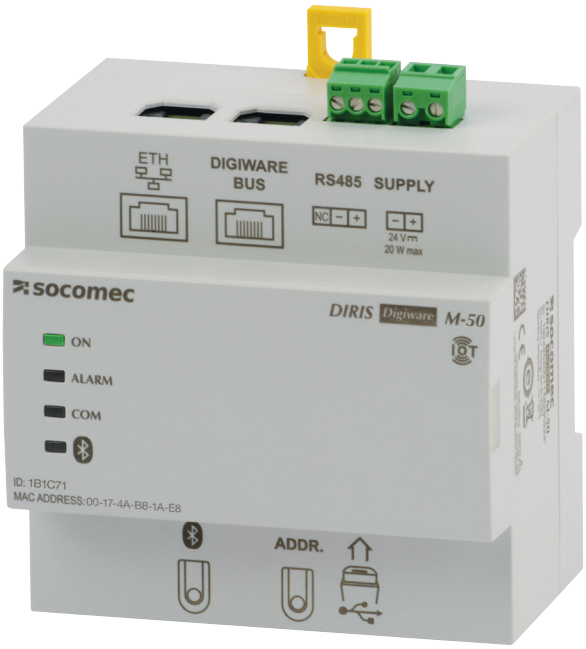
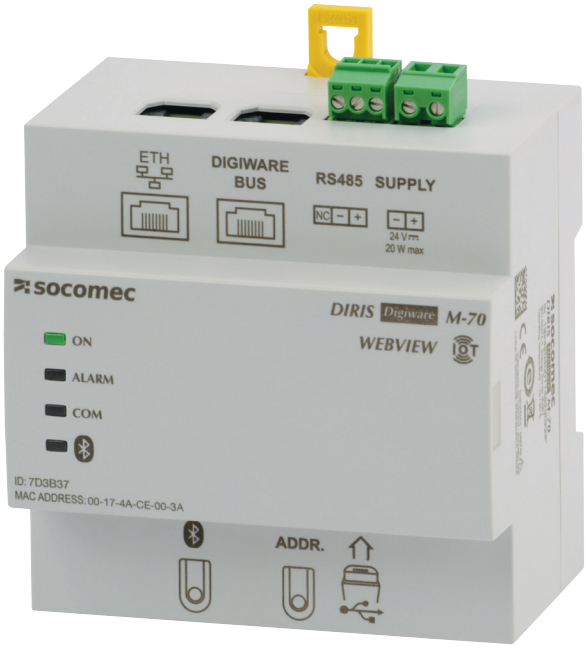
MANUEL D'INSTALLATION ET D'UTILISATION

FR

Passerelle de communication multifonction

DIRIS Digiware M-50 & M-70





socomec
Innovative Power Solutions

INDEX

1. DOCUMENTATION 4

2. DANGERS ET AVERTISSEMENTS 4
   2.1. Risque d'électrocution, de brûlure ou d'explosion 4
   2.2. Risque de détérioration du produit 5
   2.3. Responsabilité 5

3. OPÉRATIONS PRÉLIMINAIRES 6

4. PRÉREQUIS 6

5. RECOMMANDATIONS ET MEILLEURES PRATIQUES EN MATIÈRE DE CYBERSÉCURITÉ* 7

6. INTRODUCTION 9
   6.1. Gamme 9
   6.2. Introduction aux DIRIS Digiware M-50 & M-70 10
      6.2.1. Introduction au DIRIS Digiware M-50 10
      6.2.2. Introduction à la DIRIS Digiware M-70 11
   6.3. Affichage LED sur la face avant 12
   6.4. Dimensions (mm / in) 12

7. MONTAGE 13
   7.1. Recommandations et sécurité 13
   7.2. Montage sur rail DIN 13

8. CÂBLAGE DU SYSTÈME 14
   8.1. Architectures de communication 15
   8.2. Câblage des DIRIS Digiware M-50/M-70 15
      8.2.1. Maître RS485 15
      8.2.2. Esclave RS485 15

9. BLUETOOTH LOW ENERGY 15

10. AUTO-DÉTECTION DES DISPOSITIFS ESCLAVES 16

11. CONFIGURATION VIA LE SERVEUR WEB EMBARQUÉ DANS LES PASSERELLES M-50/M-70 18
   11.1. Profils utilisateurs 18
   11.2. Profil Admin 21
      11.2.1. Menu « Équipements » 21
      11.2.2. Menu « Protocoles » 24
   11.3. Profil Cybersécurité 28
      11.3.1. Menu Cybersécurité 28
      11.3.2. Onglet « Politique de sécurité » 29
      11.3.3. Onglet « HTTPS » 30
      11.3.4. Onglet « CAs (FTPS/SMTPS) » 30
      11.3.5. Onglet « Pare-feu » 31
      11.3.6. Mise à jour du firmware de la passerelle M-50/M-70 31
   11.4. WEBVIEW-M 32

12. CONFIGURATION VIA LE LOGICIEL EASY CONFIG SYSTEM 33
   12.1. Mode de connexion USB 33
   12.2. Mode de connexion Ethernet 34

13. ALARMES 36
14. CHECKLIST EN 10 ÉTAPES POUR LA MISE EN SERVICE DU SYSTÈME DIGIWARE 37
15. CARACTÉRISTIQUES TECHNIQUES DES DIRIS DIGIWARE M-50/M-70 38
15.1. Caractéristiques mécaniques 38
15.2. Caractéristiques communication 38
15.3. Caractéristiques électriques 38
15.4. Caractéristiques environnementales 39
15.5. Caractéristiques CEM 39
ANNEXE I. COMMUNICATION SNMP AVEC LE DIRIS DIGIWARE M-50/M-70 40
Annexe I - 1. Généralités sur SNMP 40
Annexe I - 2. Fonctions de SNMP prises en charge 41
Annexe I - 3. Versions de SNMP prises en charge 41
Annexe I - 4. Ports SNMP 42
Annexe I - 5. Extraction des données à l'aide du fichier MIB de DIRIS Digiware M-50/M-70 42
Annexe I - 6. Configuration SNMP via Easy Config System 44
Annexe I - 7. Configuration SNMP via le serveur Web embarqué 45
ANNEXE II. COMMUNICATION BACNET AVEC DIRIS DIGIWARE M-50/M-70 46
Annexe II - 1. Généralités sur BACnet 46
Annexe II - 2. Objets BACnet 46
Annexe II - 3. Services BACnet 51
Annexe II - 4. Configuration du protocole BACnet IP via Easy Config System 52
Annexe II - 5. Configuration du protocole BACnet IP depuis le serveur Web embarqué 53
ANNEXE III. CONFIGURATION DES EXPORTS FTP 54
Annexe III - 1. Activation du serveur FTP 54
Annexe III - 2. Configuration de la planification FTP 56
Annexe III - 3. Comprendre le fichier .csv exporté en mode EMS 57
ANNEXE IV. RECHERCHER ET AJOUTER LE CA (AUTORITÉ DE CERTIFICATION) D'UN SERVEUR À UNE PASSERELLE DIRIS DIGIWARE M-50/M-70 58

1. DOCUMENTATION

Toute la documentation relative aux DIRIS Digiware M-50 et M-70 est disponible sur le site Internet de SOCOMEC :
www.socomec.fr/fr/centre-de-telechargement

Notices complémentaires

Des notices complémentaires liées au système DIRIS Digiware sont disponibles sur le site de Socomec :

Notice d'utilisation	Référence
DIRIS Digiware - Système de surveillance de l'énergie et capteurs de courant associés	542875
WEBVIEW-M - Serveur web de visualisation embarqué dans DIRIS Digiware M & D	551295
Easy Config System - Logiciel de configuration	551765
Product Upgrade Tool - Logiciel de mise à jour firmware	545534

2. DANGERS ET AVERTISSEMENTS

Le terme « dispositif » utilisé dans les paragraphes suivants désigne les deux DIRIS Digiware M-50 et M-70.
Le montage, l'utilisation, l'entretien et la maintenance de cet équipement ne doivent être effectués que par des professionnels qualifiés dûment formés.

Le non-respect des instructions de la présente notice ne saurait engager la responsabilité de SOCOMEC.

2.1. Risque d'électrocution, de brûlure ou d'explosion

	Attention : risque de choc électrique	Réf. ISO 7000-0434B (2004-01)
	Attention : consulter la documentation qui accompagne le produit à chaque fois que ce symbole apparaît.	Réf. ISO 7000-0434B (2004-01)

- Seul du personnel dûment autorisé et qualifié peut travailler sur ou installer/désinstaller le dispositif.
- Les instructions sont applicables en association avec les instructions spécifiques du dispositif.
- Le dispositif est strictement réservé à l'usage pour lequel il a été conçu comme indiqué dans les instructions.
- N'utiliser le dispositif qu'avec des accessoires autorisés ou recommandés par SOCOMEC.
- Avant de procéder à l'installation, à l'entretien, au nettoyage, au démontage, au raccordement ou à des travaux de maintenance, le dispositif et le système doivent être déconnectés du secteur pour éviter toute électrocution et tout endommagement du système et du dispositif.
- Ce dispositif n'a pas été conçu pour être réparé par l'utilisateur.
- Pour toute question à propos de la mise au rebut du dispositif, contacter SOCOMEC.

	Ne PAS enserrer ou retirer de conducteurs NON ISOLÉS sous TENSION DANGEREUSE pouvant entraîner un choc électrique, une brûlure ou un arc électrique. Réf. CEI 61010-2-032

Le non-respect des instructions du dispositif et de ces informations de sécurité peut causer des blessures corporelles, des chocs électriques, des brûlures, la mort ou des dommages aux biens.

2.2. Risque de détérioration du produit

	Attention : risque de choc électrique	Réf. ISO 7000-0434B (2004-01)
	Attention : consulter la documentation qui accompagne le produit à chaque fois que ce symbole apparaît.	Réf. ISO 7010-W001 (2011-05)

Afin d'assurer le bon fonctionnement du produit, veiller à respecter :

- Le dispositif est installé correctement.
- La tension d'alimentation auxiliaire indiquée sur le dispositif est respectée : 24 VDC ± 10 %.
- Une alimentation SOCOMEC 230 VAC / 24 VDC (P15 réf. 4829 0120) ou une alimentation 24 VDC max. 20 W de classe 2 / TBTS est utilisée.
- En cas d'utilisation d'une alimentation autre que SOCOMEC, le dispositif doit être protégé par un fusible 1 A / 24 VDC.
- Utiliser uniquement des câbles RJ45 SOCOMEC pour raccorder les modules via le bus Digiware. Lorsque la température ambiante dépasse +50°C, la température nominale minimale du câble en cuivre à raccorder à la borne doit être de +85°C.
- Le dispositif ne doit pas être nettoyé.
- Ne pas installer le dispositif à l'extérieur.

Le non-respect de ces précautions pourrait gravement endommager le dispositif.

2.3. Responsabilité

- Le montage, le raccordement et l'utilisation doivent être effectués conformément aux normes d'installation actuellement en vigueur.
- Le dispositif doit être installé conformément aux consignes données dans cette notice.
- Le non-respect des consignes d'installation de cette unité peut compromettre la protection intrinsèque du dispositif.
- Le dispositif doit être placé dans un système qui soit à son tour conforme aux normes applicables et aux règlementations de sécurité du pays d'installation.
- Tout câble devant être remplacé doit obligatoirement l'être par un câble de mêmes caractéristiques nominales.
- En dépit de tous ses efforts visant à améliorer la qualité lors de la préparation de cette notice, des erreurs ou des omissions restent possibles, sans engager la responsabilité de SOCOMEC.

3. OPÉRATIONS PRÉLIMINAIRES

Pour assurer la sécurité du personnel et du produit, lire attentivement le contenu de ces instructions avant l'installation.

Vérifier les points suivants à la réception du colis contenant l'équipement :

- l'emballage doit être en bon état,
- le dispositif ne doit pas avoir été endommagé pendant le transport,
- la référence du dispositif correspond à votre commande,
- l'emballage contient l'équipement doté des borniers amovibles et un Guide de démarrage rapide.

4. PRÉREQUIS

Avant la mise en service de la passerelle DIRIS Digiware M-50/M-70 vérifier qu'elle utilise la version firmware la plus à jour. Les dernières versions firmware sont disponibles sur le site Web SOCOMEC.

La mise à jour firmware s'effectue à l'aide du logiciel Product Upgrade Tool, en raccordant un ordinateur portable au port Micro-USB de la passerelle M-50/M-70.

Elle peut également se faire à distance, directement depuis leur serveur web embarqué.

5. RECOMMANDATIONS ET MEILLEURES PRATIQUES EN MATIÈRE DE CYBERSÉCURITÉ*

Comme tout dispositif connecté à un réseau Ethernet, la passerelle DIRIS Digiware M-50/M-70 doit être protégé contre tous risques de cyberattaque ou de perte/destruction de données.

(*) Nos passerelles M-50/M-70 assurent des fonctions de cybersécurité pour empêcher ces attaques et aider les utilisateurs à mettre en œuvre et garantir la protection informatique la plus robuste possible. Les paragraphes suivants énoncent certaines recommandations. Vérifiez qu'elles s'inscrivent dans la politique de sécurité de votre entreprise :

- **Sensibilisation à la politique de sécurité :** Les utilisateurs et administrateurs des passerelles DIRIS Digiware M-xx et de WEBVIEW-M doivent être sensibilisés aux pratiques appropriées de sécurité informatique (information et respect de la politique de sécurité d'entreprise, gestion des procédures d'authentification, fiabilité des mots de passe, gestion des sessions en ligne, risques de hameçonnage, …) et y être dûment formés.
- **Sécurité du réseau :** L'architecture du système informatique doit permettre de préserver les ressources, en segmentant le réseau en fonction du degré de sensibilité et en utilisant différents dispositifs de protection (pare-feu, zone démilitarisée, VLAN, antivirus réseau, etc.).

Contribution des passerelles DIRIS Digiware M-50/M-70 à la cybersécurité :

Obligation aux utilisateurs d'utiliser des versions sécurisées des protocoles de communication standard :

- FTPS : exportation sécurisée des données
- SMTPS : notification sécurisée des alarmes par e-mail
- SNMPv3 : version sécurisée du protocole de communication SNMP
- HTTPS : navigation sécurisée sur le serveur Web (WEBVIEW-M) en téléchargeant les certificats TLS/SSL

> Pour plus d'informations sur l'ajout des certificats numériques, voir les paragraphes 11.3.3 et 11.3.4.

Pare-feu conçu pour surveiller et contrôler le trafic entrant et sortant : les passerelles DIRIS Digiware M-50/M-70 sont ainsi protégées en cas d'attaques par déni de service (inondation) afin de garantir la continuité de service de la passerelle.

> Pour plus d'informations sur la configuration de la protection pare-feu, voir le paragraphe 11.3.5.

- **Sécurité des dispositifs :** La sécurité dépend de l'environnement du réseau, mais également du comportement de l'utilisateur. En termes d'environnement, il est vivement recommandé d'appliquer des mesures de protection élémentaires (filtrage des stations autorisées par adresse MAC, ouverture de ports de service, choix d'applications autorisées, etc.). Il convient de faire preuve d'une plus grande prudence pour gérer les supports mobiles (disque dur externe, clé USB, équipement de communication sans fil, etc.). Enfin, en termes de serveur comme la passerelle DIRIS Digiware M-50/M-70, elle doit être protégée en contrôlant et en limitant l'accès physique aux locaux et aux armoires qui abritent le dispositif.

Contribution des passerelles DIRIS Digiware M-50/M-70 à la cybersécurité :

Les passerelles DIRIS Digiware M-50/M-70 réduisent l'exposition aux attaques en bloquant ou en limitant l'accès à certains périphériques et services qui ne sont pas essentiels pour l'utilisateur (USB, RS485 etc.).

> Pour plus d'informations sur la politique de sécurité des passerelles, voir le paragraphe 11.3.2.

De plus, les applications de logiciel et de serveur Web sont signées par une clé asymétrique, afin de garantir que toute mise à jour logicielle utilisera la signature de concordance correcte pour permettre la mise à niveau du dispositif. Ce qui empêche toute utilisation non conforme du dispositif, telle que prévue par SOCOMEC (par exemple, en téléchargeant un logiciel factice) et garantit que le logiciel ne sera pas infecté par des virus.

- **Sécurité des données :** La sécurité des données couvre plusieurs aspects, en particulier la confidentialité, l'intégrité, l'authenticité et la disponibilité des données. Il convient d'être particulièrement vigilant en ce qui concerne la sécurité des données et les procédures d'archivage sur des dispositifs de sauvegarde, en interne comme en externe à l'entreprise.

Contribution des passerelles DIRIS Digiware M-50/M-70 à la cybersécurité :

Il est possible d'exporter des données, comme des index d'énergie, des courbes de charge et des mesures historiques, manuellement ou automatiquement, aux fins de sauvegarde.

Il est également possible d'enregistrer la topologie (cartographie d'esclaves connectés à la passerelle M-50/M-70) depuis le serveur Web embarqué, ainsi que le fichier de configuration depuis le logiciel Easy Config System.

La confidentialité est garantie par le cryptage AES 256 bits (AES 256) pour les données personnelles, comme les mots de passe accompagnant le produit. Ceci signifie qu'il faudrait 2256 combinaisons pour déchiffrer la clé de cryptage.

- **Gestion des accès et des authentifications :** La gestion des accès aux ressources et aux données est un aspect essentiel de la politique de sécurité des systèmes informatiques. Chaque utilisateur doit disposer d'un compte et de droits d'accès correspondant à son profil. L'accès aux ressources est contrôlé par un processus d'authentification des utilisateurs sur la base, au minimum, d'un nom d'utilisateur et d'un mot de passe sécurisés. La procédure de gestion des mots de passe, qui spécifie la modification systématique des mots de passe par défaut et leur période de validité, fait partie intégrante de la politique de sécurité informatique.

Contribution des passerelles DIRIS Digiware M-50/M-70 à la cybersécurité :

Plusieurs profils peuvent accéder à l'application Web. Le profil le plus important est celui de « Cybersécurité » qui permet de gérer l'accès des utilisateurs à l'application Web en fonction de leurs besoins.

Les profils sont protégés par mot de passe. Certaines mesures sont prises en compte dans les passerelles M-50/M-70 de SOCOMEC, afin de réduire le risque de vol de mot de passe :

- Les informations de connexion (mot de passe) sont chiffrées.
- Le mot de passe doit répondre à des exigences de sécurité minimales (minimum 10 caractères, y compris au moins une majuscule, une minuscule, un chiffre et un caractère spécial).
- Le mot de passe doit être modifié au moins une fois par an.
- Après 3 échecs d'identification, le compte est bloqué pendant 1 heure.
- Une «passphrase» est prévue pour récupérer le mot de passe en cas de perte de ce dernier.

> Pour plus d'informations sur les différents profils et leur protection par mot de passe, voir le paragraphe 11.1.

6. INTRODUCTION

6.1. Gamme

	DIRIS Digiware M-50 Passerelle de communication Réf. 4829 0219 (sans Bluetooth) Réf. 4829 0221 (avec Bluetooth)	**DIRIS Digiware M-70** Passerelle de communication Réf. 4829 0220 (sans Bluetooth) Réf. 4829 0222 (avec Bluetooth)
Ports de communication	Digiware x 1 (entrée) RS485 x 1 (entrée / sortie) Ethernet x 1 (sortie)	Digiware x 1 (entrée) RS485 x 1 (entrée / sortie) Ethernet x 1 (sortie)
Protocoles de communication	Modbus RTU Modbus TCP BACnet IP SNMP v1, v2, v3 & Traps	Modbus RTU Modbus TCP BACnet IP SNMP v1, v2, v3 & Traps
Autres services	FTP(S), SMTP(S), SNTP, HTTP(S), DHCP	FTP(S), SMTP(S), SNTP, HTTP(S), DHCP
Serveur Web	WEB-CONFIG	Logiciel de surveillance et gestion de l'énergie WEBVIEW-M

6.2. Introduction aux DIRIS Digiware M-50 & M-70

Les DIRIS Digiware M-50 et M-70 agissent comme interface du système Digiware et comme passerelle de communication pour centraliser les mesures provenant des modules DIRIS Digiware et les communiquer par Ethernet.

Elles peuvent aussi centraliser des mesures provenant d'autres compteurs et dispositifs de surveillance de l'énergie SOCOMEC :
COUNTIS, DIRIS A, DIRIS B.

Ils centralisent les données de jusqu'à 32 dispositifs (192 circuits maximum).

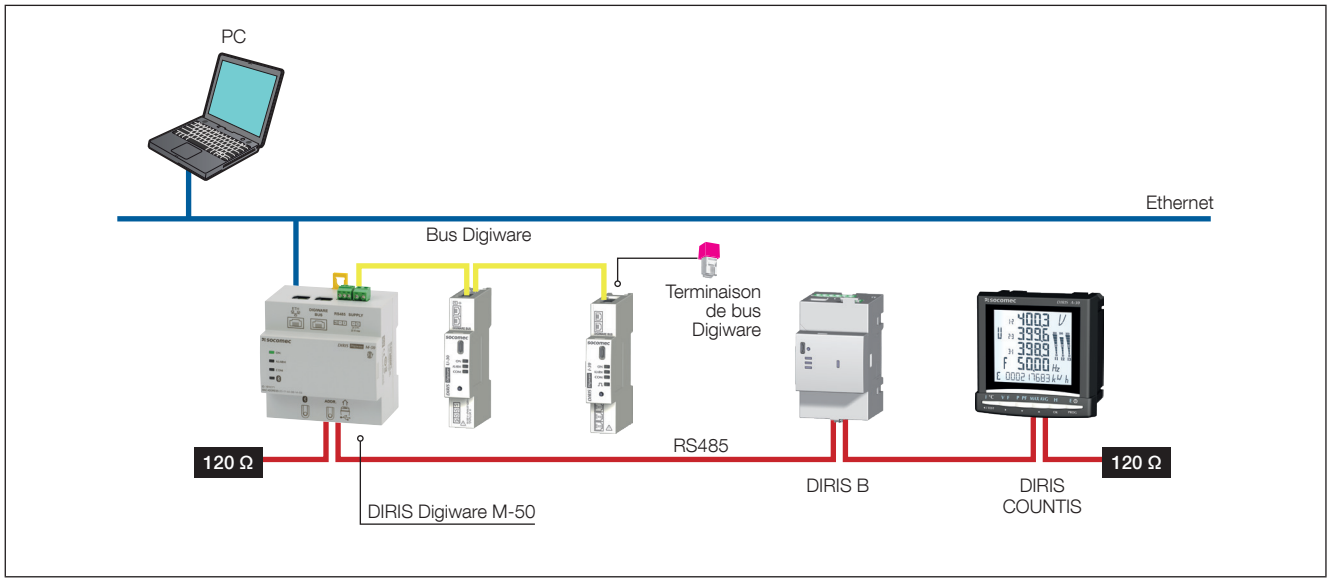
Ces produits peuvent être connectés par un bus Digiware et/ou un bus RS485.

