EY6BM15: Building Data Integrity Manager, modu615·BM

EY6BM15F011

Egenskaper

- En del av SAUTER modulo 6-systemfamiljen
- Blockchain-baserad lösning för övervakning av dataintegriteten hos automatiseringsstationer
- Krypterad kommunikation i fastighetssautomationsnätverket
- Integrerad webbserver för lokal driftsättning, visualisering, drift och användaradministration
- Meddelande och enhetsisolering eller självläkning i händelse av dataintegritetsbrott
- NTP-klient för tidssynkronisering och certifikatskydd
- Verifieringskedja (Audit trail)

Tekniska data

Strömförsörjning		
	Strömförsörjning	24 V= ± 10%
	Effekt förbrukning	≤ 2 W utan last
	Förlust effekt	≤ 2 W utan last
	Topp ingångsström [1)]	≤ 2 A, ≤ 10 ms
Parametrar		
	Anslutning	5-pin fjäderbelastad plint, plug-in kontakt, 0.5…1.5 mm^2 (enkeltrådig) 0.5…2.5 mm^2, min 8 mm skalad
	Batteri (backup av: RTC)	CR2032, plugg-in
	Jord anslutning	Fjäderbelastad kontakt mot DINskena och PE plint
Omgivningsförhållanden		
	Drift temperatur	0…45 °C
	Lager-och transporttemperatur	−20…70 °C
	Tillåten omgivande fuktighet	10…90% rh, utan kondensation
Funktion		
	Antal slavar	Max. 100
	Hash-funktion	SHA-256 (för TLS)
Arkitektur		
	Processor	ARM 8, 1 GHz
	RAM (minne)	512 MB (DDR3)
	Flash	512 MB
	Inbyggd webbserver	moduWeb Unity
	Operativ system	Embedded Linux
Gränssnitt och kommunikation		
	Kommunicktion	Via SMTP, NTP, HTTPS, MQTT
Ethernet network	Ethernet nätverk	3 × RJ45 connector
	10/100 BASE-T(X) switched	10/100 Mbit/s
	Användning	Blockchain nätverk
Konstruktion		
	Montage	På metallisk DIN-skena 35 x 7.5/15 enligt EN 60715.Kapsling enligt DIN 43880
	Mått B x H x D	92.6 (5 HP) × 100.9 × 58.3 mm
	Vikt	260 g
Standarder och direktiv		
	Kapslingsgrad	Anslutningar och plintar: IP00 (EN 60730) Front i DIN utskärning: IP30 (EN 60730)

[1)] *Uppmätt med EY-PS021F021 kraftmatnings enhet*

	Kapslingsklass	I (EN 60730-1)
	Omgivningsklass	3K3 (IEC 60721)
	Mjukvaruklass	A (EN 60730-1, Appendix H)
	Energiklass	I till VIII = upp till 5% Enligt EU 811/2013, 2010/30/EU, 2009/125/EC
CE conformity according to	EMC Direktiv 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
	Lågspänningsdirektiv 2014/35/EU	EN 60730-1, EN 60730-2-9, EN 62479
	RoHS Direktiv 2011/65/EU	EN 50581
	RED Direktiv 2014/53/EU	EN 300 328 V2.1.1

Översikt typer	
Typ	Beskrivning
EY6BM15F011	Building Data Integrity Manager och web server

Manualer

Dokument nummer	Språk	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
	se	EY-modulo 6 –Bästa praxis I
D100402676	fr	Description du système SAUTER modulo
D100410203	fr	EY-modulo 6 – Meilleures pratiques I

Funktionsbeskrivning

Modu615-BM Building Data Integrity Manager och webbserver kontrollerar regelbundet integriteten för statisk data i en fördefinierad grupp av kompatibla automatiseringsstationer. Kontrollen utförs via en integritetskedja (blockchain). Om ett integritetsbrott upptäcks rapporteras det via e-post eller MQTT och matas in i granskningsspårloggen. Omkonfigurerad därefter kan hanteraren automatiskt återställa affekterad enhet (självhelande). Detta möjliggörs av den digitala tvillingen på den berörda automatiseringsstationen som skapas under initieringen. Den digitala tvillingen skriver över korrupta data.
Webbservern integrerad i modu615-BM är endast tillgänglig via HTTPS (automatisk omdirigering från http). Åtkomst skyddas av ett användarnamn och lösenord. Säkerheten kan förbättras med tvåfaktorautentisering (kod mottagen via e-post och inmatad).

