

BMENOR2200H

Module RTU avancé Modicon X80

Manuel utilisateur

Traduction de la notice originale

EIO0000004870.01

11/2023

Mentions légales

Les informations fournies dans ce document contiennent des descriptions générales, des caractéristiques techniques et/ou des recommandations concernant des produits/solutions.

Ce document n'est pas destiné à remplacer une étude détaillée ou un plan de développement ou de représentation opérationnel et propre au site. Il ne doit pas être utilisé pour déterminer l'adéquation ou la fiabilité des produits/solutions pour des applications utilisateur spécifiques. Il incombe à chaque utilisateur individuel d'effectuer, ou de faire effectuer par un professionnel de son choix (intégrateur, spécificateur ou équivalent), l'analyse de risques exhaustive appropriée ainsi que l'évaluation et les tests des produits/solutions par rapport à l'application ou l'utilisation particulière envisagée.

La marque Schneider Electric et toutes les marques de commerce de Schneider Electric SE et de ses filiales mentionnées dans ce document sont la propriété de Schneider Electric SE ou de ses filiales. Toutes les autres marques peuvent être des marques de commerce de leurs propriétaires respectifs.

Ce document et son contenu sont protégés par les lois sur la propriété intellectuelle applicables et sont fournis à titre d'information uniquement. Aucune partie de ce document ne peut être reproduite ou transmise sous quelque forme ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement ou autre), à quelque fin que ce soit, sans l'autorisation écrite préalable de Schneider Electric.

Schneider Electric n'accorde aucun droit ni aucune licence d'utilisation commerciale de ce document ou de son contenu, sauf dans le cadre d'une licence non exclusive et personnelle, pour le consulter tel quel.

Schneider Electric se réserve le droit d'apporter à tout moment des modifications ou des mises à jour relatives au contenu de ce document ou à son format, sans préavis.

Dans la mesure permise par la loi applicable, Schneider Electric et ses filiales déclinent toute responsabilité en cas d'erreurs ou d'omissions dans le contenu informatif du présent document ou pour toute conséquence résultant de l'utilisation des informations qu'il contient.

Table des matières

Consignes de sécurité.....	7
Avant de commencer	8
Démarrage et test.....	9
Fonctionnement et réglages	9
A propos de ce manuel	11
Présentation du module RTU avancé Modicon X80	
BMENOR2200H.....	14
Introduction.....	14
Description physique	18
Voyants du module	23
Carte mémoire SD (BMXRMS004GPF).....	26
Commutateur rotatif de cybersécurité.....	28
Connecteur d'embase	30
Caractéristiques électriques	32
Normes et certifications.....	32
Normes de sécurité et certifications.....	32
Module BMENOR2200H dans les réseaux	34
Réseaux autonomes.....	34
Architectures M580 autonomes.....	34
Réseau autonome avec un sous-réseau	35
Réseau autonome avec deux sous-réseaux.....	36
Réseau autonome avec redondance de liaison	37
Réseau autonome avec trois sous-réseaux.....	38
Réseau isolé sous contrôleur autonome	39
Réseaux M580 redondants	40
Introduction	40
Architecture redondante avec un sous-réseau.....	41
Architecture redondante avec réseau isolé.....	43
Installation du matériel	44
Montage du module sur le rack	44
Communications Ethernet	52
Services Ethernet	52
Services Ethernet disponibles.....	52
Service SNMP.....	53
Présentation de SNMP	53
Communication SNMP	54
Versions de SNMP.....	55
Informations détaillées sur l'agent SNMP	56
Exemple d'opérations SNMP	57
Prise en charge de MIB	58
Mise à niveau du micrologiciel	59
Outil EcoStruxure™ Automation Device Maintenance.....	59
Service client FDR de base	60
Service client FDR de base.....	60
Messagerie Modbus TCP.....	61
Accès aux données.....	61
Echange de données	61

Utilisation des protocoles RTU.....	63
Protocoles de communication.....	63
Protocoles IEC60870-5-101/104.....	64
Types de données pris en charge par IEC60870-5-101/104	70
Caractéristiques de IEC60870-5-101/104	72
Protocole DNP3	74
Types de données pris en charge par DNP3	76
Fonctionnalités DNP3	78
Concepts de l'authentification sécurisée DNP3.....	80
Synchronisation d'horloge	82
Synchronisation d'horloge avec le protocole RTU	82
Synchronisation d'horloge avec SNMP	83
Synchronisation d'horloge avec le contrôleur	84
Gestion des événements.....	85
Introduction à la gestion des événements	85
Routage d'événements.....	87
Sauvegarde des événements	90
Flux de données du protocole RTU	91
Communications RTU	91
Etat de la connexion	94
Etat de connexion	94
Réinitialisation de la communication.....	95
Capacité de redondance d'UC (Hot Standby).....	96
Capacité de redondance d'UC	96
Gestion des services Ethernet	100
SOE (Sequence Of Events)	101
Séquence d'événements horodatés	101
Configuration du module.....	105
Présentation de la configuration.....	105
Composants de configuration	105
Utilisation du module dans un projet Control Expert.....	106
Ajouter le DTM et le module à Control Expert	106
A propos du navigateur de DTM de Control Expert	107
Ajout du module à un projet	110
Configuration avec Control Expert.....	111
Configuration d'adresse IP.....	111
Débogage avec Control Expert	112
Ecran de mise au point du module.....	112
Configuration dans le DTM	113
Accès au DTM	113
Configuration de voies DNP3	115
Configuration d'équipement DNP3	120
Mappage des objets de données DNP3	125
Evénements DNP3	140
Configuration de voies IEC60870	141
Configuration de session / d'équipement IEC60870	145
Mappage d'objets de données IEC60870.....	150
Evénements IEC60870	155
Configuration de SNMP	156
Configuration du service de temps réseau	158
Configuration des ports de contrôle	163

Exportation et importation de fichiers .xml avec le DTM.....	165
Informations du module dans le DTM	168
Journalisation des données	169
A propos de la journalisation des données	169
Avant de commencer	171
Configuration de la journalisation des données dans Control Expert.....	171
Diagnostics des pages Web et des DDT d'équipement.....	180
Accès aux pages Web	180
Diagnostics des pages Web	182
Diagnostics des pages Web.....	182
Diagnostics du module	183
Diagnostics des équipements connectés	187
Diagnostics des services	189
Diagnostic de DDT d'équipement.....	193
Structure des DDT d'équipement	193
Diagnostic de DDT d'équipement	195
Explorateur de fichiers	199
Configuration de la cybersécurité.....	201
Présentation des pages Web de cybersécurité.....	201
Pages Web de configuration.....	202
Page Web Stratégie des comptes utilisateur	204
Page Web Journaux d'événements.....	205
Page Web Services Réseau	206
Page Web Bannière de sécurité.....	207
Page Web HSBY	208
Page Web SNMP	209
Gestion des certificats.....	210
Page Web de configuration de PKI.....	212
Page Web de gestion de la liste de confiance	216
Page Web de gestion d'autorité de certification racine	218
Page Web Gestion des clés DNP3.....	220
Page Web de configuration de client DNP3.....	222
Page Web de configuration du serveur DNP3	223
Configuration de l'authentification sécurisée DNP3	224
Pages Web client et serveur IEC60870	227
Page Web Gestion des utilisateurs.....	228
Page Web Gestion de la configuration.....	229
RBAC	231
Annexes	232
Interopérabilité	232
Interopérabilité DNP3.....	233
Interopérabilité IEC60870-5-104	252
Serveur IEC60870-5-101 et profils d'équipement client	273
Migration de projet.....	284
Migration de fichiers XML	284
Migration des types de données DNP3	285
Migration des types de données IEC60870	288
Événements journalisés	293
Codes de diagnostic Modbus.....	294

Mappage de données pour le code de fonction Modbus 3 avec ID d'unité 100	294
Codes d'erreur détectée	323
Messagerie explicite : rapports de communication et d'opération	323
Codes d'erreur détectée pour la communication RTU	325
Codes d'erreur détectée pour Open SSL/TLS	326
Codes d'erreur détectée pour Open SSL/TLS	326
Compatibilité des versions de micrologiciel	334
Compatibilité des versions de micrologiciel	334
Mise à jour d'application depuis BMENOR2200.2	334
Glossaire	335

Consignes de sécurité

Informations importantes

Lisez attentivement ces instructions et examinez le matériel pour vous familiariser avec l'appareil avant de tenter de l'installer, de le faire fonctionner, de le réparer ou d'assurer sa maintenance. Les messages spéciaux suivants que vous trouverez dans cette documentation ou sur l'appareil ont pour but de vous mettre en garde contre des risques potentiels ou d'attirer votre attention sur des informations qui clarifient ou simplifient une procédure.



La présence de ce symbole sur une étiquette "Danger" ou "Avertissement" signale un risque d'électrocution qui provoquera des blessures physiques en cas de non-respect des consignes de sécurité.



Ce symbole est le symbole d'alerte de sécurité. Il vous avertit d'un risque de blessures corporelles. Respectez scrupuleusement les consignes de sécurité associées à ce symbole pour éviter de vous blesser ou de mettre votre vie en danger.

DANGER

DANGER signale un risque qui, en cas de non-respect des consignes de sécurité, **provoque** la mort ou des blessures graves.

AVERTISSEMENT

AVERTISSEMENT signale un risque qui, en cas de non-respect des consignes de sécurité, **peut provoquer** la mort ou des blessures graves.

ATTENTION

ATTENTION signale un risque qui, en cas de non-respect des consignes de sécurité, **peut provoquer** des blessures légères ou moyennement graves.

AVIS

AVIS indique des pratiques n'entraînant pas de risques corporels.

Remarque Importante

L'installation, l'utilisation, la réparation et la maintenance des équipements électriques doivent être assurées par du personnel qualifié uniquement. Schneider Electric décline toute responsabilité quant aux conséquences de l'utilisation de ce matériel.

Une personne qualifiée est une personne disposant de compétences et de connaissances dans le domaine de la construction, du fonctionnement et de l'installation des équipements électriques, et ayant suivi une formation en sécurité leur permettant d'identifier et d'éviter les risques encourus.

Avant de commencer

N'utilisez pas ce produit sur les machines non pourvues de protection efficace du point de fonctionnement. L'absence de ce type de protection sur une machine présente un risque de blessures graves pour l'opérateur.

⚠ AVERTISSEMENT

EQUIPEMENT NON PROTEGE

- N'utilisez pas ce logiciel ni les automatismes associés sur des appareils non équipés de protection du point de fonctionnement.
- N'accédez pas aux machines pendant leur fonctionnement.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Cet automate et le logiciel associé permettent de commander des processus industriels divers. Le type ou le modèle d'automatisme approprié pour chaque application dépendra de facteurs tels que la fonction de commande requise, le degré de protection exigé, les méthodes de production, des conditions inhabituelles, la législation, etc. Dans certaines applications, plusieurs processeurs seront nécessaires, notamment lorsque la redondance de sauvegarde est requise.

Vous seul, en tant que constructeur de machine ou intégrateur de système, pouvez connaître toutes les conditions et facteurs présents lors de la configuration, de l'exploitation et de la maintenance de la machine, et êtes donc en mesure de déterminer les équipements automatisés, ainsi que les sécurités et verrouillages associés qui peuvent être utilisés correctement. Lors du choix de l'automatisme et du système de commande, ainsi que du logiciel associé pour une application particulière, vous devez respecter les normes et réglementations locales et nationales en vigueur. Le document National Safety Council's Accident Prevention Manual (reconnu aux Etats-Unis) fournit également de nombreuses informations utiles.

Dans certaines applications, telles que les machines d'emballage, une protection supplémentaire, comme celle du point de fonctionnement, doit être fournie pour l'opérateur. Elle est nécessaire si les mains ou d'autres parties du corps de l'opérateur peuvent entrer dans la zone de point de pincement ou d'autres zones dangereuses, risquant ainsi de provoquer des blessures graves. Les produits logiciels seuls, ne peuvent en aucun cas protéger les opérateurs contre d'éventuelles blessures. C'est pourquoi le logiciel ne doit pas remplacer la protection de point de fonctionnement ou s'y substituer.

Avant de mettre l'équipement en service, assurez-vous que les dispositifs de sécurité et de verrouillage mécaniques et/ou électriques appropriés liés à la protection du point de fonctionnement ont été installés et sont opérationnels. Tous les dispositifs de sécurité et de verrouillage liés à la protection du point de fonctionnement doivent être coordonnés avec la programmation des équipements et logiciels d'automatisation associés.

NOTE: La coordination des dispositifs de sécurité et de verrouillage mécaniques/électriques du point de fonctionnement n'entre pas dans le cadre de cette bibliothèque de blocs fonction, du Guide utilisateur système ou de toute autre mise en œuvre référencée dans la documentation.

Démarrage et test

Avant toute utilisation de l'équipement de commande électrique et des automatismes en vue d'un fonctionnement normal après installation, un technicien qualifié doit procéder à un test de démarrage afin de vérifier que l'équipement fonctionne correctement. Il est essentiel de planifier une telle vérification et d'accorder suffisamment de temps pour la réalisation de ce test dans sa totalité.

⚠ AVERTISSEMENT

RISQUES INHERENTS AU FONCTIONNEMENT DE L'EQUIPEMENT

- Assurez-vous que toutes les procédures d'installation et de configuration ont été respectées.
- Avant de réaliser les tests de fonctionnement, retirez tous les blocs ou autres cales temporaires utilisés pour le transport de tous les dispositifs composant le système.
- Enlevez les outils, les instruments de mesure et les débris éventuels présents sur l'équipement.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Effectuez tous les tests de démarrage recommandés dans la documentation de l'équipement. Conservez toute la documentation de l'équipement pour référence ultérieure.

Les tests logiciels doivent être réalisés à la fois en environnement simulé et réel

Vérifiez que le système entier est exempt de tout court-circuit et mise à la terre temporaire non installée conformément aux réglementations locales (conformément au National Electrical Code des Etats-Unis, par exemple). Si des tests diélectriques sont nécessaires, suivez les recommandations figurant dans la documentation de l'équipement afin d'éviter de l'endommager accidentellement.

Avant de mettre l'équipement sous tension :

- Enlevez les outils, les instruments de mesure et les débris éventuels présents sur l'équipement.
- Fermez le capot du boîtier de l'équipement.
- Retirez toutes les mises à la terre temporaires des câbles d'alimentation entrants.
- Effectuez tous les tests de démarrage recommandés par le fabricant.

Fonctionnement et réglages

Les précautions suivantes sont extraites du document NEMA Standards Publication ICS 7.1-1995 :

(En cas de divergence ou de contradiction entre une traduction et l'original anglais, le texte original en anglais prévaudra.)

- Malgré le soin apporté à la conception et à la fabrication de l'équipement ou au choix et à l'évaluation des composants, des risques subsistent en cas d'utilisation inappropriée de l'équipement.
- Il arrive parfois que l'équipement soit dérégulé accidentellement, entraînant ainsi un fonctionnement non satisfaisant ou non sécurisé. Respectez toujours les instructions du fabricant pour effectuer les réglages fonctionnels. Les personnes ayant accès à ces réglages doivent connaître les instructions du fabricant de l'équipement et les machines utilisées avec l'équipement électrique.

- L'opérateur ne doit avoir accès qu'aux réglages fonctionnels dont il a besoin. L'accès aux autres commandes doit être limité afin d'empêcher les changements non autorisés des caractéristiques de fonctionnement.

A propos de ce manuel

Objectif du document

Ce guide décrit le module RTU avancé Modicon X80 BMENOR2200H et sa relation avec les contrôleurs Modicon M580 et les plates-formes distantes X80.

Le module BMENOR2200H joue le rôle de module de communication sur une plate-forme M580 et il applique les règles et directives générales d'utilisation de ces plates-formes.

Ce module assure la disponibilité de la connexion au protocole de télémétrie dans des configurations M580 complexes.

Ce guide traite des sujets suivants :

- Installation
 - Configuration
 - Pages Web intégrées
- Diagnostics, page 180

NOTE: Les paramètres de configuration figurant dans le présent guide sont uniquement destinés à la formation. Ceux qui sont requis par votre propre configuration peuvent différer des exemples fournis.

Champ d'application

Ce document a été actualisé pour le lancement de EcoStruxure™ Control Expert 15.3 Hotfix (ControlExpert_V153_HF003).

Les caractéristiques des produits décrits dans ce document sont censées correspondre aux caractéristiques disponibles sur www.se.com. Toutefois, en application de notre stratégie d'amélioration continue, nous pouvons être amenés à réviser le contenu du document afin de le rendre plus clair et plus précis. Si vous constatez une différence entre les caractéristiques figurant dans ce document et celles fournies sur www.se.com, considérez que le site www.se.com contient les informations les plus récentes.

Informations relatives à la cybersécurité

Des informations sur la cybersécurité sont disponibles sur le site Web de Schneider Electric : <https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp>

Document disponible en téléchargement dans la section de support de cybersécurité :

Titre du document	Adresse de la page Web
How can I ... Reduce Vulnerability to Cyber Attacks?	https://www.se.com/ww/en/download/document/STN+v2/
Recommended Cybersecurity Best Practices	https://www.se.com/ww/en/download/document/7EN52-0390/

Document(s) à consulter

Titre de documentation	Référence
<i>Modicon M580 Standalone System Planning Guide for Frequently Used Architectures</i>	HRB62666 (anglais) HRB65318 (français) HRB65319 (allemand) HRB65320 (italien) HRB65321 (espagnol) HRB65322 (chinois)
<i>Modicon M580 System Planning Guide for Complex Topologies</i>	NHA58892 (English), NHA58893 (French), NHA58894 (German), NHA58895 (Italian), NHA58896 (Spanish), NHA58897 (Chinese)
<i>Modicon M580 Hot Standby System Planning Guide for Frequently Used Architectures</i>	NHA58880 (English), NHA58881 (French), NHA58882 (German), NHA58883 (Italian), NHA58884 (Spanish), NHA58885 (Chinese)
Modicon M580 - Matériel, Manuel de référence	EIO0000001578 (Anglais), EIO0000001579 (Français), EIO0000001580 (Allemand), EIO0000001582 (Italien), EIO0000001581 (Espagnol), EIO0000001583 (Chinois)
Plates-formes Modicon M580, M340 et X80 I/O, Normes et certifications	EIO0000002726 (Anglais), EIO0000002727 (Français), EIO0000002728 (Allemand), EIO0000002730 (Italien), EIO0000002729 (Espagnol), EIO0000002731 (Chinois)
Modicon M580 - Change Configuration on the Fly, Guide utilisateur	EIO0000001590 (Anglais), EIO0000001591 (Français), EIO0000001592 (Allemand), EIO0000001594 (Italien), EIO0000001593 (Espagnol), EIO0000001595 (Chinois)
M580 - BMENOS0300 - Module de sélection d'options de réseau, Guide d'installation et de configuration	NHA89117 (Anglais), NHA89119 (Français), NHA89120 (Allemand), NHA89121 (Italien), NHA89122 (Espagnol), NHA89123 (Chinois)
Modicon eX80 - Module d'entrées analogiques HART BMEAH10812 et module de sorties analogiques HART BMEAHO0412, Guide utilisateur	EAV16400 (Anglais), EAV28404 (Français), EAV28384 (Allemand), EAV28413 (Italien), EAV28360 (Espagnol), EAV28417 (Chinois)
Modicon X80 - Modules d'entrée/sortie analogiques, Manuel utilisateur	35011978 (Anglais), 35011979 (Allemand), 35011980 (Français), 35011981 (Espagnol), 35011982 (Italien), 35011983 (Chinois)
Modicon X80 - Racks et modules d'alimentation - Manuel de référence du matériel	EIO0000002626 (anglais), EIO0000002627 (français), EIO0000002628 (allemand), EIO0000002630 (italien), EIO0000002629 (espagnol), EIO0000002631 (chinois)
Modicon X80 - Modules d'entrée/sortie TOR, Manuel utilisateur	35012474 (Anglais), 35012475 (Allemand), 35012476 (Français), 35012477 (Espagnol), 35012478 (Italien), 35012479 (Chinois)
Mise à la terre et compatibilité électromagnétique des systèmes automates - Principes et mesures de base, Manuel utilisateur	33002439 (Anglais), 33002440 (Français), 33002441 (Allemand), 33003702 (Italien), 33002442 (Espagnol), 33003703 (Chinois)
Guide d'installation électrique	EIGED306001EN (anglais)
EcoStruxure™ Control Expert - Langages de programmation et structure, Manuel de référence	35006144 (Anglais), 35006145 (Français), 35006146 (Allemand), 35013361 (Italien), 35006147 (Espagnol), 35013362 (Chinois)
EcoStruxure™ Control Expert, Modes de fonctionnement	33003101 (Anglais), 33003102 (Français), 33003103 (Allemand), 33003104 (Espagnol), 33003696 (Italien), 33003697 (Chinois)
EcoStruxure™ Control Expert, Manuel d'installation	35014793 (anglais), 35014792 (français), 35014794 (allemand), 35014795 (espagnol), 35014796 (italien), 35012191 (chinois)
Plates-formes automate Modicon - Cybersécurité, Manuel de référence	EIO0000001999 (Anglais), EIO0000002001 (Français), EIO0000002000 (Allemand), EIO0000002002 (Italien), EIO0000002003 (Espagnol), EIO0000002004 (Chinois)

Titre de documentation	Référence
Modicon X80 - Module d'horodatage BMXERT1604T, Manuel utilisateur	EIO0000001121 (Anglais), EIO0000001122 (Français), EIO0000001123 (Allemand), EIO0000001125 (Italien), EIO0000001124 (Espagnol), EIO0000001126 (Chinois)
Modicon X80 - Module RTU BMXNOR0200H - Manuel utilisateur	EIO0000000505 (anglais), EIO0000000507 (français), EIO0000000506 (allemand), EIO0000000509 (italien), EIO0000000508 (espagnol)

Reportez-vous à l'aide en ligne de l'outil Maintenance Expert.

REMARQUE : Cliquez sur le bouton " " dans l'interface pour obtenir l'aide en ligne.

Pour rechercher des documents en ligne, visitez le centre de téléchargement Schneider Electric (www.se.com/ww/en/download/).

Informations relatives au produit

L'utilisation de ce produit requiert une expertise dans la conception et la programmation des systèmes de contrôle. Seules les personnes ayant les compétences adéquates sont autorisées à programmer, installer, modifier et utiliser ce produit.

⚠ AVERTISSEMENT
FONCTIONNEMENT IMPREVU DE L'EQUIPEMENT Respectez toutes les normes et consignes de sécurité locales et nationales. Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Présentation du module RTU avancé Modicon X80 BMENOR2200H

Introduction

Présentation

Les systèmes RTU sont conçus pour répondre aux besoins de l'industrie de l'eau, du secteur du pétrole et du gaz, des transports, des services de distribution d'électricité et d'autres infrastructures où la surveillance et le contrôle à distance sont essentiels à la gestion d'un site et de sous-stations qui peuvent se répartir sur une vaste zone géographique.

DNP3, IEC60870-5-101, et IEC60870-5-104 sont des protocoles SCADA globaux, conçus avec différentes caractéristiques pour les services RTU (par exemple : événement de réponse sans requête (non sollicité)).

Le module RTU avancé Modicon X80 (BMENOR2200H) est une nouveauté pour la plate-forme PAC Modicon M580. Il offre des fonctionnalités plus puissantes pour différentes architectures et applications de télémétrie. Vous pouvez configurer ce module pour plusieurs services basés sur Ethernet, y compris la mise en œuvre du client et du serveur RTU dans un seul module tout en prenant en charge les connexions câblée Ethernet et série (ferrule). En particulier, le module RTU avancé prend en charge les systèmes de redondance d'UC (Hot Standby) M580 et implémente plusieurs fonctions de cybersécurité. Les temps d'ingénierie sont considérablement réduits grâce à la mise au point d'un nouvel outil et d'une nouvelle méthode de configuration.

AVIS

CONNEXION DE RACK INOPERANTE

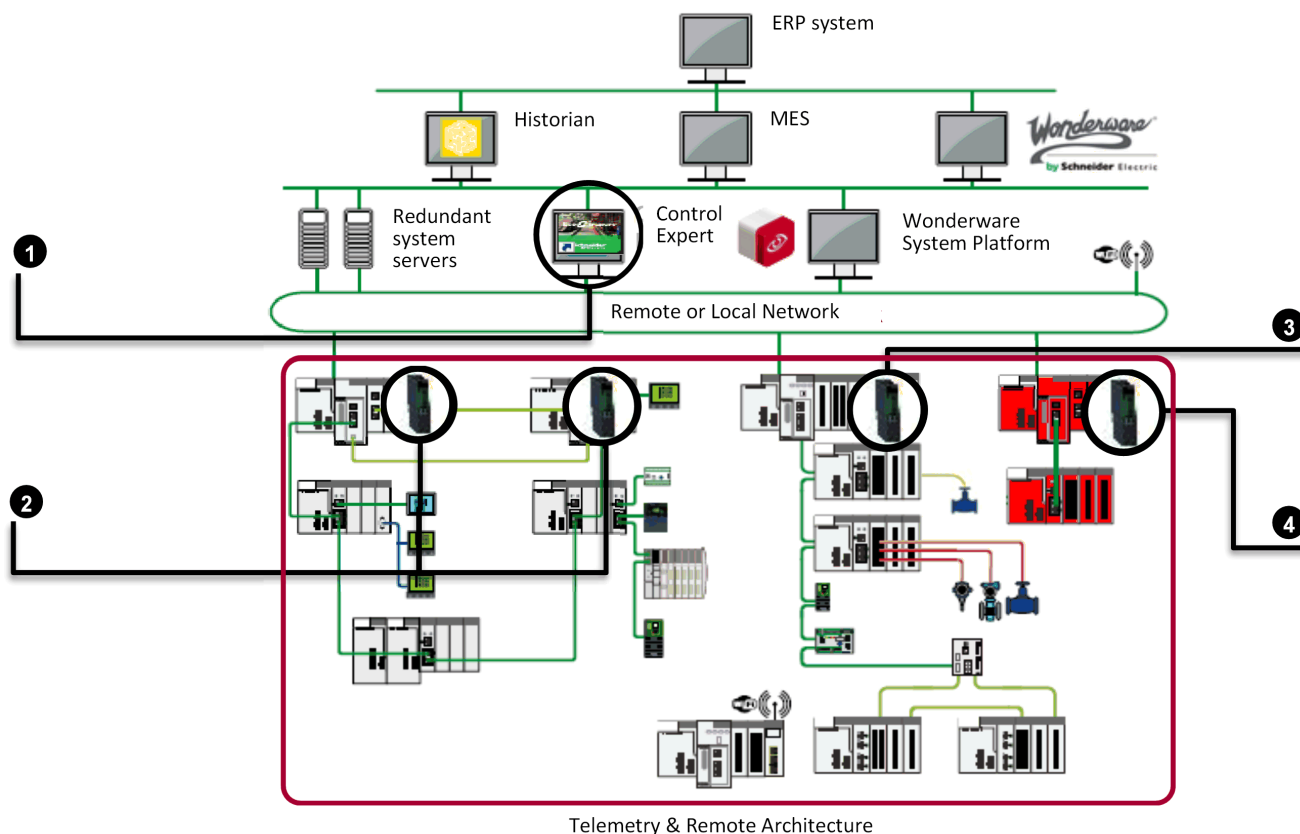
Ne montez pas le module BMENOR2200H sur une embase BMX (X Bus uniquement). Le module ne fonctionnerait pas.

Le non-respect de ces instructions peut provoquer des dommages matériels.

Le module ne peut fonctionner correctement que sur une embase BME (X Bus et Ethernet).

La description des racks et les restrictions d'emplacement sont fournis par le chapitre d'installation dans *Modicon X80 - Racks et modules d'alimentation*, *Manuel de référence du matériel* (voir Documents à consulter).

Le module RTU avancé BMENOR2200H apporte les communications DNP3, IEC60870-5-101 et IEC60870-5-104 à la plate-forme Modicon M580 :



1 Logiciel : Control Expert (outil d'ingénierie), Automation Device Maintenance (outil de mise à niveau de micrologiciel), Navigateur Web (paramètres de diagnostic et de cybersécurité)

2 Module BMENOR2200H : M580 à redondance d'UC (Hot Standby)

3 Module BMENOR2200H : M580 autonome

4 Module BMENOR2200H : M580 Safety autonome, M580 Safety Hot Standby, type 1 de non-interférence

NOTE: Avant d'utiliser le module BMENOR2200H (sans interférence) dans le cadre d'un projet de sécurité fonctionnelle Modicon M580, vous devez vérifier le statut de certification TÜV :

Sur le site <https://www.certipedia.com/>, recherchez *M580* puis sélectionnez le certificat *SCHNEIDER ELECTRIC*.

La **ligne rouge** délimite l'architecture de télémétrie et de téléconduite

Par rapport aux modules de communication et d'E/S X80 standard, le module BMENOR2200H est à *facteur long*, de la même hauteur que le contrôleur. (Reportez-vous à la section traitant des dimensions du module.)

Installez le module sur une embase Ethernet locale dans un système Modicon M580. Le module permet d'accéder à un réseau Modicon M580 via les ports externes du contrôleur et des modules de communication éventuellement installés sur le rack local.

Caractéristiques et fonctionnalités principales

Caractéristiques du module

Le module BMENOR2200H répond à un large éventail de besoins de télémetrie au sein d'un système M580 :

- Communications en amont avec les stations clientes SCADA pour l'interrogation des données, le remplissage des données d'événements horodatés et la réception des commandes émises par les clients.
- Communications en aval avec d'autres sous-stations RTU, équipements de terrain serveur et dispositifs électroniques intelligents (pour la collecte de données), envoi de commandes et synchronisation du contrôle distribué.
- Robustesse assurée par un revêtement enrobant pour les températures de fonctionnement élevées et les environnements difficiles.
- Routage d'événements du protocole RTU en tant que concentrateur de données.
- DNP3 (série et NET) niveau 3, IEC60870-5-101, IEC60870-5-104. Tous les protocoles sont certifiés par des organismes indépendants.
- Programmation à distance et téléchargement du programme de contrôle avec le logiciel Control Expert via le module BMENOR2200H (le transfert de fichiers vers le contrôleur s'effectue via X Bus lorsque le service Modbus est activé.)
- Configuration de la cybersécurité et surveillance des diagnostics à distance grâce à un serveur Web intégré.
- Compatibilité avec les systèmes M580 de redondance d'UC (Hot Standby).
- Réinitialisation de la communication RTU par des variables.
- Configuration groupée (fichier Excel/CSV) pour la table de mappage RTU.
- Améliorations de la cybersécurité :
 - Démarrage plus sécurisé
 - Signature et vérification d'intégrité des micrologiciels
 - Mise à niveau de micrologiciel plus sécurisée
 - Pages Web basées sur HTTPS
 - RBAC pour l'accès aux pages Web
 - TLS pour RTU (DNP3 NET, CEI 60870-5-104)
 - Complexité du mot de passe
 - Sélection du mode de cybersécurité par commutateur rotatif
 - Versions d'authentification DNP3 plus sécurisées SAV2 et SAV5
 - Communication redondante plus sécurisée entre les modules
 - Achilles Niveau 2
 - Authentification sécurisée DNP3 qualifiée par un organisme tiers
- Capacité de débit de données élevée lorsque le module joue le rôle de serveur RTU (transmission de 4000 événements par seconde vers les équipements clients via Ethernet).
- 150 000 événements RTU maximum stockés dans la mémoire tampon du module.
- Capacité de stockage jusqu'à 4 Go (dans la carte SD) pour la journalisation de données.
- SNMPv1 et SNMPv3.
- Synchronisation de l'heure à partir de SNTP, du protocole RTU ou du contrôleur.
- Serveur Modbus TCP local (fonction de diagnostic du module) / Client.

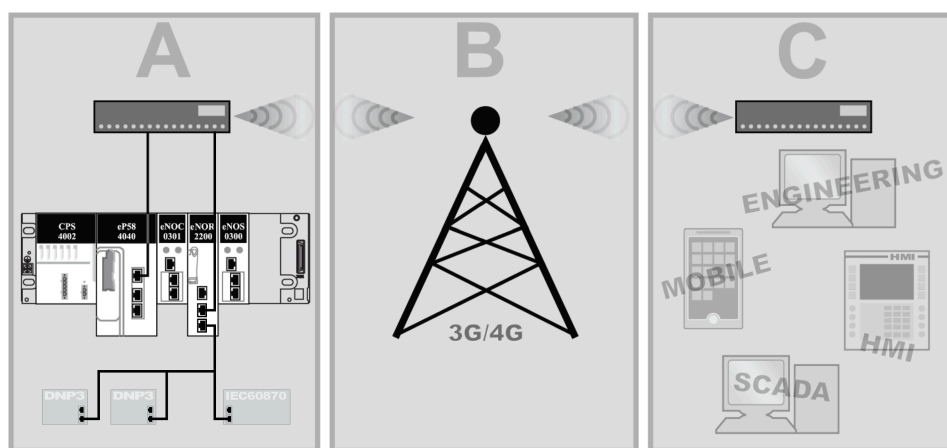
Caractéristiques de la plateforme

Le module partage les caractéristiques et applications suivantes, disponibles dans un environnement M580 :

- Accès Ethernet flexible via les ports frontaux et/ou l'embase
- Connectivité aisée avec une embase Ethernet
- Blocs fonction spécialisés (AGA, calculs de débit)
- Configurations d'E/S modulaires et évolutives basées sur des racks extensibles et fonctionnalités d'E/S distantes
- Modules d'entrées/sorties analogiques/TOR et de comptage haute densité
- Alimentation d'entrée isolée (plages de tensions : 24 Vcc, 24/48 Vcc, 125 Vcc, 100/240 Vca)
- Téléchargement local et à distance de micrologiciel de système d'exploitation
- Bande passante d'échange de données exclusive pour chaque module installé sur le même rack

Architecture RTU

Cet exemple d'architecture présente les communications à partir d'une sous-station RTU comprenant un module BMENOR2200H :



A Un module BMENOR2200H communique via le port Ethernet de l'embase et/ou les ports de contrôle en face avant avec un contrôleur connecté à un routeur réseau.