6.2.1. Introduction au DIRIS Digiware M-50

La passerelle DIRIS Digiware M-50 fonctionne en dispositif maître sur le bus RS485 et en dispositif maître sur le bus DIRIS Digiware. Elle est utilisée comme passerelle Ethernet.

Le port Ethernet est utilisé pour :

- Communiquer sur Ethernet en Modbus TCP (max. 32 connexions simultanées), les données provenant des compteurs et dispositifs de mesure connectés à ses ports Digiware et RS485.
- Communiquer sur Ethernet en utilisant les protocoles BACnet IP et SNMP, les données provenant des compteurs et dispositifs de surveillance de l'énergie connectés aux entrées Digiware ou RS485 de la passerelle DIRIS Digiware M-50.
- Exporter automatiquement et cycliquement via FTP ou FTPS les mesures historisées.
- Envoyer automatiquement des notifications d'alarme par e-mail (SMTP ou SMTPS).



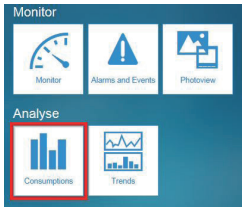
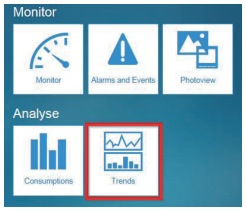
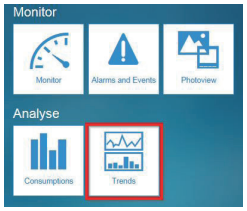
6.2.2. Introduction à la DIRIS Digiware M-70

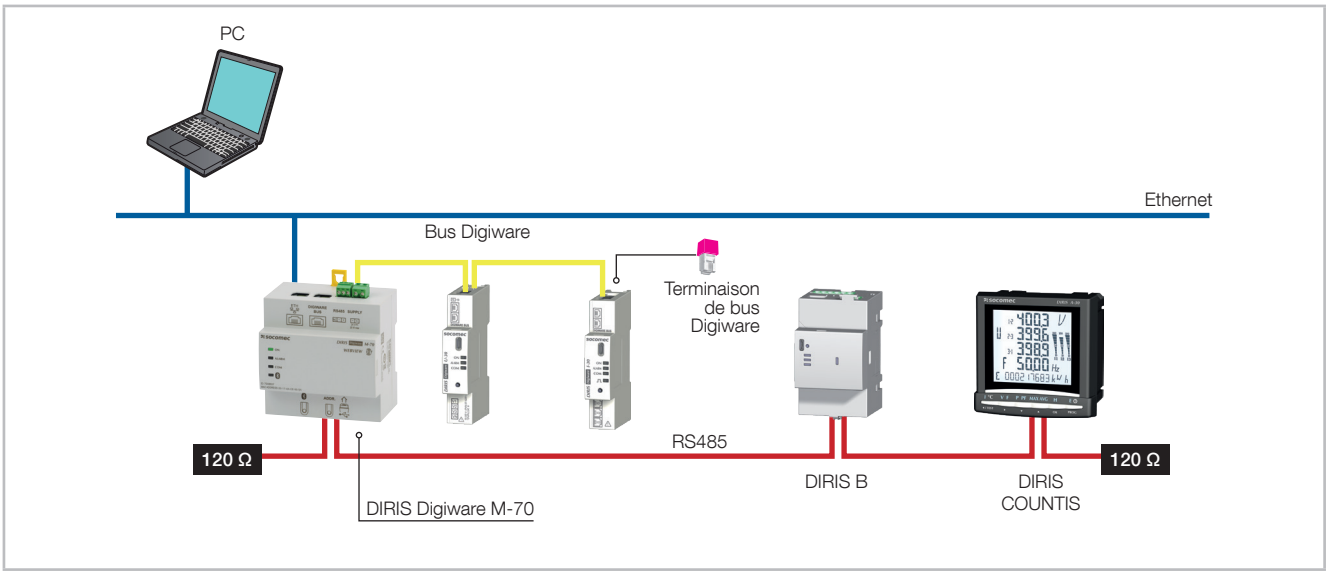
La passerelle DIRIS Digiware M-70 fonctionne en dispositif maître sur le bus RS485 et en dispositif maître sur le bus DIRIS Digiware. Il est utilisé comme passerelle Ethernet.

Le port Ethernet est utilisé pour :

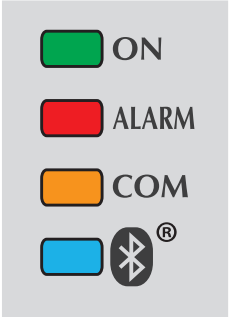
- Communiquer sur Ethernet en ModbusTCP (max. 32 connexions simultanées), les données provenant des compteurs et dispositifs de surveillance de l'énergie connectés aux entrées Digiware ou RS485 de la DIRIS Digiware M-70.
- Accéder aux mesures en temps réel et historiques dans WEBVIEW-M, le logiciel de visualisation intégré dans le DIRIS Digiware M-70.
- Communiquer sur Ethernet en utilisant les protocoles BACnet IP et SNMP, les données provenant des compteurs et dispositifs de surveillance de l'énergie connectés aux entrées de ports Digiware ou RS485 du DIRIS Digiware M-70.
- Exporter automatiquement et cycliquement via FTP ou FTPS les mesures historisées.
- Envoyer automatiquement des notifications d'alarme par e-mail (SMTP ou SMTPS).

Les capacités d'enregistrement et de visualisation des données du DIRIS Digiware M-70 sont détaillées dans le tableau ci-dessous :

	Courbes de consommation	**Courbes de charge**	**Historiques**
Données enregistrées	Énergie : kWh, kvarh, kVAh	Puissance : kW, kvar, kVA	Mesures moyennes : U, V, I, P, Q, S, PF, Température...
Produits compatibles	COUNTIS Exx (tous modèles) DIRIS Axx (tous modèles) DIRIS Bxx (tous modèles) DIRIS Digiware XXX (tous modèles)	COUNTIS Eci, COUNTIS E3x/E4x DIRIS A-30 /A40v3 + MEM / A60/A80 DIRIS B-30 DIRIS Digiware I-31 / I-61 /I-35 / I-45 / I-35dc / S-135 / S-Datacenter DIRIS A-40	DIRIS B-30 DIRIS Digiware I-35 / I-45 / U-30 / U-31dc / U-32dc / S-135 / S-Datacenter DIRIS A-40
Période d'intégration	Configurable depuis Easy Config System, 10 min à 60 min	Configurable depuis Easy Config System, 1 min à 60 min	
Durée de l'enregistrement des données	1 an avec une période d'intégration de 60 min. Proportionnelle pour différentes valeurs : Par ex. : 3 mois avec une période d'intégration de 15 min. S'applique quel que soit le nombre de dispositifs (1 à 32) connectés au M-70. Le niveau de détail du journal n'est pas lié au nombre de dispositifs connectés :		
Fonctionnement	Relevés toutes les 10 min à 60 min dans le compteur/PMD.	Les données sont enregistrées dans une mémoire cache sur le compteur puis téléchargées par la M-70. Si la communication est interrompue, les données manquantes sont récupérées par la M-70 une fois la connexion rétablie, ce qui permet la poursuite de l'enregistrement.	
Sauvegarde des données (en cas d'interruption de la communication entre le M-70 et le compteur)	NON	OUI (dans la mémoire cache du compteur)	
Exportation sur le serveur FTP	OUI	OUI	OUI
Accès à WEBVIEW-M			
Configuration spécifique	Rien à configurer (les données sont enregistrées automatiquement)	Les courbes de charge doivent être activées sur les compteurs (via Easy Config System). Les courbes de charge sont ensuite téléchargées automatiquement de la mémoire cache du compteur sur la M-70.	Les historiques doivent être activés sur les compteurs (via EasyConfig System). Les historiques sont ensuite téléchargés automatiquement de la mémoire cache du compteur sur la M-70.



6.3. Affichage LED sur la face avant



ON
- Éteinte : le dispositif est hors tension.
- Allumée : le dispositif fonctionne correctement.

«Clignotante» : 10 sec. pendant le démarrage ou au lancement de la commande de clignotement manuelle.

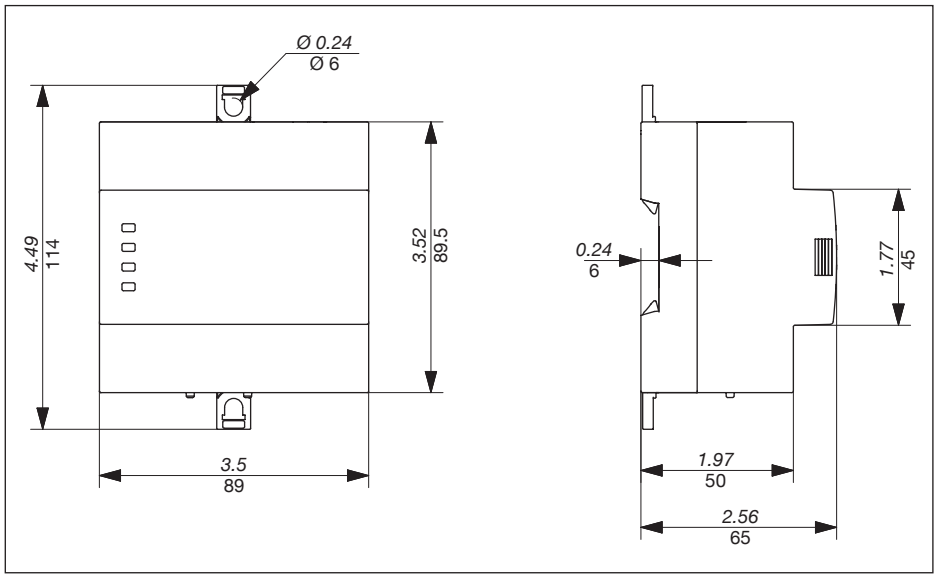
ALARM (pour plus d'informations, voir le paragraphe 12)
- Éteinte : aucune alarme en cours.
- Fixe : alarme (logique/analogique...) en cours ou terminée sans avoir été acquittée sur un dispositif connecté à la passerelle M-50/M-70.
- Clignotante : alarme système en cours sur un dispositif connecté à l'écran.

COM
- Éteinte : aucune communication.
- Clignotante : communication en cours sur le bus RS485 et/ou le bus Digiware.

BLUETOOTH (uniquement pour les M-50/M-70 avec Bluetooth)
- Éteinte : Bluetooth désactivé.
- Allumée : Bluetooth activé.

«Clignotante» : Processus d'appairage en cours.

6.4. Dimensions (mm / in)

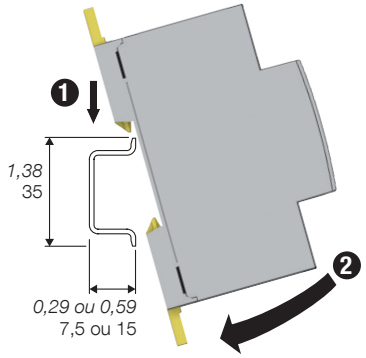


7. MONTAGE

7.1. Recommandations et sécurité

Se reporter aux consignes de sécurité (chapitre « 2. Dangers et avertissements », page 4)

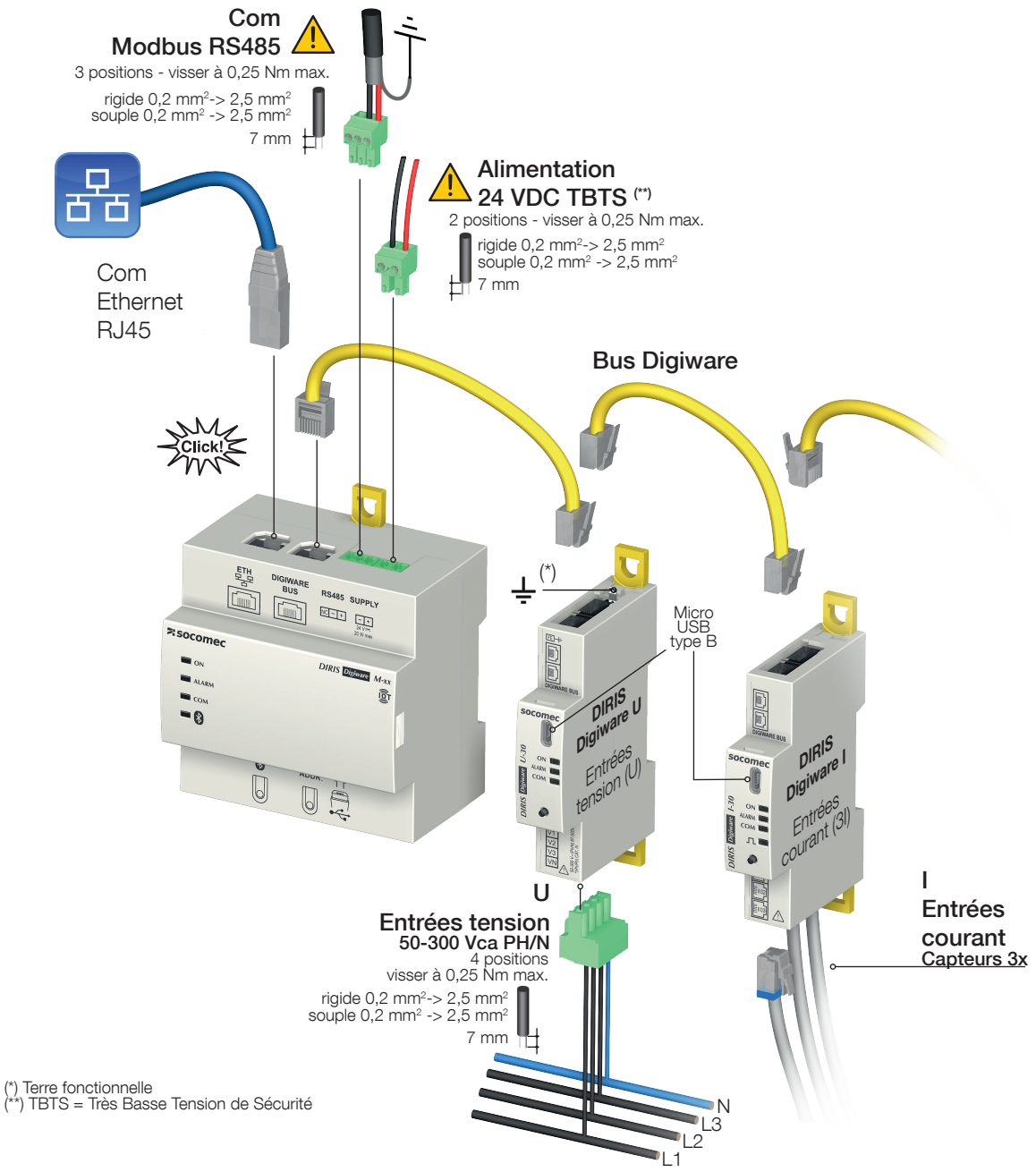
7.2. Montage sur rail DIN



Montage sur rail DIN avec accès unique par la face avant

8. CÂBLAGE DU SYSTÈME

⚠	Utiliser uniquement un câble bus SOCOMEC Digiware (UTP RJ45 droit, paires torsadées, non blindé, AWG 24, 600V CAT V -10 ... +70°C). Pour le câblage, veiller à séparer la section basse tension (BT) et la section très basse tension (TBTS) pour éviter tout risque de choc électrique.
⚠	Maximum 1200 m pour bus RS485
⚠	Longueur max. bus Digiware = 300 m (avec un maximum de 2 répétiteurs DIRIS Digiware C-32)



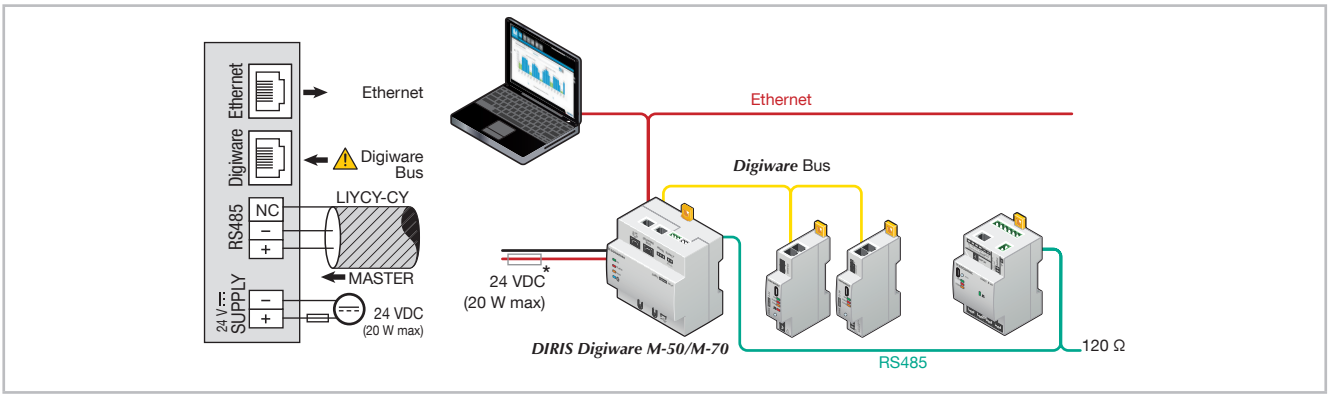
(*) Terre fonctionnelle
(**) TBTS = Très Basse Tension de Sécurité

8.1. Architectures de communication

Les passerelles DIRIS Digiware M-50 et M-70 peuvent être configurées comme esclave ou comme maître sur le bus RS485.

8.2. Câblage des DIRIS Digiware M-50/M-70

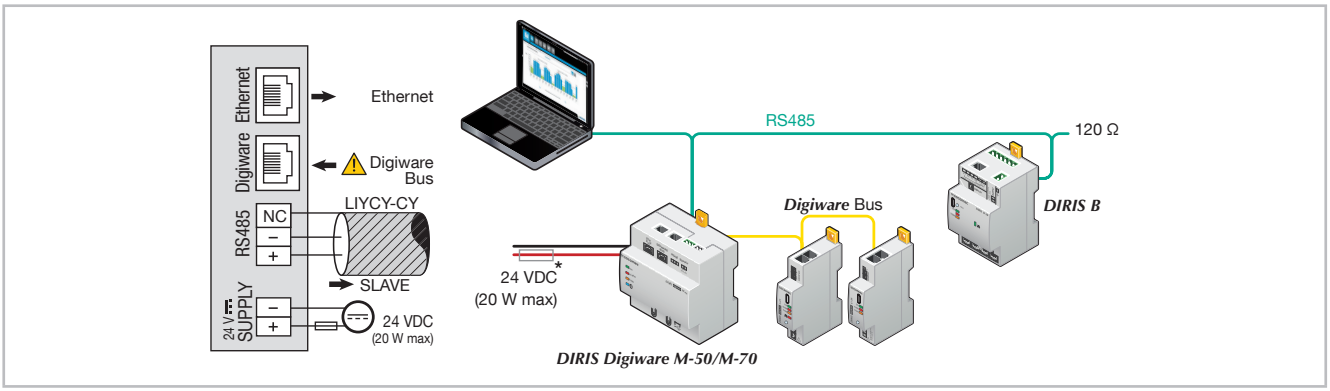
8.2.1. Maître RS485



(*) Si l'alimentation 24 VDC n'est pas fournie par SOCOMEC, il faut prévoir un fusible de 1 A / 24 VDC. L'utilisation de fusibles agréés est obligatoire en Amérique du Nord.

En configuration maître RS485, la M-50/M-70 agit comme passerelle (Digiware vers Ethernet et RS485 vers Ethernet).

8.2.2. Esclave RS485



(*) Si l'alimentation 24 VDC n'est pas fournie par SOCOMEC, il faut prévoir un fusible de 1 A / 24 VDC. L'utilisation de fusibles agréés est obligatoire en Amérique du Nord.

9. BLUETOOTH LOW ENERGY

Les passerelles DIRIS Digiware M-50/M-70 intègrent la technologie Bluetooth Low Energy (BLE).

La fonction Bluetooth est désactivée par défaut (LED bleue éteinte), mais peut être activée depuis le serveur Web de la passerelle DIRIS Digiware M-50/M-70.

SOCOMEC ne dispose pas encore d'application pour pouvoir utiliser la fonctionnalité Bluetooth, raison pour laquelle aucune explication supplémentaire à ce sujet ne sera fournie dans cette notice d'utilisation.

10. AUTO-DÉTECTION DES DISPOSITIFS ESCLAVES

Dès que le système est totalement câblé et alimenté, lancez le processus de détection automatique en appuyant sur le bouton ADDR, situé en dessous de la passerelle M-50/M-70, en le maintenant enfoncé 3 secondes.

Ce processus d'auto-détection détecte les dispositifs connectés au bus Digiware et au bus RS485 et leur attribue une adresse Modbus unique.

2 modes d'auto-détection peuvent être utilisés :

- RAPIDE (mode par défaut) : ce mode détecte uniquement les modules DIRIS Digiware sur le bus Digiware et RS485, DIRIS B et les PMD de type DIRIS A-40 sur le bus RS485.
- COMPLET : ce mode détecte également les autres PMD SOCOMEC (DIRIS A) et les compteurs (COUNTIS E) connectés au bus RS485.

Pour passer en mode de détection COMPLET, il faut utiliser le logiciel Easy Config System.

Si plusieurs dispositifs ont la même adresse Modbus (ce qui est fréquent, étant donné que certains modules et dispositifs de même type sont configurés de manière identique en sortie d'usine), un conflit d'adresse va survenir lors du processus d'auto-déctection, ce qui est tout à fait normal. Une LED COM fixe s'allume sur tous les dispositifs affectés par un conflit d'adresse.