Notera
Tvåfaktorautentisering kräver e-postkommunikation. Aktivera inte funktionen för e-postmeddelanden kan inte tas emot.

Webbservern stöder skapandet av flera användarkonton i två standardiserade roller: administratör och användare.

Notera
Ett självsignerat certifikat används för den första inloggningen till webbservern. Certifikatet utlöser larmmeddelandet «Inte säkert» i webbläsaren. Kontakta din IT-administratör för ett CA-signerat certifikat.

Användargränssnitt för webserver

Åtkomst på webbservern skyddas av ett användarnamn och lösenord. Efter en framgångsrik inloggning öppnas instrumentpanelen som standard. Navigeringsfältet med följande gränssnitt finns på vänster sida:

- DASHBOARD
- WIZARD
- EVENTS
- USERS
- SETTINGS

Klicka på ikonen i det övre högra hörnet öppnar en meny med följande funktioner:

- 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

Blockchain skapas och integritetskontrollen startas via en guidad konfigurationsprocess (guiden) i följande fyra guider steg:

1. I guiden "Välj enhet", välj enheterna som ska delta i integritetskontrollen.
   → När guiden har öppnats skannas nätverket automatiskt (nollkonfigurering) och de kompatibla enheterna visas. Enhetens ordning kan ändras med dra och släpp.
   1.1 Välj enheter för integritetskontrollen. Modu615-BM manager station (HOST) måste inkluderas. «Markera alla» väljer alla listade enheter i ett steg. Nätverket kan raderas igen med knappen «Skanna igen».
   1.2 Klicka på «Nästa» för att gå vidare till nästa guiden.
2. I guiden "Välj åtgärd" väljer du ett system respons som ska utföras i händelse av ett integritetsbrott. Följande är tillgängliga:
   • «Alarm»: E-postmeddelande och post i granskningsspårloggen.
   • «Alarm & Self Heal»: E-postmeddelande och återställning med digital tvilling.
   2.1 Klicka på «Nästa» för att gå vidare till nästa guiden.
3. Definiera cykeltiden för integritetskontrollen i guiden steg "Ställ in cykelperioden". Det minsta intervall mellan två cykler beror på antalet enheter i blockchain.
   3.1 Klicka på «Nästa» för att fortsätta till det sista guiden steg.
4. I guiden "Skapa tvillingar" skapas blockchain automatiskt av följande rutin:
   • De valda enheterna registreras i systemet.
   • Tidssynkronisering utförs. Vid behov begärs en NTP-serveradress.
   Obs: Det rekommenderas starkt att synkronisera automatiseringsstationerna i förväg (BACnet eller NTP). Tillhandahålla en NTP-server för synkronisering av modu615-BM. Enheten stöder inte BACnet-tidssynkronisering.
   • Enhetscertifikat skapas, distribueras till enheterna och signeras.
   • Digitala tvillingar av enheterna skapas och lagras i modu615-BM.
   • De lagrade digitala tvillingarna kontrolleras (hashberäkning av blockchain).
   4.1 Klicka på "Slutför" för att starta rutinen och slutföra konfigurationen.
   → Vyn ändras från guiden till instrumentpanelen och integritetskontrollen startas..

DASHBOARD

I instrumentpanelen visas den aktuella processen och statusen för blockchain i fyra fält:

• «Last Completed Cycle Status»
Visar blockchainens status (Dataintegritet brott / Behandling / Framgång / Misslyckande / Varning / Allmän varning) och vilka enheter som inte är tillgängliga eller bryter integriteten.

