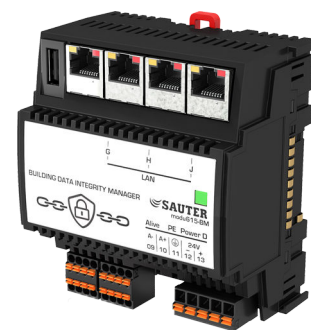


EY6BM15: Building Data Integrity Manager, modu615-BM

Features

- Part of the SAUTER modulo 6 system family
- Blockchain-based solution for monitoring the data integrity of automation stations
- Encrypted communication in the building automation network
- Integrated web server for local commissioning, visualisation, operation and user administration
- Notification and device isolation or self-healing in the event of data integrity breach
- NTP client for time synchronization and certificate protection
- Audit trail



EY6BM15F011

Technical data

Power supply

| | |
|-----------------------------------|--------------------------|
| Power supply | 24 V \pm 10% |
| Power consumption | \leq 2 W without load |
| Dissipated power | \leq 2 W without load |
| Peak inrush current ¹⁾ | \leq 2 A, \leq 10 ms |

Parameters

| | |
|-----------------------|---|
| Connection | 5-pin spring-type terminal, pluggable, 0.5...1.5 mm ² (rigid) 0.5...2.5 mm ² , at least 8 mm wire stripped |
| Battery (buffer: RTC) | CR2032, pluggable |
| Earth connector | Spring contact against DIN rail and PE terminal |

Ambient conditions

| | |
|-----------------------------------|------------------------------|
| Operating temperature | 0...45 °C |
| Storage and transport temperature | -20...70 °C |
| Admissible ambient humidity | 10...90% rh, no condensation |

Function

| | |
|------------------|-------------------|
| Number of slaves | Max. 100 |
| Hash function | SHA-256 (for TLS) |

Architecture

| | |
|---------------------|----------------|
| Processor | ARM 8, 1 GHz |
| RAM (memory) | 512 MB (DDR3) |
| Flash | 512 MB |
| Embedded web server | moduWeb Unity |
| Operating system | Embedded Linux |

Interfaces and communication

| | |
|---------------|----------------------------|
| Communication | Via SMTP, NTP, HTTPS, MQTT |
|---------------|----------------------------|

Ethernet network

| | |
|---------------------------|---------------------------|
| Ethernet network | 3 \times RJ45 connector |
| 10/100 BASE-T(X) switched | 10/100 Mbit/s |
| Use | Blockchain network |

Construction

| | |
|----------------------|--|
| Fitting | On metallic DIN rail 35 \times 7.5/15 as per EN 60715. Rail housing as per DIN 43880 |
| Dimensions W x H x D | 92.6 (5 HP) \times 100.9 \times 58.3 mm |
| Weight | 260 g |

Standards and directives

| | |
|--------------------|--|
| Type of protection | Connections and terminals: IP00 (EN 60730) Front in DIN cut-out: IP30 (EN 60730) |
|--------------------|--|

¹⁾ Measured value with EY-PS021F021 power supply unit



| | | |
|----------------------------|----------------------------------|---|
| | Protection class | I (EN 60730-1) |
| | Environment class | 3K3 (IEC 60721) |
| | Software class | A (EN 60730-1, Appendix H) |
| | Energy class | I to VIII = up to 5% as per EU 811/2013, 2010/30/EU, 2009/125/EC |
| CE conformity according to | EMC Directive 2014/30/EU | EN 61000-6-1, EN 61000-6-2, EN 61000-6-3, EN 61000-6-4, EN 50491-5-1, EN 50491-5-2, EN 50491-5-3 |
| | Low-Voltage Directive 2014/35/EU | EN 60730-1, EN 60730-2-9, EN 62479 |
| | RoHS Directive 2011/65/EU | EN 50581 |
| | RED Directive 2014/53/EU | EN 300 328 V2.1.1 |

Overview of types

| Type | Features |
|-------------|--|
| EY6BM15F011 | Building Data Integrity Manager and web server |