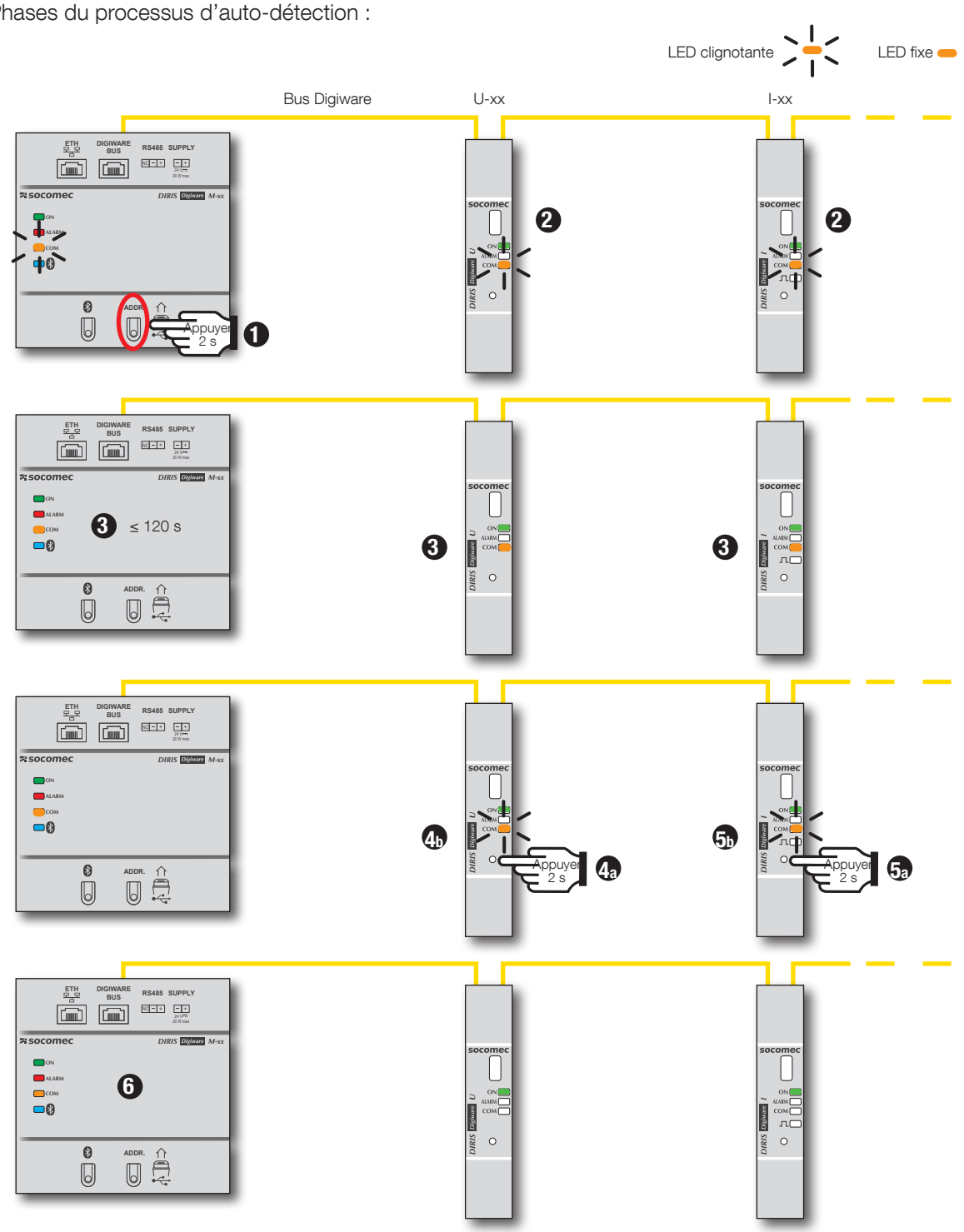
Pour résoudre le conflit d'adresse, appuyer pendant 2 secondes sur le bouton à l'avant de chaque module signalé par une LED COM fixe.

Remarques :

- L'ordre d'appui sur les boutons-poussoirs des modules détermine également l'ordre d'adressage Modbus de ces modules.
- Le processus d'auto-détection peut également être lancé depuis le logiciel Easy Config System, qui permet de sélectionner une résolution automatique des conflits plutôt que de devoir appuyer sur chaque bouton à l'avant des modules.

⚠ Pour attribuer des adresses Modbus spécifiques aux dispositifs connectés à la passerelle M-50/M-70, il faut modifier manuellement leur adresse Modbus à l'aide du logiciel Easy Config System, avant de lancer le processus d'auto-détection.

Phases du processus d'auto-détection :



1. Démarrer le processus d'auto-détection des dispositifs connectés aux bus Digiware ou RS485 en appuyant sur le bouton ADDR. et en le maintenant enfoncé 2 secondes.
2. Les LED COM de tous les dispositifs se mettent à clignoter de manière synchrone pendant toute la durée du processus. Si certaines LED COM ne clignotent pas, cela indique un éventuel problème de configuration (vitesse de communicaiton incohérente entre la passerelle M-xx et le dispositif esclave, etc.).
3. Après 1 minute environ, certains conflits d'adresses ont été détectés et la LED COM de la passerelle M-xx et des dispositifs esclaves s'allument de manière fixe.

4a/5a. Appuyer pendant 2 secondes sur le bouton à l'avant de chaque dispositif esclave comportant une LED COM fixe.

4b/5b. Les LED COM des modules se remettent à clignoter.

6. La LED COM de la passerelle M-50/M-70 se remet à clignoter et les dispositifs esclaves communiquent désormais avec la passerelle M-50/M-70.

11. CONFIGURATION VIA LE SERVEUR WEB EMBARQUÉ DANS LES PASSERELLES M-50/M-70

Un serveur Web est embarqué pour configurer les paramètres réseau (WEB-CONFIG, M-50/M-70) et la visualisation à distance des données de mesure (WEBVIEW-M, D-70 uniquement).

Pour se connecter au serveur Web de la passerelle, saisir son adresse IP dans la barre d'adresses du navigateur Web.

Paramètres Ethernet par défaut des passerelles DIRIS Digiware M-50/M-70 :

- Adresse IP : 192.168.0.4
- Masque : 255.255.255.0
- Passerelle : 192.168.0.1

11.1. Profils utilisateurs

Divers profils sont disponibles :

- Utilisateur (par défaut)
- Utilisateur avancé
- Utilisateur Totem
- Administrateur
- Cybersécurité

Les profils Utilisateur avancé, Administrateur et Cybersécurité sont autorisés à modifier les paramètres.

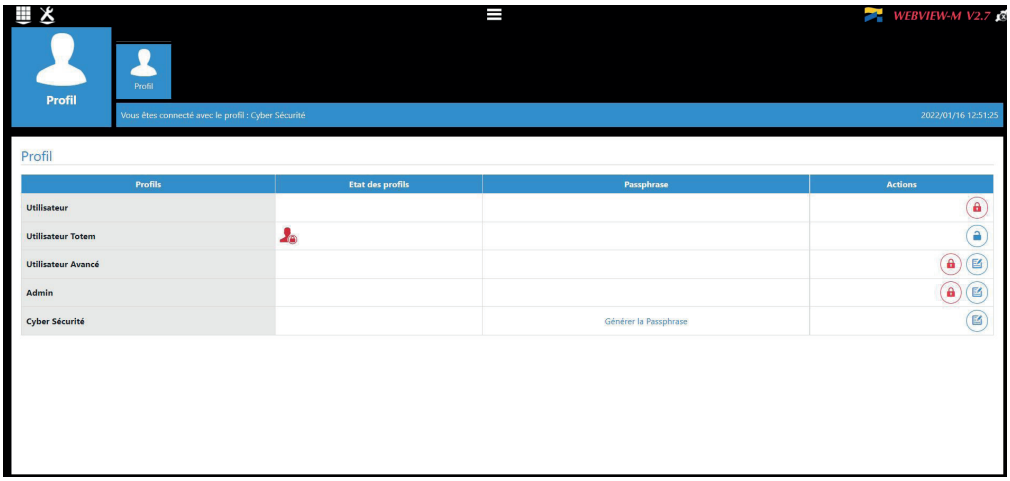
PROFIL	ACCÈS	MOT DE PASSE PAR DÉFAUT
Utilisateur	- Visualisation des données de mesure - Accès aux diagnostics	Aucune
Utilisateur avancé	- Visualisation des données de mesure - Accès aux diagnostics + Gestion du mot de passe du profil Utilisateur avancé + Réinitialisation des compteurs	Avancé
Utilisateur Totem	- Visualisation des données de mesure - Accès aux diagnostics + Gestion du mot de passe du profil Utilisateur avancé + Réinitialisation des compteurs + Pas de déconnexion automatique	Totem
Admin	- Visualisation des données de mesure - Accès aux diagnostics + Gestion du mot de passe du profil Admin + Accès au menu de configuration	Admin
Cybersécurité	- Visualisation des données de mesure - Accès aux diagnostics - Gestion des mots de passe de tous les profils - Accès au menu de configuration + Menu de configuration de la cybersécurité + Mise à jour logicielle via serveur Web	Cyber

Lors de la première connexion aux profils Admin, Utilisateur avancé ou Cybersécurité, il est obligatoire de modifier les mots de passe par défaut. Si les mots de passe ne sont pas modifiés, l'alarme « Mot de passe expiré » reste active.

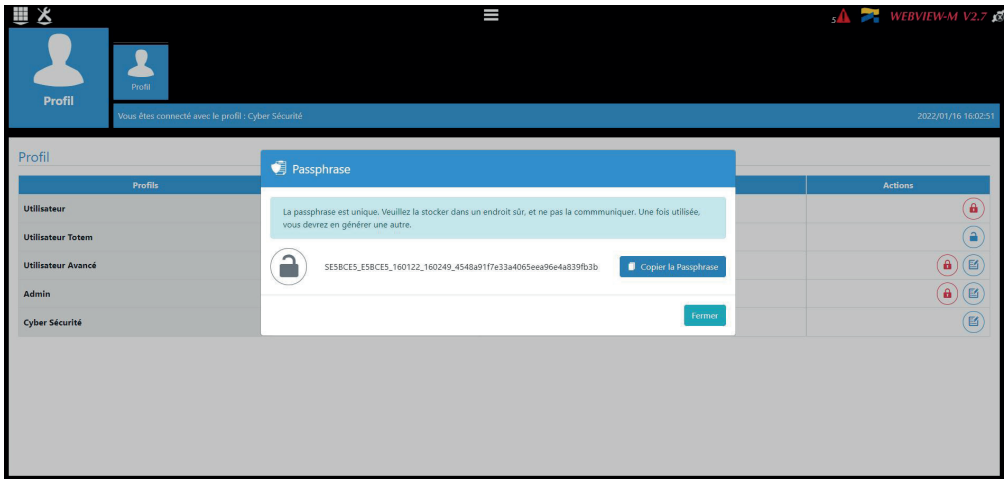
Le profil Utilisateur Totem est bloqué par défaut. Il est nécessaire de se connecter avec le profil Cybersécurité et de débloquer le profil Utilisateur Totem depuis le menu « Profil ».

Il est vivement recommandé de modifier immédiatement tous les mots de passe, en particulier le mot de passe du profil Cybersécurité qui détient les plus hauts privilèges, notamment la modification des mots de passe des autres comptes.

Dès que les mots de passe ont été modifiés, se connecter au profil Cybersécurité, ouvrir le menu « Profil » et cliquer sur « Générer la passphrase » :



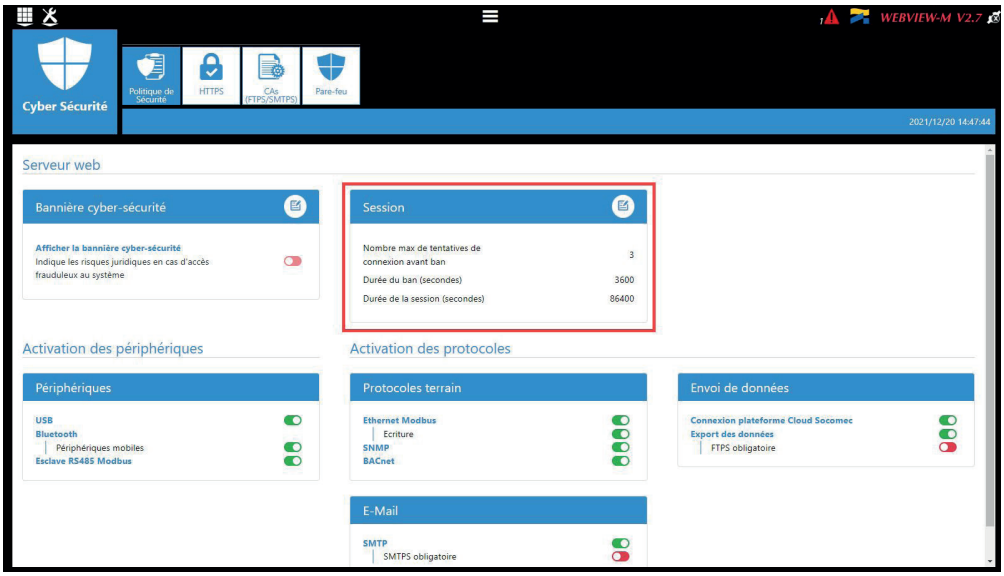
Copier la passphrase à l'aide du bouton « Copier la passphrase » à droite de la clé, la coller et la conserver en lieu sûr. Cela permettra de récupérer le mot de passe du compte Cybersécurité en cas de perte de ce mot de passe.



En cas de perte de la passphrase, la seule option est de réinitialiser les paramètres par défaut d'usine du M-50/M-70.

Politique de blocage des profils : par défaut, après 3 échecs d'identification au profil Admin, Utilisateur avancé ou Cybersécurité, le profil est bloqué pendant 1 heure. Si l'on ne souhaite pas attendre 1 heure, il est possible de rebooter la passerelle M-50/M-70.

La politique de verrouillage peut être modifiée depuis le menu « Cyber Sécurité », dans l'onglet « Politique de sécurité ».



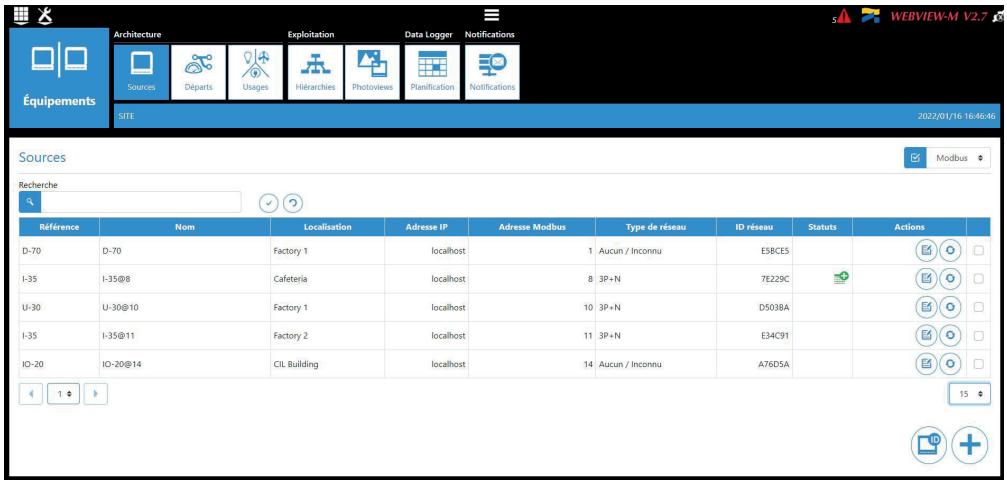
11.2. Profil Admin

En se connectant avec le profil Admin, vous pouvez accéder à la page de configuration en cliquant sur l'icône « Boite-à-outils » dans le coin supérieur gauche :

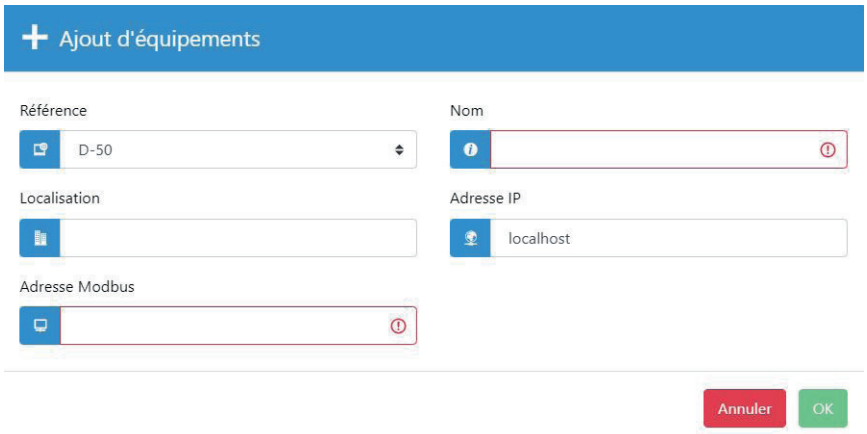
11.2.1. Menu « Équipements »

- Ouvrir le menu « Équipements » :

- Après quelques secondes de chargement, la liste des équipements présents dans la topologie de la passerelle M-50/M-70 est ajoutée :



- Vous pouvez aussi cliquer sur l'icône « + » dans le coin inférieur droit pour ajouter manuellement des produits, les uns après les autres. L'ajout d'une passerelle M-xx ou d'un afficheur D-xx ajoute l'ensemble de la topologie sous cette passerelle ou cet passerelle.



• Les divers dispositifs SOCOMEC pris en charge par WEBVIEW-M sont repris dans la liste suivante :

Passerelles
- D-50
- D-50v2
- D-70
- G-30/G-40
- G-50/G-60
- M-50
- M-70

DIRIS B
- B-10
- B-30 RF
- B-30 RS485

DIRIS Digiware
- D-40
- I-30
- I-30 dc
- I-31
- I-33
- I-35
- I-35 dc
- I-43
- I-45
- I-60
- I-61
- IO-10
- IO-20
- S-130
- S-135
- S-Datacenter
- U-10
- U-20
- U-30
- U-31 dc
- U-32 dc
- R-60

COUNTIS
- Ci
- E03
- E04
- E13
- E14
- E17
- E18
- E23
- E24
- E27
- E28
- E33
- E34
- E43
- E44
- E44R
- E47
- E48
- E53
- ECI32
- ECI3

DIRIS A
- A-10
- A-20
- A-30
- A-40
- A-40 Ethernet
- A-40 Profibus
- A14
- A17
- A17 2In
- A17 THD
- A17 THD In
- A60
- A80

Commutateurs
- ATyS p M
- C55
- C65
- C66

Ancien DIRIS A
- A10
- A20
- A20v2
- A40v2
- A40v3

Les autres onglets, comme « Hiérarchie » et « Photoview » peuvent également être configurés. Ils proposent des modes supplémentaires pour la visualisation et l'analyse des mesures et consommations via le serveur embarqué WEBVIEW-M (uniquement disponible sur D-70).

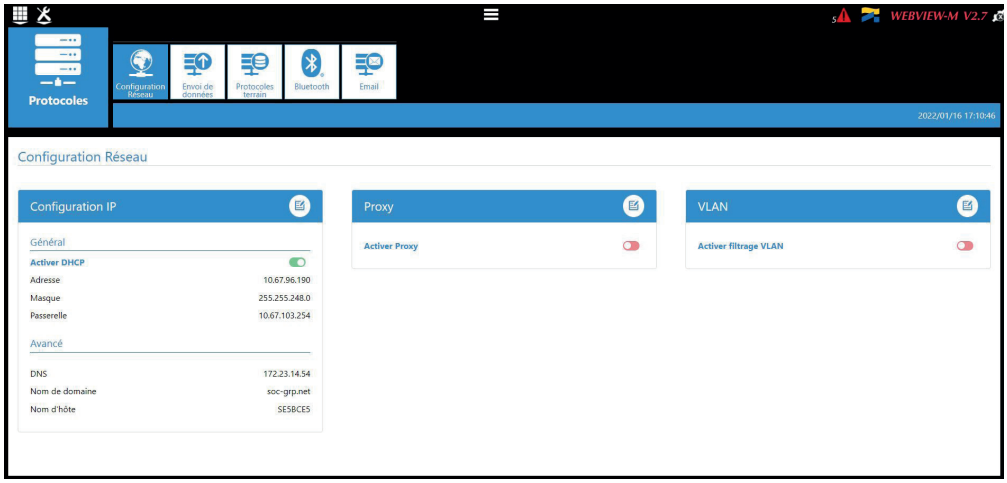
Référez-vous à la notice de WEBVIEW-M pour plus d’informations sur les différents menus de visualisation des données mesurées.

11.2.2. Menu « Protocoles »

Après une configuration intégrale du système, pour visualiser les mesures et la consommation sur WEBVIEW-M, les protocoles de communication qui seront utilisés par la passerelle M-50/M-70 pour échanger des données avec un superviseur externe (SCADA, système de gestion de l'énergie, etc.) peuvent être configurés depuis menu « Protocoles ».

- **Configuration réseau**

Cet onglet permet de régler la configuration IP de la passerelle M-50/M-70 :



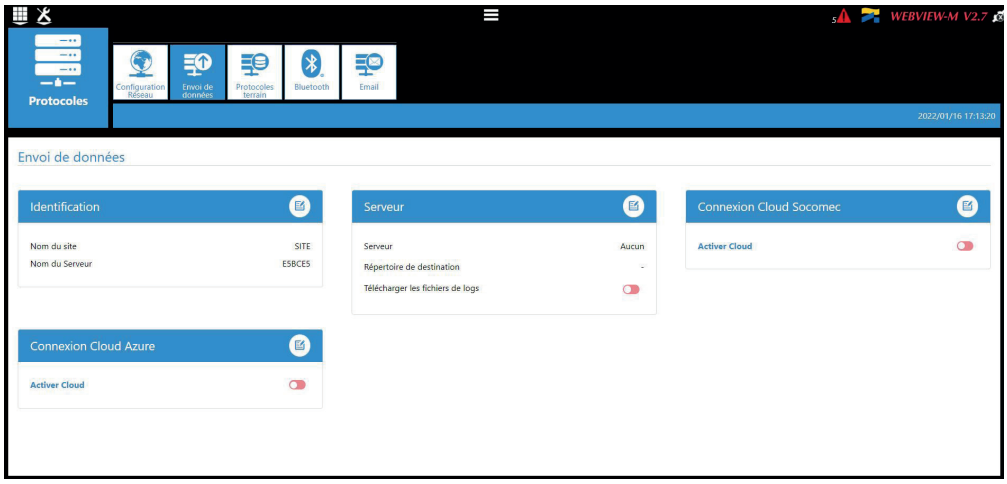
Après avoir modifié ces paramètres, il faut redémarrer la passerelle M-50/M-70.

• **Envoi de données**

- Identification

▪ Nom du site : ce paramètre est essentiel pour connecter la passerelle M-50/M-70 à un emplacement physique dans la structure du projet. Le nom du site par défaut est « SITE » et doit être modifié (en mode d'export EMS uniquement), à défaut de quoi une alarme système se déclenchera.

▪ Nom du serveur : identifiant unique de la passerelle M-50/M-70. Par défaut, le nom du serveur est le NET ID gravé sur le nez de la passerelle M-50/M-70.



- Serveur

▪ Serveur : pour envoyer des fichiers de données à un serveur distant, l'Administrateur sélectionne le serveur FTP(S).

▪ Répertoire de destination : saisir le répertoire du serveur distant qui va recevoir les fichiers.

▪ Télécharger les fichiers de logs : choisir si la la passerelle M-50/M-70 doit également envoyer le fichier de logs au serveur distant.

