

EY6BM15: Building Data Integrity Manager, modu615-BM

Eigenschaften

- Teil der SAUTER modulo 6 Systemfamilie
- Blockchain-basierte Lösung zur Überwachung der Datenintegrität von Automationsstationen
- Verschlüsselte Kommunikation im Netzwerk der Gebäudeautomation
- Integrierter Webserver für lokale Inbetriebnahme, Visualisierung, Bedienung und Benutzerverwaltung
- Benachrichtigung und Geräteisolation oder Selbstheilung bei Datenintegritätsbruch
- NTP-Client zur Zeitsynchronisation und Absicherung der Zertifikate
- Audit-Trail



EY6BM15F011

Technische Daten

Elektrische Versorgung

Speisespannung	24 V \pm 10%
Leistungsaufnahme	\leq 2 W ohne Last
Verlustleistung	\leq 2 W ohne Last
Einschaltstromspitze ¹⁾	\leq 2 A, \leq 10 ms

Kenngrossen

Anschluss	5-polige Federzugklemme, steckbar, 0,5...1,5 mm ² (starr) 0,5...2,5 mm ² , mindestens 8 mm Ab- isolierung
Batterie (Pufferung RTC)	CR2032, steckbar
Erdanschluss	Federkontakt gegen DIN-Rail und PE-Klemme

Umgebungsbedingungen

Betriebstemperatur	0...45 °C
Lager- und Transporttemperatur	-20...70 °C
Umgebungsfeuchte	10...90% rF ohne Kondensation

Funktion

Anzahl Slaves	Max. 100
Hashfunktion	SHA-256 (für TLS)

Architektur

Prozessor	ARM 8, 1 GHz
RAM (Arbeitsspeicher)	512 MB (DDR3)
Flash	512 MB
Embedded Web Server	moduWeb Unity
Betriebssystem	Embedded Linux

Schnittstellen, Kommunikation

Kommunikation	Über SMTP, NTP, HTTPS, MQTT
---------------	-----------------------------

Ethernet-Netzwerk

Ethernet-Netzwerk	3 \times RJ45-Buchse
10/100 BASE-T(X) Switched	10/100 Mbit/s
Verwendung	Blockchain-Netzwerk

Konstruktiver Aufbau

Montage	Auf metallische Hutschiene 35 \times 7,5/15 nach EN 60715. Reiheneinbaugehäuse nach DIN 43880
Masse B \times H \times T	92,6 (5 TE) \times 100,9 \times 58,3 mm
Gewicht	260 g

¹⁾ Messwert mit Netzteil EY-PS021F021



Normen, Richtlinien		
	Schutzart	Anschlüsse und Klemmen: IP00 (EN 60730) Front im DIN-Ausschnitt: IP30 (EN 60730)
	Schutzklasse	I (EN 60730-1)
	Umgebungs-kategorie	3K3 (IEC 60721)
	Software-kategorie	A (EN 60730-1 Anhang H)
	Energie-kategorie	I bis VIII = bis 5% nach EU 811/2013, 2010/30/EU, 2009/125/EG
CE-Konformität nach	EMV-Richtlinie 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
	Niederspannungsrichtlinie 2014/35/EU	EN 60730-1, EN 60730-2-9, EN 62479
	RoHS-Richtlinie 2011/65/EU	EN IEC 63000
	RED-Richtlinie 2014/53/EU	EN 300328 (V2.1.1)

Typenübersicht

Typ	Eigenschaften
EY6BM15F011	Building Data Integrity Manager und Webserver

Handbücher

Dokumentnummer	Sprache	Titel
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

Funktionsbeschreibung

Der Building Data Integrity Manager und Webserver modu615-BM überprüft periodisch die Integrität der statischen Daten in einer vordefinierten Gruppe von kompatiblen Automationsstationen. Die Prüfung findet über eine Integritätskette (Blockchain) statt. Wenn ein Integritätsbruch erkannt wird, wird dieser per E-Mail oder MQTT gemeldet und im Audit-Trail-Log eingetragen. Bei entsprechender Konfiguration kann der Manager das betroffene Gerät automatisch wiederherstellen (Self Healing). Dies wird durch den bei der Initialisierung erstellten digitalen Zwilling der betroffenen Automationsstation ermöglicht. Mit dem digitalen Zwilling werden die korrupten Daten überschrieben. Der im modu615-BM integrierte Webserver ist nur über HTTPS zugänglich (automatische Umleitung von http). Der Zugang ist durch Benutzername und Passwort geschützt. Die Sicherheit kann mit der Zwei-Faktor-Authentifizierung (Code per E-Mail empfangen und eingeben) erhöht werden.

