$
<i>StartUp Time</i>	This is the time for which the StartUp threshold remains activated, as calculated from the moment the activation Threshold is exceeded (page 113) The value is given in seconds and can be set within the range: 0.1 s to 30 s, in 0.01 s steps	0.1 s

Limitations and additional functions

- for E1.3N, the maximum value of t_2 is 0.6 s
- threshold I_2 must be higher than threshold I_1 (if S protection is activated)
- in the presence of curve $t = k/I^2$, the protection trip time is forced to t_2 if the calculation results give a theoretical value lower than t_2 itself
- with CB in UL standard configuration, the maximum value of t_2 is 400 ms
 - block functions
 - type of selectivity
 - Startup th. on Prog Status D

The description is available in section List of additional protections and functions on page 110.

G Protection Function

Ekip Aware calculates the vector sum of the phase currents (L1, L2, L3, Ne) and obtains the internal earth fault current (I_g).

If fault current I_g exceeds threshold I_4 , Ekip Aware activates the protection. Ekip Aware sends the TRIP command after a time established by the parameters set and value read.

To check and simulate the trip times in relation to all the parameters, please consult:

- the summary table of the protections with the calculation formulas (page 121)
- the graph with trip curve (page 128)

Certain parameters can be configured and consulted in the Protections menu.

Parameters

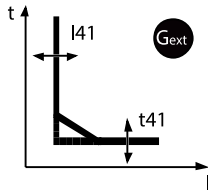
Parameter	Description	Default
<i>Enable</i>	Activates/deactivates the protection and its availability in the parameters menu.	OFF
<i>Trip Enable</i>	Activates/deactivates transmission of the open command. If disabled, the alarm and exceedance of protection time are only managed as information.	ON
<i>Curve</i>	Establishes curve dynamics and the threshold or trip time calculation: • $t = k$: fixed time trip • $t = k/I^2$: inverse time-delay dynamic trip	$t = k$
<i>Threshold I_4</i>	Establishes the value that activates the protection and contributes towards calculating the trip time. The value is given as both absolute value (A) and relative value (In) and can be set within the range: 0.1 In to 1 In, in 0.001 In steps	0,2 In
<i>Time t_4</i>	It is the trip time or contributes towards timing calculation, depending on the type of curve selected. The value is given in seconds and can be set within the range: 0.1 s to 1 s, in 0.05 s steps i NOTE: in the presence of curve: $t = k$, t_4 can also be configured as: instantaneous; in this mode, the trip time is comparable to that given for I protection (page 121)	0.1 s
<i>Prealarm I_4</i>	Warns that the measured current is near to the protection activation threshold. The value is given in percentage of threshold I_1 and can be set within the range 50% I_4 to 90% I_4 , in 1% steps. The prealarm condition deactivates in two cases: • current lower than prealarm threshold I_4 • current higher than threshold I_4	90 % I_4
<i>Zone Selectivity</i>	Activates/deactivates the function and selectivity time availability on the display (page 111) i NOTE: the function is only available with curve $t = k$	OFF
<i>Selectivity time</i>	This is the trip time of the protection with the zone selectivity function activated and selectivity input not present The value is given in seconds and can be set within the range: 0.04 s to 0.2 s, in 0.01 s steps	0,04 s
<i>StartUp enable</i>	Activates/deactivates the function and availability of the associated parameters on the display (page 113) i NOTE: the function is only available with curve $t = k$	OFF
<i>StartUp Threshold</i>	Protection threshold valid during Startup time, in the conditions in which the function is activated (page 113) The value is given as both absolute value (A) and relative value (In) and can be set within the range: 0.2 In to 1 In, in 0.02 In steps	0,2 In
<i>StartUp Time</i>	This is the time for which the StartUp threshold remains activated, as calculated from the moment the activation Threshold is exceeded (page 113) The value is given in seconds and can be set within the range: 0.1 s to 30 s, in 0.01 s steps	0.1 s

Continued on the next page

Limitations and additional functions

- in the presence of curve $t = k/I^2$, the protection trip time is forced to t_4 if the calculation results give a theoretical value lower than t_4 itself
- in the absence of V_{aux} , the minimum threshold is $0.3 I_n$ (for $I_n = 400 A$) or $0.2 I_n$ (for all the other sizes); if lower values are set, the Trip unit forces the threshold to the minimum admissible value and the "Configuration" error appears
- The protection has a different inhibition threshold that depends on the value set for I_4 : $8 I_n$ with threshold $I_4 \geq 0.8 I_n$; $6 I_n$ with $0.8 I_n > I_4 \geq 0.5 I_n$; $4 I_n$ with $0.5 I_n > I_4 \geq 0.2 I_n$; $2 I_n$ with $I_4 > 0.2 I_n$
- with t_4 =instantaneous operation is guaranteed in the presence of V_{aux} ; in self-supply mode, the Trip unit forces the time to 100 ms and the "Configuration" error appears
- with CB in UL standard configuration, some parameters have different maximum values: I_{41} maximum = 1200A, Startup maximum = 1200A, t_4 maximum = 400ms
- all the parameters described above are available via USB-C port, Bluetooth Low Energy and system bus, as are certain further ones:
 - block functions
 - Startup th. on Prog Status D

The description is available in section List of additional protections and functions on page 110.