B Le réseau 3G/4G transfère les communications.

C Les communications sont reçues par un routeur qui se connecte à un réseau de contrôle et à des équipements de bus de terrain.

BMENOR2200H et EcoStruxure™

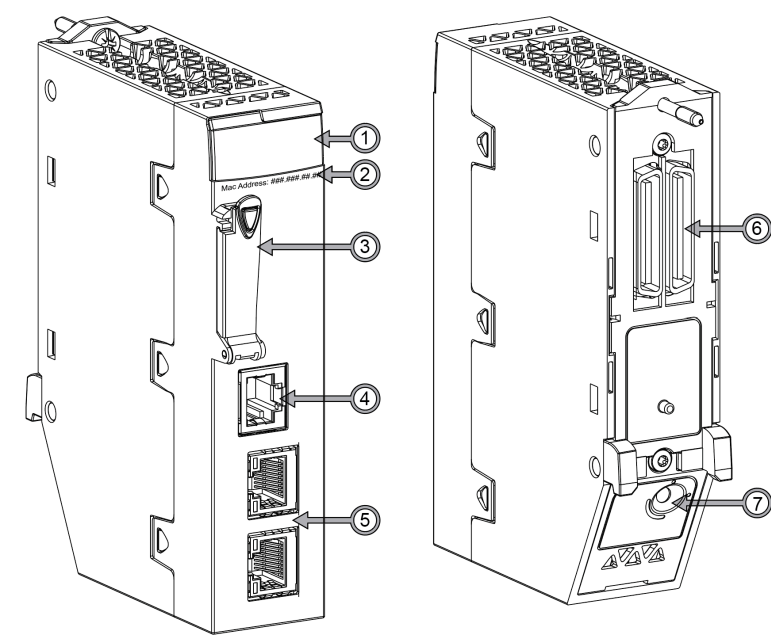
EcoStruxure™ est un programme Schneider Electric conçu pour répondre aux besoins cruciaux de nombreux types d'utilisateurs - directeurs d'usine, responsables d'exploitation, ingénieurs, équipes de maintenance et opérateurs - en fournissant un système évolutif, flexible, intégré et collaboratif.

Ce document présente l'une des fonctionnalités de EcoStruxure dans un réseau fédérateur Ethernet autour de l'offre Modicon M580, où un rack local M580 communique avec des stations d'E/S distantes (RIO) M580 et des équipements distribués dans le même réseau.

Description physique

Fonctions externes

Le module BMENOR2200H présente le même facteur de forme que les autres modules de communication avancés M580. La figure suivante montre les caractéristiques externes propres à ce module :



Légende :

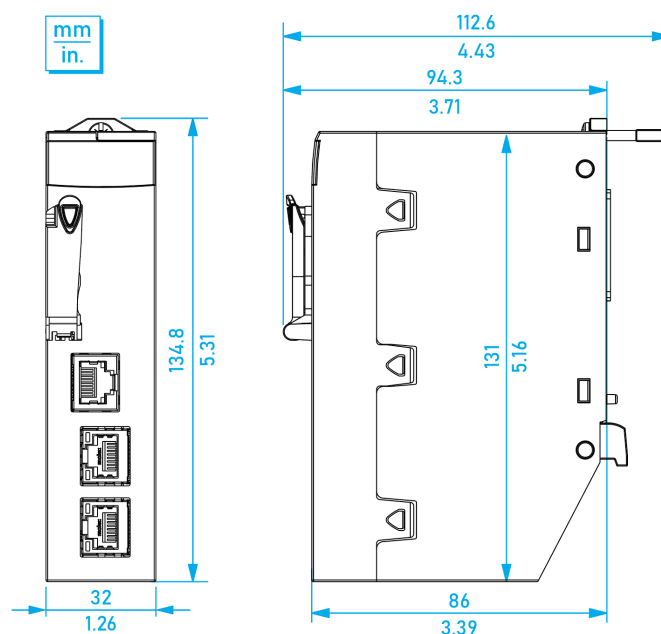
Elé- ment	Description	Fonction
1	Voyants à LED	Examinez les voyants pour diagnostiquer le module.
2	Adresse MAC	Cette adresse définie par le fabricant (ports de contrôle fontaux) est unique pour chaque module
3	emplacement de carte mémoire	Stockez les fichiers de journalisation des données (.csv) sur la carte SD.
4	port série	Ce port est un connecteur série RS232/RS485 isolé. Utilisez un câble de liaison série TCSXCN3M4F3S4 (avec ferrule) pour raccorder le port série RJ45 (RS232) du module au port de communication d'un modem. Ce câble prend en charge les neuf broches du connecteur D-sub du modem, à l'exception de la broche de signal RI (indicateur d'anneau), vendue séparément.
5	ports de contrôle	Deux ports de contrôle RJ45 présentant les caractéristiques suivantes : 1. Vitesse de transmission : 1 Gbit/s,100 Mbits/s,10 Mbits/s (configurable) 2. L'activation et la désactivation de port est autorisée 3. Partager la même adresse IP (deux ports sur le commutateur) 4. Vitesse de fonctionnement jusqu'à 1 Gbit/s. Avec une vitesse de fonctionnement de : 1 Gb/s, utilisez uniquement des câbles à quatre paires torsadées en cuivre blindés CAT6. 10/100 Gb/s, utilisez des câbles à quatre paires torsadées en cuivre blindés CAT5e ou CAT6. NOTE: Il n'existe pas de protocole de liaison redondante (RSTP, PRP, etc.) sur ces deux ports. Lorsque vous activez tous les ports de contrôle et que vous vous connectez au réseau, vérifiez la conception de la topologie de réseau

Elé- ment	Description	Fonction
		pour éviter les problèmes de boucle réseau et les comportements anormaux du module.
6	connecteur d'embase double bus	Cette connexion au rack Modicon M580 prend en charge les communications Ethernet et X Bus.
7	commutateur rotatif, page 28	Utilisez ce commutateur pour définir le niveau de cybersécurité du module.

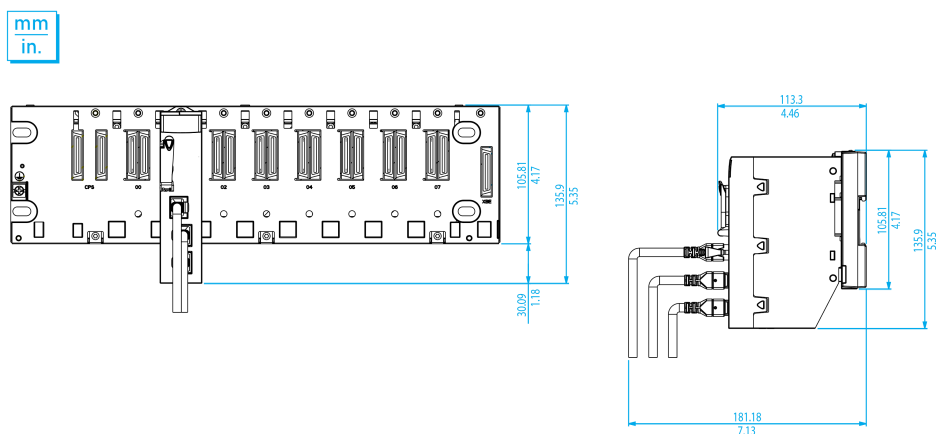
NOTE: Une fêrle placée à l'extrémité du port série réduit le pincement du câble par le cache amovible. Cela affaiblit le risque de dégradation de la qualité de la liaison en diminuant la probabilité d'atteindre le rayon de courbure maximum du câble.

Dimensions

Le module BMENOR2200H est conforme à la hauteur d'un contrôleur M580 et à la largeur d'un module de communication M580 standard à un emplacement avec emplacement pour carte SD :



Module monté sur rack :



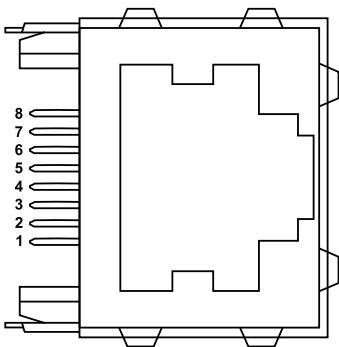
Port série

Le module BMENOR2200H intègre un port série qui prend en charge tout type de communication série via une liaison série.

Le tableau suivant décrit les voies de communication série :

Caractéristique	Description
protocoles pris en charge	Protocoles RTU : - IEC60870-5-101 - DNP3 série
raccordement	prise RJ45
liaison physique	- liaison série RS485 isolée - liaison série RS232 isolée

Broches du port série :



Affectation (fonctionnalité) des broches :

Broche	Signal	Broche	Signal
1	RXD	5	D0/DSR
2	TXD	6	CTS
3	RTS	7	DCD
4	D1/DTR	8	commun
blindage			

Le connecteur RJ45 comporte huit broches. Les broches utilisées diffèrent selon la liaison physique utilisée.

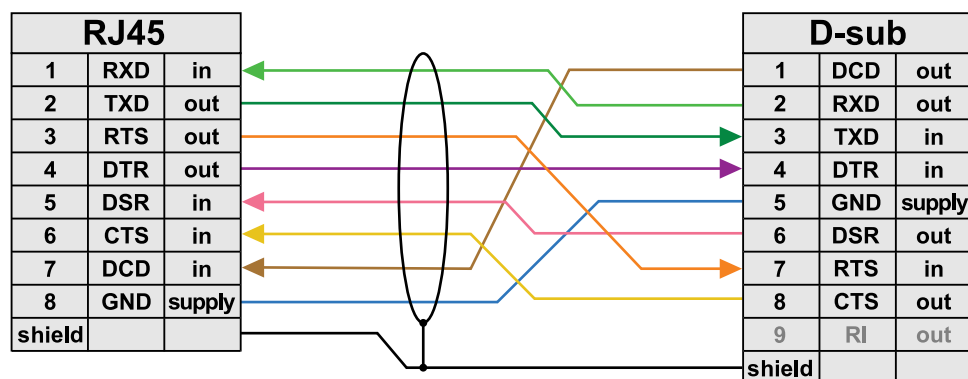
La liaison série RS 232 utilise les broches suivantes :

- broche 1 : signal RXD
- broche 2 : signal TXD
- broche 3 : signal RTS
- broche 4 : signal DTR
- broche 5 : signal DSR
- broche 6 : signal CTS

Le câble série croisé TCS MCN 3M4F3C2 (ferrule) comporte deux connecteurs :

- RJ45 mâle
- SUB-D femelle à 9 contacts

Voici l'affectation des broches entre une fiche mâle RJ45 et une prise femelle SUB-D 9 broches pour un câble croisé série TCSMCN3M4F3C2 (ferrule) :



La liaison série RS 485 utilise les broches suivantes :

- *broche 4* : signal D1
- *broche 5* : signal D0

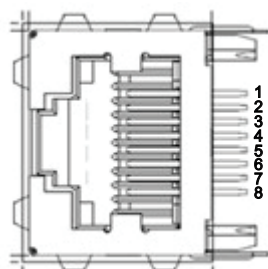
La liaison série utilise les broches ainsi :

- *broche 7* : non connectée
- broche 8* : commun de l'alimentation réseau (0 V)

NOTE: Les câbles RS232 à quatre fils, RS485 à deux fils et RS 485 à deux fils ainsi que les câbles d'alimentation (ferrule) utilisent le même connecteur mâle RJ45.

Ports de contrôle

Le module BMENOR2200H présente en face avant deux ports Ethernet RJ45.



Le tableau suivant décrit les broches des ports ETH :

Broche	Définition	Port ETH
1	TX_D1+	Transmission de données+
2	TX_D1-	Transmission de données-
3	RX_D2+	Réception de données+
4	BI_D3+	Données bidirectionnelles+
5	BI_D3-	Données bidirectionnelles-
6	RX_D2-	Réception de données-
7	BI_D4+	Données bidirectionnelles+
8	BI_D4-	Données bidirectionnelles-

Le niveau de tension d'isolation du port ETH est de 2000 VCC.

La liste ci-dessous indique les vitesses de ligne disponibles pour le module BMENOR2200H :

- 1000 Mbits/s en duplex intégral maître

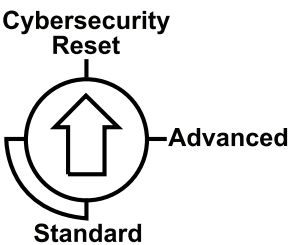
- 1000 Mbits/s en duplex intégral esclave
- 100 Mbits/s en semi-duplex
- 100 Mbits/s en duplex intégral
- 10 Mbits/s en semi-duplex
- 10 Mbits/s en duplex intégral

Les caractéristiques de l'adaptation à la vitesse sont les suivantes :

- La négociation automatique permet au module BMENOR2200H de s'adapter rapidement à la vitesse et au mode duplex du commutateur Ethernet local.
- La vitesse négociée entre deux équipements Ethernet est limitée à la vitesse de l'équipement le plus lent.
- Le module prend en charge Auto MDIX, MDI est préféré ici.

Commutateur rotatif

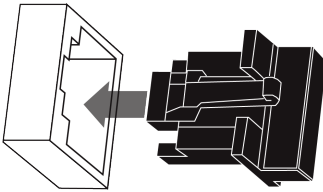
Un commutateur rotatif à trois positions est situé à l'arrière du module. Réglez-le pour configurer le mode de fonctionnement de cybersécurité du module :



Reportez-vous à la description détaillée du commutateur rotatif de cybersécurité.

Accessoires

Les accessoires matériels suivants sont disponibles en supplément :

Description	Commentaire
protection antipoussière	Protégez les ports RJ45 inutilisés du module avec ce bouchon :  Le bouchon antipoussière réduit l'exposition du port à la poussière atmosphérique.
tournevis	Utilisez uniquement le petit tournevis en plastique fourni avec le module pour régler le commutateur rotatif, page 28.

Voyants du module

Introduction

Reportez-vous aux voyants pour surveiller l'état et les performances des éléments suivants :

- Voyants du module BMENOR2200H (ci-dessous)
- Voyants de la carte SD, page 26

Description des voyants du module

Les voyants se trouvent sur la face avant du module BMENOR2200H. Les voyants fournissent les informations suivantes :

- état du module (en marche, erreur, téléchargement en cours)
- communications réseau Ethernet
- communications RTU
- état de la carte mémoire SD
- communications série
- mode de cybersécurité

Illustration des voyants à LED à l'avant du module BMENOR2200H :



Les voyants peuvent être dans les états suivants :

- *allumé* : allumé en continu
- *éteint* : éteint en continu
- *clignotant* : alternativement allumé (250 ms) et éteint (250 ms)

L'état du module est indiqué par la couleur et l'état des voyants :

Étiquette	Couleur	État	Indication
RUN : état opérationnel	vert	allumé	Le module fonctionne et il est configuré.
		clignotant	Le module est bloqué par une erreur détectée par un logiciel.
		éteint	Le module n'est pas configuré. (L'application est absente, incorrecte ou incompatible.)
ERR : erreur détectée	rouge	allumé	- Le processeur, le système ou la configuration a détecté une erreur. - Si vous effectuez un changement de position direct Standard > Advanced (ou inversement) du commutateur rotatif au lieu de passer par la position Cybersecurity Reset, une erreur est détectée : Réinitialisation de cybersécurité manquante
		clignotant	- Le module n'est pas configuré. (L'application est absente, incorrecte ou incompatible.) - Le module est bloqué par une erreur détectée par un logiciel. - Un problème de redondance d'UC est détecté.
		éteint	Les opérations sont normales (aucune erreur détectée).
DL : téléchargement du micrologiciel (mise à niveau)	rouge	allumé	Une mise à niveau du micrologiciel ou une réinitialisation aux réglages d'usine est en cours.
		éteint	Aucune mise à niveau du micrologiciel ou réinitialisation d'usine n'est en cours.
NS : état du port de contrôle	vert	allumé	L'un des deux ports de contrôle est activé et correctement relié.
	rouge	allumé	Une adresse IP est dupliquée sur le port Ethernet de l'embase ou le mode réinitialisation d'usine.
	—	éteint	Il n'y a pas de liaison sur les deux ports de contrôle.
RTUCNX : état de la connexion RTU	vert	allumé	Au moins une connexion RTU (client ou serveur) est établie dans le module.
		clignotant	Il n'y a aucune connexion RTU.
BS : état du port Ethernet de l'embase	vert	allumé	La liaison est correctement établie avec le port Ethernet de l'embase.
	rouge	allumé	Une adresse IP est dupliquée sur le port Ethernet de l'embase ou le mode réinitialisation d'usine.
CARD ERR : erreur de carte mémoire détectée	rouge	allumé	- Le service de journalisation des données est activé, mais la carte mémoire est manquante. - Le service de journalisation des données est activé, mais la carte mémoire n'est pas utilisable (format incorrect, type non reconnu, etc.).
		éteint	La carte mémoire est valide et reconnue.
SER COM : état des données série	jaune	clignotant	Un échange de données (émission/réception) est en cours sur la connexion série.
		éteint	Il n'y a pas d'échange de données sur la connexion série.
SEC : état de sécurité des communications	vert	allumé	Le niveau de sécurité des communications sélectionné est activé et fonctionne correctement.
	rouge	allumé	- Les communications ne sont <i>pas</i> sécurisées car une erreur critique est détectée dans la sécurité des communications. Par exemple, aucune configuration de sécurité n'est disponible ou le certificat a expiré lorsque les communications se sont arrêtées. - Aucune sécurité de voie n'est configurée via le nom de voie côté client ou serveur.
		clignotant	Le niveau de sécurité de communication sélectionné est activé et opérationnel, mais une erreur critique est détectée. Par exemple, aucune configuration de sécurité n'est disponible ou le certificat a expiré lorsque les communications se sont arrêtées.
	—	éteint	La fonction de cybersécurité n'est pas activée.

Etats typiques et comportement des voyants associés

Libellé	État	Indication
ERR	Rouge allumé	Réinitialisation de cybersécurité manquante : Le commutateur rotatif a été déplacé directement entre les modes Standard et Advanced . Une réinitialisation d'usine est nécessaire avant de passer à l'un ou l'autre mode.
DL		
BS		
NS		
SEC		

Etat du module	Voyant	Description
Mode usine	RUN : vert allumé	—
	DL : rouge allumé DL : rouge éteint	Réinitialisation des réglages d'usine en cours. La réinitialisation des réglages d'usine est terminée.
	BS : rouge allumé	—
	NS : rouge allumé	—
Mode de cybersécurité initial (démarrage initial sans réglage de cybersécurité valide)	ERR : rouge clignotant	Le module ne fonctionne pas ; un réglage de cybersécurité validé est nécessaire.
	BS : vert clignotant	
	SEC : rouge allumé	

Voyants sur les ports de contrôle

Il y a deux voyants sur chaque port RJ45. L'un est ACT (actif) et l'autre est LNK (liaison). Ces deux voyants permettent de diagnostiquer l'état des communications Ethernet sur les ports de contrôle :

- Le voyant ACT indique la présence d'activité Ethernet sur le port.
- Le voyant LNK indique l'existence d'une liaison Ethernet et sa vitesse.



Voyant	Etat	Description
ACT	vert	Liaison établie, aucune activité.
	vert clignotant	Liaison établie, activité détectée.
	éteint	Aucune liaison établie.
LNK	vert	Liaison établie à une vitesse égale à la capacité maximale du module (1000 Mbits/s).
	jaune	Liaison établie à une vitesse inférieure à la capacité maximale du module (10/100 Mbits/s).
	éteint	Aucune liaison établie.

Carte mémoire SD (BMXRMS004GPF)

Introduction

Vous pouvez utiliser une carte mémoire BMXRMS004GPF avec ce module pour faciliter certains services. (par exemple, la journalisation des données).

NOTE: Le module BMENOR2200H est compatible uniquement avec la carte mémoire BMXRMS004GPF formatée spécifiquement par Schneider Electric. La carte mémoire BMXRMS004GPF est une option d'achat. Elle n'est pas livrée avec le module.

Emplacement

L'emplacement pour carte mémoire SD (Secure Digital) (BMXRMS004GPF) se trouve à l'avant du module.

Il est déconseillé d'insérer la carte SD pendant le fonctionnement du module. Ce dernier risque de ne pas reconnaître la carte dans ce cas.

⚠ AVERTISSEMENT

RISQUE DE PERTE D'APPLICATION

- Ne retirez pas la carte mémoire du module tant que l'automate est en fonctionnement.
- N'insérez pas de carte SD pendant le fonctionnement du module.
- Retirez la carte mémoire uniquement lorsque l'automate est hors tension.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Fonctionnalités des cartes

Le tableau suivant décrit les fonctionnalités de la carte mémoire BMXRMS004GPF lorsqu'elle est insérée dans le module :

Carte mémoire SD	Stockage des données	Fonctionnalités
BMXRMS004GPF	4 Go	Stockage des fichiers de journalisation des données (.csv)

Voyants

Un voyant est associé à l'emplacement de la carte mémoire. Il affiche l'état de l'échange de données avec la carte :

- *allumé* : La carte SD est disponible et reconnue.
- *éteint* : La carte SD n'est pas disponible ou la fonctionnalité de journalisation de données n'est pas activée.

Services de la carte

AVIS

CARTE MEMOIRE NON OPERATIONNELLE

- Ne formatez pas la carte mémoire à l'aide d'un outil autre qu'un outil Schneider.
- N'utilisez pas de carte mémoire protégée en écriture avec le module.

Le non-respect de ces instructions peut provoquer des dommages matériels.

La carte mémoire a besoin d'une structure pour contenir le programme et les données. Effectuer un formatage avec un autre outil détruit cette structure.

Certains services ne fonctionnent pas correctement lorsque la carte mémoire est protégée en écriture.

Précautions à observer

AVIS

DESTRUCTION DE CARTE MEMOIRE

- Ne touchez pas les connexions de la carte mémoire.
- Protégez la carte mémoire des sources électrostatiques et électromagnétiques, des sources de chaleur, des rayons de soleil, de l'eau et de l'humidité.
- Protégez la carte mémoire des chocs.
- Vérifiez les règles de sécurité des services postaux avant d'envoyer une carte mémoire par service postal.

Le non-respect de ces instructions peut provoquer des dommages matériels.

En effet, par mesure de sécurité, les services postaux de certains pays exposent le courrier à de hauts niveaux de radiation. Or, ces hauts niveaux de radiation peuvent effacer le contenu de la carte mémoire et rendre cette dernière inutilisable.

Sans carte mémoire SD

Si l'emplacement de la carte mémoire est vide pendant la mise sous tension, le module peut fonctionner normalement sans le service de journalisation de données.

Commutateur rotatif de cybersécurité

Introduction

AVIS

RISQUE DE FONCTIONNEMENT IMPREVU

N'utilisez pas de tournevis métallique.

Le non-respect de ces instructions peut provoquer des dommages matériels.

Pour préserver l'intégrité du matériel, n'utilisez que le petit tournevis en plastique livré avec le module pour changer la position du commutateur.

L'utilisation d'un tournevis métallique peut endommager le commutateur et le rendre inopérant.

Un commutateur rotatif à trois positions se trouve à l'arrière du module. Réglez-le pour déterminer le mode de fonctionnement de cybersécurité du module .

Sélection de l'emplacement

AVIS

RISQUE DE FONCTIONNEMENT IMPREVU

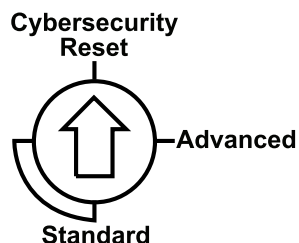
Réglez le commutateur uniquement sur la "position d'horloge" exacte correspondant à votre configuration de sécurité.

Le non-respect de ces instructions peut provoquer des dommages matériels.

Les "positions d'horloge" suivantes sont disponibles pour régler le commutateur :

- 12 heures : **Cybersecurity Reset**
- 3 heures : **Advanced**
- 6 heures/9 heures : **Standard** (Pour mettre en œuvre le niveau de cybersécurité **Standard**, réglez le commutateur *seulement* sur la position 6 heures ou 9 heures.)

Voici une vue agrandie du commutateur rotatif à trois positions à l'arrière du module :



A l'aide du tournevis, sélectionnez une position de commutateur correspondant à vos besoins en matière de cybersécurité :

Icône	Réglage	Description
Advanced	mode avancé activé	Le module prend en charge certains niveaux de cybersécurité lorsqu'une configuration de cybersécurité est disponible.
Standard	mode standard activé	Le module prend en charge un niveau de cybersécurité de base.
Cybersecurity Reset	rétablissement des paramètres d'usine	Le module met en œuvre la configuration de cybersécurité prédéfinie.

Réglage du commutateur

Configurez le mode de cybersécurité du module dans le rack :

Etape	Action
1	Retirez le module du rack : a. Vérifiez que le module est hors tension. b. Desserrez les ergots de guidage à l'arrière du module (partie inférieure) dans les emplacements correspondants du rack. c. Faites basculer le module vers le bas du rack pour le soulever et l'extraire.
2	Réglez le commutateur sur Cybersecurity Reset .
3	Réinsérez le module dans le rack pour le mettre sous tension en mode Cybersecurity Reset . Résultat : Le module rétablit ses paramètres d'usine et il est correctement alimenté lorsque le voyant RUN reste allumé fixement en vert.
4	Retirez à nouveau le module du rack.
5	Réglez le commutateur sur Advanced ou Standard .
6	Réinsérez le module dans le rack pour le mettre sous tension dans le mode sélectionné (Advanced ou Standard). Résultat : Le module est correctement alimenté lorsque le voyant est vert fixe pour les modes avancé et standard.

NOTE:

- Si vous déplacez le commutateur rotatif directement de la configuration standard(**Standard**) à la configuration sécurisée (**Advanced**) ou inversement, une erreur est détectée.
 - Mettez toujours le module sous tension avec le commutateur rotatif en position **Cybersecurity Reset** lorsque vous basculez entre les modes **Standard** et **Advanced** pour mettre en œuvre des opérations normales.
 - Vous pouvez également utiliser la boîte de dialogue **Gestion** de la page Web **Configuration** pour régler le commutateur rotatif afin de nettoyer toute la configuration de cybersécurité. Cliquez sur le bouton **Cybersecurity Reset** pour restaurer les paramètres de cybersécurité par défaut du module. Un redémarrage du module est nécessaire.
- Les modifications associées aux paramètres du commutateur prennent effet, une fois le module réinséré dans le rack et mis sous tension.

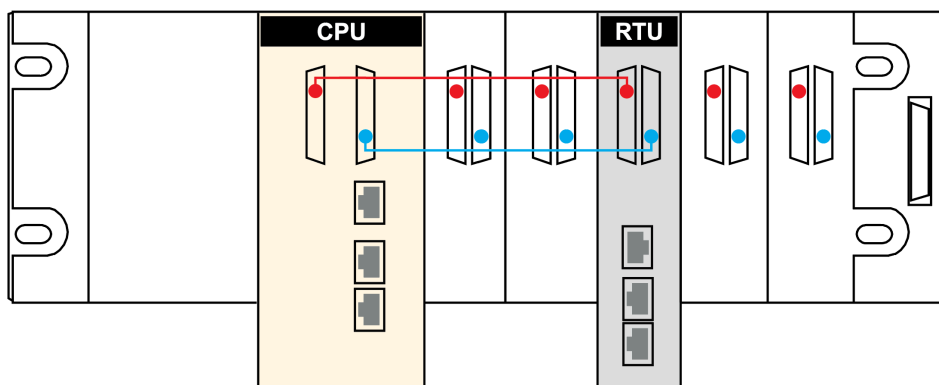
Connecteur d'embase

A propos des embases double bus

L'interface double bus à l'arrière du module BMENOR2200H est raccordée aux connecteurs de bus X Bus et Ethernet via l'embase lors du montage du module dans le rack.

Les embases BMEXBP••0• sont compatibles avec les modules Modicon X80 d'un système M580.

Les communications à travers l'embase double bus de cet exemple de rack local (qui comprend un contrôleur M580) mettent en œuvre les deux protocoles Ethernet (ligne rouge) et X-Bus (ligne bleue) :



Rouge (ligne ou pointillés) = Ethernet.

Bleu (ligne ou pointillés) = X Bus.

NOTE:

- Les embases X Bus des BMXXBP••00 ne disposent pas de connexions prenant en charge les modules eX80.
- Les racks Ethernet sont décrits en détail dans les *Modicon M580 - Matériel, Manuel de référence* (Documents à consulter).

Protocoles de connexion

Le module prend en charge les communications via une BMEXBP••0• en utilisant les protocoles suivants :

Bus	Description
<i>X Bus</i>	Le module utilise les communications X Bus pour obtenir et échanger les éléments suivants via le contrôleur : - données de configuration du module - données de diagnostic des DDT d'application et d'équipement - télécharger l'application de l'automate vers le contrôleur via le module BMENOR2200H module lorsque le service Modbus est activé. - échange de données variables entre le module et le contrôleur - messages de synchronisation horaire vers le contrôleur et d'autres modules sur l'embase L'échange de données utilise la messagerie implicite pour faciliter le partage de mémoire entre le module et le contrôleur. Pour chaque cycle de scrutation du contrôleur, ce dernier publie toutes les données en même temps pour partager les informations les plus récentes avec le RTU.
<i>Backplane Ethernet</i>	NOTE: Le port d'embase Ethernet est toujours activé pour le module BMENOR2200H. Vérifiez la conception topologique de votre réseau pour éviter les problèmes de boucle de réseau. Le module utilise les communications Ethernet pour fournir un chemin d'accès au module BMENOR2200H aux fins suivantes : - Les équipements externes peuvent communiquer avec le module BMENOR2200H lorsqu'ils accèdent à l'une des entités suivantes : - Contrôleur BMEP58••/BMEH58•• - Module de communication BMENOC03•• - Module de sélection d'options de réseau BMENOS0300 - Adaptateur BM•CRA312•• - Autres modules Ethernet présentant des capacités similaires - Le module communique avec des modules de communication Ethernet situés sur le rack local.

Echange de données d'E/S avec le contrôleur

Observez les tailles d'entrée et de sortie maximales suivantes lorsque le module échange des données d'E/S avec le contrôleur :

Protocole	Caractéristiques
- IEC 60870-5-101 - IEC 60870-5-104 - DNP3	Utilisation de la mémoire : taille des données d'entrée : 8 Ko de données incluant les données configurables par l'utilisateur et 4 Kmots de temps système. Le temps système comprend les données de diagnostic du module, les en-têtes d'objet de données et le nombre d'en-têtes selon la configuration de l'utilisateur. Par conséquent, la taille maximale des données d'entrée configurables par l'utilisateur est d'environ 7,55 Ko (1 Ko = 1024 octets). taille des données de sortie : 8 Ko de données incluant les données configurables par l'utilisateur et 4 Kmots de temps système. Le temps système comprend les données de contrôle du module, les en-têtes d'objet de données et le nombre d'en-têtes selon la configuration de l'utilisateur. Par conséquent, la taille maximale des données de sortie configurable par l'utilisateur est d'environ 7,56 Ko (1 Ko = 1024 octets). NOTE: - Vous pouvez afficher l'utilisation de la mémoire dans le DTM Control Expert (Génération > Informations du module > Etat de la mémoire). Reportez-vous à la description des informations du module dans le DTM, page 168. - En ce qui concerne les tailles d'entrée et de sortie de 8 Ko, la consommation de mémoire exacte dépend du type de mappage des données sur le contrôleur ; différents types de données consomment différentes quantités de mémoire. Reportez-vous à l'annexe sur la migration de projet, page 284.

Temps de cycle MAST minimum

Utilisez cette formule pour obtenir le temps de cycle minimum recommandé pour la tâche MAST pour un seul module BMENOR2200H :

$$T_{\text{cycle min}} = ((\text{DataInB} + 128) * 2 + (\text{DataOutB} + 32)) / 23500 \text{ B/S} * 30 \text{ ms}$$

Le résultat est un cycle de tâche MAST de 30 ms environ avec 8 Ko en entrée et 8 Ko en sortie.