Hinweis



Die Zwei-Faktor-Authentifizierung benötigt E-Mail-Kommunikation. Schalten Sie die Funktion nicht ein, wenn E-Mails nicht empfangen werden können.

Der Webserver unterstützt die Erstellung mehrerer Benutzerkonten in zwei standardisierten Rollen: Administrator und Benutzer.

Hinweis



Bei der Erstanmeldung auf dem Webserver wird ein selbstsigniertes Zertifikat verwendet. Das Zertifikat löst im Browser die Alarmmeldung «Nicht sicher» aus. Wenden Sie sich für ein CA-signiertes Zertifikat an ihren IT-Administrator.

Webserver-Benutzeroberflächen

Der Zugang auf dem Webserver ist mit Benutzername und Passwort geschützt. Nach erfolgreicher Anmelden öffnet sich standardmässig das Dashboard. Auf der linken Seite befindet sich die Navigationsleiste mit folgenden Oberflächen:

- DASHBOARD
- WIZARD
- EVENTS
- USERS
- SETTINGS

Durch Klicken auf das Symbol in der oberen rechten Ecke öffnet sich ein Menü mit folgenden Funktionen:

- Ein- oder Ausschalten des Nachtmodus
- Anzeige des angemeldeten Benutzers und Verknüpfung zum Benutzerprofil
- Abmelden vom Webserver

WIZARD

Die Erstellung der Blockchain und der Start der Integritätsprüfung erfolgt über einen geführten Konfigurationsprozess (Wizard) in den folgenden vier Wizard-Schritten:

1. Im Wizard-Schritt «Select device» die Geräte auswählen, die an der Integritätsprüfung teilnehmen sollen.
 - Nach dem Öffnen des Wizards wird das Netzwerk automatisch gescannt (zero-config) und die kompatiblen Geräte werden angezeigt. Die Reihenfolge der Geräte kann per Drag & Drop geändert werden.
 - 1.1. Geräte für die Integritätsprüfung wählen. Die Manager-Station modu615-BM (HOST) muss zwingend dabei sein. Mit «Select all» können alle gelisteten Geräte in einem Schritt ausgewählt werden. Mit der Schaltfläche «Rescan» kann das Netzwerk erneut gescannt werden.
 - 1.2. Auf «Next» klicken, um zum nächsten Schritt des Wizards zu gelangen.
2. Im Wizard-Schritt «Select action» eine Systemreaktion wählen, die bei einer Integritätsverletzung ausgeführt wird. Zur Auswahl stehen:
 - «Alarm»: E-Mail-Benachrichtigung und Eintrag im Audit-Trail-Log.
 - «Alarm & Self Heal»: E-Mail-Benachrichtigung und Wiederherstellung mit digitalem Zwilling.
 - 2.1. Auf «Next» klicken, um zum nächsten Schritt des Wizards zu gelangen.
3. Im Wizard-Schritt «Set cycle periode» die gewünschte Zykluszeit der Integritätsprüfung festlegen. Der Mindestabstand zwischen zwei Zyklen ist abhängig von der Anzahl der Geräte in der Blockchain.
 - 3.1. Auf «Next» klicken, um zum letzten Schritt des Wizards zu gelangen.
4. Im Wizard-Schritt «Create twins» wird die Blockchain über die folgende Routine automatisch erstellt:
 - Die gewählten Geräte werden im System registriert.
 - Zeitsynchronisation wird durchgeführt. Bei Bedarf wird eine NTP-Server-Adresse abgefragt. Hinweis: Es wird streng empfohlen die Automationsstationen schon im voraus zu synchronisieren (BACnet oder NTP). Für die Synchronisation des modu615-BM einen NTP-Server bereitstellen. Das Gerät unterschützt keine BACnet-Zeitsynchronisation.
 - Gerätezertifikate werden erstellt, an die Geräte verteilt und signiert.
 - Digitale Zwillinge der Geräte werden im modu615-BM angelegt und gespeichert.
 - Die gespeicherten digitalen Zwillinge werden geprüft (Hash-Berechnung der Blockchain).
 - 4.1 Auf «Finish» klicken, um die Routine zu starten und die Konfiguration abzuschliessen.
 - Die Ansicht wechselt vom Wizard zum Dashboard und die Integritätsprüfung wird gestartet.