▪ Adresse : Saisir l'adresse IP du serveur distant.

▪ Port : Saisir le port du logiciel (généralement 20 ou 21 pour FTP et 990 pour FTPS).

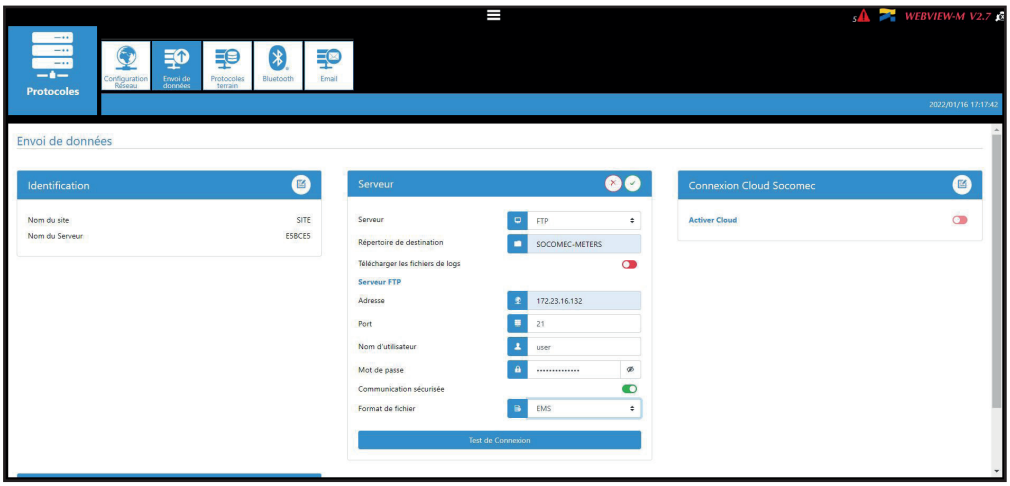
▪ Nom d'utilisateur : saisir le nom d'utilisateur pour accéder au serveur distant. Il doit concorder avec le nom d'utilisateur configuré sur le serveur FTP.

▪ Mot de passe : saisir le mot de passe pour accéder au serveur distant. Il doit concorder avec le mot de passe configuré sur le serveur FTP.

▪ Communication sécurisée : ouvrir une session entre la passerelle M-50/M-70 et le serveur distant.

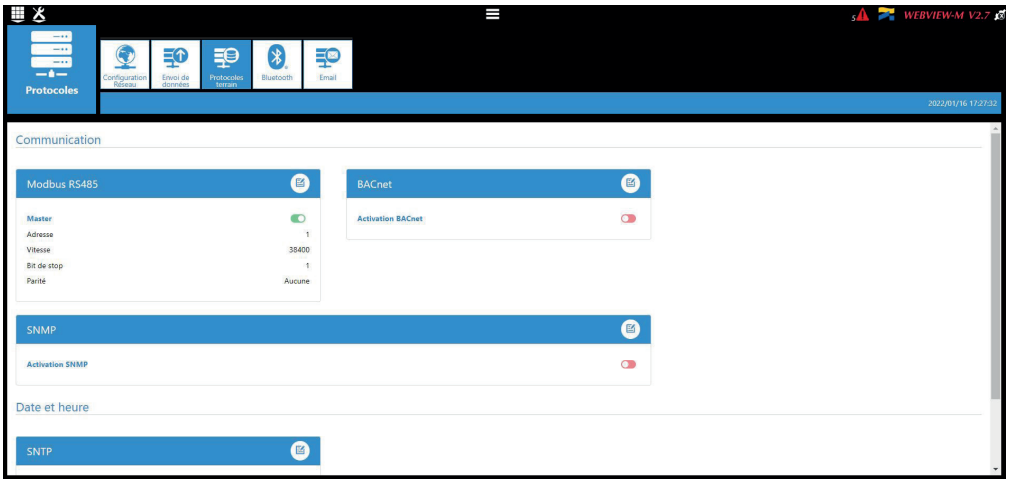
▪ Format de fichier : les données peuvent être exportées en différents formats de fichiers (CSV et EMS – se référer à l'ANNEXE III). Le format CSV est plus facile à utiliser, mais EMS est préférable pour importer des données dans un logiciel externe de gestion de l'énergie.

▪ Test de connexion : pour tester la fonction d'export FTP.



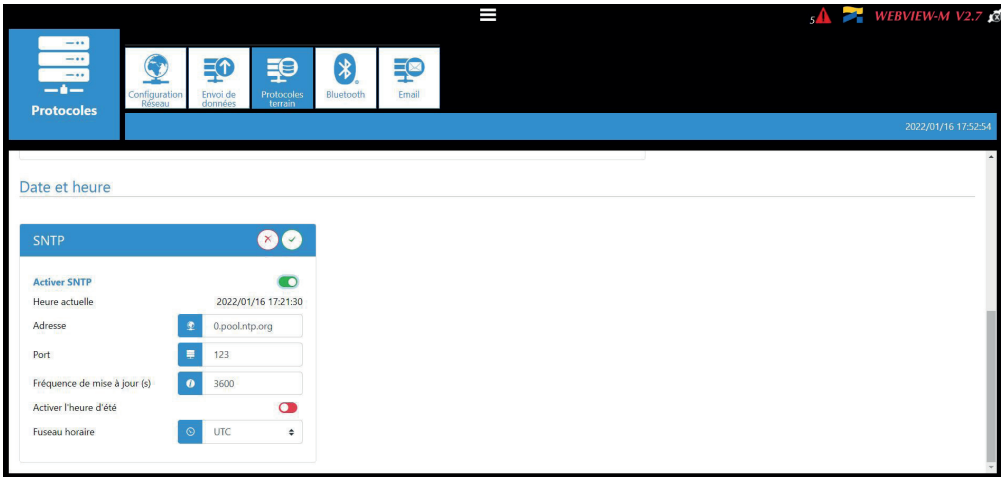
• **Protocoles terrain**

- Communication : permet de configurer les différents protocoles terrain que la passerelle M-50/M-70 peut utiliser pour communiquer avec des systèmes externes de gestion de l'énergie.



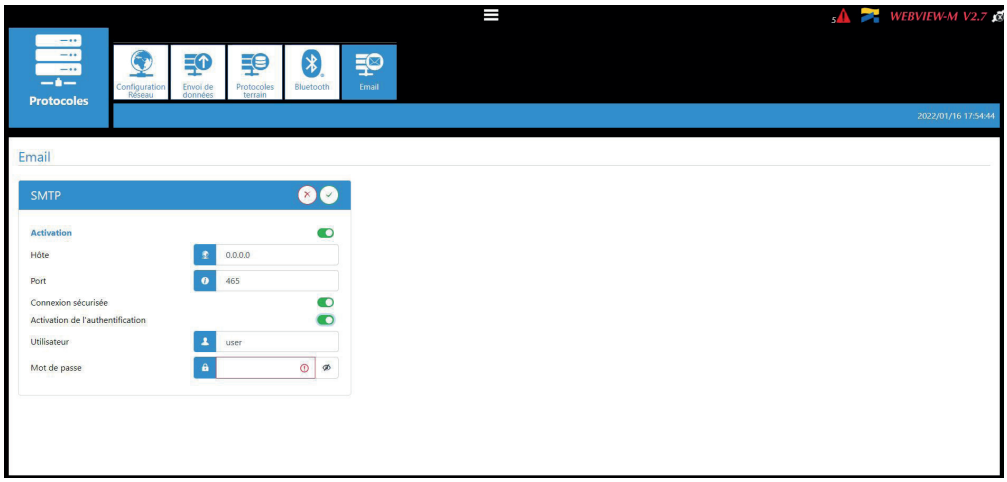
Se référer aux Annexes I et II pour plus d'informations sur les protocoles de communication SNMP et BACnet avec la passerelle M-50/M-70.

- Date et heure : permet de configurer un serveur SNTP pour qu'il synchronise automatiquement l'horloge de la passerelle M-50/M-70 avec un ordinateur externe.



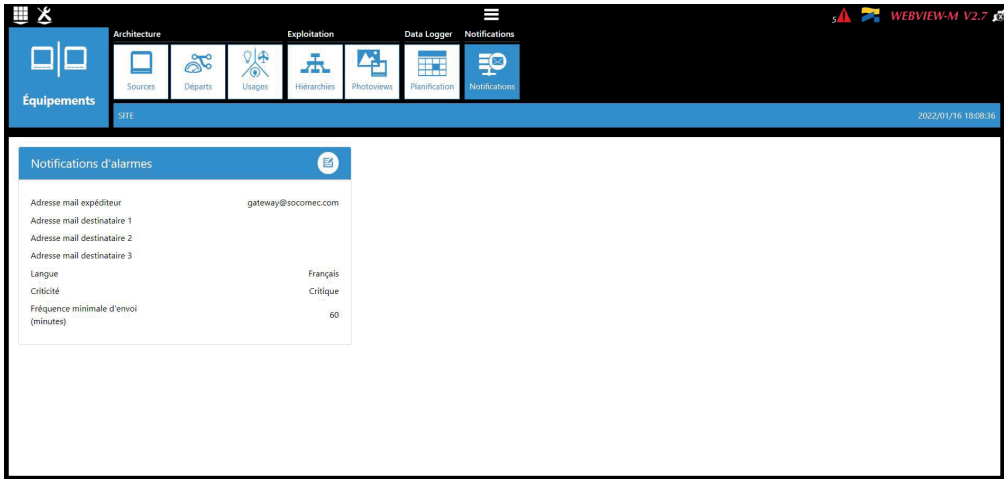
• **E-mail**

Cet onglet permet d'activer et de configurer les notifications par e-mail en cas d'alarmes :



- Activation : activer/désactiver la fonction d'envoi d'e-mails SMTP.
- Hôte : saisir l'adresse IP ou le nom d' hôte du serveur SMTP.
- Port : saisir le port SMTP.
- Connexion sécurisée : activer ou désactiver le connexion sécurisée (SMTPS).
- Activation de l'authentification : activer ou désactiver l'authentification SMTP. Il est possible d'activer l'authentification, même si la connexion sécurisée est désactivée.
- Utilisateur : saisir le nom d'utilisateur pour l'authentification.
- Mot de passe : saisir le mot de passe pour l'authentification

Une fois le serveur SMTP configuré, rendez-vous dans le menu « Équipements », onglet « Notifications » pour configurer les paramètres de notification par email (adresses emails source et de destination, fréquence de notification etc.) :



- Adresse de l'expéditeur de l'e-mail : adresse e-mail utilisée par la passerelle M-50/M-70 pour envoyer des e-mails.
- Adresse e-mail destinataire 1 : adresse e-mail n°1 à laquelle les notifications par e-mail seront envoyées.
- Adresse e-mail destinataire 2 : adresse e-mail n°2 à laquelle les notifications par e-mail seront envoyées.
- Adresse e-mail destinataire 3 : adresse e-mail n°3 à laquelle les notifications par e-mail seront envoyées.
- Langue : langue dans laquelle les e-mails sont envoyés.
- Criticité des alarmes à envoyer : permet de choisir d'envoyer les alarmes de type « informations », les alarmes « non critiques » ou « critiques ».
- Fréquence d'envoi : temps d'attente maximum pour recevoir une notification par e-mail après activation de l'alarme sur un des équipements. Ceci permet de limiter le nombre d'e-mails transmis par la passerelle M-50/M-70, en particulier quand une alarme change fréquemment d'état.

11.3. Profil Cybersécurité

En plus des droits du profil Admin, le profil Cybersécurité permet de :

- Gérer tous les profils et modifier leurs mots de passe. Il permet également de générer la passphrase pour la récupération du mot de passe.
- Personnaliser une politique de Cybersécurité depuis un menu dédié :

11.3.1. Menu Cybersécurité

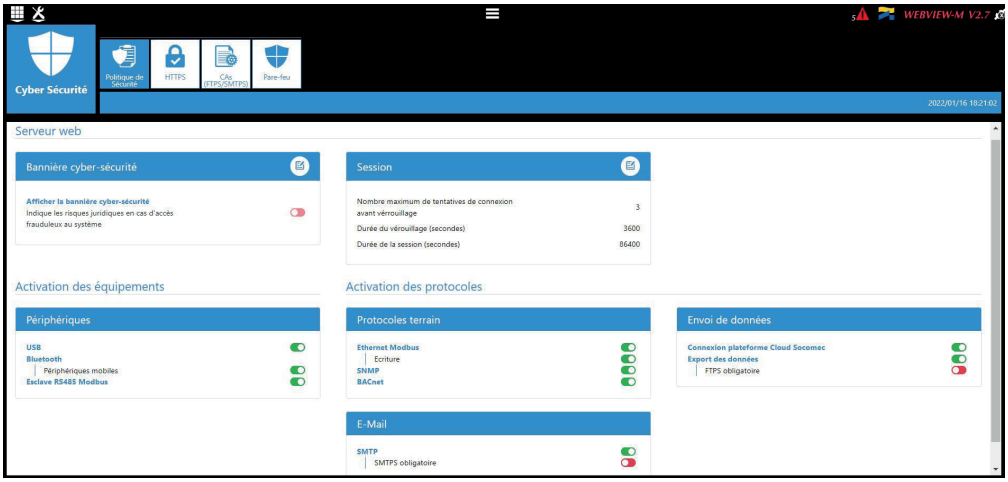
Le menu Cybersécurité menu permet de :

- Définir une politique de sécurité personnalisée.
- Sécuriser la communication client-serveur (HTTPS, FTPS, SMTPS).
- Empêcher les attaques par déni-de-service en configurant un pare-feu dans la passerelle M-50/M-70.

La configuration des fonctions de Cybersécurité est décrite aux paragraphes 11.3.2 à 11.3.4.

11.3.2. Onglet « Politique de sécurité »

Les passerelles DIRIS Digiware M-50/M-70 peuvent réduire l'exposition aux attaques en désactivant certains périphériques ou services qui ne sont pas essentiels pour l'utilisateur.



Banière cyber-sécurité

Choisir d'afficher ou non la banière de cyber-sécurité, qui explique les risques juridiques en cas d"accès frauduleux au système. Le message sera affiché sur la page de connexion.

Session

Il est possible de personnaliser la politique de session (nombre maximum de tentatives de connexion avant vérouillage, durée du vérouillage et durée de la session).

Périphériques

- USB : permet de désactiver le port USB de la passerelle M-50/M-70.
- Bluetooth Low Energy : permet de désactiver le Bluetooth Low Energy de la passerelle M-50/M-70.
- Modbus esclave via RS485 : autorise ou désactive la communication Modbus sur le port RS485 de la passerelle M-50/M-70.

E-mail

- Impose la version sécurisée de SMTP pour les notifications par e-mail en cas d'alarme sur un dispositif connecté.

Protocoles de terrain

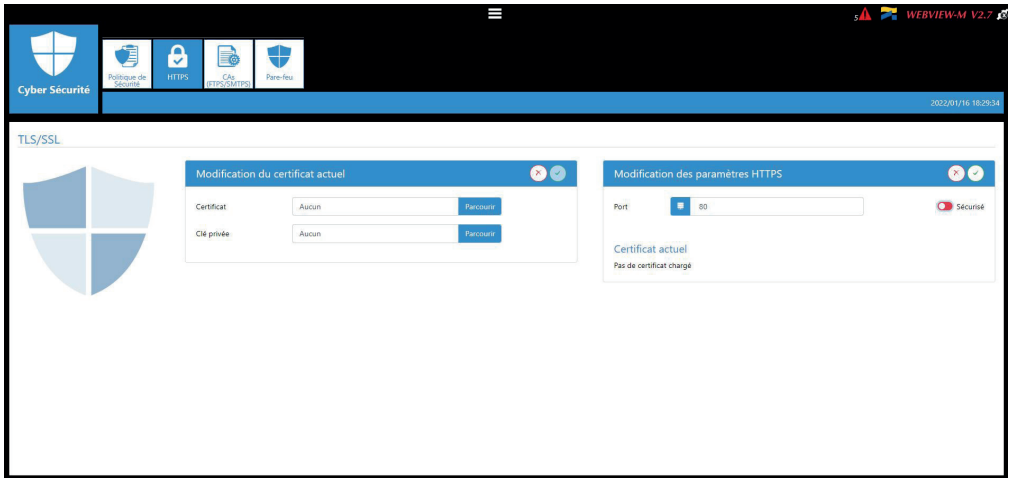
- Fonction d'écriture Modbus : à autoriser ou désactiver pour empêcher quiconque de modifier les paramètres via Modbus.
- SNMP : autorise ou désactive l'utilisation du protocole SNMP.
- BACnet : autorise ou désactive l'utilisation du protocole BACnet.

Push de données

- Plateforme cloud SOCOMEC : autorise ou bloque l'export de données vers la plateforme SOCOMEC.
- Export de données, FTPS obligatoire : impose une connexion sécurisée pour exporter des données vers un serveur FTP.

11.3.3. Onglet « HTTPS »

L'onglet HTTPS permet d'ajouter un certificat numérique pour sécuriser la navigation Web :



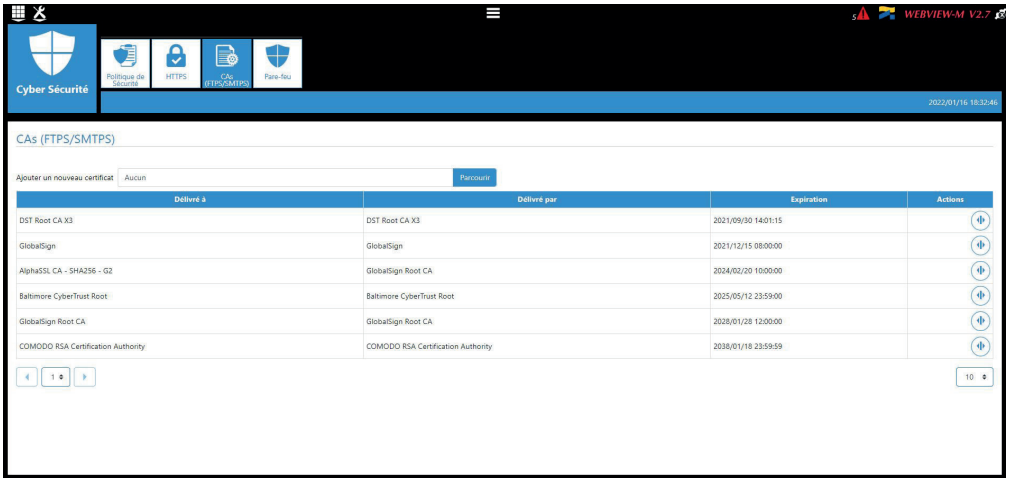
Les passerelles M-50/M-70 acceptent un certificat numérique sous le format .pem. Dès qu'un certificat numérique et une clé privée ont été téléchargés, les paramètres HTTPS peuvent être modifiés pour sécuriser la navigation Web.

- Les passerelles M-50/M-70 sont compatibles avec les certificats numériques RSA et ECDSA (Elliptic Curve Digital Signature Algorithm). Il est recommandé d'utiliser des certificats numériques ECDSA pour optimiser la vitesse de la navigation Web.
- La taille de la clé privée ne doit pas dépasser 2048 bits.

11.3.4. Onglet « CAs (FTPS/SMTPS) »

Cet onglet permet de sécuriser la communication entre le client (M-50/M-70) et le serveur (FTPS, SMTPS) en ajoutant les autorités de certification (CA = Certificate Authority) compétentes côté Client.

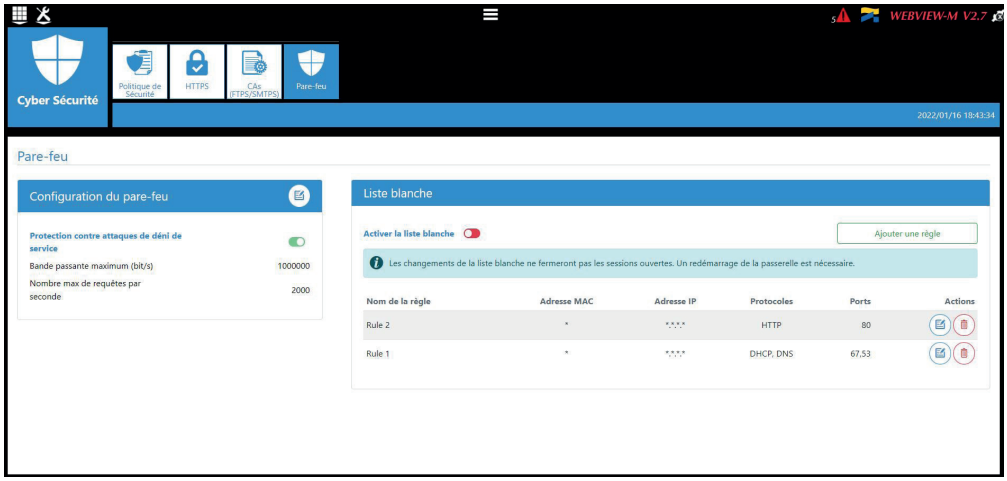
Plusieurs autorités de certification courantes sont déjà intégrées à la passerelle M-50/M-70, mais l'utilisateur peut en ajouter d'autres au besoin.



Se référer à l'annexe IV pour en savoir plus sur comment rechercher et ajouter un CA serveur à la passerelle M-50/M-70.

11.3.5. Onglet « Pare-feu »

Cet onglet permet d'installer un pare-feu pour prévenir les attaques par déni-de-service, également appelées « Flooding attacks », en saisissant un débit maximum en kbit/s et un nombre maximum de demandes par seconde :



Un client qui dépasse un des paramètres ci-dessus pendant une communication avec la passerelle DIRIS Digiware M-50/M-70 sera bloqué pendant 30 secondes.

La partie Liste blanche permet d'ajouter des règles pour filtrer la communication (entre les hôtes et la passerelle M-50/M-70) sur des Adresses MAC / Adresses IP / Protocoles / Ports.

Jusqu'à 10 règles peuvent être ajoutées.