NOTE: Lorsque plusieurs modules RTU BMENOR2200H sont installés, le temps de cycle minimum est la somme des temps de cycle associés à tous les modules.

Caractéristiques électriques

Consommation de courant

Courant consommé par le module BMENOR2200H :

Source d'alimentation	Consommation
Rack 24 Vcc	137 mA
Dissipation de puissance	3,3 W

Considérations relatives au câblage

Les modules sont réinitialisés lorsqu'ils sont remis sous tension. Cela peut provoquer une interruption temporaire de l'application ou des communications.

Normes et certifications

Télécharger

Affichez les documents à consulter correspondant à votre langue préférée pour télécharger les normes et certifications (format PDF) qui s'appliquent aux modules de cette gamme de produits.

Désignation	Langues
Plateformes Modicon M580, M340 et X80 I/O - Normes et certifications	- Anglais : EIO0000002726 - Français : EIO0000002727 - Allemand : EIO0000002728 - Italien : EIO0000002730 - Espagnol : EIO0000002729 - Chinois : EIO0000002731

Normes de sécurité et certifications

Références

Reportez-vous à ces directives extraites du document *ModiconM580 - Normes de sécurité et certifications* (voir Documents à consulter).

- Certificats et déclarations
- Conditions de stockage et de fonctionnement
- Niveaux de conformité des tests d'environnement

Module BMENOR2200H dans les réseaux

Réseaux autonomes

Architectures M580 autonomes

Introduction

Cette rubrique décrit l'utilisation du module BMENOR2200H module dans un système M580 autonome.

Support de connexion

Effectuez les connexions au module BMENOR2200H à l'aide d'un câble (ferrule) :

- *connexion amont*: Connectez le module à un système SCADA via les protocoles DNP3, IEC60870-5-101 ou IEC60870-5-104. (Une connexion Modbus TCP est également possible.)
- *connexion aval*: Connectez le module aux équipements et stations serveur distants via les protocoles DNP3, IEC60870-5-101 ou IEC60870-5-104.

Connexions Ethernet

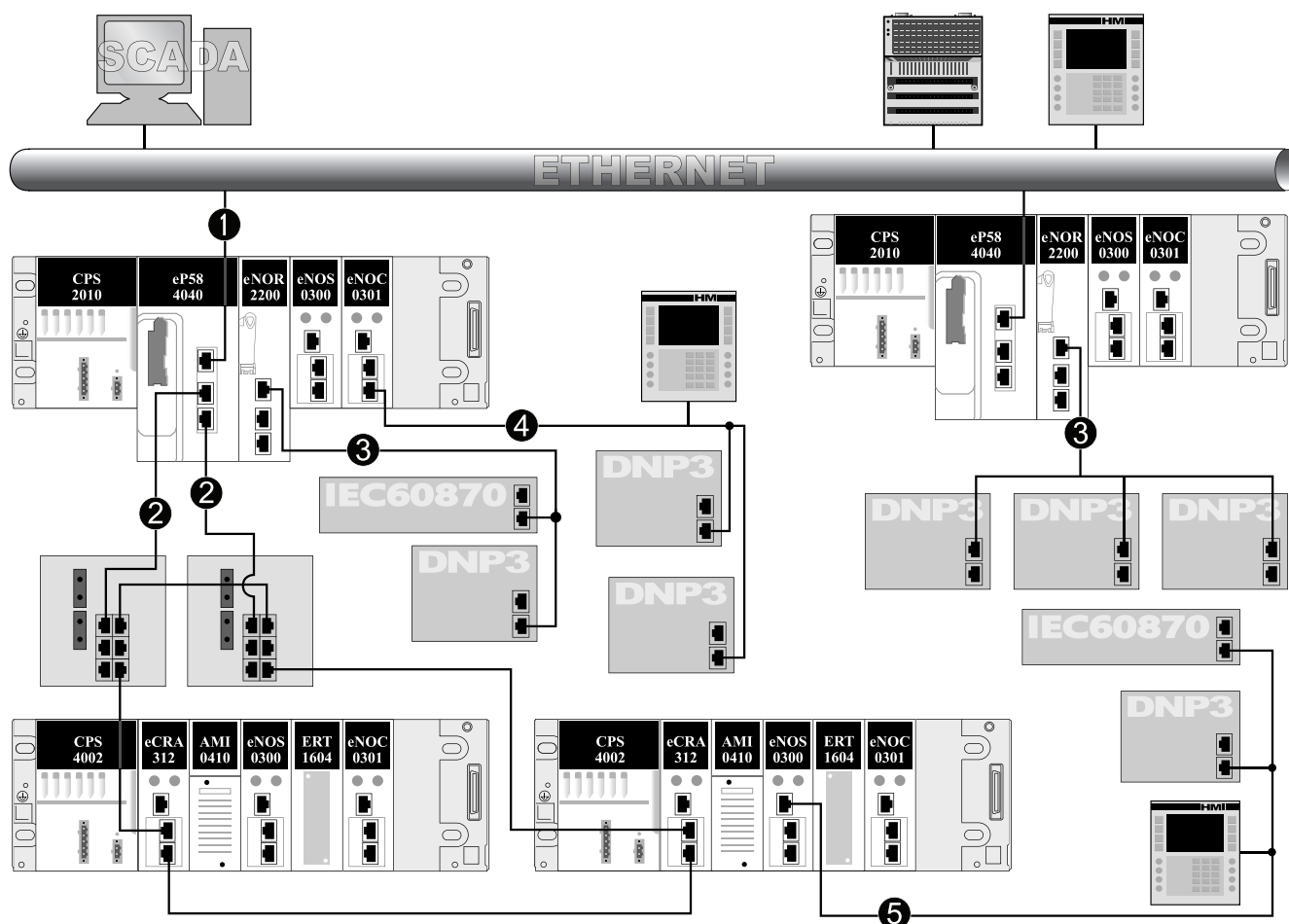
La connexion à un câble Ethernet peut passer par les ports de contrôle situés à l'avant du BMENOR2200H ou par un autre port de l'embase s'il est activé :

- *réseaux plats* : Pour ces réseaux, les connexions réseau Ethernet au BMENOR2200H sont effectuées via le port de service M580 ou un module BMENOC0301/11 ou BMENOS0300.
- *réseaux isolés* : Pour ces réseaux, les connexions réseau Ethernet sont réalisées directement via les ports de contrôle. Les ports de contrôle sont physiquement isolés avec le port d'embase (par 2 adresses MAC). Si les ports de contrôle ne sont pas activés, le réseau isolé logique peut également être réalisé via un module BMENOC0321 avec le transfert IP. L'installation de plusieurs module M580+BMENOR2200H+BMENOC0321 nécessite l'utilisation d'une table de routage statique pour le système amont.

Réseau autonome avec un sous-réseau

Exemple de réseau

Cet exemple de réseau autonome comprend des modules BMENOR2200H sur des racks locaux dans un seul sous-réseau :



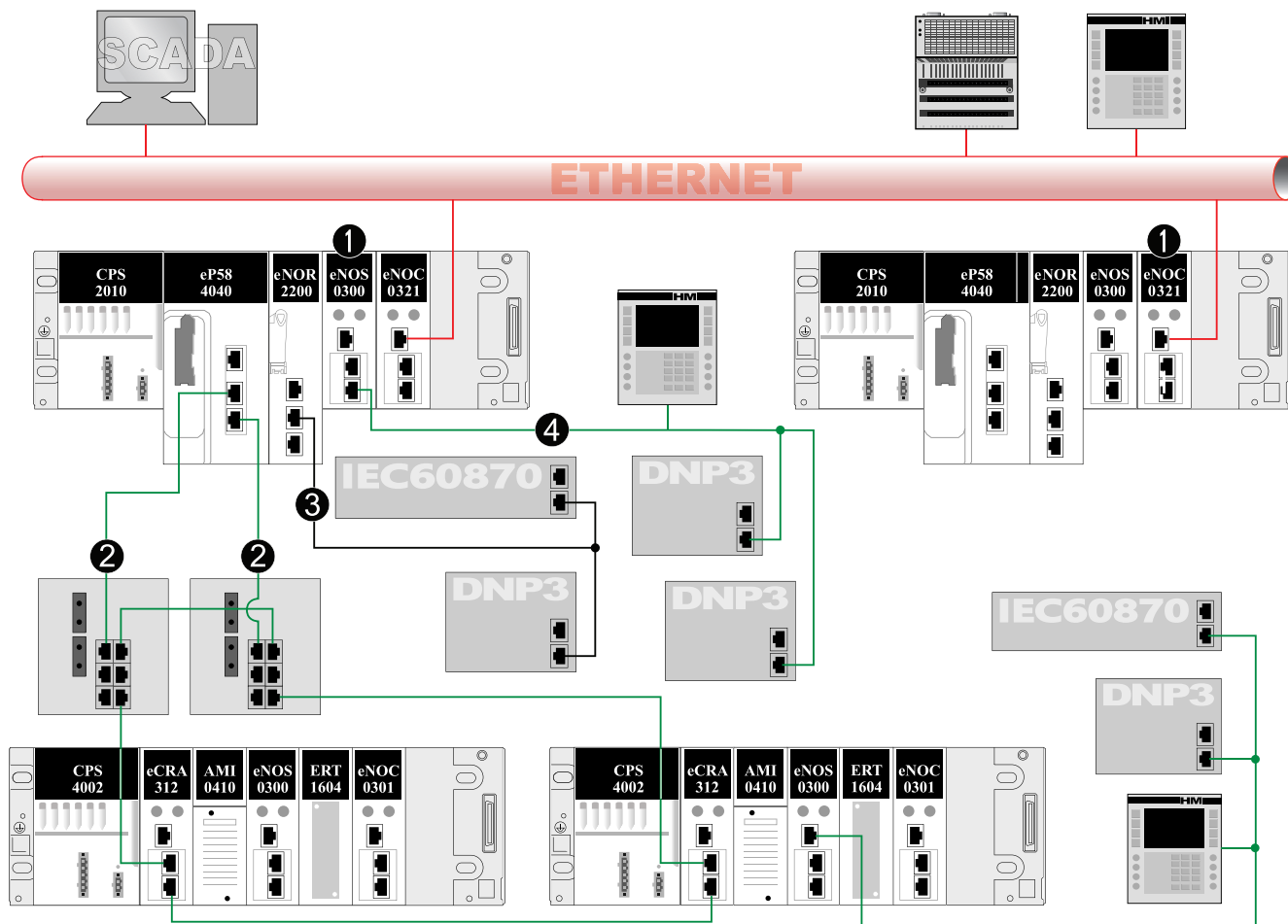
Légende :

- 1 Le port de service du contrôleur connecte l'anneau principal RIO et les équipements distribués (équipements RTU, équipements IEC 60870, IHM) au réseau de contrôle Ethernet.
- 2 Anneau principal RIO (des commutateurs double anneau connectent le rack local à une station RIO).
- 3 Un module BMENOR2200H dispose d'une connexion RS232/RS485 à des équipements RTU série.
- 4 Un module BMENOC0301 du rack local connecte les équipements distribués (équipements RTU, équipements IEC 60870, IHM) à l'anneau principal RIO.
- 5 Un module BMENOS0300 d'une station RIO connecte les équipements distribués (équipements RTU, équipements IEC 60870, IHM) à l'anneau principal RIO.

Réseau autonome avec deux sous-réseaux

Exemple de réseau

Cet exemple de réseau autonome s'appuie sur l'exemple de sous-réseau unique et comprend des modules BMENOR2200H sur des racks locaux qui communiquent avec deux sous-réseaux différents :



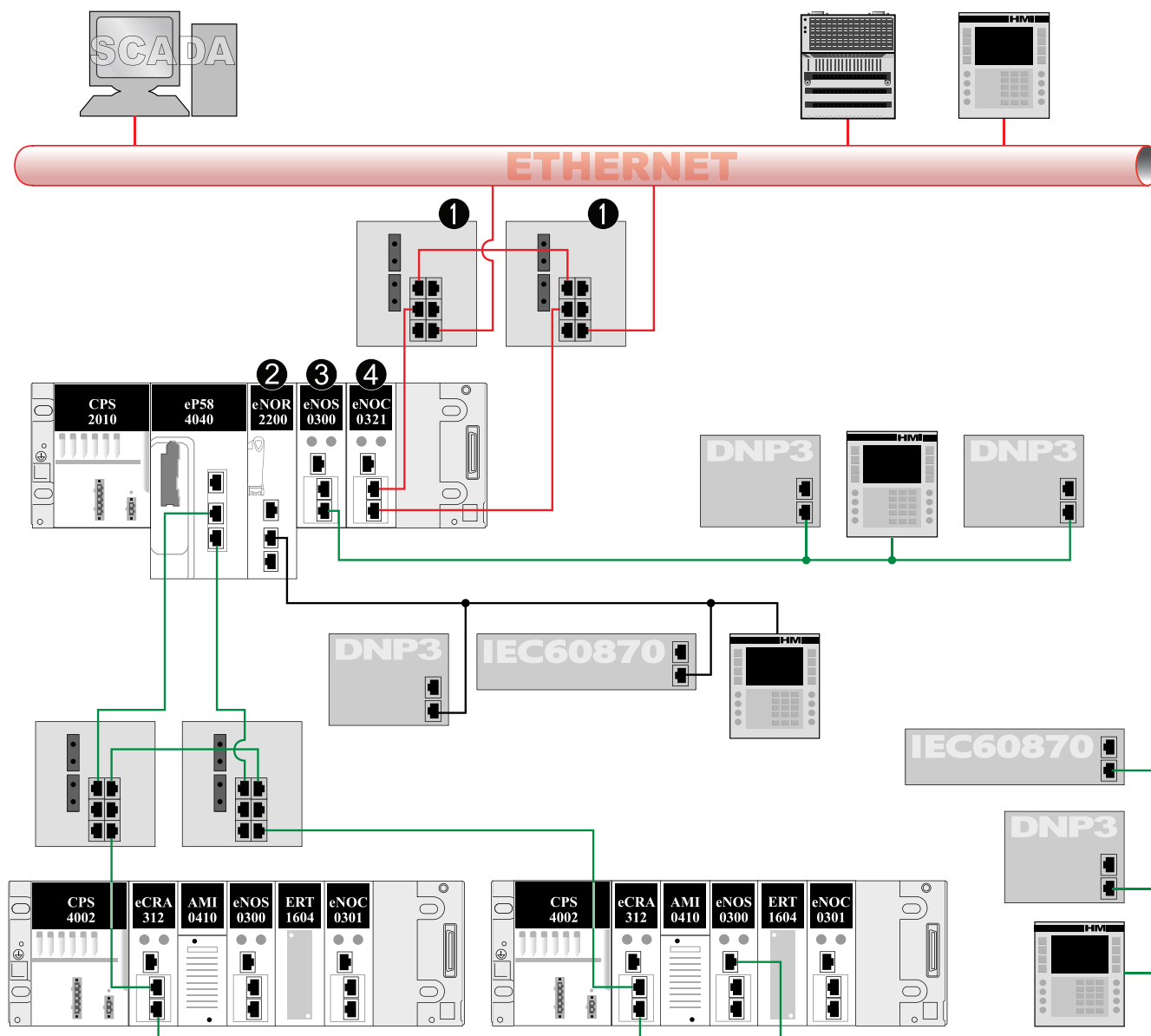
Légende :

- 1 Les modules BMENOC0321 des racks locaux connectent l'anneau principal RIO et les équipements distribués (équipements RTU, IHM) au réseau de contrôle Ethernet (rouge).
- 2 Anneau principal RIO (des commutateurs double anneau connectent le rack local à deux stations RIO et aux équipements distribués.)
- 3 Un module BMENOR2200H dispose d'une connexion RS232 à un équipement série RTU.
- 4 Un module BMENOS0300 d'une station RIO connecte des équipements distribués (RTU) à l'anneau principal RIO.

Réseau autonome avec redondance de liaison

Exemple de réseau

Cet exemple de réseau autonome s'appuie sur l'exemple à deux sous-réseaux, qui inclut les communications sur différents sous-réseaux (rouge et vert). Dans ce cas, les connexions entre les racks locaux et les commutateurs double anneau facilitent les connexions redondantes entre les sous-réseaux :



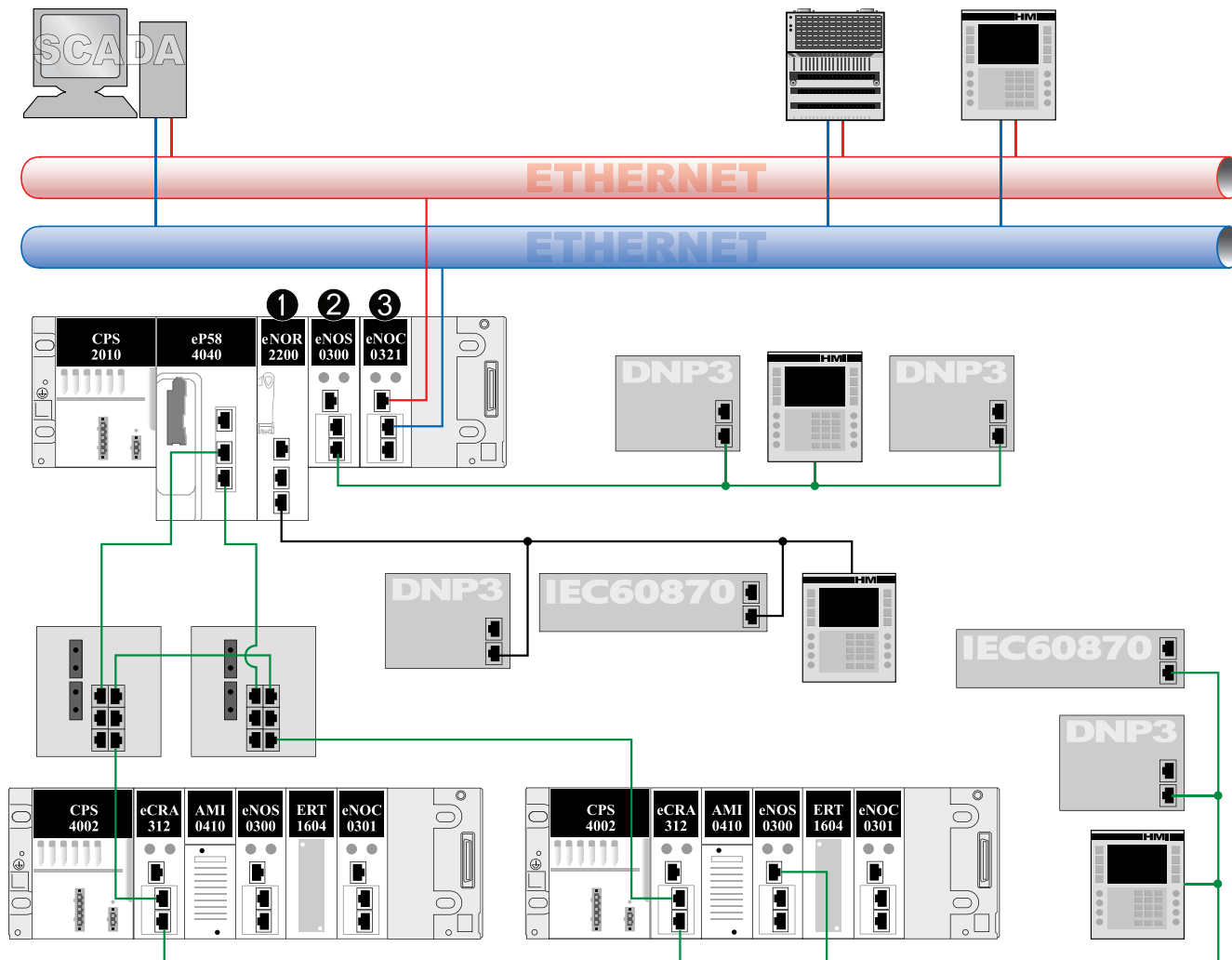
Légende :

- 1** Un commutateur double anneau connecté au port Ethernet d'un module BMENOC0321 du rack local crée une liaison redondante avec le réseau de contrôle (rouge).
- 2** Un module BMENOR2200H connecte le rack local aux équipements distribués (équipements RTU, IHM) via le port de contrôle ou le port série.
- 3** Un module de commutation intégré BMENOS0300 connecte le rack local aux équipements distribués (équipements RTU) à l'aide de liaisons redondantes.
- 4** Le port de service d'un module BMENOC0321 permet aux équipements distribués (équipements RTU, IHM) de communiquer avec le réseau de contrôle à l'aide de liaisons redondantes.

Réseau autonome avec trois sous-réseaux

Exemple de réseau

Cet exemple de réseau autonome s'appuie sur l'exemple à deux sous-réseaux avec différents sous-réseaux (rouge et vert). Dans ce cas, des modules BMENOC0321 avec transfert IP intégré dans les racks locaux facilitent la connexion à un troisième sous-réseau (bleu) :



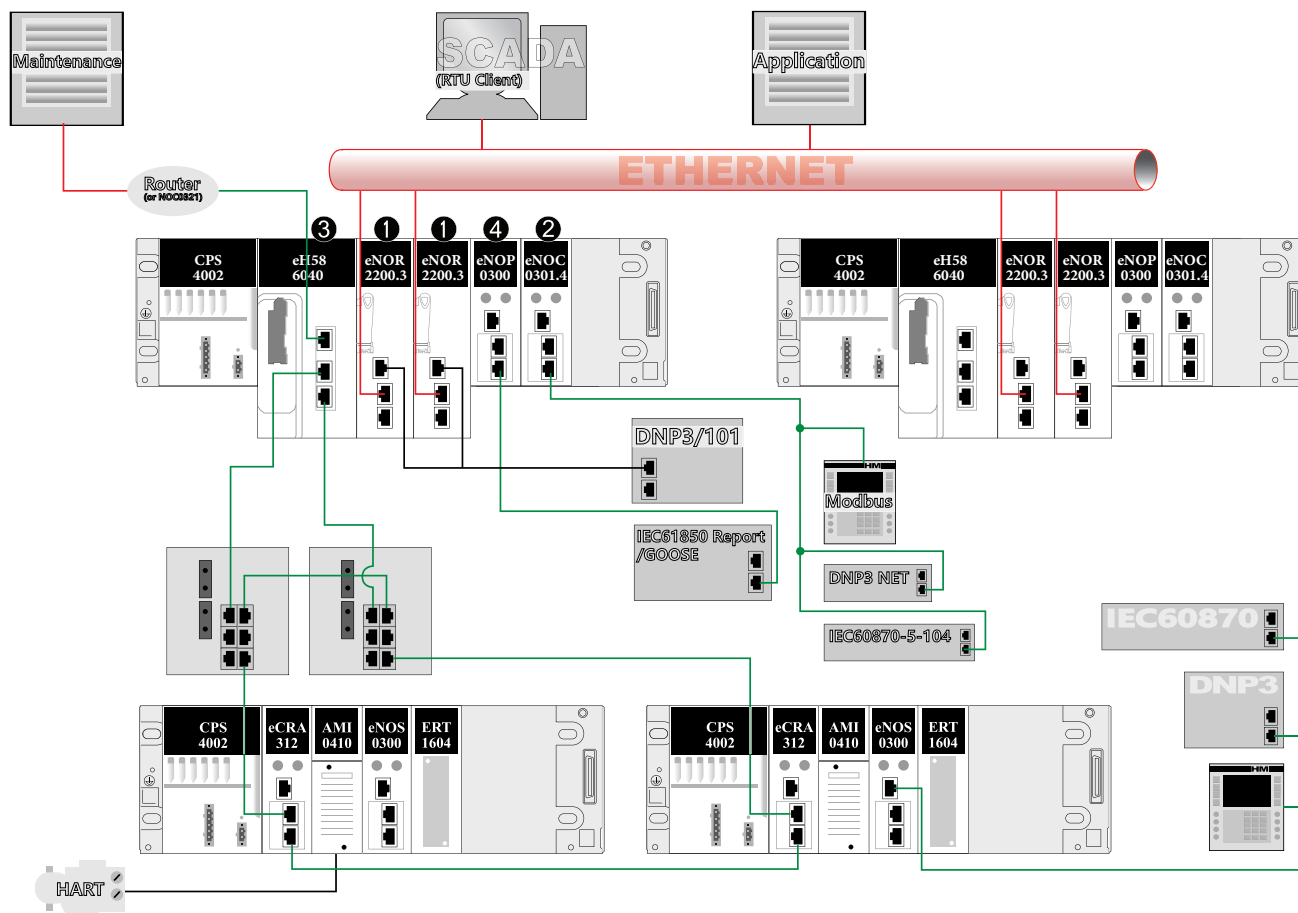
Légende :

- 1** Un module BMENOR2200H connecte le rack local aux équipements distribués (équipements RTU, IHM) via les ports de contrôle ou le port série.
- 2** Les modules BMENOS0300 des racks locaux connectent les équipements distribués (DNP3/IEC60870, IHM) aux anneaux principaux RIO en utilisant des liaisons redondantes
- 3** Les modules BMENOC0321 avec transfert IP activé connectent les anneaux principaux RIO et les équipements distribués (équipements DNP3/IEC60870, IHM) au réseau bleu via le port de service et au réseau rouge via le port réseau de contrôle en utilisant des liaisons redondantes

Réseau isolé sous contrôleur autonome

Exemple de réseau

Cet exemple de réseau autonome isolé inclut des modules BMENOR2200H sur des racks locaux. Le module BMENOR2200H fournit deux sous-réseaux isolés différents pour le réseau de contrôle (rouge) et le réseau d'embase (vert).



Légende :

- 1** Un module BMENOR2200H connecte l'équipement en amont (SCADA, par exemple) via le port de contrôle et connecte le rack local à d'autres équipements Ethernet (équipements RTU, IHM) via le port d'embase Ethernet ou le port série.
- 4** Les modules BMENOC0301 des racks locaux connectent les équipements distribués (équipements RTU, équipements Modbus, IHM).
- 3** Accès réseau à contrôler pour application d'ingénierie/maintenance (Control Expert, outil de mise à niveau du micrologiciel etc.)
- 4** Les modules BMENOP0300 des racks locaux connectent les équipements IEC61850 (serveur ou client).

Réseaux M580 redondants

Introduction

Adresse IP du module

Les systèmes redondants contiennent des réseaux de contrôle primaire et redondant distincts. La configuration des racks primaire et redondant est identique.

Un système redondant qui met en œuvre des modules BMENOR2200H inclut par conséquent un tel module dans chacun des racks primaire et redondant avec les adresses IP suivantes :

- *Adresse IP* : module BMENOR2200H de la configuration primaire
- *Adresse IP + 1* : module BMENOR2200H de la configuration redondante

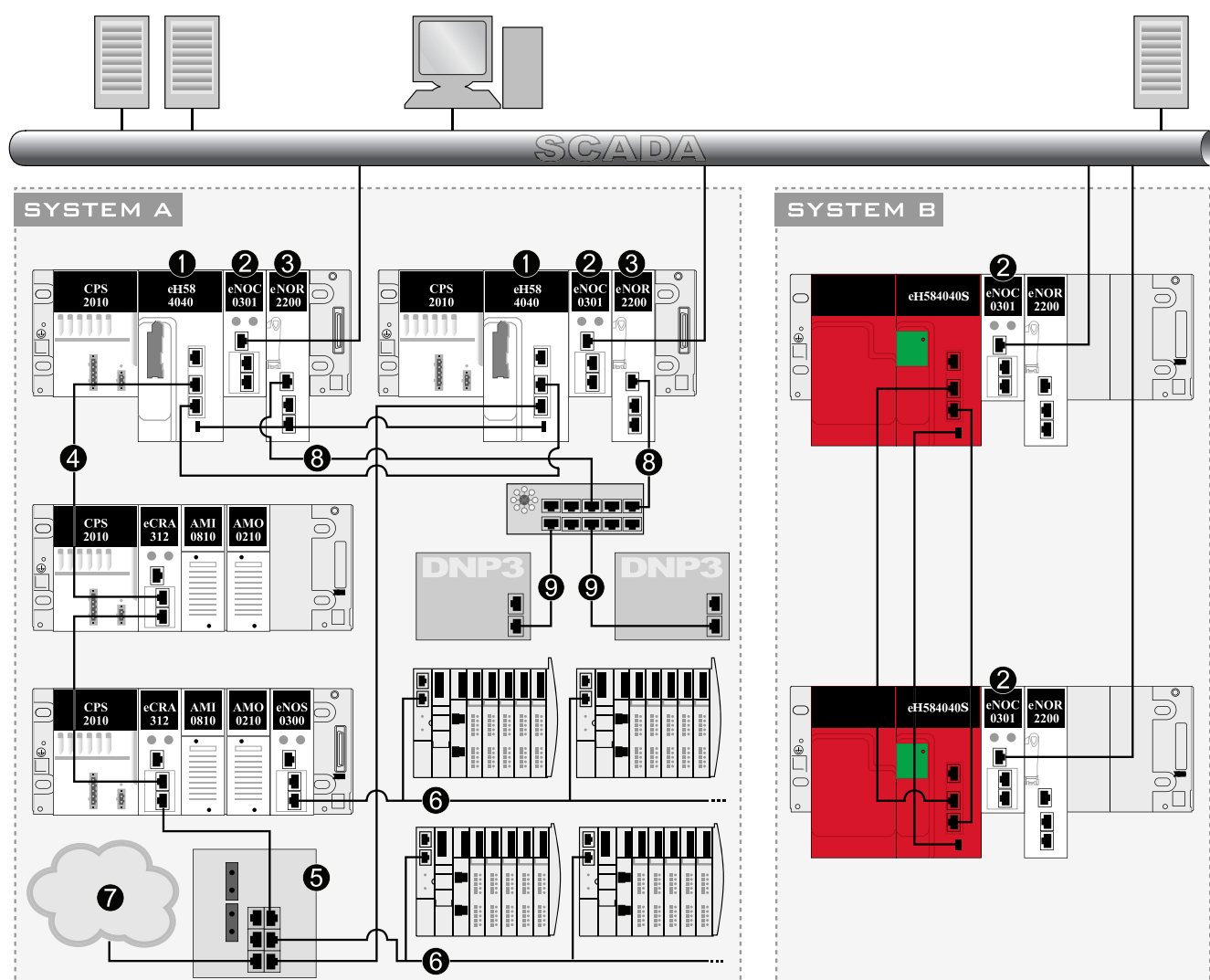
Lors d'un basculement, le réglage d'adresse IP est automatiquement transféré de l'ancien module BMENOR2200H primaire à l'ancien module BMENOR2200H redondant. Le paramètre *Adresse IP + 1* est également transféré de l'ancien module BMENOR2200H redondant au nouveau module BMENOR2200H redondant.

Architecture redondante avec un sous-réseau

Exemple de réseau

Cette architecture M580 met en œuvre des modules BMENOR2200H dans deux configurations de rack, un système redondant M580 et un système redondant M580 Safety.

Le système redondant (*SYSTEME A*) et le système redondant Safety (*SYSTEME B*) ont tous les deux des configurations de rack primaire et secondaire avec fonctionnalité de routage pour prendre en charge la redondance. Le réseau SCADA connecté est également équipé d'un routage commuté :



Légende :

- 1 Un PAC redondant M580 relie l'anneau principal au réseau de contrôle.
- 2 Un module BMENOC0301 se connecte aux PAC redondants autonomes et Safety via l'embase Ethernet qui prend en charge les équipements distribués.
- 3 Un module BMENOR2200H joue le rôle de serveur RTU pour prendre en charge les communications DNP3, IEC60870-5-101 ou IEC60870-5-104.
- 4 Anneau principal RIO
- 5 Un commutateur double anneau (DRS) connecte les équipements distribués à la station RIO de l'anneau principal.
- 6 Des équipements distribués se connectent à l'anneau principal via le DRS en utilisant des communications DNP3, IEC60870-5-101, ou IEC60870-5-104.
- 7 Un nuage DIO se connecte à l'anneau principal via le DRS.

