EY6BM15 : Building Data Integrity Manager, modu615-BM

EY6BM15F011

Caractéristiques

- Produit faisant partie de la famille de systèmes SAUTER modulo 6
- Solution basée sur une blockchain pour contrôler l'intégrité des données des unités de gestion locale
- Communication cryptée dans le réseau d'automatisation de bâtiments
- Serveur web intégré pour mise en service, visualisation, commande et gestion des utilisateurs locales
- Notification et isolement du dispositif ou auto-réparation en cas de violation de l'intégrité des données
- Client NTP pour la synchronisation horaire et la protection des certificats
- Journal utilisateur

Caractéristiques techniques

Alimentation électrique		
	Tension d'alimentation	24 V= ± 10 %
	Puissance absorbée	≤ 2 W sans charge
	Puissance dissipée	≤ 2 W sans charge
	Courant d'enclenchement maximal[1)]	≤ 2 A, ≤ 10 ms
Valeurs caractéristiques		
	Raccordement	Borne à ressort à 5 pôles, enfichable, 0,5...1,5 mm^2 (rigide) 0,5...2,5 mm^2, au moins 8 mm de dénudage isolant
	Pile (mise en mémoire tampon RTC)	CR2032, enfichable
	Terminal de mise à la terre	Contact à ressort contre rail DIN et borne PE
Conditions ambiantes		
	Température de service	0…45 °C
	Température de stockage et de transport	−20…70 °C
	Humidité ambiante	10…90 % HR sans condensation
Fonction		
	Nombre d'esclaves	Max. 100
	Fonction de hachage	SHA-256 (pour TLS)
Architecture		
	Processeur	ARM 8, 1 GHz
	RAM (mémoire vive)	512 Mo (DDR3)
	Flash	512 MB
	Serveur web embarqué	moduWeb Unity
	Système d'exploitation	Linux intégré
Interfaces, communication		
	Communication	Via SMTP, NTP, HTTPS, MQTT
Réseau Ethernet	Réseau Ethernet	3 connecteurs femelles RJ45
	10/100 BASE-T(X) Switched	10/100 Mbits/s
	Utilisation	Réseau de blockchains
Structure constructive		
	Montage	Sur rail métallique DIN 35 × 7,5/15 selon EN 60715. Boîtier pour montage en série selon DIN 43880
	Dimensions l × H × P	92,6 (5 UD) × 100,9 × 58,3 mm
	Poids	260 g

1) *Valeur de mesure avec alimentation EY-PS021F021*

Normes, directives		
	Indice de protection	Raccordements et bornes : IP00 (EN 60730) À l'avant dans la découpe DIN : IP30 (EN 60730)
	Classe de protection	I (EN 60730-1)
	Classe climatique	3K3 (IEC 60721)
	Classe de logiciel	A (EN 60730-1, annexe H)
	Classe énergétique	I à VIII = jusqu'à 5 % selon (UE) n° 811/2013, 2010/30/UE, 2009/125/CE
Conformité CE selon	Directive CEM 2014/30/UE	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
	Directive basse tension 2014/35/UE	EN 60730-1, EN 60730-2-9, EN 62479
	Directive RoHS 2011/65/UE	EN IEC 63000
	Directive RED 2014/53/UE	EN 300328 (V2.1.1)

Aperçu des types	
Modèle	Caractéristiques
EY6BM15F011	Building Data Integrity Manager et serveur web

Manuels

Numéro de document	Langue	Titre
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 du fonctionnement

Le modu615-BM (Building Data Integrity Manager et serveur web) vérifie périodiquement l'intégrité des données statiques dans un groupe prédéfini d'unités de gestion locales compatibles. Ce contrôle est effectué à l'aide d'une chaîne d'intégrité (blockchain). Si une violation de l'intégrité est détectée, elle est signalée par e-mail ou par MQTT et consignée dans le journal utilisateur. Si l'appareil affecté est configuré de la sorte, le gestionnaire peut le restaurer automatiquement (Self Healing). Cette restauration est rendue possible grâce au jumeau numérique de l'unité de gestion locale concernée, créé lors de l'initialisation et utilisé pour écraser les données corrompues.
Le serveur web intégré au modu615-BM n'est accessible que via HTTPS (redirection automatique depuis http). L'accès est protégé par un nom d'utilisateur et un mot de passe. La sécurité peut être renforcée par une authentification à deux facteurs (réception du code par courrier électronique et saisie).