Gext Protection Function

Gext protection protects against earth faults and detects the fault current with a dedicated external toroid S.G.R.

if S.G.R. toroid current exceeds threshold I_{41} , the protection trips and, after a time established by the value read and by the parameter settings, transmits the TRIP command.

To check and simulate the trip times in relation to all the parameters, please consult:

- summary table of the protections with the operating characteristics (page 121)
- the graph with trip curve (page 128)

Certain parameters can be configured and consulted in the Protections menu.

Parameters

Toroid configuration is available in the Settings menu (page 75)

Parameter	Description	Default
<i>External Toroid</i>	It allows the presence of <i>external toroid S.G.R.</i> to be activated	OFF
<i>Toroid size</i>	Allows the reference current of the protection to be selected from among four available quantities, from 100 A to 800 A IMPORTANT: the current selected from the menu must be consistent with the size of the external toroid S.G.R. connected to the unit	100 A

The protection configuration is available in the Advanced menu (page 64)

Parameter	Description	Default
<i>Enable</i>	Activates/deactivates the protection and its availability in the parameters menu	OFF
<i>Trip Enable</i>	Activates/deactivates transmission of the open command: if disabled, the alarm and exceedance of protection time are only managed as information	ON
<i>Curve</i>	Establishes curve dynamics and the threshold or trip time calculation: • $t = k$: fixed time trip • $t = k/I^2$: inverse time-delay dynamic trip	$t = k$
<i>Threshold I_{41}</i>	Establishes the value that activates the protection and contributes towards calculating the trip time. The value is given as both absolute value (amperes) and relative value (I_n) and can be set within the range: 0.1 I_n to 1 I_n , in 0.001 I_n steps	0,2 I_n
<i>Time t_{41}</i>	It is the trip time or contributes towards timing calculation, depending on the type of curve selected. The value is given in seconds and can be set within the range: 0.1 s to 1 s, in 0.05 s steps	0,4 s
<i>Threshold I_{41}</i>	Warns that the measured current is near to the protection activation threshold. The value is given in percentage of threshold I_1 and can be set within the range 50% I_{41} to 90% I_{41} , in 1% steps. The prealarm condition deactivates in two cases: • current lower than prealarm threshold I_{41} • current higher than threshold I_{41}	90 % I_{41}
<i>Zone Selectivity</i>	Activates/deactivates the function and selectivity time availability on the display ⁽¹⁾ NOTES : • the function is only available with curve $t = k$ • if at least two of the selectivity G, Gext and MDGF are enabled, the input and output are shared with the OR function; it is sufficient that even a selectivity is activated to stimulate inputs and outputs	OFF
<i>Selectivity time</i>	This is the trip time of the protection with the zone selectivity function activated and selectivity input not present ⁽¹⁾ The value is given in seconds and can be set within the range: 0.04 s to 0.2 s, in 0.01 s steps	0,04 s

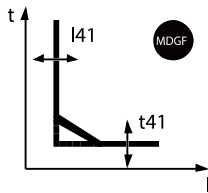
Continued on the next page

Parameter	Description	Default
<i>StartUp enable</i>	Activates/deactivates the function and availability of the associated parameters on the display ⁽²⁾ i NOTE: the function is only available with curve $t=k$	OFF
<i>StartUp Threshold</i>	Protection threshold valid during Startup time, in the conditions in which the function is activated ⁽²⁾ Value is given as both absolute value (Amperes) and relative value (In) and can be set within range: 0.2 In to 1 In, in 0.02 In steps	0,2 In
<i>StartUp Time</i>	This is the time for which the StartUp threshold remains activated and is calculated from the moment the activation Threshold is exceeded ⁽²⁾ The value is given in seconds and can be set within the range: 0.1 s to 30 s, in 0.01 s steps	0.1 s

⁽¹⁾ details on page 111⁽²⁾ details on page 113**Limitations and additional functions**

- in the presence of curve $t= k/I^2$, the protection trip time is forced to t_{41} if the calculation results give a theoretical value lower than t_{41} itself
- Ekip Aware activates and displays Gext protection parameters if the presence of toroid S.G.R has been enabled in the Settings menu (page 75); protection activation includes checking for the presence of toroids S.G.R and signaling on the diagnosis bar in the event of alarm/absence
- the protection is automatically inhibited by the unit if absence of toroid S.G.R is detected
- all the parameters described above are available via USB-C port, Bluetooth Low Energy and system bus, as are certain further ones:
 - block functions
 - type of selectivity
 - Startup th. on Prog Status D

The description is available in section List of additional protections and functions on page 110.