• «Default Action»:
Visar typen av integritetskontroll som är konfigurerad. Tillåter att detta ändras (Alarm / Alarm & Self Heal).

• «Last Cycle» / «Next Cycle»:
Visar tiden sedan den senaste kontrollcykeln eller fram till nästa kontrollcykel. Låter kontrollen pausas (pausikonen) eller tvingas (Tvinga om omstart).

• «Chain» / «Table»:
Visar blockchainens status grafiskt (Chain) eller i tabellform (Tabell). Om displayen är grön är allt OK. Om skärmen är röd har enhetens integritet kränkt.

När du klickar på en enhet visas en dialog med två flikar: Fliken «Info» visar serienumret och typen av enhet. Fliken «Files» visar filhierarkin. Filer med integritetsbrott markeras med rött. Filer utan avvikelser visas i grönt.

EVENTS

På EVENTS-sidan listas händelser som användarinloggningar, initialiseringar och ändringar i enhetslistan med status och datum. Om «Avancerad logg» är aktiverad visas ytterligare händelsetyper, t.ex. integritet kontrollerar och återställer.
När du klickar på en händelse visas en dialog med ytterligare information.

USERS

På USERS-sidan kan användare hantera sin egen användarprofil.
Administratören (Admin) kan skapa eller ta bort användarkonton.

SETTINGS

I SETTINGS sidan kan följande inställningar göras:

- «NOTIFICATIONS SETTINGS»:
  E-mail notifikation frekventa inställningar
- «SMTP SETTINGS»:
  Inställningar för SMTP-klienttjänsten
- «MQTT SETTINGS»
  Enheten kan loggas in i en MQTT-broker som utgivare. Följande poster krävs:
  - «Broker address»: Adress på MQTT broker.
  - «Notification topic»: Klient-ID för broker för enhetens inloggning.
    Standardpost: *sauter/<serial number>*
  - «Username»
  - «Password»

  «Verify connection» knappen kan användas för att kontrollera inloggningen eller inställningen.
  Ett testmail skickas. Nyttolasten indikerar aktuell status i JSON-format.
- «HTTPS CERTIFICATE SETTINGS»:
  Välj en av följande tre certifikatinställningar:
  - «Import»: Ladda en PKCS#12 fil. IT-administratören skapar en certifikatfil i PKCS-format för användaren såväl som ett lösenord.
  - «Self Signed»: Ladda ett självgenererat certifikat (fabriksinställning). Ladda ett självgenererat certifikat (fabriksinställning). Av säkerhetsskäl rekommenderas detta certifikat endast i begränsad utsträckning
  - «CSR» (Certificate Signing Request): Låt den offentliga nyckeln skickas till en certifieringsmyndighet (CA) och undertecknas. Detta signerade certifikat ger användaren åtkomst till webbservern.

Avsedd användning

Denna produkt är endast lämplig för det avsedda syftet av tillverkaren, som beskrivs i avsnittet "Funktionsbeskrivning". Alla relaterade produktbestämmelser måste också följas
Att ändra eller konvertera produkten är inte tillåtet.

Felaktig användning

SAUTER modulo 6-systemet har inte funktionell säkerhet och är inte felsäker.
Denna produkt är inte lämplig:

- för säkerhetsfunktioner för automatisering
- i transportmedel och lagringsanläggningar enligt direktiv 37/2005
- i utomhusområden och i rum med risk för kondens
- på transportmedel, t.ex. fartyg.:

Projektering

Konfigurationen och driften av SAUTER Building Data Integrity-lösningen är baserad på följande förutsättningar:

- Alla deltagare (enheter) måste vara i samma nätverkssegment. Enhetssökningsfunktionen är baserad på samma tekniska lösning som CASE Sun.
- Alla deltagare måste vara tidssynkroniserade. NTP-tjänsten (Network Time Protocol) används för detta ändamål. Det måste säkerställas att NTP-inställningen kan fungera med CASE Sun.
  NTP-servern måste vara tillgängliga för alla deltagare hela tiden.
- Meddelandet via e-post använder SMTP. SMTP-servern måste vara tillgänglig för enheten hela tiden.