8 Les modules BMENOR2200H se connectent à un bloc répartiteur réseau pour les équipements série.

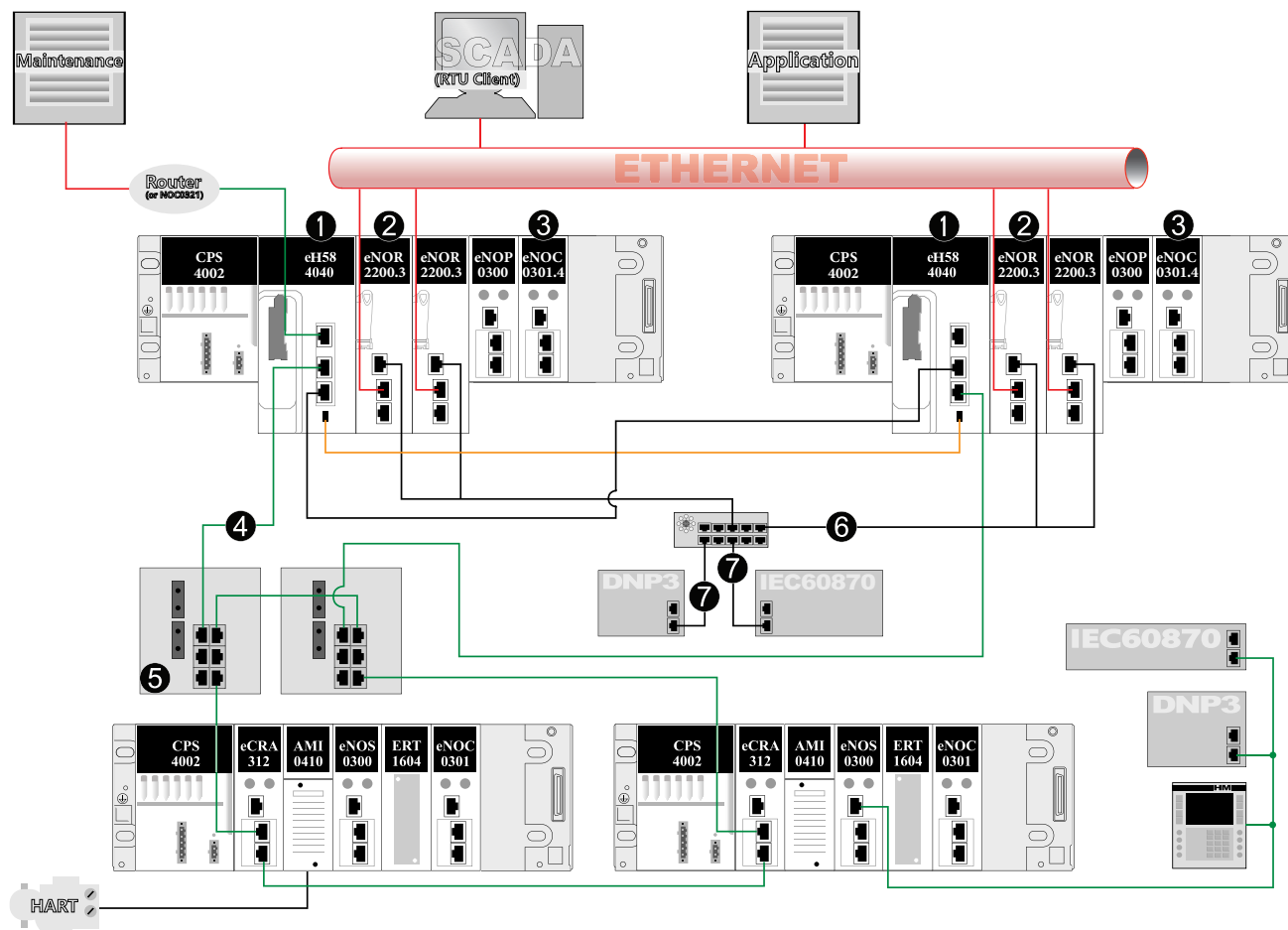
9 Les équipements série DNP3 ont des connexions RS485 au bloc répartiteur réseau.

NOTE: Les modules BMENOR2200H primaire et redondant utilisent le réseau RIO ou le réseau amont pour synchroniser les données. Sinon, la paire de modules ne peut pas instaurer la fonctionnalité de redondance Hot Standby.

Architecture redondante avec réseau isolé

Exemple de réseau

Cet exemple de réseau redondant isolé inclut des modules BMENOR2200H sur des racks locaux. Le module BMENOR2200H fournit deux sous-réseaux isolés différents pour le réseau de contrôle (rouge) et le réseau d'embase (vert).



Légende :

- 1** Un PAC redondant M580 relie l'anneau principal au réseau de contrôle.
- 2** Un module BMENOR2200H joue le rôle de serveur RTU pour prendre en charge les communications DNP3, IEC60870-5-101 ou IEC60870-5-104.
- 3** Un module BMENOC0301 se connecte aux PAC autonome et redondant de sécurité via l'embase Ethernet qui prend en charge les équipements distribués.
- 4** Anneau principal RIO
- 5** Un commutateur double anneau (DRS) connecte les équipements distribués à la station RIO de l'anneau principal.
- 6** Des modules BMENOR2200H se connectent à un bloc répartiteur réseau pour les équipements série.
- 7** Les équipements série DNP3 ont des connexions RS485 au bloc répartiteur réseau.

NOTE: Les modules BMENOR2200H primaire et redondant utilisent le réseau RIO ou le réseau amont pour synchroniser les données. Sinon, la paire de modules ne peut pas instaurer la fonctionnalité de redondance Hot Standby.

Installation du matériel

Montage du module sur le rack

Introduction

Le module BMENOR2200H comporte un connecteur double bus qui prend en charge les communications Ethernet et X Bus.

Suivez ces instructions pour installer le module à un emplacement unique d'une embase Ethernet BMEXBP.

Avant de commencer

⚠ AVERTISSEMENT

FONCTIONNEMENT IMPREVU DE L'EQUIPEMENT

Les racks Modicon X80 doivent être montés horizontalement sur un plan vertical pour faciliter la ventilation.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Avant d'installer le module sur le rack :

- Retirez le capuchon de protection du connecteur du module sur le rack.
- Déterminez le mode de fonctionnement de la cybersécurité pour le module et configurez le mode de cybersécurité approprié à l'aide du [commutateur rotatif](#), [page 28](#) avant d'installer le module dans l'emplacement. Le mode sélectionné n'est mis en œuvre qu'après la mise sous tension du module.

Considérations relatives à l'embase

Installez le module sur le rack local uniquement. Vous pouvez installer et configurer jusqu'à quatre modules de communication (y compris des modules BMENOR2200H) sur un seul rack local (en fonction du contrôleur sélectionné).

Ce tableau indique le nombre maximal de modules BMENOR2200H pouvant être installés dans le rack local en fonction des références de contrôleur :

contrôleur	BMENOR2200H
BMEP581020	2
BMEP582020	2
BMEP582040(S)	3
BMEP584020	4
BMEP584040(S)	4
BMEP586040	4
BMEH582040	2
BMEH584040	4
BMEH586040(S)	4

NOTE: Reportez-vous au tableau de sélection de contrôleur dans *Modicon M580 Autonome, Guide de planification du système pour architectures courantes*. Consultez également le document *Modicon M580 - Redondance d'UC - Guide de planification du système pour architectures courantes* ; *Modicon M580 - Guide de planification du système Safety* (voir Documents à consulter).

Installez le module dans un emplacement double bus sur l'une des embases Ethernet suivantes :

Embase	Description
BMEXBP0400(H)	Embase Ethernet 4 emplacements (renforcée)
BMEXBP0800(H)	Embase Ethernet 8 emplacements (renforcée)
BMEXBP1200(H)	Embase Ethernet 12 emplacements (renforcée)
BMEXBP0602(H)	Embase Ethernet double alimentation à 6 emplacements (renforcée)
BMEXBP1002(H)	Embase Ethernet double alimentation à 10 emplacements (renforcée)

Restrictions liées aux racks et aux emplacements

Le module occupe un seul emplacement double bus. Tenez compte des restrictions suivantes :

Rack	Emplacement	Instruction
tous les racks	0, 1	Ces emplacements ne prennent pas en charge le module BMENOR2200H. NOTE: Ces emplacements sont réservés au module contrôleur.
BMEXBP1200 (H)	2, 8, 10, 11	Ces emplacements X Bus uniquement ne prennent pas en charge la fonctionnalité Ethernet du module BMENOR2200H à double bus.
BMEXBP1002 (H)	2, 8	
racks étendus	—	Vous ne pouvez pas installer le module BMENOR2200H double bus dans un rack d'extension. NOTE: Les racks d'extension ne disposent pas de ports Ethernet.
stations RIO	—	Vous ne pouvez pas installer le module BMENOR2200H double bus dans une station RIO.

Considérations relatives au commutateur de cybersécurité

AVIS

FONCTIONNEMENT IMPREVU DE L'EQUIPEMENT

- Ne passez pas directement de la configuration Standard à la configuration Advanced ou inversement.
- Mettez toujours le module sous tension avec le commutateur rotatif en position Cybersecurity Reset lorsque vous basculez entre les modes Standard et Advanced.

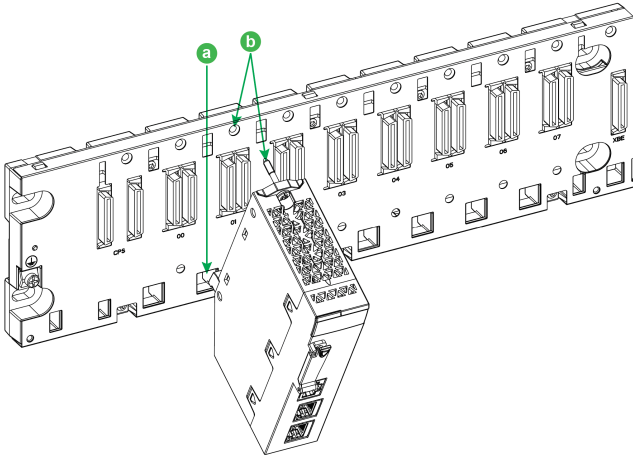
Le non-respect de ces instructions peut provoquer des dommages matériels.

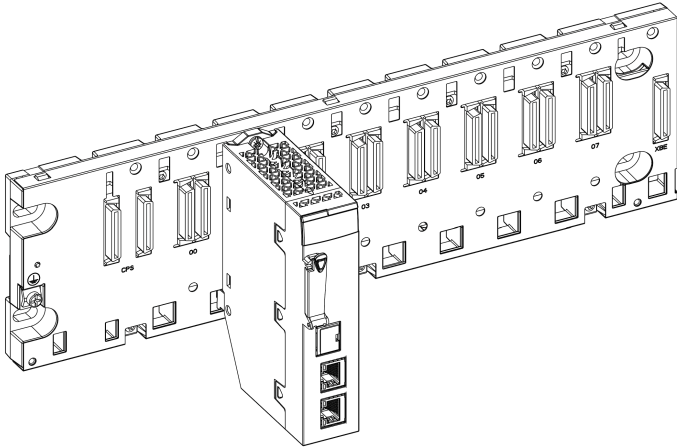
Procédez comme suit chaque fois que vous insérez un module BMENOR2200H dans un rack alimenté :

Etape	Action
1	Réglez le commutateur rotatif, page 28 du module sur la position Cybersecurity Reset .
2	Insérez le module dans le rack pour le mettre sous tension.
3	Retirez le module du rack pour le mettre hors tension.
4	Réglez le commutateur rotatif du module sur la position Advanced ou Standard .
5	Réinsérez le module dans le rack pour le mettre sous tension.

Installation du module sur le rack

Montez le module dans un seul emplacement de l'embase :

Etape	Action				
1	Mettez le rack hors tension.				
2	Retirez la protection de l'interface du module sur le rack.				
3	Configurez le niveau de cybersécurité du module à l'aide du commutateur rotatif en tenant compte des considérations relatives à la cybersécurité, page 28.				
4	Ce graphique illustre les sous-étapes a. et b. :  <table><tr><td>a.</td><td>Insérez les ergots situés sur la base du module dans les emplacements correspondants du rack.</td></tr><tr><td>b.</td><td>Utilisez les ergots pour faire basculer le module jusqu'à ce qu'il s'insère totalement dans le rack. (Le double connecteur situé à l'arrière du module s'insère dans les connecteurs du rack.)</td></tr></table> NOTE: N'insérez pas le module BMENOR2200H dans l'emplacement 0 ou 1 du rack local. Ces emplacements sont réservés au contrôleur. NOTE: N'insérez pas le module BMENOR2200H dans un emplacement réservé pour X-bus.	a.	Insérez les ergots situés sur la base du module dans les emplacements correspondants du rack.	b.	Utilisez les ergots pour faire basculer le module jusqu'à ce qu'il s'insère totalement dans le rack. (Le double connecteur situé à l'arrière du module s'insère dans les connecteurs du rack.)
a.	Insérez les ergots situés sur la base du module dans les emplacements correspondants du rack.				
b.	Utilisez les ergots pour faire basculer le module jusqu'à ce qu'il s'insère totalement dans le rack. (Le double connecteur situé à l'arrière du module s'insère dans les connecteurs du rack.)				

Etape	Action
5	Serrez la vis d'assemblage pour maintenir le module en place sur le rack :  ⚠ AVERTISSEMENT FONCTIONNEMENT IMPREVU DE L'EQUIPEMENT Serrez bien la vis de montage pour fixer fermement le module au rack. Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels. NOTE: Couple de serrage : 0,4 à 1,5 Nm (0,30 à 1,10 lbf-ft).
6	Insérez la carte SD si vous souhaitez utiliser la fonction de journalisation des données.

Consignes de mise à la terre

Cette section présente les consignes de câblage et les bonnes pratiques à respecter pour installer et câbler le module de communication Ethernet BMENOR2200H.

⚡⚠ DANGER

RISQUE D'ELECTROCUTION, D'EXPLOSION OU D'ARC ELECTRIQUE

- Coupez toutes les alimentations de tous les équipements, y compris les équipements connectés, avant de retirer les caches ou les portes d'accès, ou avant d'installer ou de retirer des accessoires, matériels, câbles ou fils, sauf dans les cas de figure spécifiquement indiqués dans le guide de référence du matériel approprié à cet équipement.
- Utilisez toujours un appareil de mesure de tension réglé correctement pour vous assurer que l'alimentation est coupée conformément aux indications.
- Remettez en place et fixez tous les caches de protection, accessoires, matériels, câbles et fils et vérifiez que l'appareil est bien relié à la terre avant de le remettre sous tension.
- Utilisez uniquement la tension indiquée pour faire fonctionner cet équipement et les produits associés.

Le non-respect de ces instructions provoquera la mort ou des blessures graves.

⚠ AVERTISSEMENT

PERTE DE CONTROLE

- Réalisez une analyse des modes de défaillance et de leurs effets (FMEA) ou une analyse de risques équivalente sur l'application et appliquez les contrôles de prévention et de détection appropriés avant la mise en œuvre.
- Prévoyez un état de repli pour les événements ou séquences de commande indésirables.
- Le cas échéant, prévoyez des chemins de commande séparés et redondants.
- Définissez les paramètres appropriés, notamment pour les limites.
- Examinez les conséquences des retards de transmission et prenez les mesures correctives nécessaires.
- Examinez les conséquences des interruptions de la liaison de communication et prenez des mesures correctives nécessaires.
- Prévoyez des chemins indépendants pour les fonctions de commande critiques (arrêt d'urgence, dépassement de limites, conditions d'erreur, etc.) en fonction de votre évaluation des risques ainsi que des réglementations et consignes applicables.
- Appliquez les réglementations et les consignes locales de sécurité et de prévention des accidents.¹
- Testez chaque mise en œuvre d'un système pour vérifier son bon fonctionnement avant de le mettre en service.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

¹ Pour plus d'informations, consultez le document NEMA ICS 1.1 (dernière édition), *Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control* (Directives de sécurité pour l'application, l'installation et la maintenance de commande statique) et le document NEMA ICS 7.1 (dernière édition), *Safety Standards for Construction and Guide for Selection, Installation, and Operation of Adjustable-Speed Drive Systems* (Normes de sécurité relatives à la construction et manuel de sélection, installation et opération de variateurs de vitesse) ou leur équivalent en vigueur dans votre pays.

Les règles suivantes doivent être respectées lors du câblage du module de communication Ethernet :

- Le câblage de communication doit être séparé du câblage d'alimentation. Ces deux types de câblage doivent avoir des chemins de câbles séparés.
- Vérifiez que les conditions de fonctionnement et d'environnement sont conformes aux valeurs indiquées dans le présent document et dans les autres guides d'utilisation associés à cet équipement.
- Utilisez des câbles blindés à paires torsadées (ferrule) présentant les caractéristiques nominales appropriées pour votre installation/ environnement.

Si vous n'utilisez pas les câbles blindés (ferrule) appropriés pour ces connexions, le signal risque d'être dégradé par des interférences électromagnétiques. Des signaux dégradés peuvent provoquer un comportement inattendu du contrôleur ou d'autres modules et équipements connectés.

⚠ AVERTISSEMENT

FONCTIONNEMENT IMPREVU DE L'EQUIPEMENT

- Utilisez des câbles blindés (ferrule) pour tous les signaux de communication.
- Reliez à la terre le blindage (ferrule) des câbles de tous les signaux de communication en un même point¹.
- Acheminez les câbles de communication séparément des câbles d'alimentation.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

¹ La mise à la terre multipoint est autorisée si les connexions sont reliées à une terre équipotentielle dimensionnée pour éviter toute dégradation du blindage des câbles en cas de courts-circuits dans le système d'alimentation.

Utilisez un câble en fibre optique pour établir une liaison de communication lorsqu'il n'est pas possible d'égaliser le potentiel entre les points de terre.

NOTE: Reportez-vous aux informations sur la protection de terre fournies dans *Electrical installation guide* et *Guide technique Tableau de contrôle, Comment protéger une machine des dysfonctionnements dus aux perturbations électromagnétiques* (voir Documents à consulter).

Remplacement d'un module

AVIS

FONCTIONNEMENT IMPREVU DE L'EQUIPEMENT

- Ne passez pas directement de la configuration Standard à la configuration Advanced ou inversement.
- Mettez toujours le module sous tension avec le commutateur rotatif en position Cybersecurity Reset lorsque vous basculez entre les modes Standard et Advanced.

Le non-respect de ces instructions peut provoquer des dommages matériels.

Tout module du rack peut être remplacé à chaud à tout moment par un autre module doté d'un micrologiciel compatible. Le module de remplacement obtient ses paramètres de fonctionnement via la connexion entre l'embase et le contrôleur. Le transfert vers l'équipement est effectué immédiatement lors du cycle suivant.

Lorsque vous passez du mode Advanced au mode Standard ou inversement, réinitialisez le module en réglant le commutateur rotatif sur la position Cybersecurity Reset pour mettre en œuvre un fichier de configuration propre et effacer les paramètres de sécurité (y compris le nom d'utilisateur et le mot de passe).

Exportez votre configuration de cybersécurité avant de remplacer le module. Lorsque le commutateur rotatif est réglé sur le mode Cybersecurity Reset d'usine, toute la configuration de cybersécurité est effacée.

Pour remplacer le module :

Etape	Action
1	Retirez le module du rack en suivant en sens inverse les étapes d'installation décrites plus haut. NOTE: Comme il s'agit d'un module remplaçable à chaud, il n'est pas nécessaire de mettre le rack hors tension pour le retirer.
2	Réglez le commutateur rotatif, page 28 du module de remplacement sur la position Cybersecurity Reset .
3	Insérez le module de remplacement dans le rack pour le mettre sous tension.
4	Retirez le module de remplacement du rack pour le mettre hors tension.
5	Réglez le commutateur rotatif du module de remplacement sur la position Advanced ou Standard .
6	Réinsérez le module de remplacement dans le rack pour le mettre sous tension.

NOTE: Le module de remplacement ne récupère pas automatiquement les paramètres de sécurité de la configuration Web. Le fichier de configuration de la sécurité est stocké localement dans le module. Exportez ce fichier pour créer une configuration de sauvegarde et importez un fichier de configuration de cybersécurité stocké vers le nouveau module via la page Web.

NOTE: La carte mémoire SD contient les fichiers CSV du [service de journalisation des données](#) indépendant. Lorsque la journalisation de données est activée, sauvegardez les tables de journalisation de données stockées sur la carte SD avant de remplacer le module.

Communications Ethernet

Services Ethernet

A propos de cette section

Cette section décrit les services Ethernet dont dispose le module BMENOR2200H.

Services Ethernet disponibles

Introduction

Cette section présente les différents services et fonctionnalités pris en charge par le module BMENOR2200H.

Protocoles RTU

Le module prend en charge les protocoles RTU suivants :

- Serveur NET DNP3 avec SAV2 ou SAV5
- Client NET DNP3 avec SAV2 ou SAV5
- Serveur série DNP3 avec SAV2 ou SAV5
- Client série DNP3 avec SAV2 ou SAV5
- Client IEC60870-5-104
- Serveur IEC60870-5-104
- Client IEC60870-5-101
- Serveur IEC60870-5-101

NOTE: Reportez-vous à la description des protocoles RTU, page 63.

Services Ethernet

Le module prend en charge les services Ethernet suivants :

- Agents SNMPv1 et SNMPv3
- Client FDR (service de base)
- Serveur et client Modbus TCP
- Client SNTpV1
- Pages Web HTTPS intégrées

Autres services

Le module BMENOR2200H prend également en charge les services suivants :

- Mise à niveau du micrologiciel
- synchronisation d'horloge
- Cybersécurité

Service SNMP

Présentation de SNMP

Introduction à SNMP

Les modules de communication Ethernet prennent en charge SNMP, le protocole standard de gestion des réseaux locaux (LAN). SNMP définit exactement comment un gestionnaire communique avec un agent. SNMP définit un format pour :

- requêtes envoyées par un gestionnaire à un agent
- réponses renvoyées par un agent au gestionnaire.

Un agent SNMP s'exécute sur :

- modules de communication Ethernet
- contrôleurs avec ports de communication Ethernet intégrés

SNMP et NMS

Un système de gestion de réseau (NMS) utilise SNMP pour surveiller et contrôler les composants de l'architecture Ethernet afin de permettre un diagnostic rapide du réseau.

Le NMS permet à un gestionnaire réseau d'exécuter les tâches suivantes :

- Surveiller et contrôler les composants du réseau.
- Isoler les problèmes et trouver leurs causes.
- Interroger des équipements (ordinateurs hôtes, routeurs, commutateurs et ponts) pour déterminer leur état.
- Obtenir des statistiques concernant les réseaux auxquels ils sont associés.

NOTE: Un grand nombre de fournisseurs proposent des systèmes de gestion réseau.

Communication SNMP

Introduction

L'agent SNMP est implémenté sur le module. Un gestionnaire peut ainsi accéder aux objets normalisés MIB II via le protocole SNMP. La base MIB II permet la gestion des couches de communication TCP/IP.

Cette section décrit le protocole SNMP (Simple Network Management Protocol).

NOTE:

- Pour configurer le service SNMP, reportez-vous aux instructions de configuration SNMP dans le DTM.
- Consultez également la description de la prise en charge de SNMP par la MIB.

Structure SNMP

SNMP définit les solutions de gestion réseau en termes de protocoles réseau et d'échange de données supervisées.

La structure SNMP repose sur les éléments suivants :

- **Gestionnaire** : Le gestionnaire permet une supervision totale ou partielle du réseau.
- **Agents** : Chaque équipement supervisé dispose d'un ou de plusieurs modules logiciels appelés Agents qui sont utilisés par le protocole SNMP.
- **MIB** : La MIB (Management Information Base) est une base de données ou un ensemble d'objets.

Protocole SNMP

Le protocole SNMP définit les types de messages entre l'agent et le gestionnaire. Ces messages sont encapsulés dans des datagrammes UDP.

Messages du gestionnaire à un agent :

- **Get_Request** : Ce message obtient la valeur d'une ou de plusieurs variables.
- **Get_Next_Request** : Obtenir la valeur des variables suivantes.
- **Set_Request** : Définir la valeur d'une variable.

Messages d'un agent au gestionnaire :

- **Get_Response** : Permet à l'agent d'envoyer à nouveau la valeur de la variable demandée.
- **Trap** : Permet le signalement d'événement asynchrone par l'agent.

Versions de SNMP

Versions disponibles

Le module exécute plusieurs versions du protocole de communication SNMP :

- **SNMPv1** : La version 1 de SNMP étend les capacités du protocole à la gestion de problèmes d'administration et de sécurité. Avec cette version, le mot de passe en texte simple est partagé entre un *gestionnaire* et un *agent*. Les commandes SNMPv1 sont de simples commandes de requête-réponse (*Get*, *Set*, *Trap*).

NOTE: Cette version offre une sécurité minimale pour les utilisateurs ayant accès au même réseau.

- **SNMPv3** : En termes d'opérations, SNMPv3 est fonctionnellement assez semblable à SNMPv1. SNMPv3 offre toutefois une sécurité renforcée pour un réseau auquel plusieurs utilisateurs accèdent, par le biais de contrôles d'authentification et de confidentialité. SNMPv3 considère les *gestionnaires* et les *agents* de SNMPv1 comme des *entités*. Dans SNMPv3, chaque *entité* se compose d'un *moteur* SNMP et d'au moins une *application* SNMP. De telles distinctions permettent au protocole d'implémenter la sécurité en fonction des relations entre ces entités dans une architecture modulaire. En outre, SNMPv3 facilite la configuration d'agents SNMP distants car chaque entité SNMP a un identifiant unique (*engineID*) qui correspond aux requêtes d'un moteur SNMP distant spécifique.

Récapitulatif des niveaux de sécurité

Il n'y a pas de compatibilité native entre les messages SNMPv1 et SNMPv3. L'agent SNMP fournit les niveaux de sécurité suivants :

- *mode standard* : Prise en charge de SNMPv1 et SNMPv3. Dans ce mode, SNMPv3 utilise `NoAuthNoPriv` ; il n'y a pas d'autorisation ni de cryptage pour les paquets envoyés entre la station de gestion du réseau et le gestionnaire SNMP.
- *mode avancé* : Prise en charge de SNMPv3 en mode avancé pour améliorer l'authentification et l'intégrité (`AuthNoPriv`) ainsi que l'authentification, l'intégrité et la confidentialité (`AuthPriv`).

SNMPv3 et HMAC

L'authentification SNMPv3 utilise HMAC (Hash Message Authentication Code) pour authentifier chaque message critique en implémentant un modèle de défi-réponse.

HMAC peut être considéré comme une somme de contrôle cryptographique sur le message SNMP associée à une clé secrète (dérivée du mot de passe utilisateur). Le code HMAC et le nom d'utilisateur sont transmis au sein du paquet. L'équipement vérifie l'intégrité et la source du message en calculant une somme de contrôle sur le message reçu avec la clé secrète issue de sa base de données utilisateurs locale. Si le code HMAC calculé et celui du paquet coïncident, l'accès est accordé.

L'algorithme de sécurité HMAC est utilisé pour *signer* les messages de sécurité afin de confirmer qu'ils n'ont pas été falsifiés. Les algorithmes HMAC SHA-256 sont plus sécurisés que les algorithmes HMAC SHA-1, mais ils requièrent davantage de traitement RTU. Les algorithmes comportant plus d'octets sont plus sécurisés, mais ils créent des messages plus longs qui requièrent davantage de bande passante pour les messages critiques.

SNMPv3 et USM

SNMPv3 prend en charge le modèle de sécurité utilisateur (USM) pour créer et associer des utilisateurs autorisés à un agent SNMPv3 spécifique en vue d'améliorer l'authentification des utilisateurs de même que la confidentialité et l'intégrité des messages.

Bibliothèques de cryptage SNMPv3

L'agent SNMPv3 utilise les bibliothèques de cryptage suivantes pour l'authentification et le cryptage :

- cryptage : CFB128-AES-128 (RFC3826)
- authentification : HMAC-SHA1-96 (RFC-2104)

Informations détaillées sur l'agent SNMP

Introduction

Ce module exécute le protocole SNMP (Simple Network Management Protocol). Ce protocole étend les capacités de SNMP à la résolution de problèmes d'administration et de sécurité. En particulier, les contenus PDU peuvent être cryptés.

Le service d'agent SNMP largement disponible permet d'accéder facilement aux informations de diagnostic du module et aux notifications d'événements pour certains services (par exemple, changement de topologie réseau, état d'un voyant, etc.).

Configurez ce service dans le DTM Control Expert pour gérer les adresses IP (navigateur de MIB, ConneXview, etc.) ou en tant que déroutement (trap) d'événement.

SNMP prend en charge une architecture cadre qui peut être facilement étendue avec de nouveaux protocoles de sécurité utilisateur. Il utilise également le protocole de couche de transport UDP via les ports 161 (interrogation) et 162 (notifications, requêtes, traps). Vous pouvez aisément étendre et adapter l'architecture cadre SNMP pour de nouveaux protocoles de sécurité utilisateur.

Services de gestion

Le tableau suivant décrit les fonctions de base de la gestion de réseau SNMP :

Fonction	Description
gestion de groupe système	Découvrir l'équipement et l'identifier de manière standard à l'aide d'un gestionnaire SNMP.
vérification d'authentification	Configurer le nom de communauté et vérifier l'authentification du demandeur.
gestion de déroutement système	Configurer le gestionnaire SNMP.
gestion MIB II	Gérer la base MIB.

Le service s'exécute sur le module pour permettre aux applications du gestionnaire SNMP de configurer les objets SNMP suivants :

- sysLocation
- sysContact

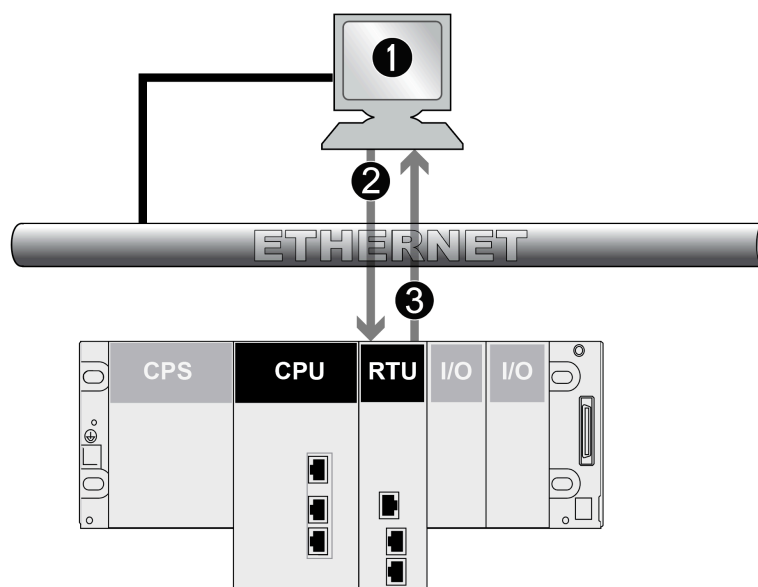
Exemple d'opérations SNMP

Introduction

Le gestionnaire SNMP transmet des requêtes de lecture ou d'écriture (**Set_Request**, **Get_Request**, **Get_Next_Request** etc.) pour les objets définis dans la base MIB - II SNMP. La réponse provient de l'agent SNMP du module BMENOR2200H.

Exemple

Dans cet exemple, un gestionnaire SNMP sur un réseau Ethernet envoie une requête à l'agent SNMP du module BMENOR2200H et reçoit une réponse :



1 gestionnaire SNMP

2 requête

3 réponse / trap

L'agent SNMP du module transmet les événements (traps) au gestionnaire. Les systèmes de trap gérés sont les suivants :

- **Démarrage à froid** : Sur le module BMENOR2200H, l'événement est transmis suite à une réinitialisation de l'alimentation du module, à une réinitialisation de processeur ou au téléchargement d'une application dans l'automate.
- **Echec d'authentification** (SNMP v1 uniquement) : Un événement transmis indique qu'un élément réseau ne peut pas être authentifié. Le champ **Nom de communauté** du message reçu est différent de celui configuré sur le module. Activez ce trap lors de la configuration du module.

Prise en charge de MIB

A propos de la MIB

L'ensemble des objets auxquels SNMP peut accéder est appelé MIB (Management Information Base). Les outils de gestion et de surveillance Ethernet utilisent le protocole SNMP standard pour accéder aux objets de gestion et de configuration inclus dans la MIB de l'équipement et permettent ainsi les opérations suivantes :

- les objets accessibles par le protocole SNMP sont définis et des noms uniques leur sont affectés,
- les programmes gestionnaire et agent s'accordent sur les noms et significations des opérations de recherche et de stockage.

Versions de MIB

Le module utilise l'agent SNMP pour prendre en charge MIB II, qui fournit les informations de diagnostic spécifiées dans les fichiers MIB.

MIB II standard : Ce premier niveau de gestion réseau est accessible via cette interface. Le gestionnaire peut identifier les équipements composant l'architecture et obtenir des informations générales sur la configuration et le fonctionnement de l'interface Ethernet TCP/IP.

Mise à niveau du micrologiciel

Outil EcoStruxure™ Automation Device Maintenance

Fonctions de l'outil

Utilisez l'outil EcoStruxure™ Automation Device Maintenance pour mettre à niveau le micrologiciel du module BMENOR2200H.

Effectuez les actions suivantes à l'aide de cet outil basé sur le Web :

- Découvrez manuellement un ou plusieurs modules BMENOR2200H dans votre projet en fonction des adresses IP.
- Mettez à niveau la version de micrologiciel sélectionnée applicable à ces modules.

Pour plus d'informations sur l'installation et l'utilisation de cet outil de mise à niveau du micrologiciel, consultez l'aide en ligne.

NOTE: Vous ne pouvez pas utiliser le logiciel Unity Loader™ de Schneider Electric pour mettre à niveau le micrologiciel des modules BMENOR2200H.

NOTE: Une version de micrologiciel inférieure à 4.0 ne peut pas être téléchargée sur le module BMENOR2200H avec ports de contrôle.

Rôle d'utilisateur

Utilisez le rôle d'utilisateur **INSTALLATEUR** pour effectuer la mise à niveau du micrologiciel.