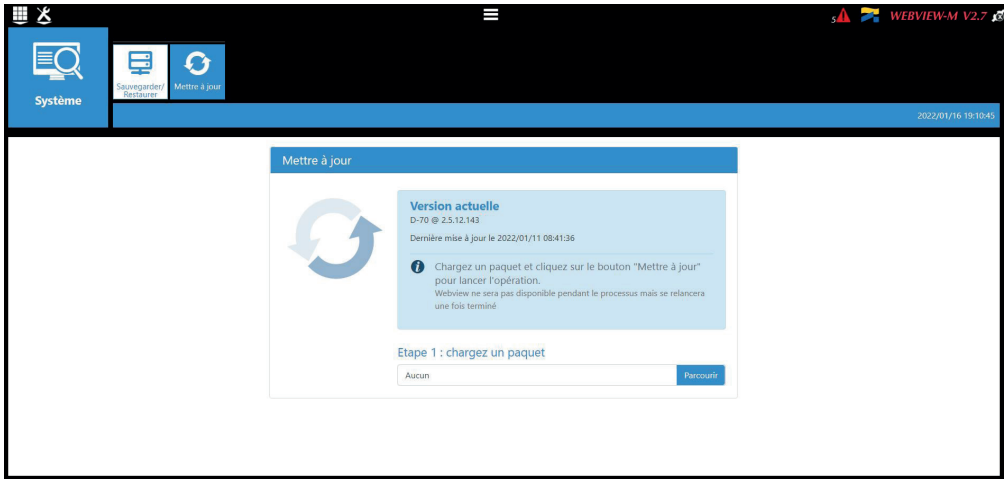
- Pour autoriser toutes les adresses MAC, il suffit de renseigner « * ».
- Pour élargir la liste d'adresses IP autorisées, il suffti de remplacer un ou plusieurs nombres par des « * ».

Exemple: 192.168.*.* autorise toutes les adresses IP commençant par 192.168.

11.3.6. Mise à jour du firmware de la passerelle M-50/M-70

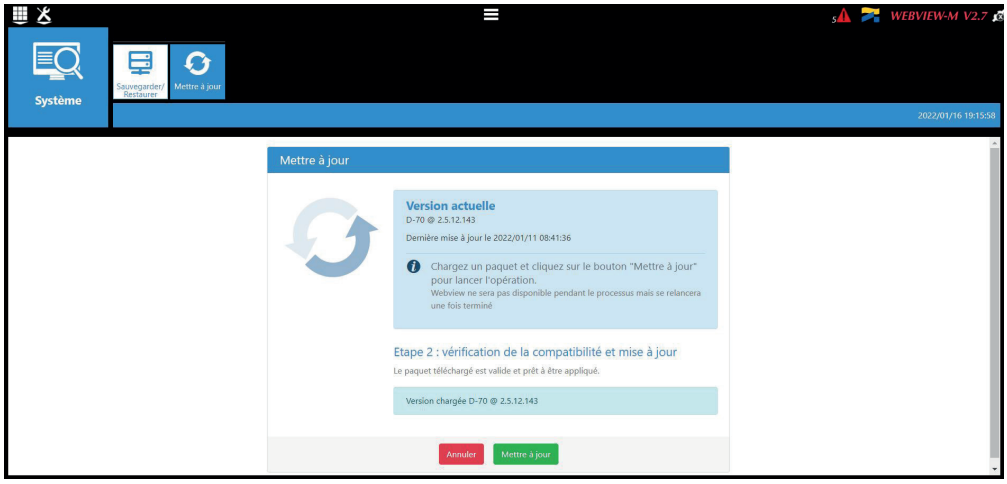
Pour mettre à jour le logiciel embarqué de la passerelle DIRIS Digiware M-50/M-70, aller dans le menu « Système »:

Aller dans l'onglet « Mettre à jour » :

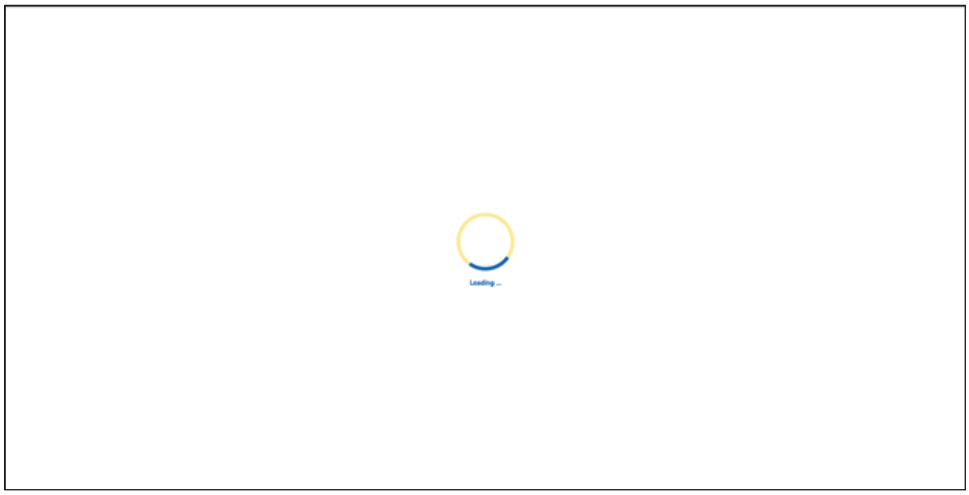


Charger le logiciel embarqué (fichier .dfu) en cliquant sur le bouton « Parcourir ».

Attendre que le fichier soit chargé, puis une fois le contrôle de cohérence terminé, cliquer sur « Mettre à jour ».



Une fois la mise à jour terminée, la page web sera rafraichie automatiquement :



11.4. WEBVIEW-M

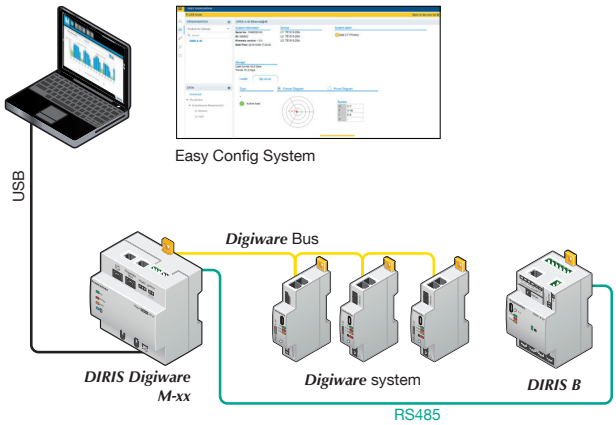
Pour plus d'informations sur la visualisation des données de mesure, voir la notice d'utilisation WEBVIEW-M, disponible sur le site Internet SOCOMEC à l'adresse suivante :
https://www.socomec.fr/fr/centre-de-telechargement?query=notice

12. CONFIGURATION VIA LE LOGICIEL EASY CONFIG SYSTEM

Le logiciel Easy Config System peut être téléchargé depuis le site Internet SOCOMEC à l'adresse suivante :
www.socomec.fr/fr/easy-config-system

La passerelle DIRIS Digiware M-50/M-70 et les dispositifs SOCOMEC en aval peuvent être configurés depuis le logiciel Easy Config System, en connectant un ordinateur à la passerelle M-50/M-70 soit via USB, soit via Ethernet.

12.1. Mode de connexion USB



> Ouvrir Easy Config System.

> Raccorder un câble USB entre la passerelle DIRIS Digiware M-50/M-70 et un ordinateur.

> Se connecter avec le profil Utilisateur ou Admin. Le mot de passe Admin par défaut est « Admin ».

> Cliquer sur « Nouvelle configuration », saisir un nom et une icône.

> Cliquer sur la nouvelle configuration créée.

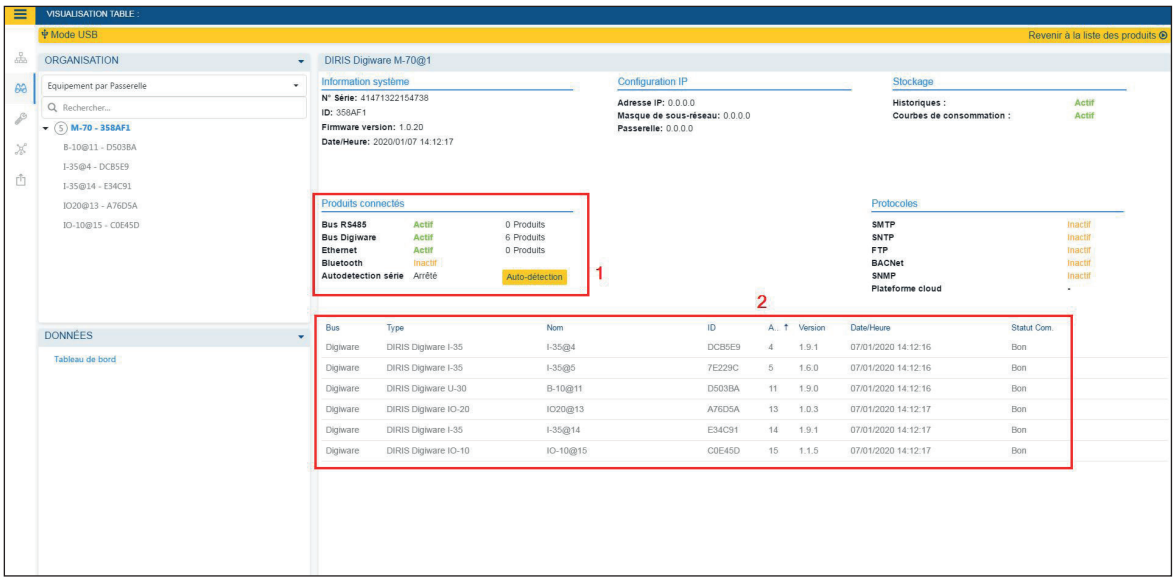
> Cliquer sur « Mode USB » dans le coin supérieur droit pour se connecter à la passerelle M-50/M-70 et accéder aux menus de configuration.

> Cliquer sur l'icône « jumelles » dans la barre de gauche.

> Dans la partie « Organisation », sélectionner la passerelle M-50/M-70.

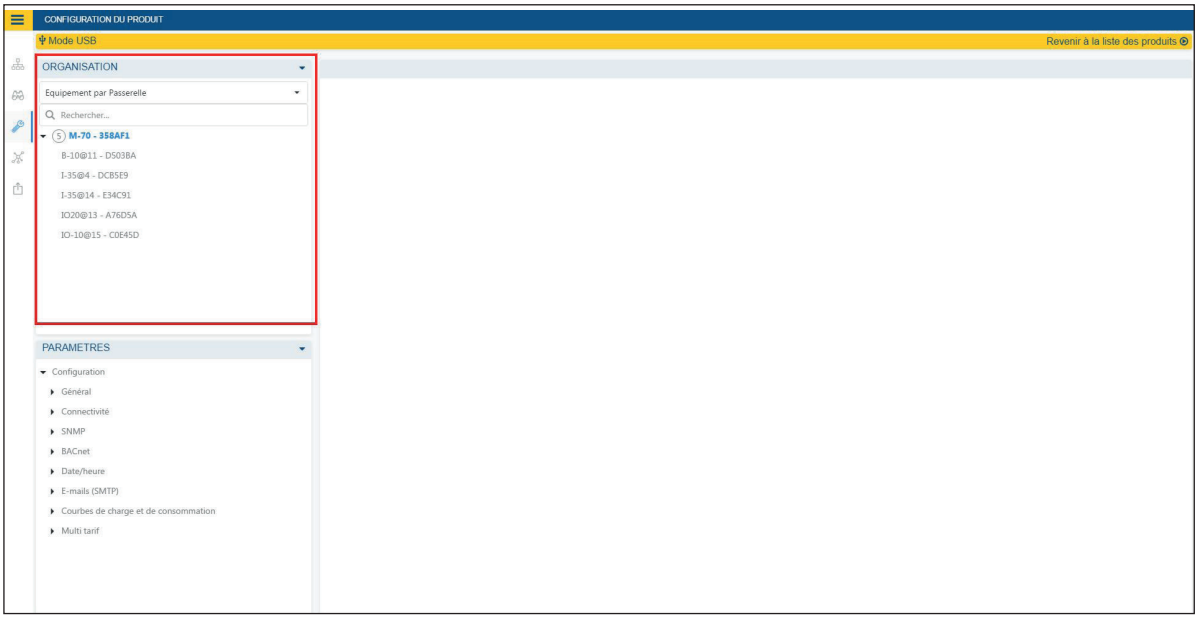
> Cliquer sur « Tableau de bord » pour visualiser les informations générales concernant la passerelle.

> Cliquer sur « Auto-détection » (1) :

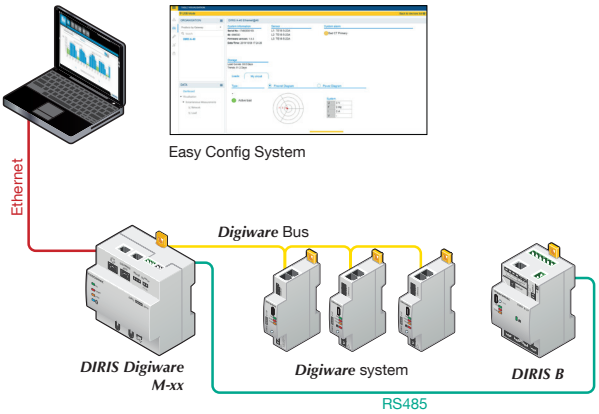


> Dès que le processus d'auto-détection est terminé, les dispositifs esclaves s'affichent dans le bas du tableau de bord (2). Le nombre de dispositifs accessibles en aval de la passerelle M-50/M-70 s'affiche également dans la partie « Organisation », à côté de la passerelle M-50/M-70.

> Les dispositifs esclaves peuvent être configurés directement, sans débrancher le câble USB, en cliquant sur l'icône « clef » dans la barre de gauche :



12.2. Mode de connexion Ethernet



> Ouvrir Easy Config System.

> Se connecter avec le profil Utilisateur ou Admin. Le mot de passe Admin par défaut est « Admin ».

> Cliquer sur « Nouvelle configuration », saisir un nom et une icône.

> Cliquer sur la nouvelle configuration créée.

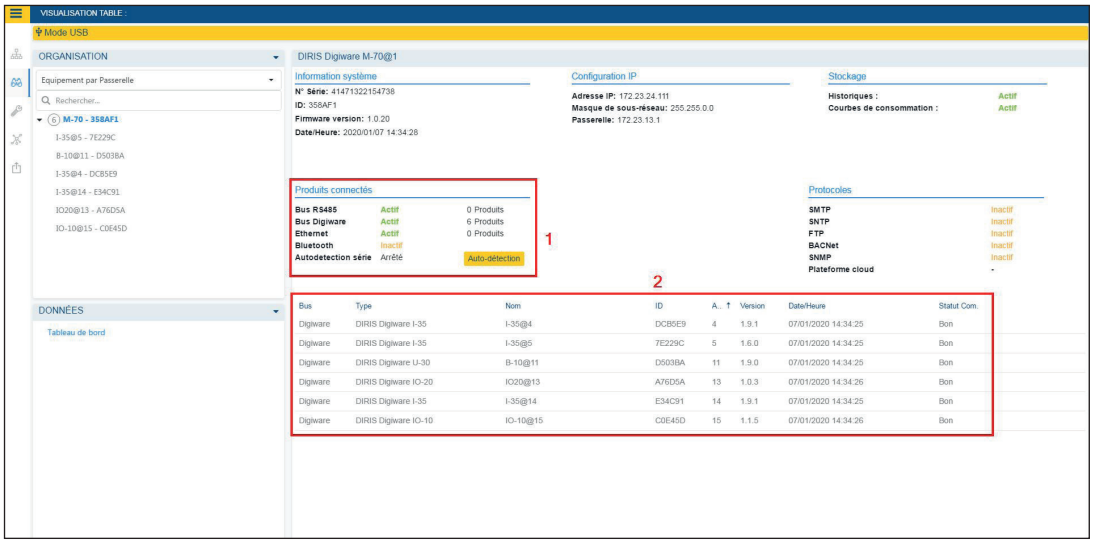
> Cliquer sur l'icône « + » pour ajouter manuellement la passerelle M-50/M-70 à la topologie, en sélectionnant le produit et en saisissant l'adresse IP et l'adresse Modbus. Pour pouvoir communiquer avec la passerelle M-50/M-70, l'ordinateur doit être connecté sur le même réseau que le M-50/M-70

> Cliquer sur l'icône « jumelles » dans la barre de gauche.

> Dans la partie « Organisation », sélectionner la passerelle M-50/M-70.

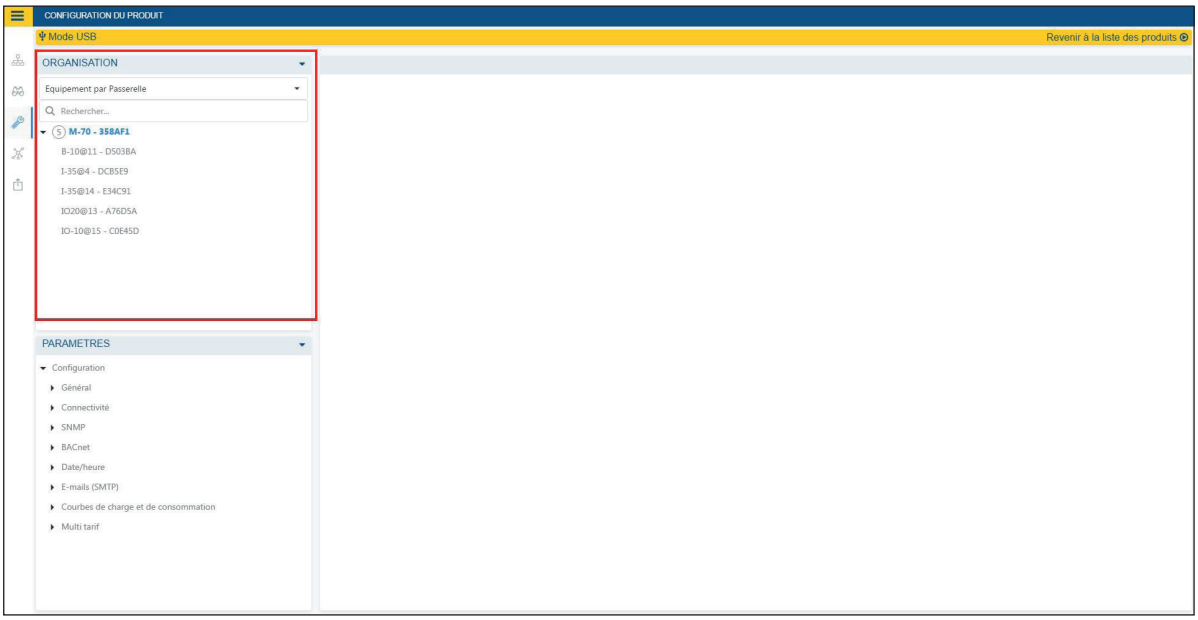
> Dans la partie « Données », cliquer sur « Tableau de bord » pour visualiser les informations générales concernant la passerelle.

> Cliquer sur « Auto-détection » (1).



> Dès que le processus d'auto-détection est terminé, les dispositifs esclaves s'affichent dans le bas du menu du tableau de bord (2). Le nombre de dispositifs accessibles en aval de la passerelle M-50/M-70 s'affiche également dans la partie « Organisation », à côté de la passerelle M-50/M-70.

> Les dispositifs esclaves peuvent être configurés directement en cliquant sur l'icône « clef » dans la barre de gauche et en sélectionnant le dispositif concerné :



13. ALARMES

Les passerelles DIRIS Digiware M-50 et M-70 centralisent les alarmes provenant des dispositifs en aval connectés au bus Digiware ou RS485.

Les passerelles DIRIS Digiware M-50 et M-70 prennent également en charge 8 alarmes système. Le tableau ci-dessous reprend la liste des types d'alarmes système et leurs causes possibles :

N° alarme système	Type d'alarme	Description	Causes possibles
Alarme système 1	Erreur de transmission e-mail	Se déclenche si la passerelle M-50/M-70 n'a pas pu transmettre une notification par e-mail en cas d'alarme.	- Incohérence du mot de passe ou du nom d'utilisateur entre le client et le serveur - Informations serveur incorrectes - Serveur non disponible
Alarme système 2	Erreur de synchronisation SNTP	Se déclenche si la passerelle M-50/M-70 n'a pas pu synchroniser son horloge interne avec le serveur SNTP.	- Informations serveur incorrectes (adresse, port, etc.) - Serveur non disponible
Alarme système 3	Erreur délai d'un esclave Modbus	Se déclenche si la passerelle M-50/M-70 n'a pas pu communiquer avec un esclave Modbus sur le bus Digiware ou RS485.	- Défaut connexion RS485 ou Digiware - Vitesse de communication trop lente sur le bus Digiware (38400 par défaut)
Alarme système 4	Conflit d'adresse Modbus	Se déclenche si la passerelle M-50/M-70 a détecté un conflit d'adresse entre esclaves.	L'adresse d'un Modbus esclave doit être unique sur les bus Digiware et RS485 ; cette alarme se déclenche si 2 esclaves ont la même adresse Modbus.
Alarme système 5	Produit endommagé	Se déclenche si le produit est identifié comme endommagé. Renvoyez le dispositif à SOCOMEC.	- Le produit a un NET ID, un numéro de série ou adresse MAC non valides. - Une version logicielle plus récente existe pour un esclave
Alarme système 6	Erreur d'exportation FTP	Se déclenche si la passerelle M-50/M-70 n'a pas pu exporter des données vers le serveur distant FTP.	- Incohérence du mot de passe ou du nom d'utilisateur entre le serveur et le client - La passerelle n'a pas l'autorisation d'écrire des fichiers sur le serveur FTP - Serveur FTP non disponible - Nom de site non configuré
Alarme système 7	Alerte cybersécurité	Se déclenche si la passerelle M-50/M-70 détecte une menace de cyber sécurité.	- Attaque par déni de service (client exclu) - Expiration d'un certificat numérique
Alarme système 8	Alarme mot de passe	Se déclenche si un problème survient avec le mot de passe du profil Admin, Utilisateur avancé ou Cyber.	- L'alarme est activée par défaut jusqu'à ce que tous les mots de passe soient modifiés - L'alarme est déclenchée une fois par an, 15 jours avant l'expiration d'un des mots de passe et reste active jusqu'à ce qu'ils soient modifiés - L'alarme est également déclenchée si un utilisateur a été bloqué après trop de tentatives de connexion infructueuses.

Si une ou plusieurs alarmes système sont actives, la LED ALARME sur la face avant de la passerelle M-50/M-70 se met à clignoter.

Les alarmes s'affichent sur WEBVIEW-M (passerelle M-70 uniquement) et une notification est transmise par e-mail si la fonction SMTP(S) est activée.

14. CHECKLIST EN 10 ÉTAPES POUR LA MISE EN SERVICE DU SYSTÈME DIGIWARE

1) Détection automatique depuis un bouton-poussoir du M-50/M-70 ou depuis le logiciel Easy Config System.

2) Configuration des modules DIRIS Digiware U et I via le logiciel Easy Config System.

3) Connexion au serveur Web (l'adresse IP par défaut est 192.168.0.4).

4) Modification des mots de passe par défaut des profils Admin, Utilisateur avancé et Cyber.

5) Connexion au profil Cyber et création de la Passphrase pour se protéger contre une perte de mot de passe.

6) Détection des dispositifs via l'onglet « Équipements » ➔ « Sources ».