DASHBOARD

Im Dashboard wird der aktuelle Ablauf und Zustand der Blockchain in vier Feldern dargestellt:

- «Last Completed Cycle Status»:
Zeigt an, in welchem Zustand sich die Blockchain befindet (Data integrity breach / Processing / Success / Failure / Warning / General warning), sowie welche Geräte nicht zugänglich sind oder die Integrität verletzen.
- «Default Action»:
Zeigt an, welche Art der Integritätsprüfung konfiguriert ist. Erlaubt, diese zu ändern (Alarm / Alarm & Self Heal).
- «Last Cycle» / «Next Cycle»:
Zeigt die Zeit seit dem letzten Prüfzyklus bzw. bis zum nächsten Prüfzyklus an. Ermöglicht die Prüfung anzuhalten (Pause-Symbol) oder zu erzwingen (Force restart).

- «Chain» / «Table»: Zeigt den Zustand der Blockchain graphisch (Chain) oder tabellarisch (Table) an. Bei grüner Anzeige ist alles in Ordnung. Bei roter Anzeige ist die Integrität eines Geräts verletzt. Beim Klicken auf ein Gerät erscheint ein Dialog mit zwei Reitern: Der Reiter «Info» zeigt die Seriennummer und den Gerätetyp an. Der Reiter «Files» zeigt die Dateihierarchie an. Dateien mit Integritätsverletzung werden rot markiert. Dateien ohne Auffälligkeiten werden grün angezeigt.

EVENTS

Auf der Seite EVENTS werden Ereignisse, z. B. Benutzer-Logins, Initialisierungen und Änderungen in der Geräteliste, mit Status und Datum gelistet. Wenn «Advanced log» aktiviert wird, werden weitere Ereignistypen angezeigt, z. B. Integritätsprüfungen und Wiederherstellungen. Beim Klicken auf ein Ereignis erscheint ein Dialog mit weiteren Informationen.

USERS

Auf der Seite USERS kann das eigene Benutzerprofil verwaltet werden. Der Administrator (Admin) kann Benutzerkonten erstellen oder löschen.

SETTINGS

Auf der Seite SETTINGS können folgende Einstellungen vorgenommen werden:

- «NOTIFICATIONS SETTINGS»: Einstellungen der Häufigkeit von E-Mail-Benachrichtigung
- «SMTP SETTINGS»: Einstellungen zum SMTP-Client-Service
- «MQTT SETTINGS»

Das Gerät kann als Publisher an einen MQTT-Broker angemeldet werden. Folgende Angaben sind erforderlich:

 - «Broker address»: Adresse des MQTT-Brokers.
 - «Notification topic»: Client-Kennung des Brokers für die Anmeldung des Geräts. Standardeintrag: *sauter/<Seriennummer>*
 - «Username»
 - «Password»

Mit der Schaltfläche «Verify connection» kann die Anmeldung bzw. Einstellung geprüft werden. Eine Test-E-Mail wird gesendet. Die Payload (Nutzlast) gibt den aktuellen Stand im JSON-Format an.
- «HTTPS CERTIFICATE SETTINGS»: Auswahl zwischen den folgenden drei Zertifikat-Einstellungen:
 - «Import»: Laden einer PKCS#12-Datei. Hierzu erstellt der IT-Administrator für den Benutzer eine Zertifikatsdatei im PKCS-Format sowie ein Passwort.
 - «Self Signed»: Laden eines selbsterstellten Zertifikats (Werkseinstellung). Dieses Zertifikat ist aus Sicherheitsgründen nur bedingt empfehlenswert.
 - «CSR» (Certificate Signing Request): Den Public-Key an eine Zertifizierungsstelle (CA) schicken und signieren lassen. Mit diesem signierten Zertifikat erhält der Benutzer Zugang zum Webserver.

Bestimmungsgemäße Verwendung

Dieses Produkt ist nur für den vom Hersteller vorgesehenen Verwendungszweck bestimmt, der in dem Abschnitt «Funktionsbeschreibung» beschrieben ist.