NOTE:

- La certification n'est pas valide et le processus de mise à niveau de micrologiciel est bloqué si l'horloge interne du module BMENOR2200H est antérieure à 2019. Le module met à jour l'horloge interne à partir du contrôleur M580. Si aucune heure n'est définie pour le contrôleur, une date par défaut est utilisée (1er janvier 1980). Il est donc recommandé de vérifier que l'horloge interne du module est réglée à la date et à l'heure actuelles avant de mettre à niveau le micrologiciel.
- Lorsque le module fonctionne en mode **Standard**, le rôle d'utilisateur par défaut est **INSTALLATEUR** :
 - nom d'utilisateur par défaut : *installer*
 - mot de passe par défaut : *Inst@ller1*
- Lorsque le module fonctionne en mode **Avancé**, le rôle d'utilisateur par défaut est **SECADM**. Dans ce cas, connectez-vous à la page des paramètres de sécurité pour créer un utilisateur en tant que **INSTALLATEUR** et mettez à niveau le micrologiciel dans ce rôle.
- Reportez-vous à la description des positions du commutateur rotatif et modes correspondants, page 28.

Service client FDR de base

Service client FDR de base

Introduction

Le service client FDR de base (FDR_CLIENT) est appliqué à la configuration IP que le module BMENOR2200H reçoit du contrôleur via X Bus.

NOTE:

- Ce module ne prend pas en charge DHCP ni BOOTP.
- Les paramètres IP statiques ne sont pas stockés localement dans ce module.
- La configuration de la cybersécurité est stockée dans le module BMENOR2200H.

Processus de configuration

Le service configure les paramètres IP du module BMENOR2200H :

Etape	Description
1	Le module obtient ses données de configuration IP à partir de la source de configuration définie par l'utilisateur.
2	Le module obtient son fichier de configuration du contrôleur.
3	Le service valide les paramètres IP (adresse IP, masque de sous-réseau et adresse de passerelle).
4	Le module configure l'équipement avec les paramètres IP validés.

Adresse IP par défaut

Les informations d'adresse par défaut basée sur l'adresse MAC sont utilisées dans les cas suivants :

- Il n'existe aucun fichier de configuration.
- Les informations IP ne sont pas valides.
- L'adresse IP configurée est en conflit avec l'adresse d'un autre module du système.

Lorsqu'une voie par défaut est utilisée, le module n'obtient pas d'adresse IP valide du contrôleur. Il utilise plutôt l'adresse IP par défaut 10.10.mac5.mac6 pour les ports de contrôle et l'adresse IP par défaut 10.20.mac5.mac6 pour le port d'embase. Dans ce cas, le module détecte une situation d'adresse IP en double et ne fonctionne pas.

NOTE: Il arrive (rarement) que la valeur mac6 soit 00 (zéro). L'adresse IP par défaut risque de ne pas fonctionner correctement. Vous pouvez configurer un M580 pour définir une adresse IP valide et la télécharger sur le module BMENOR2200H.

Fonctionnement

Lorsque vous mettez le module BMENOR2200H sous tension, le service client FDR utilise l'adresse IP par défaut. Une fois l'initialisation terminée, le service client FDR obtient la configuration IP auprès du contrôleur. Le service valide ensuite ces paramètres IP :

- **OK** : Le client FDR utilise les paramètres reçus lorsqu'ils sont valides et n'existent pas en double.
- **non OK** : Le service client FDR utilise l'adresse IP par défaut lorsque l'un au moins des paramètres IP reçus n'est pas valide, manque ou existe en double.

NOTE: Lorsqu'une adresse IP en double est détectée dans le système, le voyant BS et/ou NS s'allume fixement en rouge. Voir la description des voyants.

Lorsque les paramètres d'adresse IP représentent une adresse IP en double, le client FDR envoie des requêtes ARP pour détecter l'adresse IP. Si les paramètres IP en double disparaissent, le client FDR utilise les paramètres IP configurés. Après la configuration IP, le service client FDR envoie des requêtes ARP "gratuites".

Messagerie Modbus TCP

Accès aux données

Introduction

Le module BMENOR2200H prend en charge les fonctionnalités de serveur et de client Modbus TCP. En mode avancé, ce service est désactivé par défaut. (Il peut être activé via le Web si le module est en mode **Avancé**, page 28.) En mode standard, ce serveur est toujours activé. Le serveur Modbus TCP fournit des données de diagnostic dans le registre local du module. Le client Modbus TCP peut accéder à cette base de données via l'adresse IP du module (ID unité 100).

NOTE: Pour plus de détails sur les informations de diagnostic pour Modbus TCP, consultez l'annexe Codes de diagnostic Modbus, page 294.

Vous pouvez également utiliser le service du module pour transférer un fichier de configuration Control Expert vers le contrôleur via X Bus. Dans ce cas, il n'est pas nécessaire de connecter une station d'ingénierie externe directement au contrôleur.

Echange de données

Echanges

Les échanges de données ont lieu dans l'un des deux modes suivants :

- **mode serveur** : Le module BMENOR2200H prend en charge toutes les requêtes Modbus TCP en provenance de l'automate ou du client Modbus externe.
- **mode client** : Ce type d'échange permet l'envoi de requêtes Modbus sur TCP à l'aide des fonctions suivantes :
 - READ_VAR
 - WRITE_VAR
 - DATA_EXCH

Pour plus d'informations sur la fonctionnalité d'échange de données ou sur la définition du module BMENOR2200H en tant que client Modbus hôte, voir *EcoStruxure™ Control Expert - Communication, Bibliothèque de blocs*.

NOTE: La taille de trame Ethernet maximale dépend du type de transaction.
La longueur maximale de trame est de 256 octets pour la messagerie.

Le module BMENOR2200H gère les connexions TCP suivantes via la messagerie du port 502 :

- Serveur Modbus : 32 connexions
- Client Modbus : 16 connexions

Port 502

TCP/IP réserve des ports serveur spécifiques pour certaines applications via l'IANA (Internet Assigned Numbers Authority - Autorité d'affectation de numéros sur Internet). Les requêtes Modbus sont envoyées au port 502 du logiciel enregistré.

Chemins de messagerie du port 502 :

- chemin du serveur :
 - La messagerie du port 502 peut traiter jusqu'à 8 requêtes entrantes en provenance du réseau. Les requêtes sont reçues lors de la scrutation précédente et envoyées au serveur Modbus dans la section IN.
 - La messagerie du port 502 peut traiter jusqu'à 8 réponses en provenance du serveur Modbus dans la section IN (y compris l'écriture des données dans le socket).
- chemin du client :
 - La messagerie du port 502 peut traiter jusqu'à 16 requêtes sortantes en provenance de l'application dans la section OUT (y compris écrire les données dans le socket).
 - La messagerie du port 502 peut traiter jusqu'à 16 réponses entrantes en provenance du réseau dans la section IN. Les réponses sont envoyées à l'application.

Utilisation des protocoles RTU

Introduction

Ce chapitre décrit les caractéristiques des protocoles RTU intégrés à utiliser dans les applications de télémétrie et les applications de commande de supervision et d'acquisition de données (SCADA).

Protocoles de communication

Fonctions et protocoles

Le module BMENOR2200H assure la prise en charge en rack des fonctions et protocoles suivants dans une architecture M580 :

Protocoles RTU	protocoles RTU intégrés pour communications série ou Ethernet
	IEC60870-5-101 (serveur ou client)
	IEC60870-5-104 (serveur ou client)
	DNP3 série (serveur ou client)
	DNP3 NET (serveur ou client)
	Modbus TCP (serveur ou client)
	NOTE: Le nombre de connexions de communication affecte les performances du module (accès aux pages Web, démarrage du module et échange de données via l'embase).
Principales fonctionnalités du protocole RTU	synchronisation de l'heure au moyen d'un service de protocole ou de SNTP
	synchronisation des données à la demande du système SCADA
	gestion des événements avec horodatage (séquence d'événements, SOE)
	file d'attente d'événements stockée en mémoire RAM (jusqu'à 150 000 événements)
	remplissage des données d'événements vers l'application SCADA via un service de protocole
	routage des événements
	rapport par échanges de données d'exception
	échanges de données de messagerie non sollicités
	authentification sécurisée DNP3 SAv2 et SAv5 avec clé prépartagée
Autres fonctionnalités intégrées	serveur web pour la configuration de la sécurité et le diagnostic à distance

Protocoles IEC60870-5-101/104

Introduction

IEC60870-5 est une norme internationale publiée au début des années 1990 par la Commission électrotechnique internationale (International Electrotechnical Commission - IEC). Cette norme fournit un profil de communication pour la téléconduite et la téléprotection, ainsi que les caractéristiques de télécommunication associées pour les systèmes de génération d'électricité. Elle est largement répandue aujourd'hui dans d'autres infrastructures, notamment dans le secteur de l'eau en Europe et en Asie.

Les protocoles IEC60870-5-101 et IEC60870-5-104 sont conçus pour les systèmes qui présentent des connexions directes permanentes entre la station de contrôle (client) et la ou les stations contrôlées (serveurs). Les normes IEC60870-5-101 et IEC60870-5-104 s'appliquent à diverses configurations de réseau telles que point à point, étoile et multipoint. La norme est adaptée à la surveillance des systèmes d'alimentation, aux communications de contrôle, à la téléprotection et aux télécommunications associées pour les systèmes d'alimentation électrique.

Caractéristiques des protocoles

Le protocole IEC 60870-5-101 s'appuie sur l'architecture EPA (Enhanced Performance Architecture). Ce protocole définit uniquement les couches liaison physique et application du modèle OSI. IEC 60870-5-101 est principalement utilisé sur des liaisons série avec des supports de transmission relativement lents. Cette norme considère des débits jusqu'à 9600 bits/s, même si des débits bien supérieurs (< 115200 bits/s) soient actuellement utilisés.

Le protocole IEC60870-5-104 est une extension du protocole IEC60870-5-101. Il présente des différences relatives aux réseaux ouverts dans les couches transport, réseau, liaison et physique.

IEC60870-5-104 permet la communication entre les stations de contrôle et les sous-stations dans un réseau TCP/IP standard. Le protocole TCP est utilisé pour la transmission de données orientées connexion. Il permet de se connecter à des LAN et des routeurs présentant des installations (frame relay, etc.) différentes peuvent être utilisés pour établir une connexion au WAN. La couche application du protocole IEC60870-5-104 est identique à celle du protocole IEC60870-5-101, sauf que certains types de données et services ne sont pas utilisés. Les couches liaison distinctes définies dans la norme facilitent le transfert de données sur les liaisons Ethernet et série.

NOTE: Lorsque les liaisons entre une station de contrôle centrale et plusieurs stations satellites utilisent la même voie physique, les liaisons ne fonctionnent correctement qu'en mode déséquilibré. Cela permet de limiter les cas où plusieurs stations satellites tentent de transmettre simultanément sur la voie.

Fonctionnalités du protocole prises en charge

Fonctionnalités IEC60870-5-101/104 prises en charge :

Fonctionnalité	IEC 60870-5-101	IEC60870-5-104	Description
mode de liaison	✓		équilibré : Il existe une connexion duplex intégral de un à un entre une voie et un serveur unique. déséquilibré : Il existe une connexion semi-duplex entre une voie et un ou plusieurs serveurs (par exemple, dans une configuration multipoint).
classification des données	✓		- Les données sont classées en différents objets d'information. Chaque objet reçoit une adresse spécifique. - Les données peuvent être classées dans les niveaux de priorité suivants et transférées à l'aide de mécanismes séparés : - haute priorité (classe 1) - faible priorité (classe 2)
groupe de données	✓	✓	Les données peuvent être classées en différents groupes (1 à 16) pour lancer des commandes d'interrogation de groupe spécifiques à partir du client et récupérer des données pour tous les groupes en émettant une interrogation générale.
mise à jour de données	✓	✓	Des méthodes de mise à jour cyclique et spontanée peuvent être utilisées.
interrogation générale	✓	✓	Une commande d'interrogation générale récupère un groupe spécifié de données statiques depuis un satellite distant. Elle est généralement envoyée après un redémarrage d'équipement ou une perte de communication, ou de façon périodique pour qu'aucune modification ne manque dans les rapports de données spontanés.
synchronisation horaire	✓	✓	Le service de synchronisation horaire permet d'instaurer la précision des horloges des divers équipements d'un réseau.
transmission d'événements (horodatés ou non)	✓	✓	Configurez le seuil de transmission en fonction d'un nombre d'événements ou d'un temps écoulé depuis la dernière transmission.
interrogation de compteur	✓	✓	Les commandes d'interrogation de compteur récupèrent les valeurs de compteur du RTU.
modes de transmission de commande (mode de sélection et d'exécution)	✓	✓	<i>sélectionner/exécuter</i> : Opérations d'écriture avec commande et réponse doubles.
			<i>exécuter</i> : Opérations d'écriture avec commande et réponse simples.

Types de données pris en charge par les protocoles

Le tableau suivant indique les types de données pris en charge par les protocoles IEC60870-5-101/104 :

- entrées/sorties TOR (simples ou doubles)
- valeurs mesurées (avec différents formats)
- totaux intégrés
- commandes
- position d'étape
- chaîne de bits

Caractéristiques des protocoles

Le tableau ci-après fournit la liste des caractéristiques des protocoles RTU pris en charge :

Protocole	Caractéristiques
Serveur IEC60870-5-104	liste de validation d'adresses IP clientes (jusqu'à 10 adresses IP)
	jusqu'à quatre connexions client simultanées avec port de service TCP configurable (la norme est 2404)
	Entrées et sorties maximales (au niveau module) : • <i>entrée</i> : 8 kb • <i>sortie</i> : 8 kb NOTE: Reportez-vous à la description de l'échange de données d'E/S avec le contrôleur.
	file d'attente accueillant jusqu'à 150 000 événements pour tous les types de données sur tous les serveurs (chaque serveur dispose d'un tampon d'événements dédié)
	horodatage d'événements configurable par type (Aucun, CP56)
	redondance de voie
Client IEC60870-5-104	• <i>entrée</i> : 8 kb • <i>sortie</i> : 8 kb
	jusqu'à 64 connexions serveur
	connexions partageant une configuration de voie commune
	connexion dédiée pour chaque configuration d'équipement
	paramètres dédiés de port et d'adresse IP de destination par connexion
Serveur IEC60870-5-101	• <i>entrée</i> : 8 kb • <i>sortie</i> : 8 kb
	file d'attente accueillant jusqu'à 150 000 événements pour tous les types de données sur tous les serveurs (chaque serveur dispose d'un tampon d'événements dédié)
	horodatage d'événements configurable par type (Aucun, CP24, CP56)
	Nombre maximum de connexions/sessions actives : 4 Nombre maximum d'équipements configurés par session : 5
Client IEC60870-5-101	• <i>entrée</i> : 8 kb • <i>sortie</i> : 8 kb
	Nombre maximum de connexions actives : • RS232 : 1 • RS485 : 32
	connexions partageant une configuration de voie commune
	connexion dédiée pour chaque configuration d'équipement

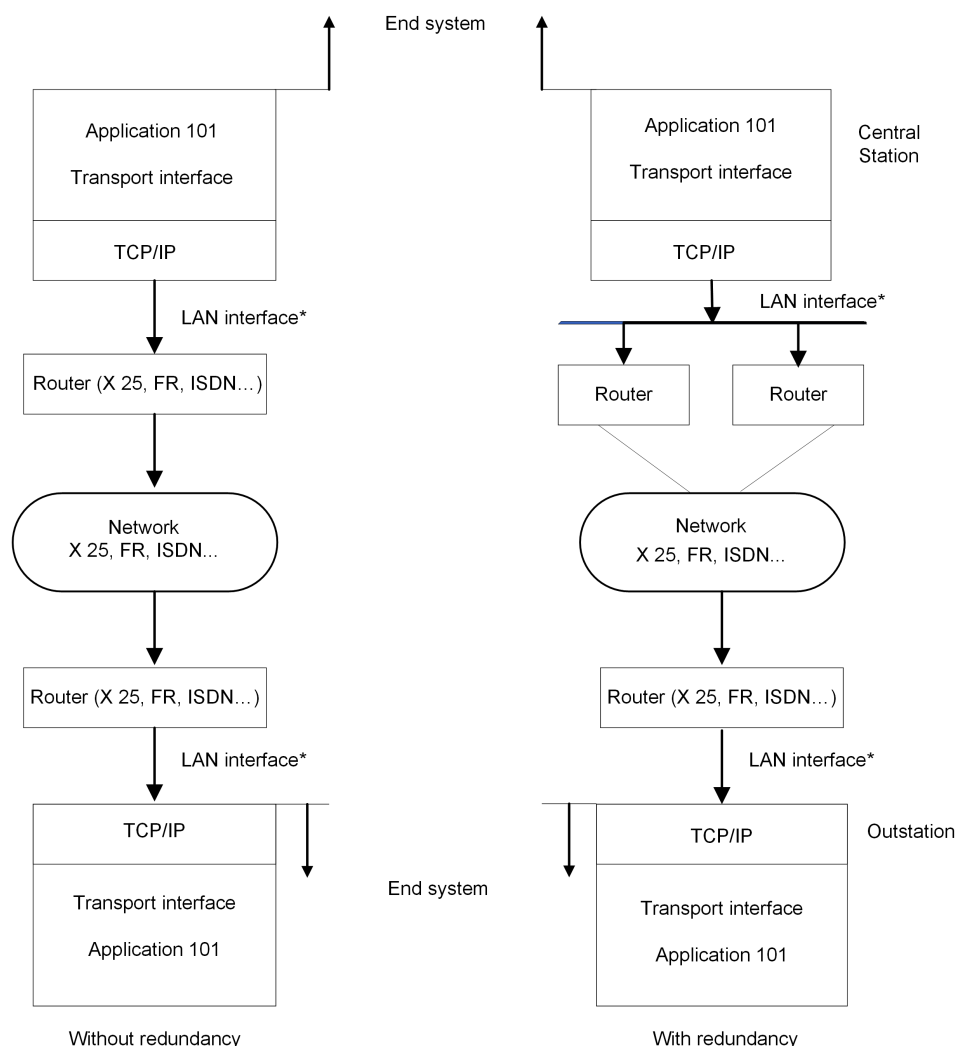
Redondance de voie

La redondance est parfois nécessaire pour augmenter la disponibilité du système de communication. Dans ces cas, vérifiez que vous établissez plusieurs connexions redondantes entre les deux stations. La communication redondante dans un système utilisant IEC60870-5-104 permet d'établir plusieurs connexions logiques entre deux stations. Une connexion logique est définie par une combinaison unique de deux adresses IP et deux numéros de port, typiquement la paire adresse IP/numéro de port de la station de contrôle et la paire adresse IP/numéro de port de la station contrôlée.

Ce tableau représente l'architecture logicielle de redondance au sein du module BMENOR2200H :

Couche application		
Groupe ou voie de redondance		
Voie 1	Voie 2	Voie 3

Ce logigramme présente l'architecture générale d'une configuration redondante dans la station centrale ainsi qu'un système non redondant :



* The LAN interface may be redundant.

Remarques :

- Chaque voie principale ou virtuelle peut être configurée sur *None*, ce qui indique l'indépendance de la voie. Cela signifie qu'elle n'appartient à aucun groupe de redondance.
- Chaque voie principale ou virtuelle peut être configurée en tant que groupe 1/2.
- Il n'y a qu'une seule voie *Active* dans un même groupe de redondance. Elle effectue toutes les communications de l'application utilisateur. Toutes les autres voies connectées sont inactives. (Les voies inactives sont surveillées pour vérifier qu'elles sont opérationnelles.)
- Si un contrôle de liaison active est configuré comme *External* et que la voie active arrête de communiquer, ses communications sont déplacées vers la voie opérationnelle suivante par un client distant via un message STARTDT.
- Si un contrôle de liaison active est configurée comme *Module* et que la voie active arrête de communiquer, le module déplace automatiquement ses communications vers la voie opérationnelle suivante.

NOTE: Pour le mode de restauration *Sauvegarde des événements*, vous pouvez sélectionner *Toutes les voies* dans *Mode de restauration* dans la configuration des voies.

Mode de lecture seule

Pour le protocole IEC 60870-5-104 serveur, les voies peuvent être configurées comme accessibles en lecture seule.

Cochez la case **Lecture seule** dans les paramètres de session serveur. Deux variables, "ReadOnly_Cmd" et "ReadOnly_Status", apparaîtront dans le DDT d'équipement.

Variable	Type	Bit	Description	Remarque
ReadOnly_Cmd	WORD	Bit 0/1/2/3 : 1	La première voie serveur IEC104 est définie en mode de lecture seule.	Les bits 0 à 3 sont des bits de contrôle pour toutes les voies IEC104 serveur (4 voies maximum).
		Bit 0/1/2/3 : 0	La première voie serveur IEC104 n'est pas définie en mode de lecture seule.	
		Bit 5/6/7...15	Réservés.	-
ReadOnly_Status	WORD	Bit 0/1/2/3 : 1	La voie est en mode de lecture seule.	Les bits 0 à 3 correspondent aux valeurs du mode Lecture seule des voies IEC104 serveur.
		Bit 0/1/2/3 : 0	La voie n'est pas en mode de lecture seule.	

NOTE:

- S'il existe un groupe de redondance et qu'une voie de ce groupe est configurée en mode de lecture seule, toutes les voies du groupe sont en mode de lecture seule. Elles seront en mode standard si toutes les voies du groupe sont réglées sur 0.
- Lorsqu'une voie est en mode de lecture seule, les types de commande C_DC/C_SC/C_RC/ C_BO/C_SE_A/C_SE_B/C_SE_C/C_CS/C_RP/P_ME_A/P_ME_B/P_ME_C/P_AC en provenance de SCADA sont rejetés et le module donne une réponse négative, mais d'autres requêtes sont autorisées.

Listes d'interopérabilité

La liste d'interopérabilité (définie par la norme) facilite l'interopérabilité entre les équipements issus de différents fabricants. Dans la liste, la plage de fonctions est décrite pour chaque équipement en marquant les fonctions applicables.

NOTE: L'annexe fournit la liste d'interopérabilité IEC60870-5-101/104 pour le module BMENOR2200H, page 232.

Types de données pris en charge par IEC60870-5-101/104

Informations de processus : Sens surveillé

Les serveurs IEC60870-5-101/104 prennent en charge les informations de processus suivantes dans le sens surveillé :

- M_SP : informations de signalisation simple
- M_DP : informations de signalisation double
- M_ME_A : valeur de mesure, valeur normalisée
- M_ME_B : valeur de mesure, valeur mise à l'échelle
- M_ME_C : valeur de mesure, valeur à virgule flottante courte
- M_IT : totaux intégrés
- M_ST : informations de position d'étape
- M_BO : chaînes de bits et d'octets

Informations de processus : Sens du contrôle

Les serveurs IEC60870-5-101/104 prennent en charge les informations de processus suivantes dans le sens du contrôle :

- C_SC : commande simple
- C_DC : commande double
- C_SE_A : commande de consigne, valeur normalisée
- C_SE_B : commande de consigne, valeur mise à l'échelle
- C_SE_C : commande de consigne, valeur à virgule flottante courte
- C_RC : commande d'étape de régulation
- C_BO : chaîne de 32 bits

Informations système : Sens surveillé

Les serveurs IEC60870-5-101/104 prennent en charge les informations système suivantes dans le sens surveillé :

- M_EI : fin de l'initialisation avec COT initialisé
- M_EI_NA : Après réception d'un message EOI M_EI_NA, vous pouvez configurer les éléments suivants :
 - informations d'interrogation générale
 - synchronisation d'horloge
 - interrogation de compteur

Informations système : Sens du contrôle

Les serveurs IEC60870-5-101/104 prennent en charge les informations système suivantes dans le sens du contrôle :

- C_IC : Ces points de commande d'interrogation prennent en charge les qualificatifs G/1~16 et les modes de fonctionnement **Désactivation/Activation**.
- C_CI : Ces commandes d'interrogation de compteur prennent en charge les qualificatifs G/1~4 et les modes de fonctionnement **Lecture/Gel/Gel avec réinitialisation/Réinitialisation**.
- C_CS : commandes de synchronisation d'horloge
- C_TS : commandes de test
- C_RP : ces points de commande de processus de réinitialisation prennent en charge les qualificatifs **Général/Événement**.
- C_RD : commandes de lecture

Informations sur les paramètres : Sens du contrôle

Les serveurs IEC60870-5-101/104 prennent en charge les paramètres suivants dans le sens du contrôle :

- P_ME_A : paramètre de mesure, valeur normalisée
- P_ME_B : paramètre de mesure, valeur mise à l'échelle
- P_ME_C : paramètre de mesure, nombre à virgule flottante court
- P_AC : prise en charge de l'activation des paramètres pour le mode de fonctionnement **Désactivation/Activation**

M_CUSTOM_IT_D

Les serveurs IEC60870-5-101/104 prennent en charge les points M_CUSTOM_IT_D 64 bits pour le support des fonctions de mappage sur les variables de DDT d'équipement du contrôleur.

Caractéristiques de IEC60870-5-101/104

Prise en charge des événements

Les serveurs IEC60870-5-101/104 prennent en charge les événements :

- La fonction événement peut être désactivée/activée par un ID de type de données.
- La fonction événement peut être désactivée/activée par un point de données.
- Le format d'heure des événements peut être configuré par un ID de type de données.
- Le format d'heure des événements peut être une option Aucun/CP24 (uniquement pour IEC 60870-5-101)/CP56.
- L'horodatage de l'événement est l'heure locale assortie de l'indicateur été/hiver.
- Vous pouvez configurer la taille du tampon d'événements via l'ID de type de données et la voie. La capacité du tampon est de 150 000 événements pour toutes les voies. Seuls les événements les plus récents sont enregistrés lorsque les événements du tampon consomment plus d'espace que la capacité configurée du tampon.
- Le tampon conserve les événements lorsqu'une voie est déconnectée. Les événements sont expulsés du tampon lorsqu'un système SCADA est connecté.
- Le tampon d'événements est effacé dans les situations suivantes :
 - Un point d'effacement d'événement est défini dans le contrôleur.
 - Une commande distante assortie d'un événement qualificatif est reçue.

Prise en charge de la sauvegarde des événements

Les serveurs IEC60870-5-101/104 prennent en charge la sauvegarde des événements :

- Les événements sont sauvegardés dans les situations suivantes :
 - Coupure d'alimentation
 - Remplacement à chaud du module
- Le module BMENOR2200H prend en charge la sauvegarde de 10 000 événements maximum en cas de coupure d'alimentation. Seuls les événements les plus récents sont enregistrés si le nombre d'événements dépasse 10 000.
- Le module BMENOR2200H prend en charge la sauvegarde d'au moins 5 000 événements lors de son remplacement à chaud. Seuls les événements les plus récents sont enregistrés dans le tampon d'événements.
- Les événements sauvegardés sont restaurés vers la pile de protocoles RTU après le rétablissement de l'alimentation, à condition que la configuration corresponde à la précédente. Sinon, les événements sauvegardés sont ignorés.
- Les événements sauvegardés sont effacés lorsque le module contrôleur redémarre à froid (par exemple, lorsqu'une nouvelle configuration est téléchargée). Dans ce cas, les communications sont réinitialisées.
- Vous pouvez activer ou désactiver la fonction de sauvegarde des événements.

Mode A la demande

Les serveurs IEC60870-5-101/104 prennent en charge le mode à la demande pour les commandes de consigne suivantes :

- C_SC
- C_DC
- C_RC
- C_SE_NA
- C_SE_NB
- C_SE_NC
- C_BO

NOTE:

- Ces points prennent en charge le réglage par variable de DDT d'équipement ou registre %MW du contrôleur.
- Ces points prennent en charge le réglage via une commande IEC60870-5-101/104.

Gel cyclique local (M_IT)

Les serveurs IEC60870-5-101/104 prennent en charge la fonction de gel cyclique pour les points M_IT :

- Vous pouvez désactiver cette fonction.
- Cette fonction peut démarrer automatiquement après le démarrage des modules, ou elle peut être contrôlée par une variable de DDT d'équipement du contrôleur en cours d'exécution.
- Cette fonction prend en charge la définition d'une période de gel pour chaque groupe.
- Cette fonction prend en charge le mode de fonctionnement Gel uniquement/ Gel avec réinitialisation.

Déclenchement de gel local (M_IT)

Les serveurs IEC60870-5-101/104 prennent en charge la fonction déclenchement de gel pour les points M_IT :

- Cette fonction est contrôlée par une variable de DDT d'équipement du contrôleur. Une modification de la valeur de la variable déclenche l'opération.
- Cette fonction prend en charge le mode de fonctionnement Gel uniquement/ Gel avec réinitialisation.
- Cette fonction prend en charge le gel d'un groupe spécifié.

Protocole DNP3

Introduction

Le protocole de réseau distribué (Distributed Network Protocol) DNP3 a été développé en vue d'assurer une interopérabilité ouverte et normalisée pour les communications entre les stations clientes, les équipements de sous-station, les RTU et les équipements électroniques intelligents (IED). Le protocole DNP3 a été principalement utilisé par des services publics tels que l'énergie électrique en Amérique du Nord et il s'est étendu largement à d'autres infrastructures distribuées telles que l'eau, les eaux usées, les transports, le pétrole et le gaz.

DNP3 s'appuie sur les travaux du Groupe 03 du Comité technique 57 de la Commission électrotechnique internationale (CEI en français, IEC en anglais). Ce groupe s'est penché sur le protocole EPA (Enhanced Performance Architecture), une norme destinée aux applications de téléconduite. Chacune des trois couches du protocole EPA correspond à une couche du modèle de référence OSI.

Le protocole DNP3 est développé spécialement pour les communications interéquipements qui utilisent des unités RTU SCADA. Il facilite les opérations des RTU vers les dispositifs électroniques intelligents (IED) et des clients vers les RTU/IED.

Le protocole était conçu à l'origine pour des communications série lentes, mais la version DNP3 IP actuelle prend également en charge les réseaux TCP/IP.

Caractéristiques des protocoles

Le tableau suivant répertorie les caractéristiques des protocoles RTU pris en charge :

Protocole	Caractéristiques
Client NET DNP3	jusqu'à 64 serveurs (une session par serveur)
	<i>entrée</i> : 8 Ko <i>sortie</i> : 8 Ko NOTE: Pour plus d'informations sur les protocoles RTU pris en charge (notamment les tailles d'entrée et de sortie), consultez la section <i>Echange de données d'E/S avec le contrôleur</i> .
Serveur NET DNP3	<i>entrée</i> : 8 Ko <i>sortie</i> : 8 Ko NOTE: Pour plus d'informations sur les protocoles RTU pris en charge (notamment les tailles d'entrée et de sortie), consultez la section <i>Echange de données d'E/S avec le contrôleur</i> .
	file d'attente pouvant contenir jusqu'à 150 000 événements pour tous les types de données
	synchronisation d'horloge à partir d'un client
	versions d'authentification sécurisée (SA) DNP3 SAV2 et SAV5
	4 connexions client simultanées
Client série DNP3	jusqu'à 32 serveurs (1 équipement/session par serveur)
	<i>entrée</i> : 8 Ko
	<i>sortie</i> : 8 Ko
Serveur série DNP3	<i>entrée</i> : 8 Ko <i>sortie</i> : 8 Ko
	file d'attente comportant jusqu'à 150 000 événements pour tous les types de données
	synchronisation d'horloge à partir d'un client
	versions d'authentification sécurisée (SA) DNP3 SAV2 et SAV5
	1 connexion client à la fois

Listes d'interopérabilité

Cette mise en œuvre de DNP3 est entièrement conforme au niveau 3 de définition des sous-ensembles DNP3, qui convient aux applications RTU plus vastes et offre la quasi totalité des fonctionnalités DNP3.

Ce standard définit l'interopérabilité, page 233 entre les équipements de fournisseurs différents. Il comprend un profil d'équipement qui décrit les fonctionnalités de base du protocole prises en charge par l'équipement, ainsi qu'un tableau d'implémentation qui définit les objets d'informations et leur représentation par l'équipement.

Types de données pris en charge par DNP3

- Groupes d'objets de type point d'entrée binaire simple bit :

Numéro de groupe	Utilisation pour
1	Signalement de la valeur actuelle d'une entrée binaire à un bit
2	Signalement des événements ou des modifications de bit indicateur de l'entrée binaire simple bit

- Groupes d'objets de type point d'entrée binaire double bit :

Numéro de groupe	Utilisation pour
3	Signalement de la valeur d'état actuelle
4	Signalement des événements ou des modifications de bit indicateur de l'entrée binaire double bit

- Groupes d'objets de type point de sortie binaire :

Numéro de groupe	Utilisation pour
10	Signalement de l'état actuel de la sortie
11	Signalement des modifications apportées aux bits d'état ou d'indicateur de la sortie
12	Emission de commandes de contrôle

- Groupes d'objets de type point de comptage :

Numéro de groupe	Utilisation pour
20	Signalement de la valeur de comptage
21	Signalement de la valeur de comptage gelée ou des bits d'indicateur modifiés
22	Signalement des événements de compteur
23	Signalement des événements de compteur gelé

- Groupes d'objets de type point d'entrée analogique :

Numéro de groupe	Utilisation pour
30	Signalement de la valeur actuelle
32	Signalement des événements d'entrée analogique ou des modifications apportées aux bits d'indicateur
34	Lecture et écriture des valeurs analogiques de bande morte

- Groupes d'objets de type point de sortie analogique :

Numéro de groupe	Utilisation pour
40	Signalement de la valeur actuelle des sorties analogiques
41	Contrôle des valeurs des sorties analogiques
42	Signalement des modifications apportées aux bits d'état ou d'indicateur de la sortie analogique

- Groupes d'objets de type données et heure :

Numéro de groupe	Utilisation pour
50	Définir ou obtenir l'heure actuelle

- Groupes d'objets de classe :

Numéro de groupe	Utilisation pour
60	Requête de lecture pour spécifier que la station satellique renvoie certains ou tous les objets ayant un attribut d'événement de classe défini.