7) Au besoin, modification du nom des charges et des usages.

8) Optionnel : configuration de Hiérarchies (M-70 uniquement).

9) Optionnel : configuration de Photoviews (M-70 uniquement).

10) Configuration des paramètres IP de la passerelle M-50/M-70 et de ses protocoles de communication via le menu « Protocoles ».

Foire aux questions

Qu'arrive-t-il en cas de perte du mot de passe ?

- Si les profils Admin ou Utilisateur avancé perdent leurs mots de passe, il peuvent être modifiés par le profil Cyber.
- Si le profil Cyber perd son mot de passe, il peut utiliser la passphrase pour créer un nouveau mot de passe.
- En cas de perte de la passphrase, la seule option est de réinitialiser les paramètres d'usine par défaut, de la passerelle M-50/M-70.

Comment configurer les paramètres IP et les protocoles de communication de mon système ?

- Avec le logiciel Easy Config System.
- Ou directement depuis le serveur Web dans le menu « Protocoles ». Ne pas oublier de redémarrer la passerelle M-50/M-70 après avoir modifié la configuration IP.

Pourquoi la LED ALARME du M-50/M-70 clignote-t-elle ?

- Si la passerelle DIRIS Digiware M-50/M-70 est utilisée pour la première fois, il est possible que les mots de passe par défaut des profils Utilisateur avancé, Admin et Cyber n'aient pas encore été modifiés. L'alarme système « Alerte Mot de passe » reste active jusqu'à ce que les mots de passe soient modifiés.

Le processus de détection automatique est terminé, pourtant certains dispositifs esclaves n'ont pas été détectés.

- Si des dispositifs esclaves n'ont pas été détectés, il se peut que le mode de détection automatique soit réglé sur « RAPIDE », qui détecte uniquement les modules DIRIS Digiware, et les dispositifs de mesure DIRIS B et DIRIS A-40. Utiliser Easy Config System pour modifier le mode d'auto-détection en « COMPLET » afin de détecter tous les dispositifs.

15. CARACTÉRISTIQUES TECHNIQUES DES DIRIS DIGIWARE M-50/M-70

15.1. Caractéristiques mécaniques

Poids DIRIS Digiware M-50/M-70	210 g

15.2. Caractéristiques communication

Paramètres Ethernet par défaut	- Adresse IP : 192.168.0,4 - Masque : 255.255.255.0 - Passerelle : 192.168.0.1
Nombre maximum de dispositifs esclaves	32
Ethernet RJ45 10/100 Mbit/s	Fonction passerelle : - MODBUS TCP / RTU - BACNET IP - SNMP v1, v2 et v3
Serveur web embarqué	Web-Config (M-50/M-70) pour configuration de M-50/M-70. WEBVIEW-M (M-70 uniquement) pour visualisation des données de mesure.
SNTP	Met à jour M-50/M-70 depuis un serveur SNTP. M-50/M-70 met à jour les dispositifs connectés.
SMTP(S)	Envoi de notifications par e-mails en cas d'alarme.
FTP(S)	Exporte automatiquement des données vers un serveur FTP (FTP standard ou sécurisé) : Index d'énergies, courbes de charge (puissances), Historiques de mesure.
RJ45 Digiware	Fonction interface de contrôle et d'alimentation
RS485 2-3 fils	1 port, configuré comme entrée (maître) ou sortie (esclave).
Vitesse	9600 bds (10 dispositifs max.). 38400 bds - 115200 bds (32 dispositifs max.).
Micro USB	Pour la configuration via Easy Config System ou la mise à jour du firmware via Product Upgrade Tool.
RJ9	Non utilisé
® Bluetooth Low Energy	Utilisation : fonction pas encore appliquée. Fréquence de fonctionnement : 2402 à 2480 MHz. Puissance EIRP : 6,23 dBm (moyenne max. mesurée).

15.3. Caractéristiques électriques

Alimentation	24 VDC ±10% - Classe 2 selon la norme UL1310 - 20 W max.
Consommation énergétique	2,5 VA
Durée de vie de la batterie	10 ans avec le profil de batterie typique suivant sur toute sa durée de vie : - Stockage du produit : 1 an d'autonomie complète de la batterie (sur la base d'une température de stockage moyenne de 25°C). - Durée de vie du produit : 10 jours / année d'autonomie de batterie sur 9 ans.
Type de batterie	Batterie au lithium de 3 V, capacité nominale 48 mAh.

15.4. Caractéristiques environnementales

Utilisation	Intérieur
Température de stockage	-25°C … +70°C (CEI 60068-2-1 / CEI 60068-2-2)
Température de fonctionnement	-10°C … +55°C (CEI 60068-2-1 / EN/CEI 60068-2-2)
Humidité	95 % à +40°C HR (CEI 60068-2-30)
Degré de pollution	2
Classe de protection	IP 40 (face avant)

15.5. Caractéristiques CEM

Caractéristique	Norme d'essais	Critères de performance	Niveau
Décharges électrostatiques (Contact)	CEI 61000-4-2	B	III
Décharges électrostatiques (Air)	CEI 61000-4-2	B	III
Immunité aux champs électromagnétiques rayonnés aux fréquences radioélectriques	CEI 61000-4-3	A	III
Immunité aux transitoires électriques rapides en salves	CEI 61000-4-4	B	III
Immunité aux ondes de choc (mode commun)	CEI 61000-4-5	B	III
Immunité aux ondes de choc (mode différentiel)	CEI 61000-4-5	s. o.	s. o.
Immunité aux perturbations conduites, induites par les champs électriques	CEI 61000-4-6	A	III
Immunité aux champs magnétiques à la fréquence du réseau	CEI 61000-4-8	A	IV, 400A/m
Immunité aux creux	CEI 61000-4-11	NA	NA
Émissions conduites	CISPR11	NA	NA
Émissions rayonnées	CISPR11	Réussi	Gr :1 – Classe B
Environnement électromagnétique	Industriel + Résidentiel		

ANNEXE I. COMMUNICATION SNMP AVEC LE DIRIS DIGIWARE M-50/M-70

Annexe I - 1. Généralités sur SNMP

SNMP qui signifie *Simple Network Management Protocol* (en français « Protocole simple de gestion de réseau ») est un protocole de communication très utilisé par les administrateurs pour surveiller facilement les dispositifs sur les réseaux IP. Il fonctionne en mode de communication client-serveur sur une couche physique Ethernet.

La passerelle DIRIS Digiware M-50/M-70 prend en charge SNMP v1, v2 et v3. La M-50/M-70 est un agent SNMP v1, v2, v3, qui répond aux requêtes de superviseurs (aussi appelés Managers).

La M-50/M-70 permet d'accéder via SNMP aux données de mesure provenant des dispositifs esclaves SOCOMEC connectés via le bus RS485 ou le bus Digiware.

Les données des dispositifs esclaves sont accessibles via un fichier appelé « MIB » (pour *Management Information Base*, en français « Base d'informations de gestion ») sous une structure hiérarchique et prédéfinie. Le fichier MIB de la M-50/M-70 est disponible sur www.socomec.com.
Le fichier doit être téléchargé sur le superviseur qui gère le système de comptage.

La structure arborescente de la MIB contient plusieurs OID (Identificateur d'objet ou ID objet). Un OID identifie de manière unique et étiquète un objet géré (= paramètre des dispositifs de comptage) dans la MIB.

Par exemple, le paramètre électrique « Current Inst I1 » [Courant Inst I1] est identifié par un OID. « Current Inst I2 » [Courant Inst I2] est identifié par un autre OID.

Termes SNMP courants	Description
Agent	Correspond à la passerelle DIRIS Digiware M-50/M-70 : Interface entre les PMD et le superviseur.
Dispositif géré	Les PMD connectés en aval de la M-50/M-70 (par ex. : I-35, DIRIS B, DIRIS A…).
MIB	Base d'informations de gestion dans laquelle les OID sont organisés dans une arborescence hiérarchique.
OID	Identificateur d'objet qui identifie de manière unique et désigne un objet géré dans la hiérarchie MIB.
Chaînes de communauté	Texte qui permet l'authentification entre un agent et le superviseur.
Traps	Notifications envoyées par l'agent et reçues par le superviseur.

Annexe I - 2. Fonctions de SNMP prises en charge

Quatre types de demandes SNMP sont pris en charge par les DIRIS Digiware M-50/M-70 :

- **GetRequest :** permet de récupérer la variable d'un OID (I1 Inst par exemple).
- **GetNextRequest :** permet de récupérer la variable de l'OID suivant (I2 Inst dans ce cas).
- **GetBulk :** permet de récupérer plusieurs variables regroupées.
- **SetRequest :** permet de modifier la valeur d'une variable telle que l'état d'une sortie numérique.
- **Traps :** contrairement aux commandes ci-dessus qui sont données par le superviseur SNMP, les traps sont générées par les agents sans sollicitation du superviseur. Les traps sont des notifications envoyées au superviseur par l'agent pour signaler un événement ou le déclenchement d'une alarme.

Les Traps sont envoyées par l'agent dans le cas où une des alarmes suivantes se produit :

- Alarme sur une mesure.
- Alarme logique (changement d'état d'une entrée numérique).
- Combinaison d'alarmes.
- Événements PQ (surcharges, surtensions, creux de tensions, interruptions).
- Alarmes système (sens de rotation des phases, CT déconnecté, association V/I).
- Les Traps sont envoyées automatiquement lorsque l'alarme se déclenche. Elles seront renvoyées une fois la durée « Fréquence d'envoi des Traps » écoulée.

L'alarme doit être activée dans le produit (en utilisant le logiciel de configuration Easy Config System) pour que les traps soient envoyées.

Les Traps peuvent être configurées pour des hôtes spécifiques ou « diffusées » sur tout le réseau. Il est possible de saisir jusqu'à deux adresses IP de serveurs pour notifier des hôtes spécifiques.

Annexe I - 3. Versions de SNMP prises en charge

La passerelle DIRIS Digiware M-50/M-70 peut utiliser les trois versions de SNMP : SNMPv1, v2 et v3.

- **SNMPv1 et v2 :**

L'identification est basée sur les mots de passe des communautés lecture seule et lecture/écriture. Ils ne sont pas chiffrés et sont transmis sur le réseau en texte en clair.

Les mots de passe doivent être saisis dans l'agent (DIRIS Digiware M-50/M-70) et dans le superviseur, et doivent être identiques.

Une communauté lecture correspondante permet aux fonctions Get d'être exécutées sur l'agent.

Une communauté lecture/écriture correspondante permet aussi à la fonction Set d'être exécutée sur l'agent.

- Le mot de passe par défaut de la communauté lecture V1 est « public » et le mot de passe par défaut de la communauté lecture/écriture V1 est « private ».
- Le mot de passe par défaut de la communauté lecture V2 est « publicv2 » et celui de la communauté lecture/écriture V2 est « privatev2 ».

- **SNMPv3 :**

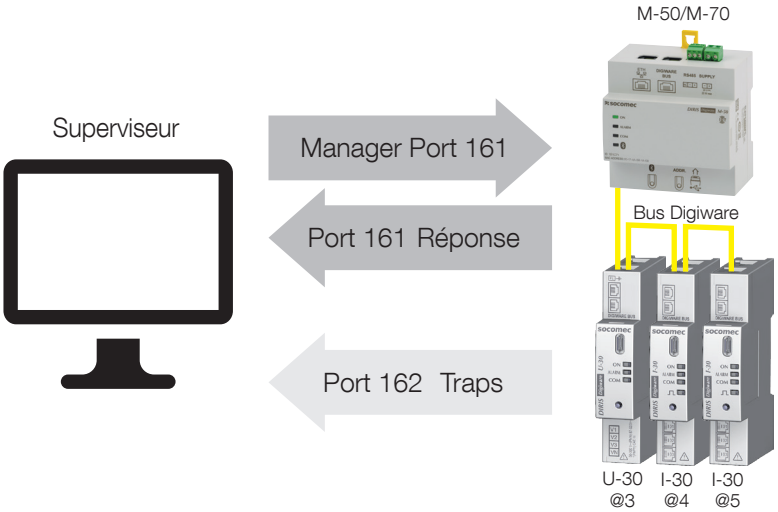
SNMPv3 utilise USM (User-based Security Module) pour contrôler l'accès aux informations disponibles via SNMP. Cette version offre une sécurité renforcée en utilisant trois fonctions importantes pour empêcher l'interception et le déchiffrement des données :

- un nom d'utilisateur (appelé nom d'utilisateur de sécurité) ;
- les protocoles d'authentification MD5 et SHA1 pour hacher les mots de passe ;
- les protocoles de confidentialité DES et AES pour chiffrer les données.

Annexe I - 4. Ports SNMP

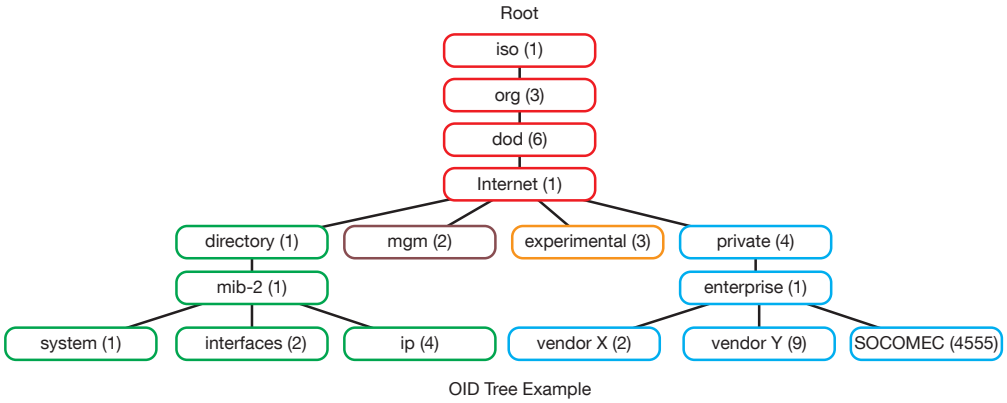
La DIRIS Digiware M-50/M-70 est configurée avec les ports SNMP standard pour recevoir les requêtes et envoyer les notifications :

Port	Description
161	Utilisé pour envoyer et recevoir des demandes depuis le superviseur.
162	Utilisé par le superviseur pour recevoir les notifications de l'agent.



Annexe I - 5. Extraction des données à l'aide du fichier MIB de DIRIS Digiware M-50/M-70

La DIRIS Digiware M-50/M-70 est conforme MIB-II selon la norme MIB RFC 1213 qui définit la structure suivante :



Les branches standard sont sous la même structure de branches mère : 1.3.6.1.4.1

Le groupe « Private (4) » permet aux constructeurs de définir des branches privées incluant les OID MIB de leurs produits. Les données relatives aux dispositifs de comptage de SOCOMEC se situent sous la catégorie d'entreprise SOCOMEC identifiée par l'OID 1.3.6.1.4.1.4555. Cela implique que toutes les demandes d'un superviseur aux agents SOCOMEC commenceront par le chemin de base 1.3.6.1.4.1.4555.

DIRIS Digiware étant un système multi-circuits, la passerelle DIRIS Digiware M-50/M-70 crée une table dynamique qui dépend des produits connectés en aval compatibles avec la DIRIS Digiware M-50/M-70 et des charges configurées sur chaque produit.
Après avoir ajouté/supprimé un dispositif en aval ou une charge, veiller à mettre à jour la topologie de la passerelle M-50/M-70. Cette opération doit être effectué depuis le serveur Web, via le menu “Equipements”:

- ajouter ou supprimer un dispositif ;
- actualiser les charges.

Exemple : l'OID de « Current Inst I1 » [Courant Inst I1] retournera une valeur pour tous les I-xx, B-xx, DIRIS A etc. Au contraire, l'OID de « THD Inst I1 » retournera « 0 » pour un module I-30 ou I-31.

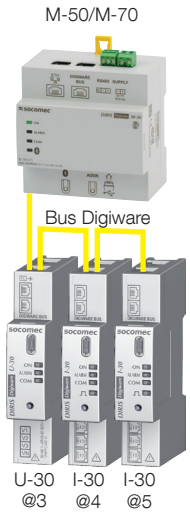
Cela implique que chaque OID peut être associé à plusieurs produits et plusieurs charges.

Par exemple, l'OID d'instCurrentI1 est représenté par la séquence 1.3.6.1.4.1.**4555.10.20.20.1.10000**.

Séquence OID	Description
4555	Branche d'entreprise « SOCOMEC »
10	Table « SocomecProducts »
20	Table « ProductMetrology »
20	« InstantaneousTable »
1	Entrée (toujours = 1)
10000	ID de service

Cet OID est associé aux divers dispositifs connectés en aval de DIRIS Digiware M-50/M-70.
Pour identifier ces différents dispositifs, l'adresse Modbus et le numéro de la charge sont ajoutés à la fin de l'OID.

Exemple : Prenons l'architecture suivante :



Produit	I-30	I-30
Adresse Modbus	4	5
Type de charge	Charge 1 : 3P + N - 3CT	Charge 1 : 1P + N - 1CT Charge 2 : 1P + N - 1CT Charge 3 : 1P + N - 1CT

L'OID final pour extraire le courant instantané I1 pour le module I-30 à l'adresse Modbus 4 pour la charge 1 est :
1.3.6.1.4.1.4555.10.20.20.1.10000.4.1

Pour le module I-30 à l'adresse 5, plusieurs charges sont configurées. Cela implique que l'adresse Modbus doit être suivie du numéro de la charge dans l'OID.

Par conséquent, l'OID final utilisé pour demander I1 Inst pour la charge 1 de l'I-30 à l'adresse 5 est :
1.3.6.1.4.1.4555.10.20.20.1.10000.5.1

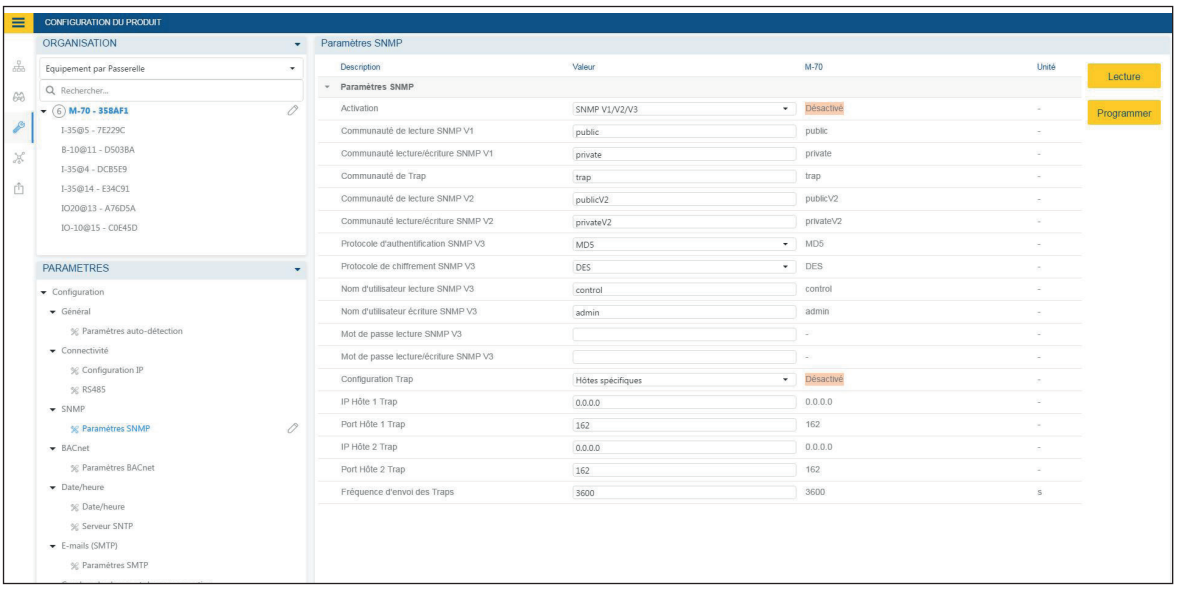
L'OID final utilisé pour demander I1 Inst pour la charge 2 de l'I-30 à l'adresse 5 est **1.3.6.1.4.1.4555.10.20.20.1.10000.5.2**
L'OID final utilisé pour demander I1 Inst pour la charge 3 de l'I-30 à l'adresse 5 est **1.3.6.1.4.1.4555.10.20.20.1.10000.5.3**

Séquence OID	Description
4555	Branche d'entreprise « SOCOMEC »
10	Table « SocomecProducts »
20	Table « ProductMetrology »
20	« InstantaneousTable »
1	Entrée (toujours = 1)
10000	ID de service
5	Adresse Modbus
3	Numéro de la charge

Remarque : une demande à l'OID 1.3.6.1.4.1.4555.10.20. 20.1.10001.5 retournera « 0 » car l'ID de service 10001 correspond à I2 inst tandis que seules des charges monophasées sont configurées dans le module I-30 à l'adresse 5, ce qui signifie que les paramètres courants I2 et I3 ne sont pas utilisés.

Annexe I - 6. Configuration SNMP via Easy Config System

Après s'être connecté à Easy Config System sur la passerelle DIRIS Digiware M-50/M-70, il est possible de trouver le paramétrage SNMP depuis le menu “SNMP”, sous “Paramètres SNMP” :



- **Configuration de communauté SNMP V1 et v2 :**

Communauté lecture SNMP V1 : chaîne de communauté lecture seule pour SNMP v1. La chaîne de communauté par défaut est « public ». Cela permet à un superviseur de récupérer des données en lecture seule d'un dispositif connecté au DIRIS Digiware M-50/M-70.

Communauté lecture/écriture SNMP V1 : chaîne de communauté lecture/écriture pour SNMP v1. La chaîne de communauté lecture/écriture par défaut est « private ». Cela permet à un superviseur de modifier un paramètre (par ex : position d'une sortie numérique) d’un un dispositif connecté à la DIRIS Digiware M-50/M-70.

Communauté de Trap : la chaîne de communauté de Trap permet au superviseur de recevoir des notifications en cas d'événement et/ou d'alarme.

Communauté lecture SNMP V2 : chaîne de communauté lecture seule pour SNMP v2. La chaîne de communauté par défaut est « publicV2 ». Cela permet à un superviseur de récupérer des données en lecture seule d'un dispositif connecté à la DIRIS Digiware M-50/M-70.

Communauté lecture/écriture SNMP V2 : chaîne de communauté lecture/écriture pour SNMP v2. La chaîne de communauté lecture/écriture par défaut est « privateV2 ». Cela permet à un superviseur de modifier un paramètre (par ex : la position d'une sortie numérique) d’un dispositif connecté à la DIRIS Digiware D-50/M-70.

- **Configuration SNMP V3 :**

Protocole d'authentification SNMP V3 : Si SNPM v3 est activé, il est possible de choisir un protocole d'authentification (MD5 ou SHA) pour hacher le mot de passe. Pour ne pas utiliser d’authentification, sélectionner « Aucun ».