Hierzu zählt auch die Beachtung aller zugehörigen Produktvorschriften. Änderungen oder Umbauten sind nicht zulässig.

Nicht bestimmungsgemäße Verwendung

Das SAUTER modulo 6 System verfügt über keine funktionale Sicherheit und ist nicht ausfallsicher.

Das Produkt ist nicht geeignet:

- für Sicherheitsfunktionen der Automation
- in Beförderungsmitteln und Lagereinrichtungen nach Verordnung 37/2005
- im Aussenbereich und in Räumen mit Kondensationsgefahr
- auf Transportmitteln, z. B. Schiffen

Projektierungshinweise

Die Konfiguration und der Betrieb der SAUTER Building Data Integrity Lösung basiert auf den folgenden Voraussetzungen:

- Alle Teilnehmer (Geräte) müssen im gleichen Netzwerk-Segment sein. Die Gerätesuchfunktion basiert auf der gleichen technischen Lösung wie CASE Sun.
- Alle Teilnehmer müssen zeitsynchron sein. Dafür wird der NTP-Service (Network Time Protocol) verwendet. Die Funktionsfähigkeit der NTP-Einstellung mit CASE Sun ist sicherzustellen. Der NTP-Server muss allen Teilnehmern jederzeit zugänglich sein.
- Die E-Mail-Benachrichtigung benutzt SMTP. Der SMTP Server muss jederzeit für das Gerät zugänglich sein.

Der modu615-BM unterstützt keine BACnet Services. Zeitsynchronisation, Gerätesuche (Discovery) und andere BACnet-basierte Funktionen sind nicht unterstützt.

Folgende modulo 6 Geräte sind mit modu615-BM kompatibel:

modu680-AS	EY6AS80F021	ab Firmware 1.2
modu660-AS	EY6AS60F011	ab Firmware 1.2
modu612-LC	EY6LC12F011	

LED-Anzeigen

Die folgenden Betriebszustände des Geräts werden angezeigt:

Zustand ²⁾	Anzeige	Beschreibung
Grün stetig		OK, Normalbetrieb
Grün blinkend		Identifikation über CASE Sun
Orange stetig		Startup-Modus, Kommunikation wird aufgebaut
Orange blinkend		Interne Backup-Batterie muss gewechselt werden
Rot stetig		Keine Konfiguration
Rot blinkend		Konfiguration aktiv
Rot schnell blinkend		Interner Gerätefehler

Parametrierung

Die Grundeinstellungen wie IP-Einstellungen werden mit CASE Sun vorgenommen.

Initialisierung

Eine Initialisierung (Konfiguration löschen, Werkseinstellungen laden) des modu615-BM kann mit CASE Sun ausgeführt werden.

Firmware/Update

Der modu615-BM wird mit aktueller Firmware ausgeliefert. Updates können über CASE Sun installiert werden.



Hinweis

Das Gerät nur mit aktueller Firmware in Betrieb setzen. Vor Inbetriebsetzung die Firmware-Version prüfen und ggf. ein Update durchführen.

Die Version der installierten Firmware kann via CASE Sun ausgelesen werden.

²⁾ LED blinkend: 500 ms ein, 500 ms aus
LED schnell blinkend: 100 ms ein, 100 ms aus

Interne Uhr

Im Gerät ist eine Echtzeituhr (Real Time Clock, RTC) integriert. Datum, Uhrzeit und Zeitzone werden in der verbundenen Automationsstation gesetzt. Die interne Uhr ist mit einer Batterie gegen Stromunterbrechungen geschützt.

Batterie

Eine Lithiumbatterie (steckbare Knopfzelle) stellt sicher, dass bei einem Spannungsausfall die Echtzeituhr für Zeitprogramme (Scheduler/Calendar) erhalten bleibt.

Die Batteriespannung wird durch das Gerät überwacht.

Die Batterie darf nur im stromlosen Zustand des Geräts ausgetauscht werden. Beim Batteriewechsel geht die aktuelle Zeit der internen Uhr verloren und muss neu eingestellt werden.

Befolgen Sie die Sicherheitshinweise und Anweisungen in der Montagevorschrift des Geräts. Kontaktieren Sie ggf. den SAUTER Service für einen Austausch der Batterie.