Modu615-BM stöder inte BACnet-tjänster. Tidssynkronisering, enhetssökning (Discovery) och andra BACnet-baserade funktioner stöds inte.

Följande modulo 6-enheter är kompatibla med modu615-BM:

modu680-AS	EY6AS80F021	från firmware 1.2
modu660-AS	EY6AS60F011	från firmware 1.2
modu612-LC	EY6LC12F011	

LED indikering

Följande driftsstatus för enheten visas:

Status [2]	Indikering	Beskrivning
Fast grön		OK, normal drift
Blinkande grön		Identifiering via CASE Sun
Fast orange		Start-up läge, kommunikation håller på att skapas
Blinkande orange		Det interna reservbatteriet måste bytas ut
Fast röd		Ingen konfiguration
Blinkande röd		Konfiguration aktiv
Snabbt blinkande röd		Internt fel i enheten

Parametrering

De grundläggande inställningarna som IP-inställningar utförs med CASE Sun.

Initiering

En initialisering (radera konfiguration, ladda fabriksinställningar) av modu615-BM kan utföras med CASE Sun.

Firmware / uppdatering

Modu615-BM levereras med den senaste firmware. Uppdateringar kan installeras via CASE Sun.

Notera
Använd bara enheten med den senaste firmware. Innan idrifttagning, kontrollera firmwareversionen och utför en uppdatering vid behov.
Versionen av den installerade firmware kan läsas via CASE Sun.

Intern klocka

En realtidsklocka (RTC) är integrerad i enheten. Datum, tid och tidszon ställs in i den anslutna automatiseringsstationen. Den interna klockan är skyddad mot strömavbrott av ett batteri.

Batteri

Ett litiumbatteri (pluggbar knappcell) säkerställer att realtidsklockan för tidsprogram (schemaläggare / kalender) fortsätter att gå i händelse av strömavbrott. Batterispänningen övervakas av enheten. Batteriet får bara bytas ut när enheten är frånkopplad från strömförsörjningen. Under batteribyte går den aktuella tiden för den interna klockan bort och måste återställas.
Följ säkerhetsinstruktionerna och anvisningarna i monteringsanvisningarna för enheten. Om det behövs, kontakta SAUTER Service för att byta ut batteriet.

Tekniska data för batteriet

Typ (standard)	CR2032 lithium button-cell
Nominell spänning	3 V
Kapacitet	210 mAh
Mått	20 mm × 3.2 mm

Litiumbatteriet ska bytas ut efter fem till tio år. Det får bara ersättas av utbildad specialistpersonal.

VARNING!
Risk of explosion if the battery is short-circuited during replacement.
► Använd endast isolerade verktyg när du byter batteri.

[2] *LED blink: 500 ms tänd, 500 ms släkt*
LED snabb blink: 100 ms tänd, 100 ms släkt

Uppförande vid strömavbrott

Vid strömavbrott stängs enheten av på rätt sätt. När strömmen återgår slås systemet på enligt prioritet. Uppförandet för att stänga av och slå på definieras autonomt av enheten.

Notera

Strömavbrott i strömförsörjningen EY-PS021F021 på primärsidan (230 V AC) som håller mindre än 100 ms överbryggas utan att stängas av eller andra konsekvenser. Systemet fortsätter att köras i normalt läge.

Skyddsmekanismer på applikationsnivå

Modu615-BM har följande skyddsmekanismer:

Åtkomsträttigheter

Åtkomst till webbservern skyddas av ett användarnamn och lösenord. Första gången en användare loggar in till webbservern måste standardlösenordet ändras. Användaradministration och inställning av åtkomst rättigheter är systemoperatörens ansvar.