Protocole de chiffrement SNMP V3 : choisir entre les protocoles de confidentialité DES ou AES pour le chiffrement des messages de données. Pour ne pas utiliser de chiffrement, sélectionner « Aucun ».

Nom d'utilisateur lecture SNMP V3 : nom d'utilisateur autorisant l'authentification pour les fonctions de lecture seule.

Nom d'utilisateur écriture SNMP V3 : nom d'utilisateur autorisant l'authentification pour les fonctions de lecture et d'écriture.

Mot de passe lecture SNMP V3 : mot (ou phrase) de passe accompagnant les protocoles d'authentification et de confidentialité, et permettant les fonctions de lecture seule. La longueur du mot de passe doit être comprise entre 8 et 16 caractères.

Mot de passe lecture/écriture SNMP V3 : mot de passe (aussi appelé phrase de passe) accompagnant les protocoles d'authentification et de confidentialité, et permettant les fonctions de lecture et d'écriture. La longueur du mot de passe doit être comprise entre 8 et 16 caractères.

Configuration Traps : activation ou désactivation des Traps. Si activés, il est possible de choisir entre diffuser les notifications Traps à tous les superviseurs du réseau ou de les limiter à des postes hôtes spécifiques (2 max.).

IP Hôte 1 Trap : saisir l'adresse IP du 1er poste hôte qui recevra les notifications Traps.

Port Hôte 1 Trap : saisir le port utilisé pour envoyer les Traps au 1er poste hôte.

IP Hôte 2 Trap : saisir l'adresse IP du 2ème poste hôte qui recevra les notifications Traps.

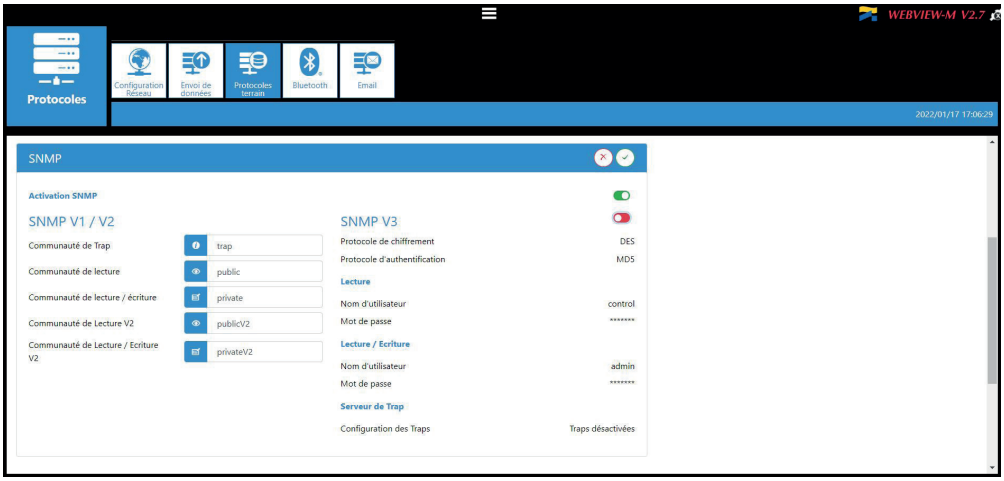
Port Hôte 1 Trap : saisir le port utilisé pour envoyer les Traps au 2ème poste hôte.

Fréquence d'envoi des Traps : saisir la durée au bout de laquelle une notification de rappel est envoyée pour les alarmes en cours. Par défaut, ce paramètre est réglé sur 60 min.

Annexe I - 7. Configuration SNMP via le serveur Web embarqué

Cliquer sur l'icône « Boîte-à-outils » dans le coin supérieur gauche et cliquer sur « Protocoles »:

Cliquer sur l'onglet « Protocoles terrain » et faire défiler la partie SNMP pour saisir les paramètres SNMP V1/V2 / V3, ainsi que les notifications Traps :



ANNEXE II. COMMUNICATION BACNET AVEC DIRIS DIGIWARE M-50/M-70

La passerelle DIRIS Digiware M-50/M-70 prend en charge le protocole BACnet IP.
Elle fonctionne comme une passerelle BACnet IP pour tous les dispositifs compatibles et connectés en aval via le bus RS485 ou Digiware.

Le PICS (Protocol Implementation Conformance Statement, Déclaration de conformité de mise en œuvre de protocole) de la DIRIS Digiware M-50/M-70 est disponible sur le site Internet SOCOMEC à l'adresse :
www.socomec.fr/fr/centre-de-telechargement?query=notice

Annexe II - 1. Généralités sur BACnet

Le protocole BACnet fournit une méthode permettant de rendre interopérable l'équipement de commande basé sur des ordinateurs de différents constructeurs. BACnet est conçu pour gérer différents types de gestion technique de bâtiments, y compris celles de CVC, d'éclairage, de sécurité, de protection incendie, de contrôle d'accès, de maintenance, de gestion des déchets, etc.

Termes courants utilisés dans la communication BACnet :

Objet : représente un dispositif et ses données. Plusieurs types d'objet peuvent être disponibles pour chaque dispositif (entrée analogique, entrée binaire, …). Chaque objet a un certain nombre de propriétés qui décrivent complètement l'objet BACnet pour le réseau.

Identifiant d'objet : identifie de manière unique un objet au sein d'un dispositif BACnet.

Propriété : une propriété décrit un objet BACnet au réseau.

Valeur présente : une des propriétés de l'objet Analog_Input. Elle représente la valeur actuelle d'un objet entrée analogique.

Service : type d'échange entre un dispositif BACnet et un autre.

BACnet utilise un mode de communication client/serveur entre les dispositifs. Les dispositifs communiquent les uns avec les autres en utilisant les services qui décrivent le type d'échange.
Un client BACnet est un dispositif qui demande un service et un serveur BACnet un dispositif qui exécute un service.
Les données au sein d'un dispositif BACnet sont organisées sous la forme d'une série d'objets, composés chacun de plusieurs propriétés.

Par ex. : l'objet analog_input définit une propriété pour present_value, une propriété pour average_value, etc.

Un client BACnet lance une requête à un serveur BACnet en demandant un service (par ex. : read_property) à une propriété spécifique (par ex. : present_value) contenues dans un objet BACnet (ex : analog_input).

Annexe II - 2. Objets BACnet

BACnet définit un ensemble standard « d'objets », qui sont tous composés d'un ensemble standard de « propriétés » qui décrivent l'objet et son état actuel à d'autres dispositifs sur l'interréseau BACnet. Les propriétés permettent le contrôle de l'objet par d'autres dispositifs BACnet.

BACnet définit 54 objets. Chaque élément du système de gestion technique de bâtiment est représenté par un ou plusieurs objets.
La passerelle DIRIS Digiware M-50/M-70 prend en charge les objets ci-dessous :

Type d'objet	Exemple d'utilisation
Device [Dispositif]	Pour décrire le dispositif au réseau BACnet.
Analog input [Entrée analogique]	Courant instantané pour la phase 1 (I1) mesuré par un module courant DIRIS Digiware I-xx avec capteur de courant associé
Binary input [Entrée binaire]	État (ON/OFF) d'un contact auxiliaire
Binary output [Sortie binaire]	Changement d'état de la sortie d'un DIRIS Digiware IO-10

Une liste de propriétés définit chaque objet BACnet. Une propriété peut être :

- Obligatoire, requise par la spécification BACnet.
- Facultative. Dans ce cas, les constructeurs peuvent choisir si les mettre en œuvre pour leurs dispositifs.
- Propriétaire. Les constructeurs peuvent ajouter des propriétés de leur création.

Objet Device [Dispositif] :

Chaque dispositif BACnet compatible avec la DIRIS Digiware M-50/M-70 doit avoir l'objet Device et ses propriétés obligatoires associées qui décrivent complètement le dispositif BACnet au réseau.

Exemple d'objet Device de la DIRIS Digiware M-50/M-70 :

Propriété	BACnet
Object_Identifier (OID)	Obligatoire
Object_Name	Obligatoire
Object_Type	Obligatoire
System_Status	Obligatoire
Vendor_Name	Obligatoire
Vendor_Identifier	Obligatoire
Model_Name	Obligatoire
Firmware_Revision	Obligatoire
Application_Software_Version	Obligatoire
Protocol_Version	Obligatoire
Protocol_Conformance_Class	Obligatoire
Protocol_Services_Supported	Obligatoire
Protocol_Object_Types_Supported	Obligatoire
Object_List	Obligatoire
Max_APDU_Length_Supported	Obligatoire
Segmentation_Supported	Obligatoire
APDU_Timeout	Obligatoire
Emplacement	Facultative
Description	Facultative
Local_Time	Facultative
Utc_Offset	Facultative
Local_Date	Facultative
Daylight_Saving_Status	Facultative
Active_COV_Subscriptions	Facultative
Serial_Number	Facultative
Property_List	Facultative
Version_Build_Date	Propriétaire
Operating_Hour_Counter	Propriétaire

L'OID est attribué à un dispositif (numéro d'instance) de la manière suivante :

OID = OID principal (= 100 par défaut) + Adresse Modbus :

- Le dispositif qui a l'OID principal (100) est la passerelle DIRIS Digiware M-50/M-70 elle-même.
- Le dispositif qui a l'OID (1xx) est le dispositif dont l'adresse Modbus est xx.

Objet Analog Input [Entrée analogique] :

DIRIS Digiware M-50/M-70 fait office de passerelle BACnet. Elle fournit un nombre d'objets Analog Input qui peuvent être disponibles depuis des dispositifs compatibles et connectés à la DIRIS Digiware M-50/M-70.
Qu'un dispositif prenne en charge ou non un objet AI dépend de ses fonctionnalités de mesure.

Par ex. : L'OID pour THD_I1 retournera 0 pour un module DIRIS Digiware I-30 car ce paramètre n'est pas géré.

L'objet AI définit 25 propriétés. Les dispositifs compatibles et connectés en aval du DIRIS Digiware D-50 / D-70 prennent en charge les propriétés suivantes :

PROPRIÉTÉ	BACnet
Object_Identifier	Obligatoire
Object_Name	Obligatoire
Object_Type	Obligatoire
Present_Value	Obligatoire
Status_Flags	Obligatoire
Event_State	Obligatoire
Out_Of_Service	Obligatoire
Units	Obligatoire
Description	Facultative
Reliability	Facultative
Min_Pres_Value	Facultative
Minimum_Value_Timestamp	Facultative
Max_Pres_Value	Facultative
Maximum_Value_Timestamp	Facultative
Average_Value	Facultative
Instantaneous_Timestamp	Propriétaire
Average_Timestamp	Propriétaire
Max_Average_Value	Propriétaire
Max_Average_Timestamp	Propriétaire
Min_Average_Value	Propriétaire
Min_Average_Timestamp	Propriétaire
Harmonics_Row_02	Propriétaire
Harmonics_Row_03	Propriétaire
Harmonics_Row_04	Propriétaire

PROPRIÉTÉ	BACnet
Harmonics_Row_05	Propriétaire
Harmonics_Row_06	Propriétaire
Harmonics_Row_07	Propriétaire
Harmonics_Row_08	Propriétaire
Harmonics_Row_09	Propriétaire
Harmonics_Row_10	Propriétaire
Energy_Total_Residual	Propriétaire
Energy_Total_Hourmeter	Propriétaire
Energy_Partial	Propriétaire
Energy_Partial_Residual	Propriétaire
Energy_Partial_Hourmeter	Propriétaire
Energy_Total_Lagging	Propriétaire
Energy_Total_Lagging_Res	Propriétaire
Energy_Total_Leading	Propriétaire
Energy_Total_Leading_Res	Propriétaire
Energy_Last_Partial	Propriétaire
Energy_Last_Partial_Res	Propriétaire
Energy_Last_Partial_Timestamp	Propriétaire
Multifluid_Partial	Propriétaire
Multifluid_Weight	Propriétaire
Instant_Min_Max_Reset	Propriétaire
Average_Min_Max_Reset	Propriétaire

L'OID est attribué à un objet Analog Input [Entrée analogique] (numéro d'instance) de la manière suivante :
OID = LLMM

- Où LL = N° de la charge du dispositif (en partant de 1)
- Et MM = Indice du type de mesure (voir la liste des mesures d'entrée analogique).

Par exemple, une entrée analogique d'OID 204 correspond à la tension Phase/Neutre V1 de la charge 2 du dispositif correspondant.

La table contenant les indices de la liste des mesures d'entrée analogique est la suivante :

Indice	Nom de l'objet	Description de l'objet	Unité	Type	Présent. + horodatage	Min/Max présent. + horodatage	Moyenne + horodatage	Min/Max moyen. + horodatage	Harmoniques 2 -> 10	Énergies Totale + Partielle +/DernPartielle	Énergies Totale Ind/Cap	Multifluide	RAZ Min/Max
0	VystPhN	Tension Ph-N système	V	Non signé	•								•
1	VystPhPh	Tension Ph-Ph système	V	Non signé	•								•
2	CurrentSyst	Courant système	A	Non signé	•								•
3	Fréquence	Fréquence système	Hz	Non signé	•	•	•	•					•
4	VoltPhNV1	Tension Ph-N V1	V	Non signé	•	•	•	•					•
5	VoltPhNV2	Tension Ph-N V2	V	Non signé	•	•	•	•					•
6	VoltPhNV3	Tension Ph-N V3	V	Non signé	•	•	•	•					•
7	VoltPhNVn	Tension Ph-N Vn	V	Non signé	•	•	•	•					•
8	VoltPhPhU12	Tension Ph-Ph U12	V	Non signé	•	•	•	•					•
9	VoltPhPhU23	Tension Ph-Ph U23	V	Non signé	•	•	•	•					•
10	VoltPhPhU31	Tension Ph-Ph U31	V	Non signé	•	•	•	•					•
11	CurrentI1	Courant I1	A	Non signé	•	•	•	•					•
12	CurrentI2	Courant I2	A	Non signé	•	•	•	•					•
13	CurrentI3	Courant I3	A	Non signé	•	•	•	•					•
14	CurrentIn	Courant In	A	Non signé	•	•	•	•					•
15	CurrentInba	Courant Inba	%	Non signé	•								•
16	CurrentIdir	Courant Idir	A	Non signé	•								•
17	CurrentIinv	Courant Iinv	A	Non signé	•								•
18	CurrentIhom	Courant Ihom	A	Non signé	•								•
19	CurrentInb	Courant Inb	%	Non signé	•								•
20	PowerApparentNom	Puissance apparente nominale	VA	Non signé	•								•
21	TotalPowerActive	Puissance active totale	L	Signé	•	•	•	•					•
22	TotalPowerRActive	Puissance réactive totale	VAr	Signé	•	•	•	•					•
23	TotalPowerApparent	Puissance apparente totale	VA	Non signé	•	•	•	•					•
24	TotalPowerFactor	Facteur de puissance total	-	Signé	•	•	•	•					•
25	TotalPowerFactorType	Type de facteur de puissance total	-	Non signé	•	•	•	•					•
26	PowerActiveP1	Puissance active P1	L	Signé	•	•	•	•					•
27	PowerActiveP2	Puissance active P2	L	Signé	•	•	•	•					•
28	PowerActiveP3	Puissance active P3	L	Signé	•	•	•	•					•

Indice	Nom de l'objet	Description de l'objet	Unité	Type	Présent. + horodatage	Min/Max présent. + horodatage	Moyenne + horodatage	Min/Max moyen. + horodatage	Harmoniques 2 -> 10	Énergies Totale + Partielle +/DernPartielle	Énergies Totale Ind/Cap	Multifluide	RAZ Min/Max
29	PowerRActiveQ1	Puissance réactive Q1	VAr	Signé	•	•	•	•					•
30	PowerRActiveQ2	Puissance réactive Q2	VAr	Signé	•	•	•	•					•
31	PowerRActiveQ3	Puissance réactive Q3	VAr	Signé	•	•	•	•					•
32	PowerApparentS1	Puissance apparente S1	VA	Non signé	•	•	•	•					•
33	PowerApparentS2	Puissance apparente S2	VA	Non signé	•	•	•	•					•
34	PowerApparentS3	Puissance apparente S3	VA	Non signé	•	•	•	•					•
35	PowerFactorPF1	Facteur de puissance PF1	-	Signé	•	•	•	•					•
36	PowerFactorTypeSPF1	Type de facteur de puissance sPF1	-	Non signé	•	•	•	•					•
37	PowerFactorPF2	Facteur de puissance PF2	-	Signé	•	•	•	•					•
38	PowerFactorTypeSPF2	Type de facteur de puissance sPF2	-	Non signé	•	•	•	•					•
39	PowerFactorPF3	Facteur de puissance PF3	-	Signé	•	•	•	•					•
40	PowerFactorTypeSPF3	Type de facteur de puissance sPF3	-	Non signé	•	•	•	•					•
41	LoadCurve_P+	Puissance active positive de la courbe de charge	L	Non signé	•								•
42	LoadCurve_P-	Puissance active négative de la courbe de charge	L	Non signé	•								•
43	LoadCurve_ Q+	Puissance réactive positive de la courbe de charge	VAr	Non signé	•								•
44	LoadCurve_Q-	Puissance réactive négative de la courbe de charge	VAr	Non signé	•								•
45	LoadCurve_S	Puissance apparente de la courbe de charge	VA	Non signé	•								•
46	THD_I1	I1 THD	%	Non signé	•	•			•				•
47	THD_I2	I2 THD	%	Non signé	•	•			•				•
48	THD_I3	I3 THD	%	Non signé	•	•			•				•
49	THD_In	In THD	%	Non signé	•	•			•				•
50	THD_V1	V1 THD	%	Non signé	•	•			•				•
51	THD_V2	V2 THD	%	Non signé	•	•			•				•
52	THD_V3	V3 THD	%	Non signé	•	•			•				•
53	THD_U12	U12 THD	%	Non signé	•	•			•				•
54	THD_U23	U23 THD	%	Non signé	•	•			•				•

Indice	Nom de l'objet	Description de l'objet	Unité	Type	Présent. + horodatage	Min/Max présent. + horodatage	Moyenne + horodatage	Min/Max moyen. + horodatage	Harmoniques 2 -> 10	Énergies Totale + Partielle +/DernPartielle	Énergies Totale Ind/Cap	Multifluide	RAZ Min/Max
55	THD_U31	U31 THD	%	Non signé	•	•			•				•
56	A+	Énergie active positive	Wh	Non signé	•					•			•
57	A-	Énergie active négative	Wh	Non signé	•					•			•
58	ER+	Énergie active positive	VArh	Non signé	•					•	•		•
59	ER-	Énergie réactive négative	VArh	Non signé	•					•	•		•
60	ES	Énergie apparente	VAh	Non signé	•					•			•
61	Mff	Départ multifluide	-	Signé	•							•	•

Annexe II - 3. Services BACnet

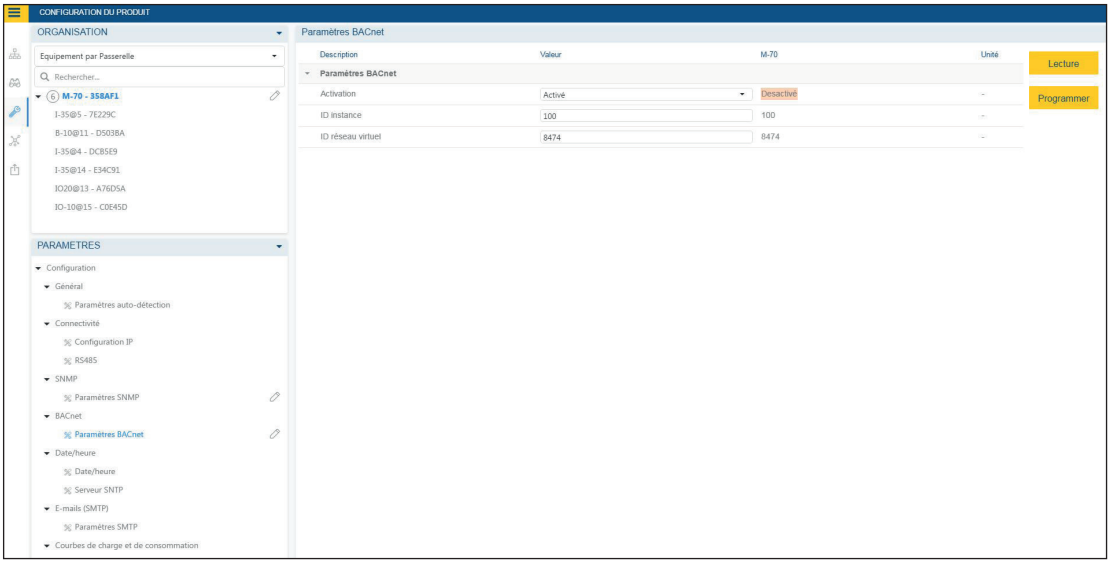
Les services définissent les méthodes que les dispositifs BACnet utilisent pour communiquer et échanger des données entre eux.
La DIRIS Digiware M-50/M-70 supporte les services suivants :

Liste des services	Description
readProperty	Utilisé par un dispositif BACnet (le client) pour demander à un autre dispositif BACnet (le serveur) de fournir la valeur d'une de ses propriétés d'objet.
readPropertyMultiple	Utilisé par un dispositif BACnet (le client) pour demander à un autre dispositif BACnet (le serveur) de fournir les valeurs de plusieurs propriétés d'objet.
writeProperty	Utilisé par un dispositif BACnet (le client) pour demander à un autre dispositif BACnet (le serveur) de modifier la valeur d'une de ses propriétés d'objet.
timeSynchronization	Utilisé pour diffuser l'heure courante sur un ou plusieurs serveurs BACnet.
who_Has	Demande quels dispositifs BACnet contiennent un objet particulier.
who_Is	Utilisé par un client BACnet pour s'enquérir de la présence de serveurs BACnet.

Annexe II - 4. Configuration du protocole BACnet IP via Easy Config System

Le fichier PICS (Protocol Implementation Conformance Statement, Déclaration de conformité de mise en œuvre de protocole) est disponible sur www.socomec.fr/fr/centre-de-telechargement?query=notice

Après s'être connecté à Easy Config System sur DIRIS Digiware M-50/M-70, il est possible de trouver le paramétrage BACnet IP dans le menu “BACnet”, sous “Paramètres BACnet”:



Activation : Active ou désactive le protocole BACnet IP.

ID principal : 100 par défaut. Cet ID doit être unique au sein du réseau BACnet.

ID réseau virtuel : Règle l’identifiant du réseau virtuel. Cet ID doit être unique au sein du réseau BACnet.