- Groupes d'objets de type point de chaîne d'octet :

Numéro de groupe	Utilisation pour
110	Transmettre la valeur actuelle

- Groupes d'objets de type point de statistique de sécurité :

Numéro de groupe	Utilisation pour
121	Signalement de la valeur actuelle des statistiques
122	Signalement des modifications apportées aux statistiques

Fonctionnalités DNP3

Fonctionnalités du protocole prises en charge

Voici les principales fonctionnalités prises en charge par DNP3 :

- synchronisation d'horloge
- interrogations sélectives
- rapport par exception interrogé
- rapport par exception non sollicité
- authentification de sécurité DNP3
- transmission d'événements (horodatés ou non)
- traitement spécifique à un compteur
- commandes client
- Configuration multisession pour le serveur DNP3

Prise en charge des événements

Le serveur DNP3 prend en charge les événements :

- La fonction événement peut être désactivée/activée par un ID de type de données.
- La fonction événement peut être désactivée/activée par un point de données.
- L'événement peut être configuré avec ou sans horodatage par un point de données.
- L'horodatage de l'événement est l'heure absolue à laquelle l'événement s'est produit.
- Vous pouvez configurer la taille du tampon d'événements via l'ID de type de données et la voie. La capacité du tampon est de 150 000 événements pour toutes les voies. Seuls les événements les plus récents sont enregistrés lorsque les événements du tampon consomment plus d'espace que la capacité configurée du tampon.
- Le tampon conserve les événements lorsqu'une voie est déconnectée. Les événements sont expulsés du tampon lorsqu'un système SCADA est connecté.
- Le tampon d'événements est effacé dans les situations suivantes :
 - Un point d'effacement d'événement est défini dans le contrôleur.

Prise en charge de la sauvegarde des événements

Le serveur DNP3 prend en charge la sauvegarde des événements :

- Les événements sont sauvegardés dans les situations suivantes :
 - Coupure d'alimentation
 - Remplacement à chaud du module
- Le module BMENOR2200H permet de sauvegarder jusqu'à 10 000 événements en cas de coupure d'alimentation. Seuls les événements les plus récents sont enregistrés si le nombre d'événements dépasse 10 000.
- Le module BMENOR2200H prend en charge la sauvegarde d'au moins 5 000 événements lors de son remplacement à chaud. Seuls les événements les plus récents sont enregistrés dans le tampon d'événements.
- Les événements sauvegardés sont restaurés vers la pile de protocoles RTU après le rétablissement de l'alimentation, à condition que la configuration corresponde à la précédente. Sinon, les événements sauvegardés sont ignorés.

- Les événements sauvegardés sont effacés lorsque le module contrôleur redémarre à froid (par exemple, lorsqu'une nouvelle configuration est téléchargée). Dans ce cas, les communications sont réinitialisées.
- Vous pouvez activer ou désactiver la fonction de sauvegarde des événements.

Mode à la demande

Le serveur DNP3 prend en charge le mode à la demande pour les commandes de consigne suivantes :

- Type de point de sortie binaire
- Type de point de sortie analogique

NOTE:

- Ces points prennent en charge le réglage par variable DDT d'équipement ou registre %MW du contrôleur.
- Ces points prennent en charge le réglage via une commande DNP3.

Mode de déclenchement-fermeture

Le serveur DNP3 prend en charge la spécification d'un ou de deux points de sortie binaires pour implémenter la fonction déclenchement-fermeture. (Pour plus d'informations, consultez *Comportement d'une sortie binaire*)

- Mode pair : les deux points de sortie binaires contigus sont regroupés pour implémenter la fonction de déclenchement et fermeture ; le premier est utilisé comme point de fonction de fermeture et le second comme point de fonction de déclenchement.
- Mode consécutif : un même point de sortie binaire contient les variables déclenchement et fermeture permettant d'implémenter la fonction.

Configuration multisession pour le serveur DNP3

Le serveur DNP3 prend en charge la configuration de paramètres de session pour 4 voies, respectivement et indépendamment.

- Si la fonction *Multisession* n'est pas activée, seule la session 1 peut être configurée.
- Lorsque la fonction *Multisession* est activée, chaque paramètre de session peut être configuré.

Concepts de l'authentification sécurisée DNP3

Introduction

Dans certains cas, un attaquant peut apprendre le protocole utilisé par une unité RTU pour bénéficier de l'accès à numérotation automatique. Si l'unité RTU n'utilise pas d'authentification forte ou d'autres mécanismes de sécurité, elle accepte et répond à tout appelant.

Pour remédier à ces problèmes, le module BMENOR2200H utilise les services d'autorisation de sécurité de DNP3 pour faciliter les communications entre les unités RTU distantes.

La mise en œuvre de l'authentification sécurisée (SA) DNP3 simplifie l'authentification mutuelle pour les communications entre un client DNP3 et un serveur DNP3 :

- Un serveur DNP3 utilise l'authentification sécurisée DNP3 pour déterminer sans ambiguïté qu'il communique avec un utilisateur autorisé à accéder à ses services.

NOTE: L'option d'authentification sécurisée est activée par défaut. Le serveur ne fonctionne correctement que si une voie serveur est configurée dans les paramètres de cybersécurité. Désactivez cette fonction lorsque votre application ne requiert pas d'authentification sécurisée. Ce paramètre global s'applique à toutes les voies serveur. Vous ne pouvez pas l'activer ou le désactiver pour une voie spécifique indépendamment des autres. Si le service DNP3 est désactivé, aucune voie ne fonctionne, quel que soit le niveau de sécurité configuré.

- Un client DNP3 utilise l'authentification sécurisée DNP3 pour déterminer sans ambiguïté qu'il communique avec le serveur approprié.

NOTE: Côté client, vous pouvez configurer des voies client individuelles pour l'authentification sécurisée. Dans ce cas, assurez-vous que ces voies figurent dans le tableau avec un niveau de sécurité affecté (Aucun, SAV2, SAV5).

Versions

Le RTU prend en charge les versions suivantes de l'authentification sécurisée (SA) DNP3 :

- **SAv2:** *Authentification sécurisée version 2* est une famille de protocoles au sein de DNP3 qui facilite l'authentification des commandes et contrôles critiques et qui contribue à augmenter la confidentialité des messages lorsque le module BMENOR2200H est utilisé conjointement avec un hôte SCADA approprié ou d'autres équipements prenant en charge SAV2.

SAv2 requiert l'installation préalable de clés pré-partagées sur tous les équipements.

SAv2 est défini par la norme IEEE 1815-2010 DNP3.

- **SAv5:** *Authentification sécurisée version 5* est une famille de protocoles plus récente au sein de DNP3 qui traite les menaces en évolution.

SAv5 est défini par la norme IEEE 1815-2012 DNP3.

NOTE:

- Schneider Electric recommande d'utiliser la même version d'authentification sécurisée (SAv2 ou SAV5) côté client et côté serveur.
- Les fabricants conçoivent chaque équipement pour qu'il soit compatible avec une seule version de ce service.
- La mise en œuvre de l'authentification SAV2 ou SAV5 nécessite l'utilisation d'une application administrateur de la sécurité.
- BMENOR2200H fournit le réglage de sécurité DNP3 sur la page Web intégrée.

Clés prépartagées

Le module BMENOR2200H met en œuvre des communications DNP3 sécurisées via des clés pré-partagées.

De nombreuses installations qui ne choisissent pas de moyen plus sophistiqué de gérer les informations d'identification de sécurité peuvent néanmoins nécessiter le niveau de protection fourni par les clés prépartagées.

Par définition, les utilisateurs côté SCADA et côté module emploient la même clé pré-partagée pour leur authentification mutuelle. Les communications sont facilitées par une clé de session dérivée de la clé prépartagée.

NOTE:

- Reportez-vous aux instructions relatives à la gestion des clés prépartagées.
- Pour plus d'informations sur les clés prépartagées, consultez le document *Plates-formes automate Modicon - Cybersécurité, Manuel de référence*.

Synchronisation d'horloge

Présentation

Le service de synchronisation d'horloge permet d'établir l'exactitude de l'heure entre les horloges d'équipements en réseau. Le module BMENOR2200H offre deux méthodes de synchronisation d'horloge avec le système SCADA (client) et les équipements connectés :

- par l'intermédiaire du protocole RTU
- par l'intermédiaire du protocole NTP

NOTE:

- ces méthodes de synchronisation d'horloge sont indépendantes l'une de l'autre. Configurez votre application pour éviter les conflits de synchronisation d'horloge.
- Si le protocole NTP n'est pas configuré, le module obtient son horodatage du contrôleur lorsqu'il redémarre ou lors d'une réinitialisation pour le protocole RTU par DDT d'équipement.

Synchronisation d'horloge avec le protocole RTU

Présentation

L'une des principales fonctionnalités de RTU est de gérer les événements avec horodatage. L'horodatage nécessite une synchronisation horaire efficace.

Comportement

Le comportement de la commande de synchronisation d'horloge est déterminé par le rôle du module BMENOR2200H :

Rôle(s)	Description
serveur	Lorsqu'il joue le rôle de serveur, le module BMENOR2200H peut synchroniser son horloge avec une station client (SCADA). Lorsque vous alignez l'horloge sur le contrôleur, le module reçoit la commande de synchronisation d'horloge, met à jour son horloge interne et communique la nouvelle valeur au contrôleur. Cela permet de maintenir une heure cohérente sur le rack local.
client	Lorsqu'il fonctionne en tant que client, le module BMENOR2200H envoie des commandes de synchronisation d'horloge aux serveurs connectés. Comme dans le cas ci-dessus, l'horloge est initialisée à partir du contrôleur à son démarrage.

Configuration

Le client SNTP s'exécute uniquement lorsque vous configurez le service dans le DTM. Pour configurer le service SNTP, reportez-vous aux [instructions de synchronisation d'horloge](#).

Synchronisation d'horloge avec SNTP

Introduction

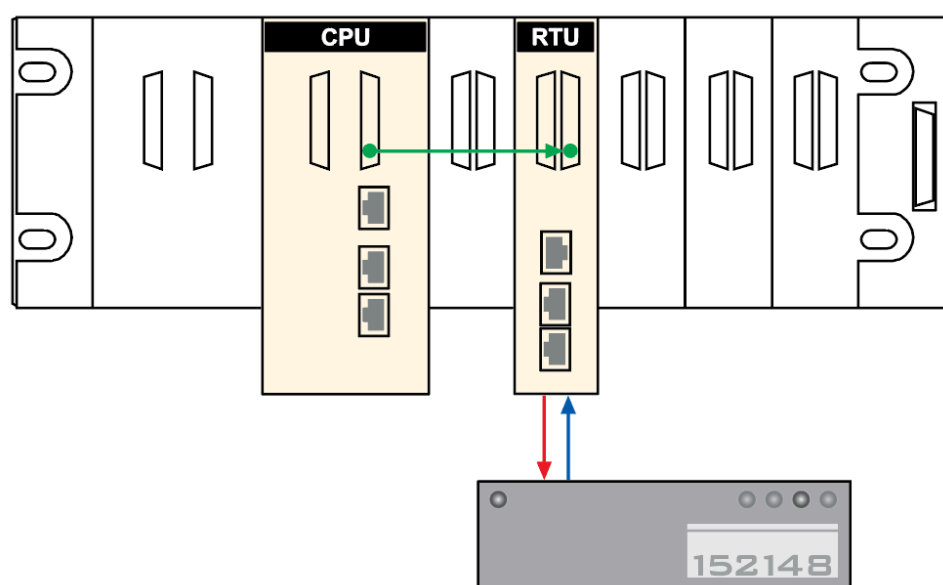
Le module BMENOR2200H prend en charge la synchronisation d'horloge en tant que client SNTP.

Lorsque le client SNTP est activé, le module synchronise l'horloge interne à partir du serveur de temps. Cette heure est la base de l'horodatage des événements RTU.

NOTE: Consultez les instructions de configuration du service de temps réseau dans le DTM.

Synchronisation d'horloge et horodatage

Cet exemple de réseau montre le flux du signal de synchronisation du point de vue du client SNTP dans un module BMENOR2200H :



ligne rouge : Le module BMENOR2200H envoie une requête SNTP sur le port Ethernet à destination du serveur SNTP.

ligne bleue : Le serveur SNTP envoie une réponse au module BMENOR2200H via le port Ethernet.

ligne verte : Le module BMENOR2200H envoie le signal de synchronisation d'horloge source au contrôleur via X Bus.

NOTE:

- Le module BMENOR2200H envoie le signal de mise à jour d'horloge interne du contrôleur uniquement lorsque vous sélectionnez **Alignement de l'horloge sur le contrôleur** dans les paramètres de synchronisation horaire. La mise à jour du signal horaire sur le contrôleur s'arrête automatiquement lorsque le module détecte que sa qualité horaire n'est pas valide.
- La précision de l'horloge du module BMENOR2200H est généralement autour de 5 ms par rapport à l'heure du serveur SNTP, 10 ms au pire, avec une dérive d'exécution libre de +/- 2,6 secondes par jour.
- Entre les signaux de synchronisation d'horloge, le module BMENOR2200H met à jour sa propre horloge toutes les millisecondes avec son minuteur interne.

Synchronisation d'horloge avec le contrôleur

Introduction

Vous pouvez configurer le contrôleur en tant que serveur NTP. Dans ce cas, le contrôleur utilise son horloge interne et joue le rôle de serveur Ethernet pour les équipements qui sont connectés au même réseau Ethernet.

Configurer le contrôleur en tant que serveur NTP

Accédez aux paramètres NTP et définissez-les dans Control Expert :

Etape	Action
1	Ouvrez un projet Control Expert.
2	Développez ces éléments dans le Navigateur du projet : Projet > Configuration
3	Double-cliquez sur Bus automate pour afficher les modules et les racks de votre projet.
5	Sélectionnez l'onglet NTP .
6	Dans le menu déroulant NTP , sélectionnez Serveur NTP .
7	Configurez les paramètres de la section Configuration du serveur NTP .

Lorsque le contrôleur est configuré en tant que serveur NTP, la période d'interrogation est un paramètre utilisé par les modules distants dans le PAC. Il représente le temps écoulé avant que les modules distants resynchronisent leurs horloges internes avec l'heure du serveur NTP du contrôleur.

Gestion des événements

Introduction à la gestion des événements

Présentation

Le module BMENOR2200H génère des événements en cas de changement d'état, gère des listes d'événements et fournit les services suivants :

- La gestion d'un tampon d'événements (horodatés ou non), la taille totale du tampon (file d'attente) peut atteindre 150 000 événements.

NOTE: Un tampon d'événements dédié est géré par application serveur (quatre applications serveur au maximum sont prises en charge).

- Remplissage automatique des événements vers le SCADA ou la station cliente via le protocole RTU (sur DNP3, IEC60870-5-101, ou IEC60870-5-104).

Pour la configuration du serveur RTU (DNP3, IEC60870-5-101, IEC60870-5-104), chaque type d'objet est associé à un réglage de file d'attente d'événements indépendant. Pour permettre la génération d'événements, définissez une file d'attente d'événements pour le type d'objet correspondant.

Horodatage des événements

Le module BMENOR2200H offre deux méthodes d'horodatage des événements :

- Horodatage effectué à la source dans le contrôleur (nécessite une programmation de l'automate).
- Horodatage effectué dans le module BMENOR2200H (ne nécessite *pas* de programmation de l'automate).

NOTE: Une résolution d'horodatage améliorée peut être obtenue lors de l'exécution dans le contrôleur. La résolution de l'horodatage dépend du temps de scrutation du contrôleur et du type de module d'E/S.

Capacité du tampon d'événements en mémoire RAM

Le nombre d'événements dans le tampon est soumis aux limitations suivantes :

- Le module enregistre jusqu'à 150 000 événements dans le tampon d'événements.
- Le tampon d'événements est synchronisé (si la *synchronisation des événements* est activée) entre les modules primaire et redondant dans un système redondant.
- Le module enregistre jusqu'à 10 000 événements de sécurité par voie serveur dans le tampon d'événements.

Conserver ou effacer la RAM

Le tampon d'événements en mémoire RAM est conservé dans les situations suivantes :

- Le contrôleur subit un démarrage à chaud.
- Une permutation de réseau se produit dans une application à double réseau.

Le tampon d'événements en mémoire RAM est effacé dans les situations suivantes :

- Utilisation d'une commande **Effacer des événements** pour vider le tampon en mémoire RAM.
- Le contrôleur subit un redémarrage à froid (lors du téléchargement d'une nouvelle configuration, par exemple) ou vous appuyez sur le bouton de réinitialisation de l'alimentation. Toutes les communications sont réinitialisées.
- La configuration de la cybersécurité DNP3 est modifiée sur la page Web pour effacer le tampon.
- Une commande SCADA efface explicitement la mémoire tampon.
- Réinitialisez le protocole RTU par le DDT d'équipement.

Performances des événements en mode Hot Standby

Lorsqu'un module BMENOR2200H génère jusqu'à 4 000 événements par seconde, il prend encore en charge un basculement Hot Standby sans perte d'événement (en fonction de la configuration).

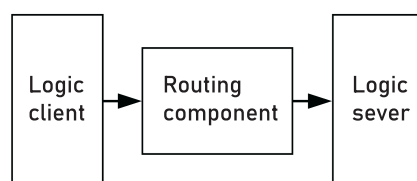
Routage d'événements

Introduction

Le composant de routage d'événements permet d'acheminer les événements des sous-stations vers SCADA au sein d'un seul module BMENOR2200H.

Pour router des événements, le système doit comprendre une ou plusieurs voies client RTU et au moins une voie serveur RTU. La solution consiste à créer un client et un serveur RTU logiques dans un seul module BMENOR2200H. Dans le client logique, des points sont créés pour représenter les points des sous-stations ; dans le serveur logique, des points sont créés pour simuler le comportement des points dans les sous-stations. Le composant de routage d'événements est chargé de collecter les événements dans le client logique. Ces événements sont envoyés depuis les sous-stations et déclenchent les mêmes événements dans le serveur logique.

Composants du module BMENOR2200H :



NOTE: Les fonctionnalités de routage d'événements ne sont possibles qu'au sein d'un même module.

Il n'existe aucune fonctionnalité de routage automatique des événements entre deux modules BMENOR2200H (un serveur et un client) configurés dans la même station.

Dans une architecture hiérarchique, les événements horodatés sont automatiquement transférés des sous-stations serveur de niveau inférieur vers le système SCADA (ou client) via la station. Le transfert automatique utilise la fonctionnalité d'événements traversants avec un seul module BMENOR2200H configuré dans le client et le serveur.

Configuration

Configurez le module BMENOR2200H pour le routage d'événements sur la page de configuration du mappage des données.

Observations :

- Le module BMENOR2200H ne détecte pas les événements relatifs aux points de routage d'événements dans un serveur.
- Dans une configuration valide pour les points de routage d'événements, un seul point est occupé dans la base de données pour réduire la taille des données stockées en mémoire. Utilisez le DDT d'équipement pour afficher le point et sa structure dans la liste **Variables**.

Considérations relatives à la configuration des points :

Configuration	Description
Voie (Voir remarque ci-après.)	Pour le routage d'événements, configurez une voie client et au moins une voie serveur. Une seule voie client est nécessaire pour que le système puisse se connecter à davantage de sous-serveurs, et un nombre plus important de voies serveur permet d'avoir plus de SCADA dans le système. NOTE: Reportez-vous aux instructions de configuration des voies.
Mappage de données client (Voir remarque ci-après.)	Ajoutez des points de données dans la voie client. Ces points montrent le mappage des points client dans le sous-serveur, lesquels communiquent avec la voie client. NOTE: Reportez-vous aux instructions de mappage d'objets de données DNP3.
Point serveur	Après la configuration des points dans la voie client, le point correspondant apparaît dans la voie serveur. Les points utilisés pour le routage sont différents des points normaux du serveur. Les paramètres (type de CPU, adresse de la CPU, nom de variable et horodatage) du mappage du contrôleur ne sont plus disponibles, et les paramètres disponibles sont accessibles en lecture seule. <i>Leur durée de vie est cohérente avec la configuration des points homologues dans le client.</i>
NOTE: Lorsque vous configurez ces points de routage dans la voie client, le module sélectionne les événements des points à router et il achemine les événements vers la voie serveur correspondante. Par exemple, si la voie client reçoit des événements Binary Input point du sous-serveur et les achemine vers la voie du serveur logique, ils deviennent les événements de Binary Input point de la voie du serveur logique. Remarques : - Lorsque vous spécifiez un seul point dans le client pour le routage d'événements, par exemple le point d'entrée binaire, une configuration de point correspondante est automatiquement générée dans la voie du serveur logique. La configuration de point pour la voie du serveur logique est en lecture seule ; elle ne peut pas être modifiée ni supprimée dans son panneau de mappage de base de données. Ces points côté serveur ne consommeront pas de mémoire (8kentrée/8ksortie). - Si le numéro de voie, le numéro de session ou le numéro de point ne correspondent pas dans la voie serveur, une page d'erreur s'affiche. - Si vous choisissez l'option Disable pour l'itinéraire vers cette voie, le point n'a pas besoin d'être routé vers un serveur.	

Combinaison de voies pour le routage d'événements

Pour router des événements à l'intérieur du module BMENOR2200H, utilisez les instructions de configuration concernant la combinaison de voies client et serveur.

Les combinaisons autorisées sont les suivantes :

Voie client	Voie serveur
Client NET DNP3	Serveur NET DNP3
Client série DNP3	Serveur NET DNP3
Client IEC60870-5-101	Serveur IEC60870-5-104
Client IEC60870-5-104	Serveur IEC60870-5-104

Limites

- Les événements sont routés à l'intérieur du module. Cela signifie qu'il n'est pas possible de router des événements entre deux modules ou plus et que l'application d'automate dans le contrôleur ne peut pas obtenir et traiter les événements. (Le contrôleur peut toujours obtenir la valeur du point dans les événements tout comme la voie client autonome.)
- Seuls les événements sont routés. Les requêtes (commandes) du SCADA ne sont pas routées vers le sous-serveur. Cela signifie qu'à l'intérieur du module BMENOR2200H, il n'y a pas d'échange ou de communication autre que des événements entre la voie client et la voie serveur. La fonction de routage d'événements ne prend pas en charge toutes les combinaisons de voies client et serveur.
- Dans le système, SCADA ne peut pas communiquer avec les sous-serveurs. La solution utilise le serveur logique du module BMENOR2200H pour simuler des sous-serveurs, de sorte que SCADA ne peut communiquer qu'avec le serveur logique du module BMENOR2200H et le sous-serveur ne peut communiquer qu'avec le client logique du module BMENOR2200H.
- Certaines informations concernant les événements sont modifiables. Les informations clés relatives aux événements, telles que la valeur du point et l'horodatage, sont conservées pendant le routage des événements. La qualité des événements routés dépend de la configuration. Par exemple, si un changement de qualité est sélectionné lorsque l'équipement routé est hors ligne, le bit de qualité devient non valide lorsque l'équipement de terrain est hors ligne. D'autres informations relatives aux événements sont modifiées en fonction de la configuration de la voie client, notamment le numéro de point, la classe d'événements et la variation.

Taille du tampon d'événements

Assurez-vous que la taille du tampon d'événements du serveur est supérieure à celle du tampon d'événements du sous-serveur.

Sauvegarde des événements

Introduction

Le tampon de sauvegarde d'événements du module BMENOR2200H peut stocker les événements en cas de coupure d'alimentation du module.

Caractéristiques de la sauvegarde des événements

Vous pouvez configurer le module pour enregistrer les événements via des types de données en cas de coupure d'alimentation ou de remplacement à chaud d'un module.

Les capacités de stockage d'événements en mémoire flash sont les suivantes pour le module BMENOR2200H et le protocole RTU :

- Le module enregistre jusqu'à 10 000 événements en mémoire flash en cas de coupure d'alimentation.
- Le module enregistre uniquement les événements les plus récents lorsque le nombre d'événements enregistrés dépasse 10 000.
- Le module lit les événements dans la mémoire flash lors du rétablissement de l'alimentation.

Comportement de la sauvegarde des événements

Le module BMENOR2200H adopte différents comportements de sauvegarde dans différents cas. Le type de cas est présenté du point de vue de l'utilisateur :

	Cas	Description	Événement
1	Coupure de courant	perte d'alimentation	Enregistre les événements dans la mémoire non volatile en cas de coupure de courant.
2	Démarrage	Mise sous tension/rétablissement de l'alimentation	Restaure les événements au démarrage du protocole RTU.
3	Redémarrage du protocole	Ces actions effacent le tampon d'événements du module : • La configuration du protocole RTU change. • Le RTU reçoit une commande de démarrage à chaud ou à froid de la part d'un client RTU. • Le BMENOR2200H reçoit une commande de réinitialisation RTU en provenance du DDT d'équipement.	N'enregistre pas les événements en cas de fermeture du protocole.

Limites

- Le module BMENOR2200H scrute et stocke les événements dans chaque voie tour à tour. Lorsque le nombre d'événements dépasse la capacité de la mémoire Flash, le module n'enregistre que les événements les plus récents.
- Les systèmes à redondance d'UC (Hot Standby) ne prennent pas en charge la fonction de sauvegarde des événements.

Flux de données du protocole RTU

Communications RTU

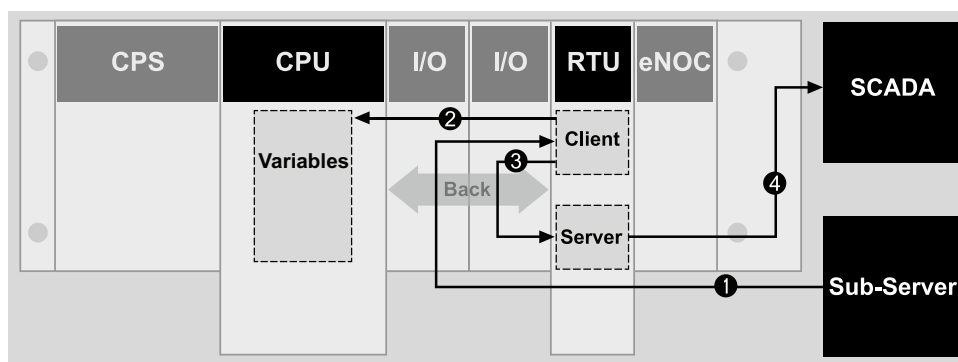
Comportement de communication

Le module BMENOR2200H est équipé d'un connecteur double bus qui prend en charge les communications Ethernet et X Bus.

Ce port d'embase Ethernet est principalement utilisé pour communiquer avec le client ou le serveur distant en utilisant les protocoles RTU. L'interface d'embase permet de communiquer avec d'autres modules de communication en rack et RIO. L'activité principale de l'interface d'embase consiste à synchroniser les données entre les registres de la CPU et la base de données des points RTU dans le module. Le cycle de synchronisation peut comprendre un ou plusieurs cycles de scrutation de l'application automate, en fonction de la quantité de données et de la charge de l'embase.

Lorsque la voie client reçoit des événements provenant du sous-serveur

Lorsqu'un changement significatif survient dans le sous-serveur (changement de valeur d'un point, par exemple), le sous-serveur envoie un événement. Le système reçoit cet événement, qui est ensuite acheminé vers un système SCADA, comme illustré dans cet exemple :



1 Le sous-serveur envoie des événements à la voie client du module BMENOR2200H.

2 La voie client met à jour les valeurs de point dans le module et la base de données de la voie du serveur logique et synchronise la valeur sur les variables de la CPU.

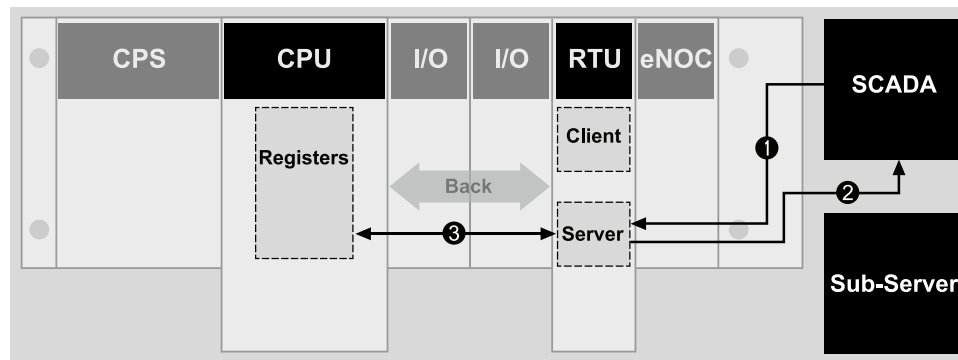
3 Les événements sont routés vers les voies serveur conformément à la configuration des points.

4 La voie serveur met ces événements en mémoire tampon et les envoie au SCADA lorsque la liaison de communication est établie.

Lorsque la voie serveur reçoit une demande du système SCADA

Dans le système RTU, un système SCADA envoie des requêtes (commandes) telles que Integrity Poll au serveur qui lui est connecté. La voie serveur reçoit cette requête et envoie une réponse au système SCADA. Avec le routage d'événements, le comportement de la voie serveur est exactement le même que celui d'une voie serveur autonome (pas de routage d'événements). La voie client et les sous-serveurs ne sont pas impliqués dans ce cas.

L'exemple suivant illustre une requête provenant d'un système SCADA :

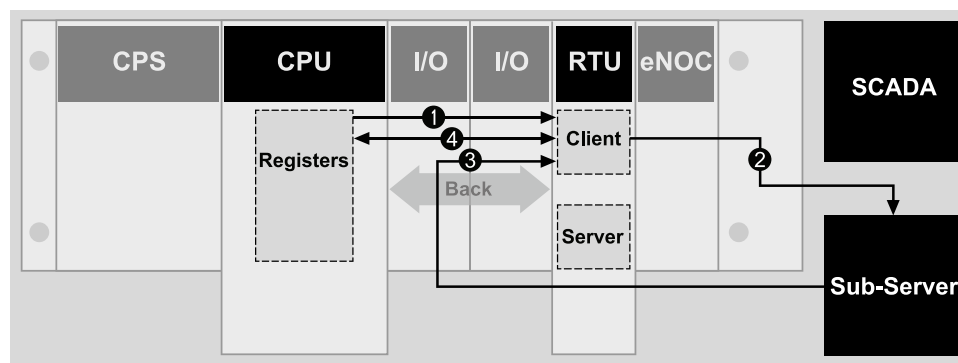


- 1 Le système SCADA envoie une requête Integrity Poll à la voie serveur.
- 2 La voie serveur répond à la requête SCADA avec les valeurs de point figurant dans la base de données.
- 3 Les valeurs de point sont synchronisées de manière cyclique entre la base de données de la voie serveur et les registres de la CPU.

Lorsque la voie client envoie une requête au sous-serveur

La voie client peut envoyer des requêtes à un sous-serveur qui lui est connecté, et un sous-serveur lui renvoie la réponse. Dans ce cas, le comportement de la voie client est identique à celui d'une voie client autonome. **Les points de la voie de serveur logique doivent être synchronisés avec le point mis à jour dans la voie client.**

Exemple d'envoi de requête à un sous-serveur :



- 1 L'application exécutée dans la CPU M580 envoie une commande Integrity Poll à la voie client.
- 2 La voie client envoie des requêtes Integrity Poll au sous-serveur.
- 3 Le sous-serveur répond à la requête en renvoyant la valeur des points les plus récents.
- 4 La base de données du serveur logique est synchronisée pendant que la voie client met à jour la base de données.

NOTE: Les valeurs des points sont synchronisées de manière cyclique entre la base de données de la voie client et les registres de la CPU.

Etat de la connexion

Etat de connexion

Introduction

L'état de connexion de chaque voie du module BMENOR2200H est placé dans un descripteur de type mot double dans le mappage du DDT d'équipement :

- Serveur : <Nom DTM>_CONN.<Nom Serveur>.Error_Code
- Client : <Nom DTM>_CONN.<Nom Client>.Error_Code

Codes d'erreur détectée

Les tableaux suivants décrivent les codes d'erreur détectée concernant l'état de connexion pour les rôles serveur et client.