Manuals

| Document number | Language | Title |
|-----------------|----------|--------------------------------------|
| D100397589 | de | Systembeschreibung SAUTER modulo |
| D100408512 | de | EY-modulo 6 – Best Practice I |
| D100402674 | en | SAUTER modulo system description |
| D100410201 | en | EY-modulo 6 – Best Practice I |
| D100402676 | fr | Description du système SAUTER modulo |
| D100410203 | fr | EY-modulo 6 – Meilleures pratiques I |

Description of operation

The modu615-BM Building Data Integrity Manager and web server periodically checks the integrity of the static data in a predefined group of compatible automation stations. The check is performed via an integrity chain (blockchain). If an integrity breach is detected, it is reported by e-mail or MQTT and entered in the audit trail log. If configured accordingly, the manager can automatically restore the affected device (self-healing). This is made possible by the digital twin of the affected automation station that is created during initialisation. The digital twin overwrites the corrupt data.

The web server integrated in the modu615-BM is only accessible via HTTPS (automatic redirection from http). Access is protected by a user name and password. The security can be enhanced using two-factor authentication (code received by e-mail and entered).

Note



The two-factor authentication requires e-mail communication. Do not activate the function if e-mails cannot be received.

The web server supports the creation of multiple user accounts in two standardised roles: administrator and user.

Note



A self-signed certificate is used for the initial login to the web server. The certificate triggers the alarm message «Not secure» in the browser.

Contact your IT administrator for a CA-signed certificate.

Web server user interfaces

The access on the web server is protected by a user name and password. After a successful login the dashboard opens by default. The navigation bar with the following interfaces is located on the left-hand side:

- DASHBOARD
- WIZARD
- EVENTS
- USERS
- SETTINGS

Clicking the icon in the top right-hand corner opens a menu with the following functions:

- Switching night mode on or off
- Display of the logged-in user and a link to the user profile
- Logout from the web server

WIZARD

The blockchain is created and the integrity check started via a guided configuration process (wizard) in the following four wizard steps:

1. In the «Select device» wizard step, select the devices that are to participate in the integrity check.
→ After the wizard is opened, the network is automatically scanned (zero-config) and the compatible devices are displayed. The order of the devices can be changed using drag & drop.
 - 1.1 Select devices for the integrity check. The modu615-BM manager station (HOST) must be included. «Select all» selects all the listed devices in one step. The network can be rescanned using the «Rescan» button.
 - 1.2 Click «Next» to proceed to the next wizard step.
2. In the «Select action» wizard step, select a system response to be executed in the event of an integrity breach. The following are available:
 - «Alarm»: E-mail notification and entry in the audit trail log.
 - «Alarm & Self Heal»: E-mail notification and restore with digital twin.
 - 2.1 Click «Next» to proceed to the next wizard step.
3. In the «Set cycle period» wizard step, define the cycle time for the integrity check. The minimum interval between two cycles depends on the number of devices in the blockchain.
 - 3.1 Click «Next» to proceed to the last wizard step.
4. In the «Create twins» wizard step, the blockchain is automatically created by the following routine:
 - The selected devices are registered in the system.
 - Time synchronization is executed. If necessary, an NTP server address is requested.
Note: It is strongly recommended to synchronize the automation stations in advance (BACnet or NTP). Provide an NTP server for the synchronization of the modu615-BM. The device does not support BACnet time synchronization.
 - Device certificates are created, distributed to the devices, and signed.
 - Digital twins of the devices are created and stored in the modu615-BM.
 - The stored digital twins are checked (hash calculation of the blockchain).
 - 4.1 Click «Finish» to start the routine and complete the configuration.
→ The view changes from the wizard to the dashboard and the integrity check is started.

DASHBOARD

In the dashboard, the current process and status of the blockchain is displayed in four fields:

- «Last Completed Cycle Status»:
Shows the status of the blockchain (Data integrity breach / Processing / Success / Failure / Warning / General warning) and which devices are not accessible or are breaching the integrity.
- «Default Action»:
Shows the type of integrity check that is configured. Allows this to be changed (Alarm / Alarm & Self Heal).
- «Last Cycle» / «Next Cycle»:
Shows the time since the last check cycle or until the next check cycle. Allows the check to be paused (pause icon) or forced (Force restart).
- «Chain» / «Table»:
Displays the status of the blockchain graphically (Chain) or in table form (Table). If the display is green, everything is OK. If the display is red, the integrity of a device has been breached. When a device is clicked, a dialogue with two tabs appears: The «Info» tab shows the serial number and the type of device. The «Files» tab displays the file hierarchy. Files with an integrity breach are marked in red. Files without anomalies are displayed in green.