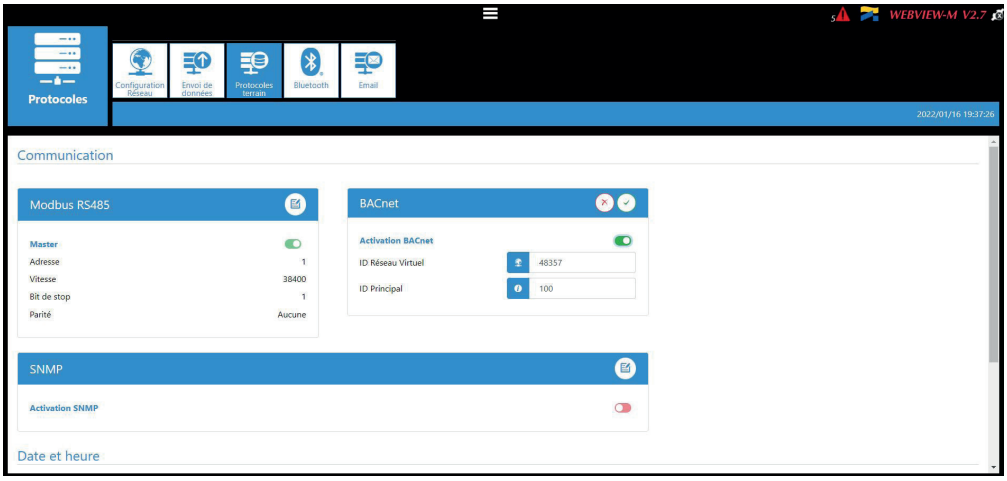
Le port utilisé par la DIRIS Digiware M-50/M-70 pour la communication BACnet IP est 47808 (BAC0 en hexadécimale) et ne peut pas être modifié.

Annexe II - 5. Configuration du protocole BACnet IP depuis le serveur Web embarqué

Cliquer sur l'icône « Boîte-à-outils » dans le coin supérieur gauche et cliquer sur « Protocoles »:

Cliquer sur l'onglet « Protocoles Terrain » et, dans « Communication », puis BACnet, saisir les paramètres BACnet :

- **Activation BACnet :** active ou désactive la communication BACnet IP de la passerelle M-50/M-70.
- **ID réseau virtuel :** définit l'identifiant du réseau virtuel de la passerelle M-50/M-70. Cet ID doit être unique au sein du réseau BACnet.
- **ID principal :** définit l'ID de l'instance principale (100 par défaut) de la passerelle M-50/M-70. Cet ID doit être unique au sein du réseau BACnet.



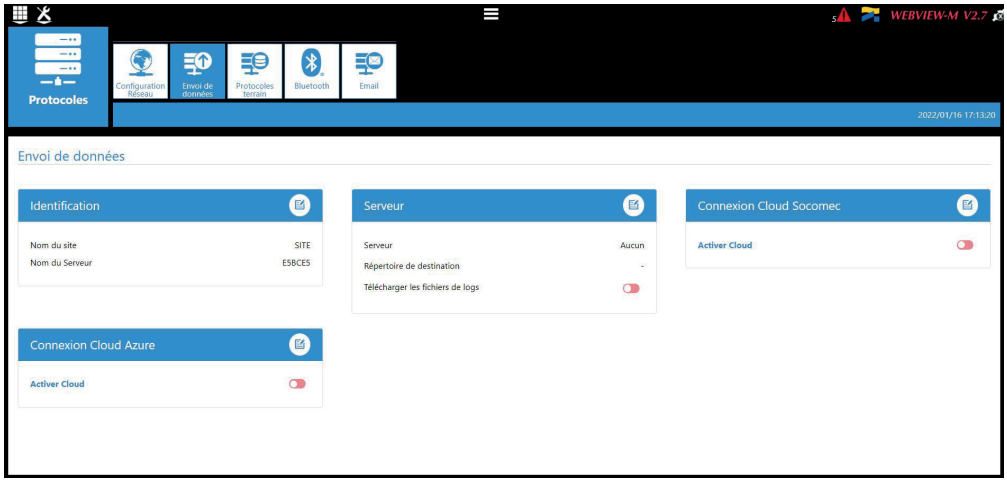
ANNEXE III. CONFIGURATION DES EXPORTS FTP

Les historiques de mesures (voir « 6.2.2. Introduction au DIRIS Digiware D-70 », page 10) peuvent être exportés automatiquement via FTP(S).

Annexe III - 1. Activation du serveur FTP

Cliquer sur l'icône « Boîte-à-outils » dans le coin supérieur gauche et cliquer sur « Protocoles » :

Cliquer sur « Envoi de données » :

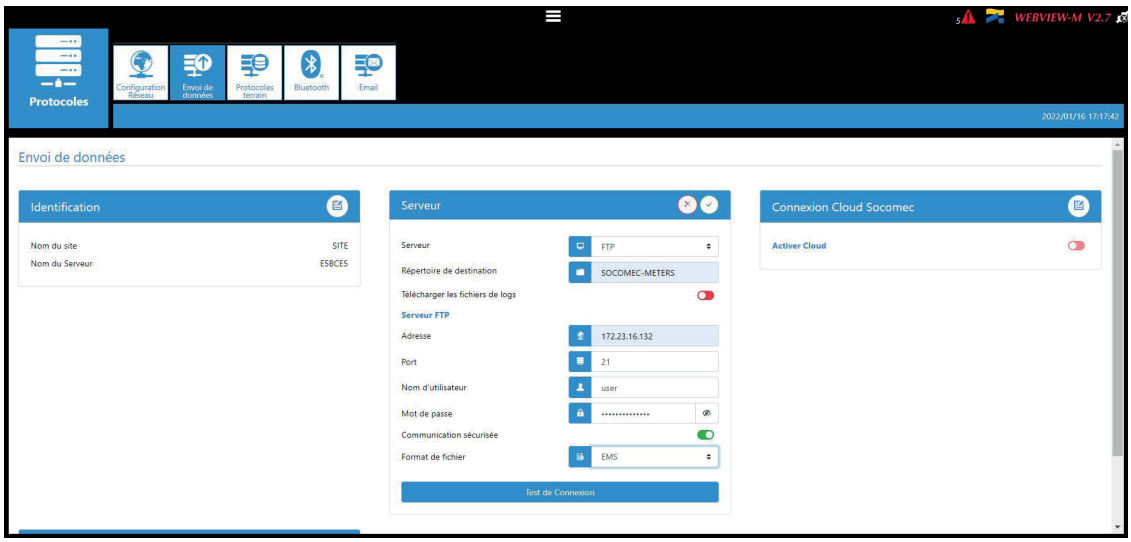


Partie Identification :

Nom du site et nom du serveur : utilisé pour identifier le DIRIS Digiware D-50/D-70 à partir duquel les fichiers sont exportés.

Le nom du site par défaut est « SITE » (à modifier impérativement en mode d'export EMS) et le nom par défaut du serveur correspond à l'ID gravé sur la face avant de la passerelle M-50/M-70.

Partie Serveur :



Serveur : activer le serveur FTP pour activer l'export automatique des données vers un serveur FTP distant.

Répertoire de destination : arborescence du dossier du serveur FTP dans lequel exporter les fichiers.

Télécharger les fichiers de logs : activer cette option pour disposer d'informations supplémentaires pour le dépannage en cas d'anomalie lors de l'exportation.

Serveur FTP : Cette partie contient les détails de connexion du serveur FTP (standard ou sécurisé).

Adresse : saisir l'adresse IP du serveur FTP.

Port : saisir le port sécurisé ou non sécurisé à utiliser pour l'export FTP.

Nom d'utilisateur : Nom d'utilisateur : saisir le nom d'utilisateur pour accéder au serveur distant. Il doit concorder avec le nom d'utilisateur configuré sur le serveur FTP.

Mot de passe : saisir le mot de passe pour accéder au serveur distant. Il doit concorder avec le mot de passe configuré sur le serveur FTP.

Communication sécurisée : activer ou désactiver l'exportation sécurisée (FTPS).

Format de fichier : il existe deux types de fichiers de données différents :

- **CSV :** fichier dans lequel les données sont présentées à l'utilisateur de manière conviviale.
- **EMS :** fichier au format .csv dont la disposition est plus pratique pour une intégration dans un logiciel de gestion de l'énergie.

En mode EMS, les fichiers exportés sont nommés de la façon suivante :

Nom du site_Nom du serveur_Nom du dispositif_Type des données_date_heure.csv

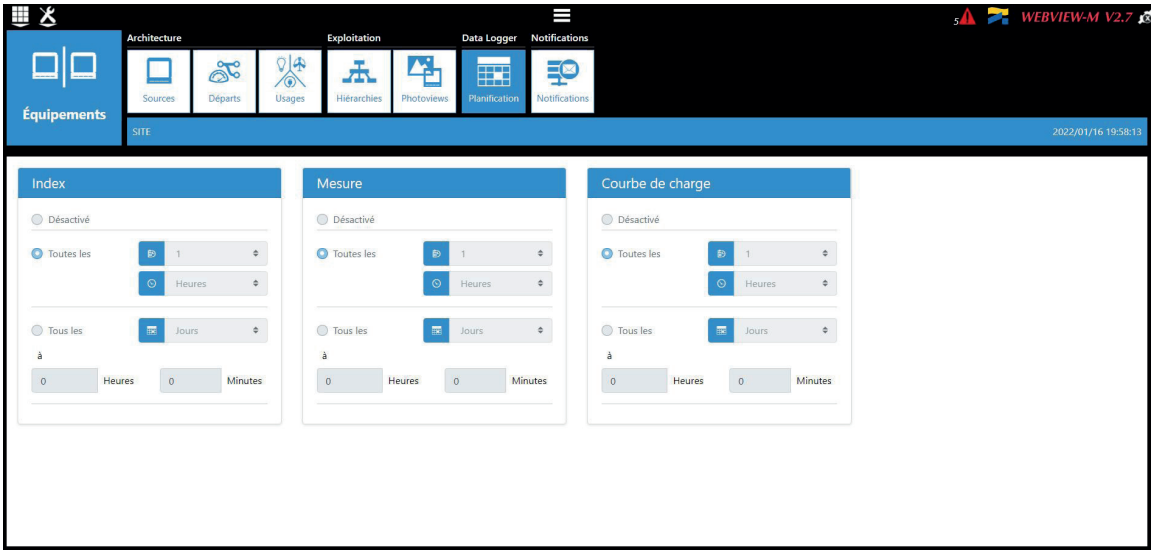
Exemple : si un fichier d'exportation est nommé « ***socomec_E5C801_I35_LoadCurve_2017-08-15_20-00-00.csv*** », cela signifie que ce fichier a été exporté le 15 août 2017 à 20h00 (8h00 pm), qu'il contient des courbes de charge (Load curves) d'un dispositif nommé I35 depuis une passerelle dont le nom de serveur est E5C801 et le nom de site est socomec.

En mode EMS, le nom du site doit être différent du nom par défaut (« SITE »), à défaut de quoi l'alarme système « Erreur FTP » se déclenchera.

Test de Connexion : une fois la configuration terminée, il est possible de tester la connexion en exportant manuellement un fichier de test vers le serveur FTP.

Cliquer sur « Équipements » :

Cliquer sur « Planification ».



Sélectionner le type de données à exporter pour les exporter automatiquement. Le DIRIS Digiware D-50/D-70 peut enregistrer et exporter trois types de données :

Index d'énergie : Ea, Er, Es etc.

Historiques de mesures : paramètres historisés U, I, F, PF etc. (Mesures)

Courbes de charge : P, Q, S

Pour chaque type de données, préciser la fréquence à laquelle les données seront exportées (une fois par heure, une fois par jour, etc.) et à quelle heure.

socomec_E5C801_I-35@4_Avg_2019-01-18_15-15-10.csv

	A	B	C	D	E	F	G	H	I	J	K	L
1	Data Type	TimeZone	Datation	Transfer Cycle (sec)	Pooling Ti	Version	Site name	Server name				
2	Avg	UTC	Local	600	N/A	1	socomec	E5C801				
3												
4	Index Key	Key	Type	Name	Fluid	Use	Coef	Unit	Path	Device Id	Index	Data Id
5	0	socomec|E5C801|14|1|ANA|100006	ANA	THD I1 of PC 1-2-3 of I-35@4	ELEC	Use2	100	%	/	14	1	100006
6	1	socomec|E5C801|14|1|ANA|100007	ANA	THD I2 of PC 1-2-3 of I-35@4	ELEC	Use2	100	%	/	14	1	100007
7	2	socomec|E5C801|14|1|ANA|100008	ANA	THD I3 of PC 1-2-3 of I-35@4	ELEC	Use2	100	%	/	14	1	100008
8	3	socomec|E5C801|14|1|ANA|10023	ANA	I1 AVG of PC 1-2-3 of I-35@4	ELEC	Use2	1000	A	/	14	1	10023
9	4	socomec|E5C801|14|1|ANA|10024	ANA	I2 AVG of PC 1-2-3 of I-35@4	ELEC	Use2	1000	A	/	14	1	10024
10	5	socomec|E5C801|14|1|ANA|10025	ANA	I3 AVG of PC 1-2-3 of I-35@4	ELEC	Use2	1000	A	/	14	1	10025
11												
12	Index Key	Date	Value	Quality								
13	0	2019-01-18T15:14:00	234	192								
14	0	2019-01-18T15:13:00	237	192								
15	0	2019-01-18T15:12:00	190	192								
16	0	2019-01-18T15:11:00	201	192								
17	0	2019-01-18T15:10:00	200	192								
18	0	2019-01-18T15:09:00	198	192								
19	0	2019-01-18T15:08:00	210	192								
20	0	2019-01-18T15:07:00	231	192								
21	0	2019-01-18T15:06:00	211	192								
22	0	2019-01-18T15:05:00	199	192								
23	1	2019-01-18T15:14:00	20001	192								
24	1	2019-01-18T15:13:00	21605	192								
25	1	2019-01-18T15:12:00	19804	192								
26	1	2019-01-18T15:11:00	20901	192								

1

2

Le fichier csv est divisé en deux parties :

- La partie (1) en rouge correspond à l'en-tête. Elle contient un code unique, créé à partir de plusieurs paramètres tels que le nom du site et celui du serveur, le type des données, l'ID des données et l'ID du dispositif, afin d'identifier de manière unique chaque paramètre exporté.
- La partie (2) en vert contient les mesures enregistrées et d'horodatage. Chaque ligne est identifiée par le code d'index simplifié, qui fait référence à un code unique dans les cellules B5 à B10.

La valeur finale pour les cellules C13 à C26 est obtenue en prenant en compte le bon coefficient dans les cellules G5 à G10 avec la bonne unité dans les cellules H5 à H10.

Exemple pour la ligne 13 :

La valeur finale de THD I1 pour le circuit PC1-2-3 sur le module I-35@4 est égale à 2,34 % le 18 janvier, 2019 à 15:14:00.

Lors de l'intégration des données dans un logiciel de surveillance ou de gestion énergétique de tiers, faire toujours référence au code unique dans la colonne « B » , partie (1) comme à un code d'importation unique et ne pas utiliser uniquement le code d'index simplifié de la colonne « A », partie (2).

En effet, si plusieurs passerelles DIRIS Digiware M-50/M-70 exportent dans le même dossier, le code d'index simplifié ne permet pas de les différencier.

ANNEXE IV. RECHERCHER ET AJOUTER LE CA (AUTORITÉ DE CERTIFICATION) D'UN SERVEUR À UNE PASSERELLE DIRIS DIGIWARE M-50/M-70.

Exigences :

1. Une connexion internet non filtrée
2. Le logiciel OpenSSL installé

Instructions

> Utiliser la commande suivante :

```
openssl s_client -connect <server>:<port> -build_chain
```

> Exemple pour Gmail (SMTP):

```
openssl s_client -connect smtp.gmail.com:465 -build_chain
```

> Vérifier la dernière ligne de la chaîne de certificats dans le résultat de la commande :

```
$ openssl s_client -connect smtp.gmail.com:465 -build_chain
CONNECTED(00000268)
---
Certificate chain
 0 s:CN = smtp.gmail.com
   i:C = US, O = Google Trust Services LLC, CN = GTS CA 1C3
 1 s:C = US, O = Google Trust Services LLC, CN = GTS CA 1C3
   i:C = US, O = Google Trust Services LLC, CN = GTS Root R1
 2 s:C = US, O = Google Trust Services LLC, CN = GTS Root R1
   i:C = BE, O = GlobalSign nv-sa, OU = Root CA, CN = GlobalSign Root CA
```

> Aller sur le site web de l'autorité correspondante et trouver la page de téléchargement des certificats racines.
Pour Gmail, GlobalSign Root CA : https://support.globalsign.com/ca-certificates/root-certificates/globalsign-root-certificates

> Télécharger le certificat PEM (ou Base64).

Si le certificat est donné sous forme de texte, copiez le texte entre `BEGIN CERTIFICATE` et `END CERTIFICATE` dans un fichier texte et enregistrez-le avec une extension .pem, comme indiqué dans l'exemple ci-dessous :

R1 GlobalSign Root Certificate

GlobalSign Root R1

SHA1 • RSA • 2048

Valid until: 28 January 2028

Serial #: 04:00:00:00:00:01:15:4b:5a:c3:94

Thumbprint: b1:bc:96:8b:d4:f4:9d:62:2a:a8:9a:81:f2:15:01:52:a4:1d:82:9c

Root R1 was GlobalSign's first root certificate embedded in browsers (back in 1999, Netscape and Windows 98), making Root R1 GlobalSign's oldest and most ubiquitous root certificate. The original use case was for personal certificates, but this quickly expanded as GlobalSign's business and expertise broadened. Due to its hash algorithm, GlobalSign will begin scaling back Root R1 use.

Does my browser trust this certificate?

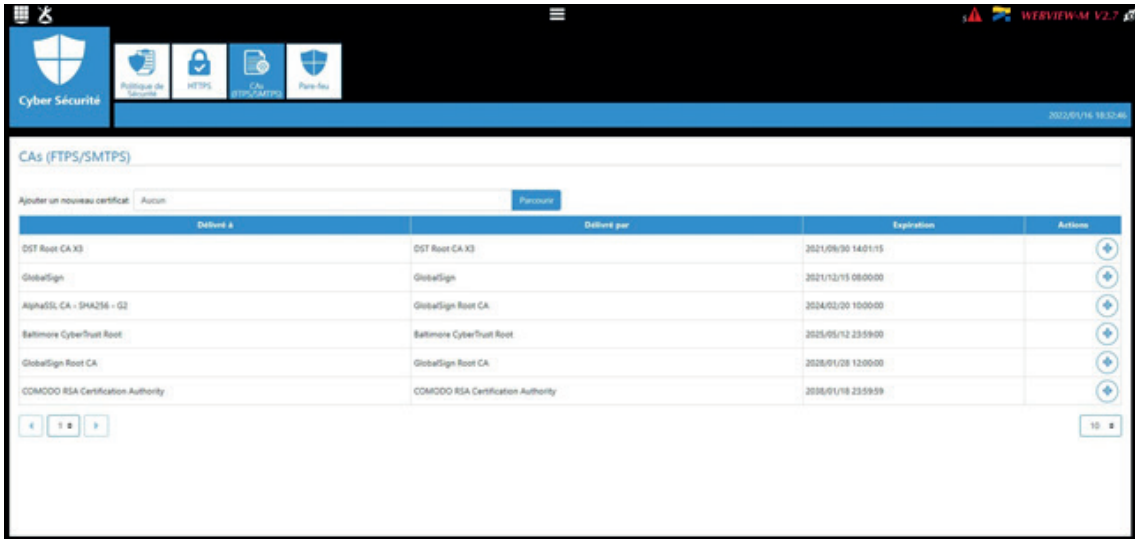
Download Certificate (Binary/DER Encoded) | View in Base64

-----BEGIN CERTIFICATE-----
MIIDdTCCAl2gAwIBAgILBAAAAAABFUtaw5QwDQYJKoZIhvcNAQEFBQAwVzELMAkG
A1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv
b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNpZ24gUm9vdCBDQTAeFw05ODA5MDExMjAw
MDBaFw0yODAxMjgxMjAwMDBaMFcxCzAJBgNVBAYTAkJFMRkwFwYDVQQKExBHbG9i
YWxTaWduIG52LXNhMRAwDgYDVQQLEwdSb290IENBMRswGQYDVQQDExJHbG9iYWxT
aWduIFJvb3QgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDaDuaZ
jc6j40+Kfvvxi4Mla+pIH/EqsLmVEQS98GPR4mdmzxzdzxtIK+6NiY6arymAZavp
xy0Sy6scTHAHoT0KMM0VjU/43dSMUBUc71DuxC73/OlS8pF94G3VNTCOXkNz8kHp
1Wrjsok6Vjk4bwY8iGlbKk3Fp1S4bInMm/k8yuX9ifUSPJJ4ItbcdG6TRGHRjcdG
snUOhugZitVtbNV4FpWi6cgKOOvyJBNPc1STE4U6G7weNLWLBYy5d4ux2x8gkasJ
U26Qzns3dLlwR5EiUWMWea6xrkEmCMgZK9FGqkjWZCrXgzT/LCrBbBlDSgeF59N8
9iFo7+ryUp9/k5DPAgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIBBjAPBgNVHRMBAf8E
BTADAQH/MB0GA1UdDgQWBBRge2YaRQ2XyolQL30EzTSo//z9SzANBgkqhkiG9w0B
AQUFAAOCAQEA1nPnfE920I2/7LqivjTFKDK1fPxsnCwrvQmeU79rXqoRSLblCKOz
yj1hTdNGCbM+w6DjY1Ub8rrvrTnhQ7k4o+YviiY776BQVvnGCv04zcQLcFGUl5gE
38NflNUVyRRBnMRddWQVDf9VMOyGj/8N7yy5Y0b2qvzfvGn9LhJIZJrglfCm7ymP
AbEVtQwdpf5pLGkkeB6zpxxxYu7KyJesF12KwvhHhm4qxFYxldBniYUr+WymXUad
DKqC5JlR3XC321Y9YeRq4VzW9v493kHMB65jUr9TU/Qr6cf9tveCX4XSQRjbgbME
HMUfpIBvFSDJ3gyICh3WZlXi/EjJKSZp4A==
-----END CERTIFICATE-----

> Se connecter au serveur web (WEBVIEW pour M-70 et WEB-CONFIG pour M-50) sous le profil Cyber Sécurité.

> Aller dans le menu Cyber Sécurité :

> Cliquer sur l'onglet « CAs (FTPS/SMTPS) » et cliquer sur « Parcourir » pour ajouter le fichier .PEM précédemment téléchargé :



SIÈGE GÉNÉRAL, CONTACTER :
SOCOMEC SAS
1-4 RUE DE WESTHOUSE
67235 BENFELD, FRANCE

www.socomec.com

548751E

socomec
Innovative Power Solutions