Serveur :

Bit	Description
0	La sécurité de la voie n'est pas configurée.
1	Une erreur d'initialisation est détectée pour une variable non localisée.
2	Une erreur interne est détectée (erreur de création de tuyau, erreur d'initialisation d'IPT, etc.).
3 à 14	Ces bits sont réservés.
15	Une erreur TLS est détectée.

Client :

Bit	Description
0	La sécurité de la voie n'est pas configurée.
1	Une erreur d'initialisation est détectée pour une variable non localisée.
2	Une erreur interne est détectée (erreur de création de tuyau, erreur d'initialisation d'IPT, etc.).
3	Il y a un problème d'authentification.
4	Il y a une réponse inattendue.
5	Il n'y a pas de réponse.
6	Le mode agressif n'est pas pris en charge.
7	L'algorithme MAC n'est pas pris en charge.
8	L'algorithme d'enveloppe de clé n'est pas pris en charge.
9	Il y a un problème d'autorisation.
10	La méthode de changement de clé de mise à jour n'est pas autorisée.
11	La signature n'est pas valide.
12	Les données de certification ne sont pas valides.
13	Un utilisateur inconnu est détecté.
14	La capacité des requêtes d'état de clé de session est dépassée.
15	Une erreur TLS est détectée.

Réinitialisation de la communication

Introduction

Le module BMENOR2200H communique avec les autres parties via TCP/IP. Le protocole est DNP3 ou IEC104 et les autres parties peuvent être SCADA, RTU ou d'autres contrôleurs. La connexion réseau est variée et associée à de nombreux commutateurs/routeurs et autres équipements réseau.

Dans certains cas anormaux (par exemple, le câble Ethernet entre l'équipement distant et le commutateur est rompu), la communication peut être arrêtée en raison de la perte du paquet heartbeat émis par l'équipement partenaire, la liaison fonctionnant toujours correctement. Dans ces situations, il faut un certain temps pour réessayer de se connecter et finalement aboutir à un timeout.

Le module BMENOR2200H fournit un nouveau DDT d'équipement qui permet de réinitialiser manuellement la communication pour la récupérer rapidement.

Réinitialiser la communication RTU par des variables

La communication ou le protocole TCP peut être réinitialisé(e) sur le DDT d'équipement.

Dans le **Navigateur du projet**, développez **Projet > Variables et instances FB > Variables DDT d'équipement > Variables**.

Développez les paramètres "CONN" pour afficher la variable **RESET_TCP** :

Nom : RESET_TCP

Type : WORD

W : accessible en écriture

Nom de la variable	Valeur	Description
RESET_TCP	0	0 est la valeur initiale et signifie "aucune commande".
	Remplacer la valeur par 1	Si la valeur passe à 1, la voie TCP serveur et le client sont réinitialisés, ce qui signifie que la connexion TCP est fermée puis ouverte à nouveau. Il n'y a aucun impact sur le protocole et les événements.
	Remplacer la valeur par 2	Si la valeur passe à 2, la voie TCP client et le serveur sont réinitialisés, ce qui signifie que la connexion TCP est fermée puis ouverte à nouveau. Il n'y a aucun impact sur le protocole et les événements.
	Remplacer la valeur par 3	Si la valeur passe à 3, le protocole est réinitialisé. La réinitialisation de protocole a deux fonctions : - Fermer toutes les connexions de voie, puis les ouvrir à nouveau en ayant supprimé et reconstruit les configurations, événements de point et valeurs de point associés. - Après avoir réinitialisé le protocole, le module BMENOR2200H obtient le réglage d'horloge auprès du contrôleur M580 et se synchronise.

Capacité de redondance d'UC (Hot Standby)

Introduction

Cette section décrit les fonctionnalités des modules redondants BMENOR2200H, y compris l'état de fonctionnement des modules RTU redondants, en fonction de l'état du PAC, des services Ethernet et de la fonction de basculement Hot Standby.

Capacité de redondance d'UC

Présentation

Dans un système de redondance d'UC (Hot Standby) en cours d'exécution, vous pouvez effectuer les actions suivantes (dans le rack primaire ou redondant, câblé ou non câblé), sans entraîner de basculement ni de duplication d'adresse IP :

- remplacement à chaud d'un module BMENOR2200H
- retrait ou reconnection d'un câble à un module BMENOR2200H

Lorsque vous supprimez un défaut détecté sur un BMENOR2200H dans un rack redondant (coupure du câblage réseau, mise hors tension, remplacement à chaud), cette action n'affecte pas le fonctionnement de l'équipement primaire du système de redondance. En d'autres termes, aucun arrêt ou extinction, aucun à-coup d'E/S et aucun basculement ne se produit. Le module BMENOR2200H peut commuter ses serveurs ou connexions SCADA en douceur lors d'un basculement en mode de redondance d'UC (Hot Standby).

NOTE:

- Lors d'une permutation Hot Standby du module BMENOR2200H, toutes les valeurs sont définies sur 0 dans le [tableau de diagnostics Hot Standby](#).
- Le contrôleur bascule automatiquement dans certaines conditions, mais une erreur détectée (par exemple, dans le module xxxx) peut arrêter le basculement. Il est possible que vous deviez configurer une logique pour détecter l'état du module qui déclenche le basculement souhaité.
- La sauvegarde d'événements n'est pas prise en charge dans un système Hot Standby. Lorsqu'elle est activée dans un système autonome où le contrôleur est remplacé par un contrôleur Hot Standby, redondance d'UC, la fonction de sauvegarde des événements est automatiquement désactivée.
- Pour DNP3, IEC60870-5-101 et IEC60870-5-104, l'acquittement des événements dans le dernier cycle n'a pas forcément été synchronisé du primaire au redondant. L'acquittement entraîne également la réception par SCADA de l'événement en double, lequel a le même horodatage.
- IEC60870-5-101 (via RS232) n'est pas pris en charge dans un système Hot Standby.

Activation/désactivation de la fonctionnalité Hot Standby

La synchronisation des événements Hot Standby peut être activée/désactivée via la configuration de DTM :

Configuration des voies > Serveur > Paramètres avancés > Event Buffer Sync Enable

Sélection de chemin Hot Standby

Configurez le port de communication Hot Standby via le DTM. La sélection par défaut est le port d'embase et une fois les ports de contrôle activés, il existe deux options pour la sélection du chemin :

- Port de contrôle
- Port d'embase

Le service Hot Standby applique l'adresse IP appropriée des différents ports pour établir la connexion et toutes les données HTSB sont échangées via ce port.

Service RTU Hot Standby

Dans un système de redondance d'UC, l'image d'E/S d'entrée (DDT d'équipement `..._CONN`) est synchronisée de manière cyclique entre les PAC M580 primaire et redondant.

Le contenu du DDT d'équipement de diagnostic n'est pas nécessaire aux échanges entre modules BMENOR2200H primaire et redondant.

Vérifiez que seule la première section du contrôleur redondant est en cours d'exécution.

NOTE: Une erreur est détectée si vous mettez à jour les variables Ethernet du RTU dans la première section du contrôleur redondant.

Serveur DNP3/IEC60870-5-101/IEC60870-5-104

Avec un serveur DNP3, IEC60870-5-101 ou IEC60870-5-104, seul le module primaire fonctionne comme d'habitude dans un système de redondance d'UC ; le module redondant n'a aucune communication avec les connexions SCADA.

- Lorsque la configuration DTM, le mode de sécurité et la version de micrologiciel du module primaire sont identiques à ceux du module redondant, les deux modules peuvent se synchroniser. Dans ce cas, le module primaire synchronise l'historique des événements et les données internes (état non sollicité, compteur gelé....) avec le module redondant.

NOTE: Vérifiez que les modules primaire et redondant présentent la même configuration de cybersécurité. S'ils ont des configurations différentes, les modules peuvent toujours se synchroniser, mais ils risquent de ne pas fonctionner correctement car certaines voies sont désactivées en raison d'une règle de sécurité manquante.
- En mode de marche, si les modules primaire et redondant sont synchronisés, les éléments suivants sont synchronisés via le protocole interne :
 - Événement DNP/IEC
 - Acquiescement d'événement DNP/IEC
 - Compteur gelé DNP
 - Bande morte tout DNP
 - Activation/désactivation non sollicitée DNP
 - Démarrage à froid/à chaud
 - DNP IIN
 - IEC MIT (gelé, numéro séquentiel)
 - IEC CRPNA
- Lors d'un basculement en Hot Standby :
 - Le module primaire ferme la connexion avec SCADA.
 - Le module secondaire obtient les données en valeur auprès du PAC dans la base de données locale (AO, BO, String, CMD status, P_ME_A, P_ME_B, P_ME_C, IEC P_AC), puis il commence à prendre le relais et à accepter de nouvelles connexions SCADA.
 - Lors d'un basculement, toutes les méthodes côté serveur signalent des codes d'erreur détectée.
 - Lorsque l'authentification sécurisée DNP3 est activée, la clé de session est forcée à expirer.
 - Pour MIT :
 - > Lorsque l'option de gel local est Automatique, le nouveau module primaire force un gel immédiatement après le basculement.
 - > Lorsque l'option de gel local est réglée sur Gel par l'application, si la valeur du point Gel cyclique est 1, le nouveau module primaire force un gel immédiatement après le basculement.
 - Le nouveau module primaire gère les données des deux derniers cycles et génère un événement.
 - Pour AI, M_ME_A, M_ME_B et M_ME_C :
 - > L'avant-dernier cycle avant un basculement est défini comme valeur de base sur laquelle repose la vérification des modifications de données.
 - > Certains événements des deux derniers cycles peuvent être déjà synchronisés avec le module redondant, ce qui entraîne la réception d'événements en double par SCADA.
- Si la source horaire du module est définie à partir du protocole RTU, l'heure est synchronisée cycliquement entre les modules BMENOR2200H primaire et redondant via le protocole interne.
- Pour les intervalles de message et périodes d'arrière-plan IEC60870-5-101 et IEC60870-5-104, les modules primaire et redondant ne synchronisent pas les informations d'état du compteur de temps. Après le basculement, le premier

message cyclique/d'arrière-plan peut ne pas rester en situation de timeout. Le deuxième message cyclique/d'arrière-plan reste en situation de timeout conformément au paramètre utilisateur.

Client DNP3/IEC60870-5-101/IEC60870-5-104

Pour un client DNP/IEC, le module primaire communique généralement avec le serveur distant et le module redondant n'établit pas de connexion avec l'IED distante.

- Les modules primaire et secondaire synchronisent les données provenant de la mémoire du PAC avec la base de données locale, mais le module redondant n'envoie pas de données au serveur distant. Par conséquent, le serveur distant reçoit uniquement les données de sortie du module primaire.
- Lorsqu'un basculement Hot Standby se produit, le module primaire ferme la connexion avec le serveur distant et le module redondant endosse le rôle de communication avec le serveur distant.
- Lors d'un basculement, si certaines commandes (lecture classe, lecture groupe, commande d'interrogation, opération de contrôle) ne sont pas terminées, un code d'erreur détectée est renvoyé dans l'état d'instance DDT. L'utilisateur peut gérer cet état pour envoyer à nouveau les commandes qui n'ont pas abouti.

NOTE: Pour IEC60870-5-101 et IEC60870-5-104, le client n'envoie pas immédiatement un acquittement d'événement, cela dépend de la valeur W (nombre maximum d'APDU reçues mais non acquittées) et de la période de trame S T2 (temps à attendre avant d'envoyer un acquittement d'ADPU de supervision). Lors du remplacement à chaud d'un module Hot Standby, le client peut recevoir des événements en double parce qu'un événement n'est pas acquitté avant le remplacement à chaud.

Gestion des services Ethernet

Le tableau suivant décrit l'état des services exécutés dans les modules BMENOR2200H primaire et redondant aux états RUN et STOP du PAC :

Liste des services	Module BMENOR2200H primaire		Module BMENOR2200H redondant	
Etat du PAC	RUN	STOP	RUN	STOP
Serveur DNP3/IEC	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>	EN COURS D'EXECUTION (synchronisation à partir du module primaire)	EN COURS D'EXECUTION (synchronisation à partir du module primaire)
Routage d'événements	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>	EN COURS D'EXECUTION (synchronisation à partir du module primaire)	EN COURS D'EXECUTION (synchronisation à partir du module primaire)
Client DNP3/IEC	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>	ARRETE	ARRETE
Client SNTP	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>
Client Modbus TCP	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>	ARRETE	ARRETE
Syslog	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>
Serveur Modbus TCP	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>
Mise à niveau du micrologiciel	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>
SNMPv1	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>
SNMPv3				
Serveur Web (paramètre de cybersécurité + diagnostic)	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>
OEB (FDR+LLDP)	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>
Journalisation des données	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>	<i>EN COURS D'EXECUTION</i>

SOE (Sequence Of Events)

Introduction

Utilisez les informations de ce chapitre pour configurer les événements d'horodatage d'un module BMXERT1604.

Séquence d'événements horodatés

Introduction

Les applications logicielles de séquence d'événements (SOE) permettent de comprendre une chaîne d'occurrences qui peut entraîner des conditions d'insécurité des processus et éventuellement des arrêts.

Un grand nombre d'événements de processus peut être généré rapidement lorsqu'un système ne se comporte pas comme prévu. Dans ce cas, le module d'horodatage X80 BMXERT1604 enregistre tous les événements avec une précision d'horodatage de 1 ms. Les données sont stockées dans le module jusqu'à leur transmission par l'application. Le module BMENOR2200H peut appeler ces données d'événement et les transférer vers un système de supervision externe (SCADA, DCS, etc.) via le protocole RTU.

Cette section décrit SOE dans le transfert de la fonction d'horodatage depuis un module BMXERT1604 vers le protocole RTU dans un projet Control Expert qui inclut un module BMENOR2200H.

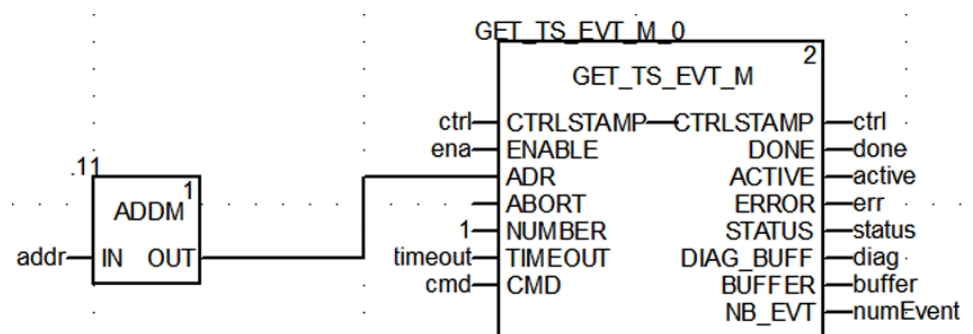
Présentation du processus

Il s'agit d'une présentation très générale du processus SOE d'horodatage.

Etape	Description
1	Utilisez un DFB pour lire et envoyer un événement d'horodatage d'un module BMXERT1604 à un module BMENOR2200H. Dans un même cycle d'automate, une instance de DFB traite au maximum un événement d'horodatage.
2	Selon la structure du tampon brut lu sur le module d'horodatage, vous pouvez extraire et convertir les données.
3	Utilisez un EFB T850_TO_T870 pour convertir le format d'horodatage au format IEC60870.

GET_TS_EVT_M Function Block

Utilisez un bloc fonction GET_TS_EVT_M pour lire un événement d'horodatage d'un module BMXERT1604 spécifique :



NOTE: Lisez un événement dans un même cycle d'automate pour chaque module d'horodatage. Lorsque le paramètre `DONE` prend la valeur `TRUE`, l'événement a été lu et stocké dans le tampon. Vous pouvez passer à l'étape suivante.

Le document Ecostruxure Control Expert - Bibliothèque de blocs système (voir EcoStruxure™ Control Expert - Système - Bibliothèque de blocs) fournit des descriptions détaillées des paramètres du bloc fonction `GET_TS_EVT_M`.

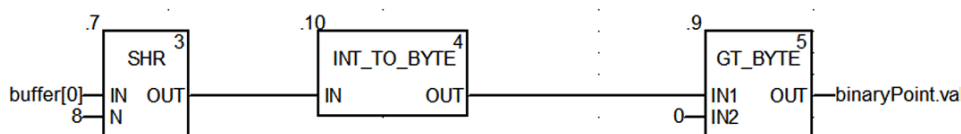
Format des événements dans le tampon de réponse

Le tableau suivant décrit le format de l'événement d'horodatage dans le tampon de réponse :

Structure de données	Élément	Type	Définition
Format de tampon brut	Réservé	BYTE	Réservé
	Valeur	BYTE	Valeur d'entrée
	Event ID	WORD	ID d'événement défini par l'utilisateur ou numéro de voie
	SecondSinceEpoch	DWORD	Intervalle en secondes compté en continu à partir de l'époque 1970-01-01 00:00:00 UTC
	FracOfSec_L	WORD	Fraction de la seconde en cours où la valeur d'horodatage a été déterminée. La fraction de seconde est calculée par la formule (SUM de $i = 0$ à 23 de $bi \cdot 2^{32-i-1}$ s).
	FracOfSec_H	BYTE	
	TimeQuality	BYTE	Qualité de l'heure : • Bit 7 : LeapSecondsKnown (non pris en charge) • Bit 6 : ClockFailure (non pris en charge) • Bit 5 : ClockNotSynchronized • Bits 0-4 : Précision de l'heure

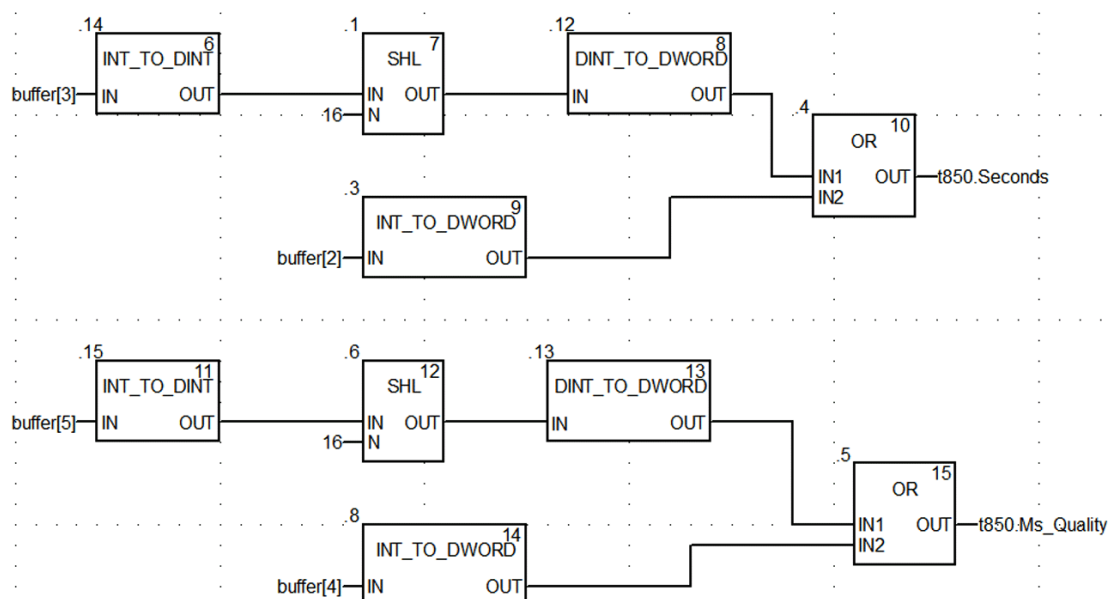
Extraire l'événement d'horodatage

Selon la structure du tampon brut lu sur le module d'horodatage, vous pouvez extraire et convertir les données. Commencez par extraire la valeur du point binaire comme indiqué dans cet exemple, qui suppose que le premier événement commence à `Buffer[0]` :



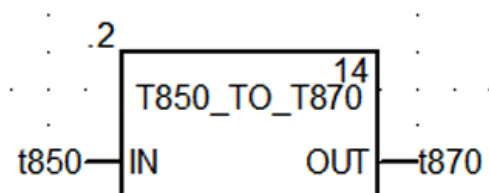
Extraire les données T850

Pour extraire les données T850, comme illustré dans cet exemple d'application classique, placez la valeur de point binaire à la bonne position du DDT en fonction de l'adresse et de la voie du module BMXERT1604 dans le tampon brut :



Convertir le format d'horodatage

Pour convertir le format d'horodatage de IEC61850 en IEC60870, utilisez le bloc EFB T850_TO_T870 de la manière suivante, où le paramètre d'entrée est le format d'heure 850 et le paramètre de sortie le format d'heure 870 :



Le tableau suivant décrit la structure des formats d'heure 850 et 870 :

Structure de données	Élément	Type	Définition
TIME_870_FORMAT	ms	WORD	Millisecondes : 0 à 59999 ms
	min	BYTE	Minutes : 0 à 59 min, le bit de poids fort est un bit non valide, 1 : heure non valide, 0 : heure valide
	hour	BYTE	Heure : 0 à 23 h, l'heure d'été (SU) n'est pas pris en charge
	day	BYTE	Jour : 1 à 31, le jour de la semaine n'est pas pris en charge
	mon	BYTE	Mois : 1-12
	year	BYTE	Année: 0-99
	réservé	BYTE	Réservé
TIME_850_FORMAT	Secondes	DWORD	Secondes depuis 1970, vérifier que l'horodatage est postérieur à 2000.

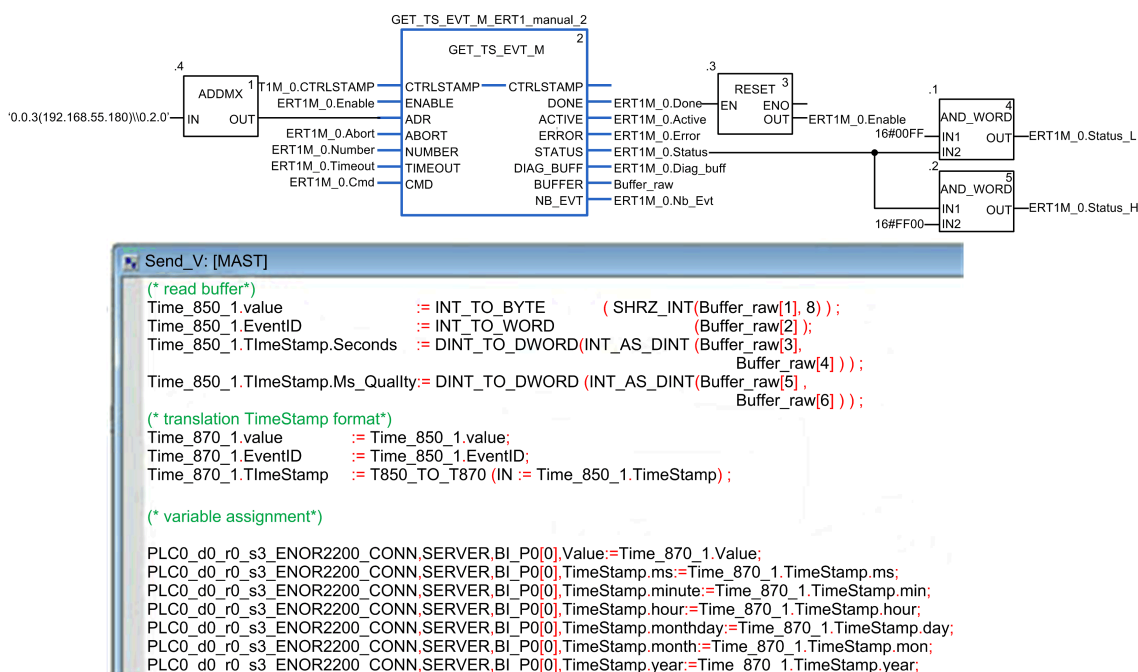
Structure de données	Élément	Type	Définition
	Ms_Quality	DWORD	- Bit 0-23: Fraction de la seconde en cours où la valeur d'horodatage a été déterminée. La fraction de seconde est calculée par la formule (SUM de $i = 0$ à 23 de $bi \cdot 2^{**}-(i+1)$ s). - Bits 24-31 : Qualité de l'heure - Bit 31 : LeapSecondsKnown (non pris en charge) - Bit 30 : ClockFailure (non pris en charge) - Bit 29 : ClockNotSynchronized - Bits 24-28 : Précision de l'heure

REMARQUE : Le bloc fonction T870_TO_T850 ne tient pas compte du fuseau horaire ni de l'heure d'été lors de la conversion de l'heure. Réglez la valeur T870 sur l'horodatage du point DNP comme suit :

```
binaryPoint.ms:=t870.ms;
binaryPoint.min:=t870.min;
binaryPoint.hour:=t870.hour;
binaryPoint.day:=t870.day;
binaryPoint.mon:=t870.mon;
binaryPoint.year:=t870.year;
```

Exemple d'application SOE typique

Cette capture d'écran illustre l'utilisation de la commande `Send_V` pour transférer la sortie de `GET_TS_EVT_M` (tampon brut) aux points RTU dans une application SOE typique dans laquelle le tampon de lecture et le format d'horodatage de traduction dans `Send_V` sont identiques aux blocs fonction des exemples précédents :



Configuration du module

Présentation de la configuration

Composants de configuration

Introduction

Respectez ces consignes pour configurer le module BMENOR2200H après avoir ajouté le module et le DTM correspondant à un projet Control Expert.

Composants de l'environnement de configuration

Sélectionnez le composant approprié dans l'environnement de configuration avec le rôle de configuration souhaité :

Composant	Caractéristique fonctionnelle
Présentation de la configuration Control Expert	définition de nom de module BMENOR2200H
	ajout du module à un projet Control Expert
	affectation d'adresse IP
	diagnostics en ligne de base
DTM d'équipement	configuration du protocole RTU
	client/serveur IEC60870-5-104, page 141
	sélection de version
	configuration des voies
	client/serveur DNP3 NET
	configuration de points RTU
	agent SNMP, client SNMP
	service de temps réseau (SNTP)
	exportation/importation
	informations du module
	lien d'accès rapide aux pages Web de diagnostic
	configuration de port série
Pages Web HTTPS	configuration de l'authentification sécurisée (SA) DNP3
	configuration de sécurité
	Configuration TLS : - DNP3, page 222 - IEC60870, page 227
	configuration RBAC, page 231
Automation Device Maintenance	mise à niveau de micrologiciel
Migration de projet	considérations relatives à la migration de projet
	variables localisées avec adresses (mode "à la demande" DNP3 AO/BO)

Utilisation du module dans un projet Control Expert

Avant de commencer

Suivez les instructions de cette section pour ajouter un module et le DTM correspondant à un projet Control Expert.

Ajouter le DTM et le module à Control Expert

A propos des DTM

Chaque module ou équipement du Control Expert **Catalogue de matériels** est représenté par un gestionnaire de type d'équipement (DTM - device type manager) qui définit ses paramètres.

Toute configuration effectuée via le DTM est exécutée dans l'environnement Control Expert.

Installation de DTM

D'une manière générale, le DTM de l'équipement est installé automatiquement lors de l'installation de Control Expert.

Sinon, vous pouvez installer le DTM sur un PC hôte (le PC qui exécute Control Expert) pour que le DTM d'équipement puisse être utilisé dans Control Expert.

Pour les modules de constructeurs tiers, la procédure d'installation du DTM est définie par le fabricant. Suivez ces instructions pour installer un DTM sur votre PC.

Une fois qu'un DTM d'équipement est installé sur votre PC, mettez à jour le **Catalogue de matériels** de Control Expert pour qu'il mentionne le nouveau DTM. Le DTM est ensuite ajouté à votre configuration Control Expert lorsque le module correspondant est ajouté au projet.

A propos du navigateur de DTM de Control Expert

Présentation du FDT/DTM

Control Expert utilise l'approche FDT (Field Device Tool) / DTM (Device Type Manager) pour intégrer des équipements distribués à votre application de contrôle de processus. Control Expert comprend un conteneur FDT qui s'interface avec les DTM d'équipements EtherNet/IP et Modbus TCP et le module BMENOR2200H.

Un équipement EtherNet/IP ou Modbus TCP est défini par un ensemble de propriétés dans son DTM. Pour chaque équipement de votre configuration, ajoutez le DTM correspondant au **Navigateur de DTM** de Control Expert. Le **Navigateur de DTM** vous permet d'ouvrir les propriétés de l'équipement et de configurer les paramètres présentés par le DTM.

Les fabricants d'équipements peuvent fournir un DTM pour chacun de leurs équipements EtherNet/IP ou Modbus TCP ou pour le module BMENOR2200H. Toutefois, si vous utilisez un équipement qui n'a pas de DTM, vous devez le configurer à l'aide d'une des méthodes suivantes :

- Configurer un DTM générique fourni dans Control Expert.
- Importer le fichier EDS pour l'équipement. Control Expert renseigne les paramètres du DTM sur la base du contenu du fichier EDS importé.

NOTE: Le DTM d'un module BMENOR2200H est automatiquement ajouté au **Navigateur de DTM** lorsque le module est ajouté au **Bus automate**.

Création automatique de DTM

Dans une application Control Expert, les DTM de certains modules de communication Ethernet et d'autres équipements préconfigurés (voir la liste suivante) sont créés automatiquement lorsque ces équipements sont ajoutés à un rack Ethernet sur les stations principales locales ou distantes. Un nom de DTM par défaut est attribué dans la topologie DTM, mais vous pouvez le modifier :

- Cliquez avec le bouton droit sur le nom de DTM souhaité dans le **Navigateur de DTM** et sélectionnez **Propriétés**.
- Sélectionnez l'onglet **Général** et modifiez le nom de DTM dans le champ **Nom d'alias**.
- Sélectionnez **Appliquer** pour enregistrer les modifications.

– ou –

Sélectionnez **OK** pour enregistrer les modifications et fermer la boîte de dialogue.

REMARQUE : Le bouton **OK** n'est valide que si Control Expert a confirmé l'unicité du DTM.

Compatibilité avec Windows

Le tableau suivant décrit les configurations minimales et recommandées du PC pour exécuter les DTM M580 au sein de Control Expert :

Configuration de l'ordinateur	Exigences
Contrôleur	2,4 GHz, 3,0 GHz ou plus recommandé.
	Core i3 ou supérieur. Core i7 ou supérieur recommandé.
RAM	8 Go, 16 Go recommandés.
	16 Go minimum pour Windows Server.
Stockage	8 Go, incluant l'espace mémoire pour l'installation et l'exécution du logiciel et pour l'enregistrement des applications.
	20 Go recommandés.
	Disques SSD recommandés.
Système d'exploitation et version	Microsoft Windows 10 64 bits, version 21H1 ou ultérieure.
	Microsoft Windows 10 64 bits Entreprise 2019 LTSC, version 1809.
	Microsoft Windows Server 2019, version 1809 standard.
	Microsoft Windows 11 64 bits, version 21H1 ou ultérieure.
	Microsoft Windows Server 2022, version 21H1 ou ultérieure.
Lecteur	DVD R pour installer le logiciel. DVD RW recommandé.
Ecran	Résolution minimale VGA (800 x 600).
	Résolution maximale prise en charge 2560 x 1440 avec échelle et disposition à 125 %.
Périphériques d'entrée	Clavier et souris ou dispositif de pointage compatible.
Accès Web	L'activation de la licence sur Internet est recommandée.
	L'activation hors ligne reste possible (reportez-vous à License Manager ou Floating License Manager).
Autre	Port USB.

NOTE: Windows 10 32 bits n'est pas pris en charge.

La version de Microsoft Excel minimale recommandée pour exécuter la est Microsoft Excel 2007.

Types de DTM

Le **Navigateur de DTM** affiche une liste hiérarchique de nœuds DTM dans une arborescence de connectivité. Les nœuds DTM qui apparaissent dans la liste ont été ajoutés à votre projet Control Expert. Chaque nœud représente un module ou un équipement réel de votre réseau Ethernet.

Il existe deux types de DTM :

- **DTM client (communication)** : Ce type de DTM est à la fois un DTM d'équipement et un DTM de communication. Le DTM client est un composant préinstallé de Control Expert.
- **DTM générique** : Le conteneur FDT de Control Expert est l'interface d'intégration pour le DTM de communication de tout équipement.

La liste contient les types de nœud suivants :

Type de DTM	Description
communication (client)	Les DTM de communication s'affichent sous le nœud racine (PC hôte). Un DTM de communication peut prendre en charge des DTMs de passerelle ou des DTMs d'équipement en tant qu'enfants si leurs protocoles sont compatibles.
passerelle	Un DTM de passerelle prend en charge d'autres DTMs de passerelle ou des DTMs d'équipement en tant qu'enfants si leurs protocoles sont compatibles.
équipement	Un DTM d'équipement ne prend en charge aucun DTMs enfant.

Noms de nœud

Chaque nœud DTM reçoit un nom par défaut lorsqu'il est inséré dans le navigateur. Le nom par défaut des DTM de passerelle et d'équipement présente le format suivant pour le module BMENOR2200H :

<IP address>PLC0_d0_rX_sY_ENOR2200

- X est le numéro du rack (généralement 0).
- Y est le numéro d'emplacement d'après la position du module dans le rack.