Datasäkerhet

Användardata lagras i krypterad form.

Kommunikationssäkerhet

Internetkommunikation är krypterad där det är tekniskt möjligt. HTTPS- och SMTP-protokollen är krypterade. Åtkomst via HTTP omdirigeras automatiskt till HTTPS.

Systemet tillåter bara kommunikation via auktoriserade portar. Alla andra portar blockeras av den inbyggda brandväggen. Dessutom kan en autorisationslista med godkända enheter skapas.

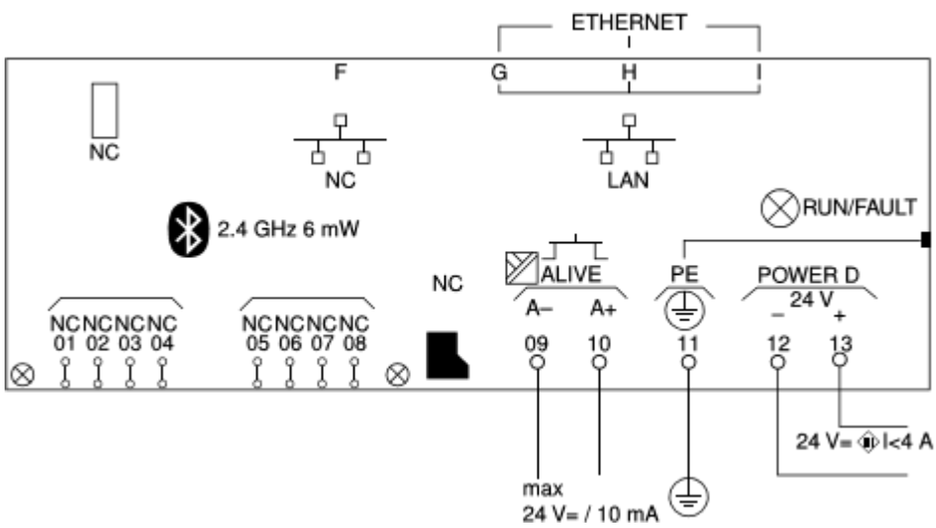
Firmware-uppdatering

Endast firmwareuppdateringar signerade av SAUTER kan installeras.

Avyttrande

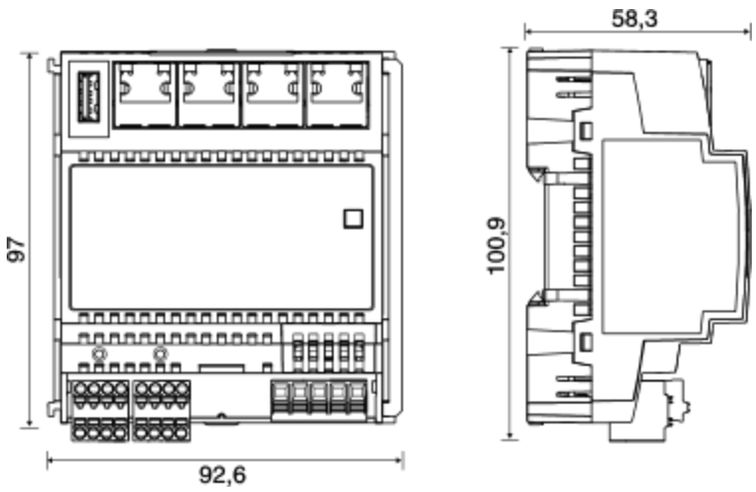
När du kasserar produkten ska du följa de gällande lokala lagarna. Mer information om material finns i deklarationen om material och miljö för denna produkt.

Anslutningsschema



Måttritning

Alla mått i millimeter.



Fr. Sauter AG
Im Surinam 55
CH-4058 Basel
Tel. +41 61 - 695 55 55
www.sauter-controls.com