Remarque
L'authentification à deux facteurs nécessitant une communication par e-mail, n'activez pas la fonction si vous ne pouvez pas recevoir d'e-mails.

Le serveur web permet de créer plusieurs comptes d'utilisateurs dans deux rôles standardisés : administrateur et utilisateur.

Remarque
Un certificat auto-signé est utilisé pour la connexion initiale au serveur web. Le certificat déclenche le message d'alarme « Non sécurisé » dans le navigateur.
Contactez votre administrateur informatique pour obtenir un certificat validé par une AC.

Interfaces utilisateur des serveurs web

L'accès au serveur web est protégé par un nom d'utilisateur et un mot de passe. Une fois la connexion réussie, le tableau de bord s'ouvre par défaut. Sur le côté gauche se trouve la barre de navigation avec les interfaces suivantes :

- DASHBOARD
- WIZARD
- EVENTS
- USERS
- SETTINGS

En cliquant sur le symbole dans le coin supérieur droit, un menu avec les fonctions suivantes s'ouvre :

- Activation ou désactivation du mode nuit
- Affichage de l'utilisateur connecté et lien vers le profil de l'utilisateur
- Déconnexion du serveur web

WIZARD

La blockchain est créée et le contrôle d'intégrité est lancé à l'aide d'un processus de configuration guidée (assistant) en quatre étapes :

1. À l'étape « Select device », sélectionnez les appareils devant participer au contrôle d'intégrité.
   → Après l'ouverture de l'assistant, le réseau est automatiquement scanné (zero-config) et les appareils compatibles sont affichés. L'ordre des appareils peut être modifié par glisser-déposer.
   1.1. Sélectionner des dispositifs pour le contrôle d'intégrité. L'unité de gestion modu615-BM (HOST) doit impérativement être incluse. La fonction « Select all » permet de sélectionner tous les appareils répertoriés en une seule étape. Le bouton « Rescan » permet de scanner à nouveau le réseau.
   1.2. Cliquer sur « Next » pour passer à l'étape suivante de l'assistant.
2. À l'étape « Select action », sélectionner une réaction du système à exécuter en cas de violation de l'intégrité. Sélections possibles :
   - « Alarm » : Notification par e-mail et inscription dans le journal de la piste d'audit.
   - « Alarm & Self Heal » : Notification par e-mail et récupération à l'aide du jumeau numérique.

   2.1. Cliquer sur « Next » pour passer à l'étape suivante de l'assistant.
3. À l'étape « Set cycle periode », définir la durée du cycle souhaitée pour le contrôle d'intégrité. L'intervalle minimal entre deux cycles dépend du nombre d'appareils dans la blockchain.
   3.1. Cliquer sur « Next » pour passer à la dernière étape de l'assistant.
4. À l'étape « Create twins », la blockchain est créée automatiquement en utilisant la routine suivante :
   - Les appareils sélectionnés sont enregistrés dans le système.
   - La synchronisation horaire est effectuée. Si nécessaire, une adresse de serveur NTP est interrogée.
     Remarque : Il est fortement recommandé de synchroniser les unités de gestion locale à l'avance (BACnet ou NTP). Fournir un serveur NTP pour la synchronisation du modu615-BM. L'appareil ne prend pas en charge la synchronisation horaire BACnet.
   - Les certificats des appareils sont créés, distribués aux appareils et signés.
   - Les jumeaux numériques des appareils sont créés et stockés dans le modu615-BM.
   - Les jumeaux numériques stockés sont contrôlés (calcul du hachage de la blockchain).

   4.1 Cliquer sur « Finish » pour lancer la routine et terminer la configuration.
   → L'affichage passe de l'assistant au tableau de bord et le contrôle d'intégrité est lancé.