EVENTS

On the EVENTS page, events such as user logins, initialisations and changes in the device list are listed with their status and date. If «Advanced log» is activated, further event types are displayed, e.g. integrity checks and restores.

When an event is clicked, a dialogue with further information appears.

USERS

On the USERS page, users can manage their own user profile.

The administrator (Admin) can create or delete user accounts.

SETTINGS

On the SETTINGS page the following settings can be made:

- «NOTIFICATIONS SETTINGS»:
 - E-mail notification frequency settings
- «SMTP SETTINGS»:
 - Settings for the SMTP client service
- «MQTT SETTINGS»
 - The device can be logged into an MQTT broker as a publisher. The following entries are required:
 - «Broker address»: Address of the MQTT broker.
 - «Notification topic»: Client ID of the broker for the device login. Default entry: *sauter/<serial number>*
 - «Username»
 - «Password»
 - The «Verify connection» button can be used to check the login or the setting. A test e-mail is sent. The payload indicates the current status in JSON format.
- «HTTPS CERTIFICATE SETTINGS»:
 - Select one of the following three certificate settings:
 - «Import»: Load a PKCS#12 file. The IT administrator creates a certificate file in PKCS format for the user as well as a password.
 - «Self Signed»: Load a self-generated certificate (factory setting). For security reasons, this certificate is only recommended to a limited extent.
 - «CSR» (Certificate Signing Request): Have the public key sent to a certification authority (CA) and signed. This signed certificate gives the user access to the web server.

Intended use

This product is only suitable for the purpose intended by the manufacturer, as described in the “Description of operation” section.

All related product regulations must also be adhered to. Changing or converting the product is not admissible.

Improper use

The SAUTER modulo 6 system does not have functional safety and is not fail-safe.

This product is not suitable:

- for security functions of the automation
- in transportation means and storage facilities as per Directive 37/2005
- in outdoor areas and in rooms with the risk of condensation
- on means of transport, e.g. ships.

Engineering notes

The configuration and operation of the SAUTER Building Data Integrity solution is based on the following prerequisites:

- All participants (devices) must be in the same network segment. The device search function is based on the same technical solution as CASE Sun.
- All participants must be time synchronized. The NTP service (Network Time Protocol) is used for this purpose. It must be ensured that the NTP setting can function with CASE Sun. The NTP server must be accessible to all participants at all times.
- The e-mail notification uses SMTP. The SMTP server must be accessible to the device at all times.








The modu615-BM does not support BACnet services. Time synchronization, device search (Discovery) and other BACnet-based functions are not supported.

The following modulo 6 devices are compatible with modu615-BM:

| | | |
|------------|-------------|-------------------|
| modu680-AS | EY6AS80F021 | from firmware 1.2 |
| modu660-AS | EY6AS60F011 | from firmware 1.2 |
| modu612-LC | EY6LC12F011 | |

LED indicators

The following operating statuses of the device are displayed:

| Status ²⁾ | Indicator | Description |
|----------------------|---|--|
| Continuous green |  | OK, normal operation |
| Flashing green |  | Identification via CASE Sun |
| Continuous orange |  | Start-up mode, communication is being set up |
| Flashing orange |  | The internal backup battery must be replaced |
| Continuous red |  | No configuration |
| Flashing red |  | Configuration active |
| Red flashing rapidly |  | Internal device error |

Parameterisation

The basic settings such as IP settings are performed with CASE Sun.

Initialisation

An initialisation (delete configuration, load factory settings) of the modu615-BM can be performed with CASE Sun.

Firmware/update

The modu615-BM is delivered with the latest firmware. Updates can be installed via CASE Sun.



Note

Only operate the device with the latest firmware. Before commissioning, check the firmware version and carry out an update if necessary.