Technische Daten Batterie

Typ (Standard)	CR2032 Lithiumknopfzelle
Nennspannung	3 V
Kapazität	210 mAh
Abmessungen	20 mm × 3,2 mm

Die Lithiumbatterie sollte nach fünf bis zehn Jahren erneuert werden. Der Austausch darf nur von eingewiesenem Fachpersonal durchgeführt werden.

WARNUNG!



Explosionsgefahr, wenn die Batterie beim Ersetzen kurzgeschlossen wird.
► Nur isoliertes Werkzeug beim Auswechseln der Batterie benutzen.

Verhalten bei Netzausfall

Netzunterbrechungen bedeuten für das Gerät ein geordnetes Ausschalten. Bei Netzspannungswiederkehr erfolgt das Einschalten nach Prioritäten. Die Verhaltensweise beim Aus- und Einschalten wird durch das Gerät selbständig definiert.

Hinweis



Netzausfälle, die am Schaltnetzteil EY-PS021F021 primärseitig (230 V AC) kürzer als 100 ms dauern, werden ohne Ausschaltung oder anderweitige Konsequenzen überbrückt. Die Anlage wird im Normalbetrieb weitergeführt.

Schutzmechanismen auf Applikationsebene

Der modu615-BM verfügt über folgende Schutzmechanismen:

Zugriffsberechtigung

Der Zugriff auf den Webserver ist mit Benutzername und Passwort geschützt. Bei der ersten Anmeldung auf dem Webserver muss das Standardpasswort geändert werden. Benutzerverwaltung und Einstellung der Zugriffsberechtigungen liegen in der Verantwortung des Anlagenbetreibers.

Datensicherheit

Benutzerdaten werden verschlüsselt gespeichert.

Kommunikationssicherheit

Die Internetkommunikation wird verschlüsselt, wenn technisch möglich. Die Protokolle HTTPS und SMTP sind verschlüsselt. Der Zugang per HTTP wird automatisch nach HTTPS umgeleitet.

Das System lässt nur die Kommunikation über autorisierte Ports zu. Alle anderen Ports sind durch die On-board-Firewall gesperrt. Ausserdem kann eine Autorisierungsliste mit zugelassenen Geräten erstellt werden.

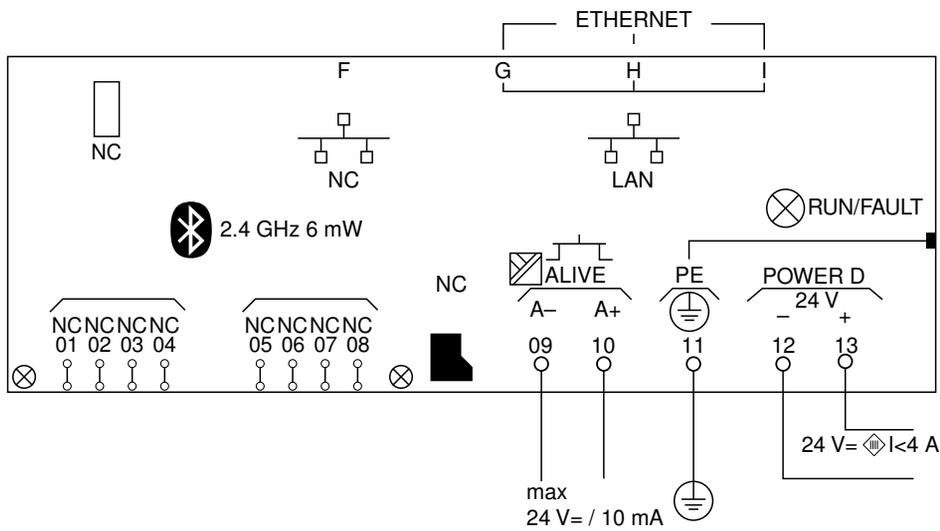
Firmware-Update

Nur von SAUTER signierte Firmware-Updates können installiert werden.

Entsorgung

Bei einer Entsorgung ist die örtliche und aktuell gültige Gesetzgebung zu beachten. Weitere Hinweise zu Material und Werkstoffen entnehmen Sie bitte der Material- und Umweltdokumentation zu diesem Produkt.

Anschlussplan



Massbild

Alle Masse in Millimeter.