DASHBOARD

Le tableau de bord affiche le processus actuel ainsi que le statut de la blockchain dans quatre champs :

- « Last Completed Cycle Status » :
  Indique l'état de la blockchain (Data integrity breach / Processing / Success / Failure / Warning / General warning) ainsi que les dispositifs qui ne sont pas accessibles ou qui violent l'intégrité.
- « Default Action » :
  Indique le type de contrôle d'intégrité configuré. Permet de modifier ce dernier (Alarm / Alarm & Self Heal).
- « Last Cycle » / « Next Cycle » :
  Affiche le temps écoulé depuis le dernier cycle de contrôle ou jusqu'au prochain cycle de contrôle. Permet d'arrêter (symbole pause) ou de forcer le contrôle (Force restart).

- « Chain » / « Table » :
  Affiche l'état de la blockchain sous forme graphique (Chain) ou sous forme de tableau (Table). Si l'affichage est vert, tout va bien. L'affichage rouge signifie que l'intégrité d'un appareil a été violée. Cliquer sur un appareil pour faire apparaître une boîte de dialogue avec deux onglets : L'onglet « Info » affiche le numéro de série et le type d'appareil. L'onglet « Files » affiche la hiérarchie des fichiers. Les fichiers dont l'intégrité a été violée sont indiqués en rouge. Les fichiers sans anomalies sont affichés en vert.

EVENTS

La page EVENTS liste les événements tels que les connexions d'utilisateurs, les initialisations et les modifications dans la liste des appareils avec l'état et la date. Lorsque la fonction « Advanced log » est activée, d'autres types d'événements sont affichés, comme les contrôles d'intégrité et les restaurations.
Lorsque vous cliquez sur un événement, un dialogue contenant des informations complémentaires apparaît.

USERS

La page USERS vous permet de gérer votre propre profil utilisateur.
L'administrateur (Admin) peut créer ou supprimer des comptes utilisateur.

SETTINGS

La page SETTINGS vous permet d'effectuer les réglages suivants :

- « NOTIFICATIONS SETTINGS » :
  Réglages de la fréquence de notification par e-mail
- « SMTP SETTINGS » :
  Réglages du service client SMTP
- « MQTT SETTINGS »
  Permet de connecter l'appareil à un Broker MQTT en tant que Publisher. Les informations suivantes sont requises :
  - « Broker address » : Adresse du Broker MQTT.
  - « Notification topic » : Identification du client du Broker pour la connexion de l'appareil. Entrée standard : *sauter/<numéro de série>*
  - « Username »
  - « Password »

  Le bouton « Verify connection » peut être utilisé pour vérifier la connexion ou les réglages. Un e-mail de test est envoyé.
  La charge utile (Payload) indique l'état actuel au format JSON.
- « HTTPS CERTIFICATE SETTINGS » :
  Sélectionner l'un des trois paramètres de certificat suivants :
  - « Import » : Chargement d'un fichier PKCS#12 L'administrateur informatique crée à cet effet un fichier de certificat au format PKCS et un mot de passe pour l'utilisateur.
  - « Self Signed » : Chargement d'un certificat auto-créé (réglage d'usine). Pour des raisons de sécurité, ce certificat n'est recommandé que sous certaines conditions.
  - « CSR » (Certificate Signing Request) : Envoyer la clé publique à une autorité de certification (AC) et la faire signer. Ce certificat signé donne à l'utilisateur accès au serveur web.

Utilisation conforme

Ce produit est conçu uniquement pour l'emploi prévu par le fabricant, décrit à la section « Description du fonctionnement ».
Le respect de la législation relative au produit en fait également partie. Les modifications ou transformations ne sont pas autorisées.

Utilisation non conforme

Le système SAUTER modulo 6 ne possède ni sécurité fonctionnelle, ni sécurité intégrée.
Le produit ne convient pas :

- pour les fonctions de sécurité de l'automatisation
- dans les dispositifs de transport et les installations de stockage conformément au règlement 37/2005
- à l'extérieur et dans les pièces présentant un risque de condensation

- sur les moyens de transport, par exemple les navires.