MDGF Protection Function

MDGF protection protects against earth faults and detects the fault current with a dedicated toroid MDGF.

If the MDGF toroid current exceeds threshold I_{41} , the protection trips and, after a time established by the value read and by the parameter settings, transmits the TRIP command.

To check and simulate the trip times in relation to all the parameters, please consult:

- summary table of the protections with the operating characteristics (page 121)
- the graph with trip curve (page 129)

Certain parameters can be configured and consulted in the Protections menu.

Parameters

Toroid configuration is available in the Settings menu (page 75)

Parameter	Description	Default
<i>External Toroid</i>	It allows the presence of <i>toroid MDGF</i> to be activated	OFF
<i>MDGF In Size</i>	Visible if External Toroid parameter setting is ON. Size of MDGF Toroid installed must be set. Value can be set within the 100 A to I_u value range, given in Amperes and in 1A steps.	I_u (A)

Parameter	Description	Default
<i>Enable</i>	Activates/deactivates the protection and its availability in the parameters menu	OFF
<i>Trip Enable</i>	Activates/deactivates transmission of the open command: if disabled, the alarm and exceedance of protection time are only managed as information	ON
<i>Curve</i>	Establishes curve dynamics and the threshold or trip time calculation: $t= k$: fixed time trip $t= k/I^2$: inverse time-delay dynamic trip	$t= k$

Continued on the next page

Parameter	Description	Default
<i>Threshold I41</i>	Establishes the value that activates the protection and contributes towards calculating the trip time. Value is given as both absolute value (Amperes) and relative value (In, with reference to MDGF In Size parameter) and can be set within a range: 0.1 In to 1 In, in 0.001 In steps	0,2 In
<i>Time t41</i>	It is the trip time or contributes towards timing calculation, depending on the type of curve selected. The value is given in seconds and can be set within the range: • 0.05 s to 1 s, in 0.05 s steps, Vaux present and curve t=k • 0.1 s to 1 s, in 0.05 s steps, with self supply or with Vaux and curve t=k/I ²	0,4 s
<i>Threshold I41</i>	Warns that the measured current is near to the protection activation threshold. Value is given in percentage of MDGF In Size and can be set within the range of 50% I41 to 90% I41, in 1% steps. The prealarm condition deactivates in two cases: • current lower than prealarm threshold I41 • current higher than threshold I41	90 % I41
<i>Zone Selectivity</i>	Activates/deactivates the function and selectivity time availability on the display ⁽¹⁾ i NOTES : • the function is only available with curve t = k • if at least two of the selectivity G, Gext and MDGF are enabled, the input and output are shared with the OR function; it is sufficient that even a selectivity is activated to stimulate inputs and outputs	OFF
<i>Selectivity time</i>	This is the trip time of the protection with the zone selectivity function activated and selectivity input not present ⁽¹⁾ The value is given in seconds and can be set within the range: 0.04 s to 0.2 s, in 0.01 s steps	0,04 s
<i>Startup enable</i>	Activates/deactivates the function and availability of the associated parameters on the display ⁽²⁾ i NOTE: the function is only available with curve t=k	OFF
<i>Startup Threshold</i>	Protection threshold valid during Startup time, in the conditions in which the function is activated ⁽²⁾ Value is given as both absolute value (Amperes) and relative value (In, with reference to MDGF In Size parameter) and can be set within a range: 0.2 In to 1 In, in 0.1 In steps	0,2 In
<i>Startup Time</i>	This is the time for which the Startup threshold remains activated and is calculated from the moment the activation Threshold is exceeded ⁽²⁾ The value is given in seconds and can be set within the range: 0.1 s to 30 s, in 0.01 s steps	0.1 s

⁽¹⁾ details on page 111⁽²⁾ details on page 113**Limitations and additional functions**

- in the presence of curve t= k/I², the protection trip time is forced to t41 if the calculation results give a theoretical value lower than t41 itself
- Ekip Aware activates and displays MDGF protection parameters if the presence of toroid MDGF has been enabled in the Settings menu (page 75);
- an error is generated if MDGF In Size value exceeds rated current value of CB
- all the parameters described above are available via USB-C port, Bluetooth Low Energy and system bus, as are certain further ones:
 - block functions
 - type of selectivity
 - Startup th. on Prog Status D

The description is available in section List of additional protections and functions on page 110.