The version of the installed firmware can be read via CASE Sun.

Internal clock

A Real Time Clock (RTC) is integrated in the device. The date, time and time zone are set in the connected automation station. The internal clock is protected against power cuts by a battery.

Battery

A lithium battery (pluggable button cell) ensures that the Real Time Clock for time programmes (scheduler/calendar) keeps running in the event of a power failure.

The battery voltage is monitored by the device.

The battery may only be replaced when the device is disconnected from the power supply. During battery replacement, the current time of the internal clock is lost and must be reset.

Follow the safety instructions and the directions in the fitting instructions for the device. If necessary, contact SAUTER Service to replace the battery.

Technical data for the battery

| | |
|-----------------|----------------------------|
| Type (standard) | CR2032 lithium button-cell |
| Nominal voltage | 3 V |
| Capacity | 210 mAh |
| Dimensions | 20 mm × 3.2 mm |

The lithium battery should be replaced after five to ten years. It may only be replaced by trained specialist personnel.



WARNING!

Risk of explosion if the battery is short-circuited during replacement.

► Only use insulated tools when replacing the battery.

²⁾ LED flashing: 500 ms on, 500 ms off
LED flashing rapidly: 100 ms on, 100 ms off

Behaviour in case of power failure

During power interruptions, the device is switched off in the correct manner. When the power returns, the system is switched back on according to priority. The behaviour for switching off and on is defined autonomously by the device.



Note

Power failures in the EY-PS021F021 switched-mode power supply on the primary side (230 V AC) that last less than 100 ms are bridged without switching off or other consequences. The system continues to run in normal mode.

Protection mechanisms at application level

The modu615-BM has the following protection mechanisms:

Access rights

The access to the web server is protected by a user name and password. The first time a user logs in to the web server, the default password must be changed. User administration and setting the access rights are the responsibility of the system operator.

Data security

User data is stored in encrypted form.

Communication security

Internet communication is encrypted where technically possible. The HTTPS and SMTP protocols are encrypted. Access via HTTP is automatically redirected to HTTPS.

The system only allows communication via authorised ports. All other ports are blocked by the on-board firewall. In addition, an authorisation list with approved devices can be created.

Firmware update

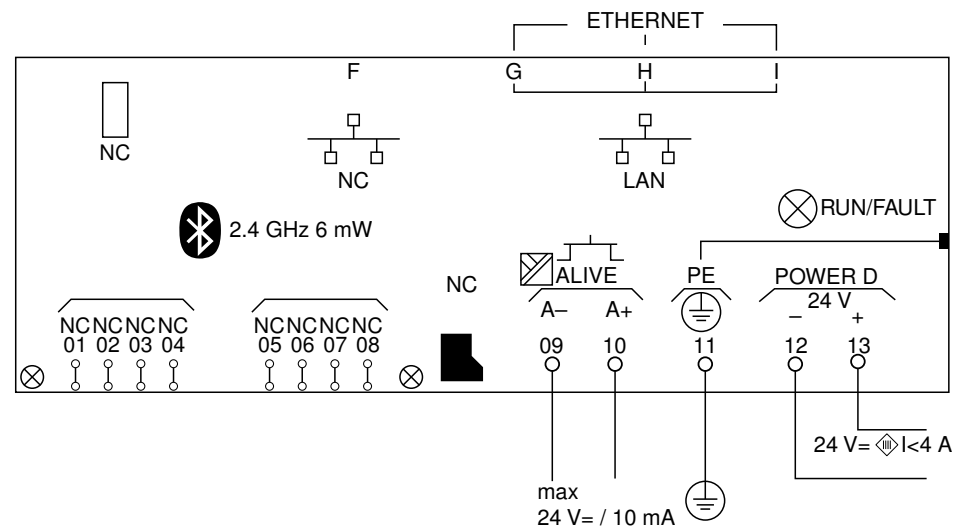
Only firmware updates signed by SAUTER can be installed.

Disposal

When disposing of the product, observe the currently applicable local laws.

More information on materials can be found in the Declaration on materials and the environment for this product.

Connection diagram



Dimension drawing

All dimensions in millimetres.