Remarques concernant l'étude de projet

La configuration et le fonctionnement de la solution SAUTER Building Data Integrity sont basés sur les exigences suivantes :

- Tous les participants (appareils) doivent se trouver dans la même zone du réseau. La fonction de recherche d'appareil est basée sur la même solution technique que CASE Sun.
- Tous les participants doivent disposer de la même synchronisation horaire. Le service NTP (Network Time Protocol) est utilisé à cette fin. S'assurer que le paramètre NTP fonctionne correctement avec CASE Sun. Le serveur NTP doit être accessible à tous les participants à tout moment.
- La notification par e-mail fait appel au protocole SMTP. Le serveur SMTP doit être accessible pour l'appareil à tout moment.

Le modu615-BM ne prend pas en charge les services BACnet. La synchronisation horaire, la recherche d'appareils (Discover) et d'autres fonctions basées sur BACnet ne sont pas prises en charge.

Les appareils modulo 6 suivants sont compatibles avec le modu615-BM :

modu680-AS	EY6AS80F021	à partir du micrologiciel 1.2
modu660-AS	EY6AS60F011	à partir du micrologiciel 1.2
modu612-LC	EY6LC12F011	

Voyants LED

Les états de fonctionnement de l'appareil suivants sont affichés :

État [2)]	Affichage	Description
Vert en permanence		OK, fonctionnement normal
Vert clignotant		Identification via CASE Sun
Orange en permanence		Mode démarrage, établissement de la communication
Orange clignotant		La batterie de sauvegarde interne doit être remplacée
Rouge en permanence		Pas de configuration
Rouge clignotant		Configuration active
Rouge clignotant rapidement		Erreur interne de l'appareil

Paramétrage

Les réglages de base tels que les paramètres IP sont effectués avec CASE Sun.

Initialisation

Le modu615-BM peut être initialisé (suppression de la configuration, chargement des réglages d'usine) en utilisant CASE Sun.

Micrologiciel/mise à jour

Le modu615-BM est fourni avec le micrologiciel le plus récent. Les mises à jour peuvent être installées via CASE Sun.

---

2) *LED clignotante : 500 ms allumée, 500 ms éteinte*
LED clignotant rapidement : 100 ms allumée, 100 ms éteinte

Remarque
Mettre l'appareil en service uniquement avec le micrologiciel le plus récent. Avant la mise en service, vérifier la version du micrologiciel et effectuer si nécessaire une mise à jour.
La version du micrologiciel installé peut être consultée depuis CASE Sun.

Horloge interne

Une horloge temps réel (Real Time Clock, RTC) est intégrée dans l'appareil. La date, l'heure et le fuseau horaire sont réglés dans l'unité de gestion locale connectée. L'horloge interne est protégée contre les coupures de courant grâce à une pile.

Pile

Une pile au lithium (pile bouton enfichable) assure la sauvegarde de l'horloge temps réel pour les programmes horaires (Scheduler, Calendar) en cas de coupure de tension.
La tension de la pile est surveillée par l'appareil.
La pile ne doit être remplacée que lorsque l'appareil est hors tension. Une fois la pile remplacée, l'heure de l'horloge interne est effacée et doit être de nouveau réglée.
Respecter les consignes de sécurité et les instructions de montage de l'appareil. Si nécessaire, contacter le service après-vente SAUTER pour remplacer la pile.

Caractéristiques techniques de la pile

Type (standard)	Pile bouton au lithium CR2032
Tension nominale	3 V
Capacité	210 mAh
Dimensions	20 mm × 3,2 mm

Il est recommandé de remplacer la pile au lithium tous les cinq à dix ans. Le remplacement ne doit être effectué que par un personnel spécialement formé.

AVERTISSEMENT !
Risque d'explosion en cas de court-circuit de la batterie lors du remplacement.
►Utilisez uniquement des outils isolés pour remplacer la batterie.

Consignes en cas de coupure secteur

Les coupures de courant signifient que l'appareil s'éteint de manière ordonnée. Lors du retour de la tension secteur, l'activation s'effectue selon les priorités. Le comportement lors de la désactivation et de l'activation est défini de manière autonome par l'appareil.

Remarque
Les coupures secteur de l'alimentation à découpage EY-PS021F021 côté primaire (230 V AC) d'une durée inférieure à 100 ms sont surmontées sans désactivation ni autres conséquences. L'installation continue de fonctionner en mode de fonctionnement normal.

Mécanismes de protection au niveau de l'application

Le modu615-BM dispose des mécanismes de protection suivants :

Droit d'accès

L'accès au serveur web est protégé par un nom d'utilisateur et un mot de passe. Le mot de passe par défaut doit être modifié la première fois que vous vous connectez au serveur web. L'exploitant du système est en charge de la gestion des utilisateurs et du paramétrage des droits d'accès.

Sécurité des données

Les données utilisateurs sont cryptées avant d'être enregistrées.

Sécurité des communications

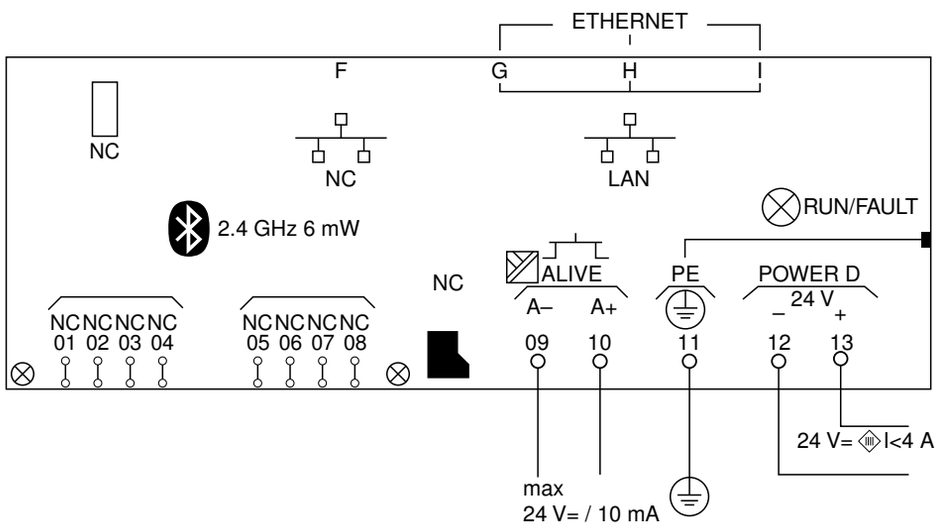
Si cela est techniquement possible, la communication Internet est cryptée. Les protocoles HTTPS et SMTP sont cryptés. L'accès via HTTP est automatiquement redirigé vers HTTPS.
Le système ne permet la communication que via des ports autorisés. Tous les autres ports sont bloqués par le pare-feu intégré. Il est également possible de créer une liste d'autorisations avec des appareils approuvés.

Mise à jour du micrologiciel
Seules les mises à jour du micrologiciel signées SAUTER peuvent être installées.

Élimination

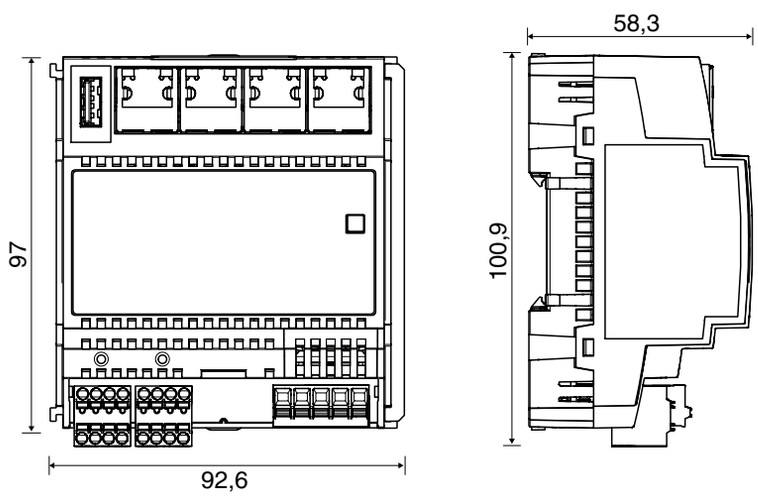
Lors de l'élimination, il faut respecter le cadre juridique local actuellement en vigueur.
Vous trouverez des informations complémentaires concernant les matériaux dans la « Déclaration matériaux et environnement » relative à ce produit.

Schéma de raccordement



Plan d'encombrement

Toutes les mesures sont exprimées en millimètres.



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