Voici un exemple réel de nom par défaut :

<172.168.12.1>PLC0_d0_r0_s2_ENOR2200

Le tableau suivant décrit les éléments du nom de nœud par défaut.

Élément	Description
adresse	Adresse de bus de l'équipement qui définit le point de connexion au réseau de la passerelle parent (par exemple, l'adresse IP de l'équipement).
nom d'équipement	Le nom par défaut est déterminé par le fournisseur dans le DTM de l'équipement, mais l'utilisateur peut modifier le nom.

Ajout du module à un projet

Ajout du module au bus automate

Pour ajouter un module BMENOR2200H à un projet Control Expert et lui attribuer un nom :

Etape	Action
1	Ouvrez un projet dans Control Expert.
2	Développez (+) le Navigateur de projet pour afficher le Bus automate (Projet > Configuration > Bus automate) .
3	Double-cliquez sur Bus automate pour afficher les racks assemblés.
4	Cliquez avec le bouton droit de la souris sur un emplacement de rack vide et faites défiler la liste pour sélectionner Nouvel équipement . NOTE: Sélectionnez une position en rack conforme aux restrictions d'emplacement du module.
5	Dans la colonne Référence de la boîte de dialogue Nouvel équipement , développez Communication pour afficher les modules disponibles.
6	Double-cliquez sur le module BMENOR2200H pour ouvrir la boîte de dialogue Propriétés de l'équipement . NOTE: Plusieurs modules BMENOR2200H sont répertoriés dans la Liste d'équipements . Les versions plus récentes correspondent aux nouvelles fonctionnalités de la version du logiciel.
7	Dans le champ Nom , attribuez un nom au module (ou acceptez le nom par défaut).
8	Vérifiez que le DTM du module a été automatiquement ajouté au projet (Outils > Navigateur de DTM). NOTE: Lorsque vous ajoutez un module à la configuration du rack local, le DTM de communication correspondant est automatiquement ajouté à la liste (Tous les équipements > Types d'équipements > Equipements de communication).
9	Répétez ces étapes pour ajouter d'autres modules BMENOR2200H au Bus automate . NOTE: Le rack local d'un système M580 peut contenir jusqu'à quatre modules de communication, dont des modules BMENOR2200H.

Configuration avec Control Expert

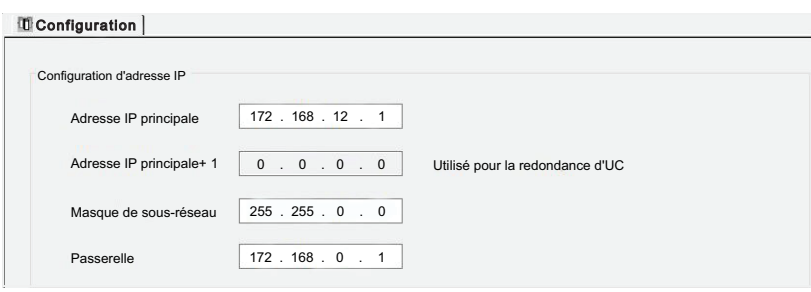
Configuration d'adresse IP

Introduction

Suivez ces instructions pour configurer les paramètres d'adresse IP d'un module BMENOR2200H. Deux adresses IP différentes peuvent être affectées au module. L'adresse IP du port d'embase est configurée par Control Expert et celle des ports de contrôle est configurée par DTM.

Configurer l'adresse IP du port Ethernet de l'embase

Accédez à **Configuration des adresses IP** dans Control Expert :

Etape	Action
1	Ouvrez un projet Control Expert qui inclut un module BMENOR2200H.
2	Double-cliquez sur le module BMENOR2200H pour afficher l'onglet Configuration. 
3	Configurez les paramètres suivants : • Adresse IP : Entrez l'adresse IP du module. • Masque de sous-réseau : Entrez un masque de sous-réseau qui correspond à l'adresse IP. • Passerelle par défaut : Adresse IP de la passerelle à laquelle les messages destinés à d'autres réseaux sont transmis. NOTE: Le champ Adresse IP principale + 1 est utilisé pour configurer un système redondant.
4	• Cliquez sur le bouton Appliquer pour appliquer vos changements de configuration. • Cliquez sur le bouton OK pour implémenter les modifications et fermer la boîte de dialogue.

Configurer l'adresse IP des ports de contrôle

Deux ports de contrôle partagent la même adresse IP. L'adresse IP doit être configurée manuellement dans le DTM. Pour plus d'informations, reportez-vous à [Configuration des ports de contrôle](#), page 163.

Limites

Le module BMENOR2200H utilise le service de base client FDR pour obtenir les paramètres IP auprès du contrôleur.

NOTE:

- Ce module ne prend pas en charge DHCP ni BOOTP.
- Ce module ne stocke pas localement les paramètres IP statiques.
- Pour plus d'informations, consultez la description de la [Configuration du service client FDR](#).

Débogage avec Control Expert

Présentation

Cette section décrit les procédures de mise au point de la configuration d'un module BMENOR2200H avec Control Expert.

Ecran de mise au point du module

Introduction

Utilisez l'écran de mise au point pour diagnostiquer un port Ethernet sur le module BMENOR2200H.

Informations d'adresse

Paramètres

Les paramètres de mise au point des utilitaires TCP/IP du module BMENOR2200H s'affichent dans l'écran **Mise au point** du module :

Champ	Description
Adresse MAC	Adresse MAC de l'embase du module BMENOR2200H
Adresse IP	Adresse IP de l'embase du module BMENOR2200H
Masque de sous-réseau	Adresse du masque de sous-réseau de l'embase du module BMENOR2200H
Adresse de passerelle	Adresse de la passerelle du module BMENOR2200H

Voyants

Examinez les voyants suivants dans le coin supérieur droit de la fenêtre pour surveiller les états du module ::

Emplacement	Voyant	Description
coin supérieur droit de la fenêtre	Run	<i>allumé</i> : Le module fonctionne normalement.
		<i>éteint</i> : L'automate n'est pas configuré.
	ERR	<i>allumé</i> : Une erreur de configuration ou système est détectée.
		<i>éteint</i> : Le module fonctionne normalement.

Observez le voyant dans l'onglet Défaut pour plus d'informations relatives au module :

Emplacement	Voyant	Description
Onglet Défaut	Défaut	Description des problèmes : • problème interne détecté • problème de configuration détecté • erreur de communication détectée • problème d'application détecté • erreur de configuration détectée • Ethernet désactivé • adresse IP en double • déconnexion de liaison • en attente d'adresse IP • détection de tempête

Configuration dans le DTM

Introduction

Suivez les instructions exposées dans cette section pour configurer des services via le DTM après avoir accédé au lien de configuration des services.

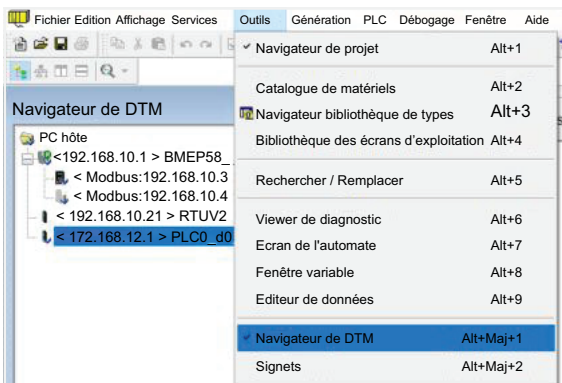
Accès au DTM

Introduction

Certaines fonctionnalités et services de votre module sont configurés à l'aide d'un gestionnaire de type d'équipement ou DTM (Device Type Manager). Vous pouvez accéder au DTM dans Control Expert.

Accès à la configuration du DTM

Il existe deux façons d'accéder aux écrans de configuration des services fournis par le DTM dans Control Expert.

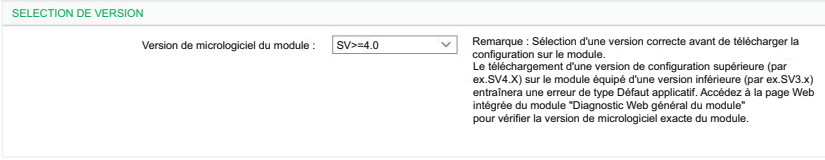
Etape	Action
1	Ouvrez le projet Control Expert qui comprend le module approprié.
2	Ouvrez le Navigateur de DTM (Outils > Navigateur de DTM) . 
3	Dans le Navigateur de DTM , double-cliquez sur le nom que vous avez attribué au module pour ouvrir la fenêtre de configuration.

– OU –

Etape	Action
1	Développez (+) le Navigateur de projet pour afficher le Bus automate (Projet > Configuration > Bus automate) .
2	Double-cliquez sur Bus automate pour afficher les racks assemblés.
3	Double-cliquez sur le module.
4	Cliquez sur le lien Configuration des services . 

Sélection de version

Avant de configurer le module dans le DTM, sélectionnez le modèle de DTM correspondant au micrologiciel de votre module :

Etape	Action
1	Cliquez sur Sélection de version dans le menu CONFIGURATION . 
2	Accédez à la version appropriée dans le menu déroulant Vers ion du micrologiciel du module.
3	Appuyez sur le bouton OK ou Appliquer .

NOTE:

- Sélectionnez une version correcte avant de télécharger la configuration sur le module. Le téléchargement d'une version de configuration supérieure sur un module de version inférieure entraîne une erreur Défaut d'application.
- Accédez à la page Web intégrée du module *Diagnostic Web - Informations générales sur le module* pour vérifier la version exacte du micrologiciel du module.

Configuration de voies DNP3

Introduction

Configurez les communications DNP3 de votre module dans le DTM Control Expert.

Dans les instructions de configuration suivantes, effectuez les sélections appropriées au type de voie (serveur ou client).

Configuration des voies NET ou série

Pour configurer des voies NET *CLIENT* ou *SERVEUR* :

Etape	Action
1	Accédez à la configuration DTM de votre module.
2	Dans la fenêtre <i>CONFIGURATION</i> ouverte, développez (+) <i>Communication</i> et sélectionnez <i>Configuration des voies</i> . NOTE: L'option de menu <i>Voies/Equipements</i> ne peut pas être développée car aucune voie n'est configurée.
3	Sélectionnez l'onglet approprié : - Sélectionnez l'onglet <i>CLIENT</i> pour ajouter des voies client. - Sélectionnez l'onglet <i>SERVEUR</i> pour ajouter des voies serveur.
4	Cliquez sur le bouton <i>Ajouter nouveau</i> pour afficher les paramètres de configuration <i>AJOUTER UNE NOUVELLE VOIE</i> .
5	Configurez les paramètres conformément à la description des paramètres de configuration d'une nouvelle voie.
6	Cliquez sur le bouton <i>Ajouter</i> pour afficher la nouvelle voie configurée dans le tableau. NOTE: Le menu <i>Voies/Equipements</i> peut désormais être développé car une voie au moins est configurée. Toutes les voies configurées apparaissent dans ce menu.
7	Après avoir créé une voie <i>serveur</i> dans l'onglet <i>SERVEUR</i> , répétez les étapes ci-dessus pour créer la voie <i>client</i> correspondante dans l'onglet <i>CLIENT</i> . – ou – Après avoir créé une voie <i>client</i> dans l'onglet <i>CLIENT</i> , répétez ces étapes pour créer la voie <i>serveur</i> correspondante dans l'onglet <i>SERVEUR</i> . NOTE: Un seul type de protocole RTU peut être configuré dans le module (DNP3 ou IEC60870). Le module ne peut pas prendre en charge la configuration de plusieurs protocoles RTU simultanément.

Etape	Action
	Si l'authentification sécurisée DNP3 est configurée dans le réglage de cybersécurité Web, assurez-vous que le nom de voie RTU configuré correspond au nom de voie dans le DTM. Sinon, la configuration sécurisée n'est pas mise en correspondance avec une voie du DTM.
8	- Cliquez sur le bouton <i>Appliquer</i> pour appliquer les modifications - Cliquez sur <i>OK</i> pour appliquer les modifications et fermer la boîte de dialogue. NOTE: Lorsque vous créez la première voie, le sous-menu <i>Voies/Equipements</i> s'affiche sur l'écran <i>CONFIGURATION</i>.
9	Répétez ces étapes pour créer d'autres voies, en respectant les limites suivantes en fonction du rôle du module : <i>RTU client Ethernet</i> : 64 connexions <i>RTU serveur Ethernet</i> : 4 connexions <i>RTU client série</i> : 32 connexions <i>RTU serveur série</i> : 1 connexion NOTE: Le client série prend en charge le signal provenant d'équipements de terrain série en direction du réseau de niveau supérieur via Ethernet.

NOTE: Vous pouvez à tout moment modifier ou supprimer une voie.

Description des paramètres de voie

NOTE: Lorsque la fenêtre Control Expert est active, vous pouvez déplacer le curseur sur n'importe quel champ pour afficher une description de la fonctionnalité correspondante et de la plage de valeurs disponible.

Les champs suivants sont disponibles dans *AJOUTER UNE NOUVELLE VOIE* pour les configurations de voies client et serveur DNP3/IEC60870 :

Champ	Client	Serveur	Description
<i>Nom de la voie</i>	✓	✓	Attribuez un nom au serveur ou au client dans leurs onglets respectifs. NOTE: Les pages Web utilisent le paramètre <i>Nom de la voie</i> pour identifier la configuration appliquée à la voie. Par conséquent, attribuez une valeur <i>Nom de la voie</i> identique lorsque vous configurez les paramètres de cybersécurité.
<i>Protocole</i>	✓	✓	<i>Client NET DNP3</i> : Configurer la nouvelle voie en tant que client NET DNP3.
			<i>Serveur NET DNP3</i> : Configurer la nouvelle voie en tant que serveur NET DNP3.
			<i>Client série DNP3</i> : Configurer la nouvelle voie en tant que client série DNP3.
			<i>Serveur série DNP3</i> : Configurer la nouvelle voie en tant que serveur série DNP3.
			<i>Client IEC60870-5-101</i> : Configurer la nouvelle voie en tant que client IEC60870-5-101.
			<i>Serveur IEC60870-5-101</i> : Configurer la nouvelle voie en tant que serveur IEC60870-5-101.
			<i>Client IEC60870-5-104</i> : Configurer la nouvelle voie en tant que client IEC60870-5-104.
			<i>Serveur IEC60870-5-104</i> : Configurer la nouvelle voie en tant que serveur IEC60870-5-104.
<i>Port de dest.</i>	✓		Définir le port de destination. NOTE: Ce paramètre est disponible pour les configurations DNP3 NET et IEC60870-5-104 uniquement.
<i>Port local</i>		✓	Définir le port local pour les communications réseau. NOTE: Ce paramètre est disponible pour les configurations DNP3 NET et IEC60870-5-104 uniquement.
<i>Adresse IP</i>	✓		L'adresse IP indiquée dans ce champ est celle de la source des paquets de communication. NOTE: Ce paramètre est disponible pour les configurations DNP3 NET et IEC60870-5-104 uniquement.

Champ	Client	Serveur	Description
<i>Filtre IP</i>		✓	Entrez l'adresse IP de l'équipement distant. NOTE: - Ce paramètre est disponible pour les configurations DNP3 NET et IEC60870-5-104. - La valeur par défaut est 255.255.255.255 (present disable IP filter).
<i>Type de réseau</i>	✓	✓	Sélectionnez un protocole réseau : <i>TCP-IP</i> <i>UDP-IP</i> <i>TCP-UDP</i> NOTE: Ce paramètre est disponible pour les configurations DNP3 NET uniquement.

Configuration des paramètres avancés

Une fois que vous avez créé une voie selon les instructions ci-dessus, la nouvelle voie apparaît dans le tableau de l'onglet *CLIENT* ou de l'onglet *SERVEUR*. A ce stade, vous pouvez configurer les *PARAMÈTRES AVANCÉS* de la voie. Les paramètres avancés sont des paramètres globaux qui sont implémentés sur toutes les voies serveur ou toutes les voies client :

Etape	Action
1	Sélectionnez <i>Configuration des voies</i> dans le menu <i>Communication</i> .
2	Sélectionnez l'onglet approprié : - Sélectionnez l'onglet <i>CLIENT</i> pour afficher le tableau <i>VOIES CLIENT</i>. - Sélectionnez l'onglet <i>SERVEUR</i> pour afficher le tableau <i>VOIES SERVEUR</i>.
3	Sélectionnez une ligne dans le tableau.
4	Cliquez sur le bouton <i>Paramètres avancés</i> pour afficher le tableau <i>PARAMÈTRES AVANCÉS</i> . NOTE: Selon la taille de la fenêtre Control Expert, il se peut que vous deviez faire défiler l'onglet <i>Client</i> ou <i>Serveur</i> vers le bas pour voir les champs <i>PARAMÈTRES AVANCÉS</i> .
5	Configurez les paramètres conformément à la description des paramètres avancés .
6	- Cliquez sur le bouton <i>Appliquer</i> pour appliquer les modifications. - Cliquez sur <i>OK</i> pour appliquer les modifications et fermer la boîte de dialogue.

Description des paramètres avancés

NOTE: Lorsque la fenêtre Control Expert est active, vous pouvez déplacer le curseur sur n'importe quel champ pour afficher une description de la fonctionnalité correspondante et de la plage de valeurs disponible.

Voici les paramètres avancés disponibles pour la configuration des voies client et serveur DNP3 :

Champ	Client	Serveur	Description
Event Buffer Sync Enable		✓	- Activer (valeur 1) - Le module NOR primaire synchronise les événements DNP/IEC sur le module NOR redondant pendant l'exécution. - Lorsque le système à redondance (HSBY) bascule, le SCADA peut récupérer les événements à partir du nouveau NOR primaire. Si le taux de génération d'événements lors de l'exécution ne dépasse pas le nombre maximal d'événements pris en charge, les événements ne seront pas perdus. - Désactiver (valeur 0) - Le module NOR primaire ne synchronise pas les événements DNP/IEC sur le module NOR redondant pendant l'exécution. - Le module NOR primaire synchronise l'heure et d'autres données sur le module NOR redondant pendant l'exécution. - Lorsque le système HSBY bascule : - Le module NOR redondant efface les événements générés. - Le module NOR primaire commence à générer des événements. - Si des événements ne sont pas signalés, ils sont perdus et le système SCADA ne peut pas les récupérer à partir du module NOR primaire.
Event Buffer Sync Ports		✓	Sélectionnez le chemin réseau pour transférer les données de synchronisation des événements. - Port d'embase (par défaut) En général, les données de synchronisation interne doivent être transférées via le port d'embase. - Port(s) de contrôle Dans les cas ci-dessous, le chemin de synchronisation peut être déplacé du port d'embase aux ports frontaux. - Le réseau d'embase n'est pas disponible entre le contrôleur/NOR primaire et le contrôleur/NOR secondaire. - L'anneau RIO est très chargé et tout trafic de données supplémentaire doit être évité.
Activer la sauvegarde d'événements		✓	activé (sélectionné) : Les événements sont sauvegardés en cas de coupure d'alimentation. désactivé (vide) : Les événements ne sont pas sauvegardés en cas de coupure d'alimentation.
Taille des trames de réception	✓	✓	Configurez la taille des trames dans la couche de liaison de réception.
Temporisation des trames de réception	✓	✓	Configurez le délai d'attente d'une trame complète après réception de la synchronisation de trame.
Temporisation de confirmation	✓	✓	Configurez le temps d'attente maximum de la confirmation du niveau de liaison.
Période de détection de déconnexion	✓		Configurez un intervalle pour le renouvellement de tentative d'établissement de communication pour une session déconnectée.
Taille du tampon de réception	✓	✓	Configurez la taille du tampon de réception pour le port physique.
Taille de fragment en émission	✓	✓	Configurez les tailles maximales de fragments d'application en transit.
Temporisation de réponse de la voie	✓		Configurez le temps d'attente de la réponse du client DNP3 à une requête transmise.
Inhibition en cas d'arrêt de l'UC	✓		Cochez cette case pour arrêter l'envoi de commandes lorsque le contrôleur s'arrête.
Taille des trames d'émission	✓	✓	Configurez la taille des trames dans la couche de liaison de transmission.
Mode de confirmation	✓	✓	JAMAIS: Ne jamais demander de confirmations de la couche de liaison. PARFOIS: Demander les confirmations de la couche de liaison pour des fragments multitrames. TOUJOURS: Toujours demander les confirmations de la couche de liaison.

Champ	Client	Serveur	Description
Nbre maxi. de tentatives	✓	✓	Configurez le nombre de renouvellement de la temporisation de confirmation de la couche liaison.
Attente premier caractère	✓	✓	Configurez le délai minimum (ms) entre la réception d'un caractère et une tentative de transmission d'un caractère sur la voie.
Taille de fragment en réception	✓	✓	Configurez les tailles maximales de fragments d'application reçus.
Mode de restauration		✓	Voie principale : Restaurer les événements pour la voie principale ou le groupe de redondance principal. Toutes les voies : Restaurer tous les événements.
Taille maxi file d'attente	✓		Configurez le nombre maximal de requêtes mises en file d'attente sur un client DNP3.
Exclure la valeur 0 pour les commandes BO Pulse_Trip	✓		Cochez cette case pour arrêter l'envoi de commandes BO Pulse_Trip (<i>Select, Operate, Direct, DirectNoAct, Auto</i>) lorsque la variable prend la valeur 0.
Multiple-Session Enable		✓	Cochez cette case pour activer la configuration multisession pour le serveur DNP3. Une fois la configuration multisession activée, tous les paramètres pris en charge peuvent être configurés indépendamment. NOTE: Lorsque la configuration multisession est activée, vérifiez que chaque voie est affectée avec une <i>adresse IP</i> et un <i>numéro de port</i> uniques.

Après avoir modifié un ou plusieurs de ces paramètres, cliquez sur le bouton **Appliquer** pour mettre à jour la configuration.

Modification de voies

Pour modifier les paramètres d'une voie existante :

Etape	Action
1	Cliquez sur l'icône représentant un crayon dans la colonne Edition correspondant à la voie à modifier.
2	Reconfigurez les paramètres dans les champs MODIFIER LA VOIE et PARAMÈTRES AVANCÉS (décrits ci-dessus).
3	Cliquez sur le bouton Mettre à jour pour mettre à jour la configuration.
4	Cliquez sur le bouton OK ou Appliquer pour enregistrer les modifications.

Suppression d'une voie

Pour supprimer une voie existante :

Etape	Action
1	Cochez la case correspondant à la voie client ou serveur.
2	Cliquez sur le bouton Supprimer .
3	- Cliquez sur le bouton Appliquer pour enregistrer les modifications. - ou - - Cliquez sur OK pour enregistrer les modifications et fermer la boîte de dialogue.

Configuration d'équipement DNP3

Introduction

Pour faciliter les communications avec le module BMENOR2200H, configurez les paramètres des protocoles de communication DNP3 dans l'onglet PARAMETRES CLIENT ou PARAMETRES SERVEUR du DTM.

Accès à l'onglet Configuration

Accédez aux paramètres de configuration dans Control Expert :

Etape	Action
1	Accédez à la configuration DTM de votre module.
2	Vérifiez que vous avez déjà créé des voies client ou serveur.
3	Dans le menu CONFIGURATION , développez (+) le sous-menu Voies/Equipements .
4	Effectuez une sélection dans le sous-menu Voies/Equipements : • Serveur NET DNP3 • Client NET DNP3 • Serveur série DNP3 • Client série DNP3
5	Sélectionnez une voie / un équipement spécifique dans le sous-menu.
6	Sélectionnez l'onglet PARAMETRES CLIENT ou PARAMETRES SERVEUR correspondant à la voie.
7	Configurez les paramètres.
8	• Sélectionnez Appliquer pour appliquer vos modifications de configuration. • Sélectionnez OK pour implémenter vos modifications et fermer la boîte de dialogue.

Description des paramètres d'équipement DNP3

Les tableaux ci-après décrivent les paramètres de réseau client/serveur DNP3 qui apparaissent dans l'onglet PARAMETRES CLIENT/SERVEUR.

NOTE: Lorsque la fenêtre Control Expert est active, vous pouvez déplacer le curseur sur n'importe quel champ pour afficher une description de la fonctionnalité correspondante et de la plage de valeurs disponible.

The screenshot shows the 'PARAMETRES AVANCES' (Advanced Parameters) tab in the DNP3 configuration software. The interface is divided into two main sections: 'PARAMETRES' (Parameters) and 'PARAMETRES AVANCES' (Advanced Parameters). The 'PARAMETRES' section includes fields for 'Adresse locale' (Local Address) set to 4 and 'Adresse maître' (Master Address) set to 3. The 'PARAMETRES AVANCES' section contains numerous configuration options, including timeouts, retries, and synchronization modes. Key parameters include 'Période d'état du lien' (Link State Period) at 2500 ms, 'Période de validité de l'horloge' (Clock Validity Period) at 1800000 ms, and various timeouts for SBO and confirmation. The interface also features checkboxes for enabling/disabling certain functions like 'Activer l'adressage automatique' and 'Autoriser les réponses multi-fragments'. A sidebar on the left shows the navigation tree with options like 'Sélection de version', 'Communication', and 'Voies / Equipements'.

PARAMETRES :

Paramètre	Client	Serveur	Indépendance des voies ¹	Description
Adresse locale	✓	✓	✓	Ce champ contient l'adresse source de la session.
Adresse du client	✓	✓	✓	Ce champ contient l'adresse du client distant (destination) pour la session.
Temporisation de réponse par défaut	✓			Entrez une valeur pour la temporisation par défaut de la confirmation de requête. - La plage de valeurs va de 0 à 4294967295. - La valeur par défaut est 3000.

PARAMÈTRES AVANCÉS :

Paramètre	Client	Serveur	Indépendance des voies ¹	Description
Période d'état du lien	✓	✓	✓	Configurez la fréquence (ms) de transmission des requêtes d'état quand aucune trame DNP3 n'est reçue au cours de la session. NOTE: Assurez-vous que la période d'état du lien du client et du serveur est réglée sur une valeur différente de zéro, par exemple 2 s. Si la période d'état du lien est réglée sur zéro, lors d'un basculement Hot Standby, le module ne peut pas créer de nouvelle connexion car l'ancienne connexion n'est pas en situation de timeout.
Intégrité auto - Local	✓			Effectuer une interrogation des données d'intégrité après réglage et mise à zéro du bit IIN local. • (Par défaut : sélectionné)
Intégrité auto - Temporisation	✓			Effectuer une interrogation des données d'intégrité à l'expiration de la temporisation. • (Par défaut : désélectionné)
Interrogation d'événements auto	✓			Effectuer une interrogation des données d'événement lorsque le bit IIN de classe 1, 2 ou 3 est défini. • (Par défaut : désélectionné)
Mesure de délai auto	✓			Utiliser la mesure du retard dans la synchronisation temporelle. • (Par défaut : désélectionné)
Synchronisation horaire auto	✓			Effectuer la synchronisation horaire au moment opportun (bit IIN esclave défini). • Néant : ne pas effectuer de synchronisation horaire. • Série : utiliser la méthode série. • LAN : utiliser la méthode LAN. • (Par défaut : Néant)
Auto non sollicités	✓			Envoyer automatiquement une commande non sollicitée lors du démarrage de l'équipement distant. • Néant : ne pas envoyer de commande non sollicitée. • Désactiver : envoyer une commande de désactivation. • (Par défaut : Néant)
Activation auto non sol class 1	✓			Indiquer quelles classes d'événements doivent être activées pour la génération de rapports non sollicités. • (Par défaut : Néant)
Activation auto non sol class 2	✓			Indiquer quelles classes d'événements doivent être activées pour la génération de rapports non sollicités. • (Par défaut : Néant)
Activation auto non sol class 3	✓			Indiquer quelles classes d'événements doivent être activées pour la génération de rapports non sollicités. • (Par défaut : sélectionné)
Temporisation de lecture autorisée	✓			Nombre de fois qu'une requête de lecture est autorisée à passer en mode timeout avant que la session soit considérée comme étant déconnectée. • (Min : 0, Max : 255, Par défaut : 0)
Dépassement d'intégrité automatique	✓			Dépassement d'intégrité automatique. • (Par défaut : sélectionné)
Valider l'adresse source		✓	✓	Cochez cette case pour valider l'adresse source dans les trames reçues.
Activer l'adressage automatique		✓	✓	Cochez cette case pour que le serveur réponde à l'adresse 0xffff comme s'il avait reçu une requête à son adresse configurée. Le serveur répond avec sa propre adresse afin que le client puisse détecter automatiquement l'adresse du serveur.
Autoriser les réponses multi-fragments		✓	✓	Cochez cette case pour permettre à l'application d'envoyer des réponses à plusieurs fragments.
Confirmation multi-fragments		✓	✓	Cochez cette case pour demander des confirmations de couche d'application pour les fragments non finaux d'une réponse à plusieurs fragments. (Les confirmations de la couche d'application sont toujours demandées pour les réponses qui contiennent des événements.)
Délai d'exigibilité de la réponse		✓	✓	Cochez cette case pour demander à l'équipement de définir le bit IN de temps nécessaire en réponse à cette session lors du démarrage qui suit l'expiration de la période de validité de l'horloge.
Période de validité d'horloge		✓	✓	Configurez la durée (ms) pendant laquelle l'horloge locale reste valide après réception d'une synchronisation d'horloge.

Paramètre	Client	Serveur	Indépendance des voies ¹	Description
Timeout de confirmation de l'application		✓	✓	Configurez la durée (ms) pendant laquelle l'équipement serveur DNP3 attend une confirmation de la couche application de la part du client pour une réponse sollicitée.
Timeout SBO (sélection avant opération)		✓	✓	Configurez la durée maximale (ms) pendant laquelle une sélection reste valide avant la réception de l'opération correspondante.
Délai de redémarrage à chaud		✓	✓	Configurez la durée d'attente du client après qu'il a reçu une réponse à une demande de redémarrage à chaud. Cette valeur est codée dans un objet fin de temporisation dans la réponse à une requête de redémarrage à chaud.
Délai de redémarrage à froid		✓	✓	Configurez la durée (en ms) pendant laquelle le client attend après avoir reçu une réponse à une demande de redémarrage à froid. Cette valeur est codée dans un objet fin de temporisation en réponse à une requête de redémarrage à froid.
Autoriser les requêtes multi-CROB		✓	✓	Cochez cette case pour autoriser plusieurs objets CROB (control relay block object) dans une même requête.
Nbre maxi. de requêtes de contrôle		✓	✓	Configurez le nombre maximum de sorties de contrôle binaires (CROB) ou analogiques autorisées dans une seule requête.
Autorisation des non sollicités		✓	✓	Cochez cette case pour autoriser les réponses non sollicitées.
Envoi des non sollicités quand en ligne		✓	✓	Cochez cette case pour envoyer des réponses nulles non sollicitées lorsque la session est en ligne.
Non soll classe 1 - Événements max		✓	✓	Lorsque les réponses non sollicitées sont activées, configurez cette valeur pour spécifier le nombre maximum d'événements de la classe correspondante (1, 2 ou 3) qui sont autorisés avant qu'une réponse non sollicitée soit générée.
Non soll classe 2 - Événements max		✓	✓	
Non soll classe 3 - Événements max		✓	✓	
Non soll classe 1 - Délai max		✓	✓	Configurez la durée maximale (ms) après la réception d'un événement de la classe correspondante (1, 2 ou 3) au bout de laquelle une réponse non sollicitée est générée.
Non soll classe 2 - Délai max		✓	✓	
Non soll classe 3 - Délai max		✓	✓	
Tentatives maxi. non soll.		✓	✓	Configurez le nombre maximum de tentatives non sollicitées avant l'adoption de la valeur des tentatives hors ligne.
Délai de tentative non soll.		✓	✓	Configurez la durée du délai (ms) après une réponse non sollicitée.
Délai de tentative hors ligne non soll		✓	✓	Configurez la durée du délai (ms) après un timeout non sollicité avant de tenter à nouveau la réponse non sollicitée au bout du nombre de Tentatives maxi. non soll. configuré.
Supprimer l'événement le plus ancien		✓	✓	Configurez le comportement en cas de file d'attente d'événements saturée : • Sélectionné: Supprimer l'événement le plus ancien. • Désélectionné: Supprimer l'événement le plus récent.
Valeurs vers Class0Poll		✓	✓	Configurez le type de valeur qui est renvoyé dans une interrogation de données de classe 0 : • Valeur de comptage : Renvoie une valeur de compteur binaire statique. • Valeur gelée : Renvoie une valeur de compteur gelé statique.
Mode SBO		✓		Sélectionnez un mode pour une opération avant et après : • Mode interférence : Le serveur annule la sélection si la requête reçue suivante n'est pas une requête d'opération. (Seules les requêtes de lecture sont traitées.) • Mode sans interférence : Le serveur n'annule pas la sélection même si la requête reçue suivante n'est pas une demande d'opération en suivant la sélection. Le groupe DNP3 recommande cette sélection.
Timeout de confirmation non sollicité		✓	✓	Configurez la valeur d'un timeout de confirmation non sollicité.

Paramètre	Client	Serveur	Indépendance des voies ¹	Description
Mode de synchronisation des données		✓		Sélectionnez un mode de synchronisation des données : • Synchronisation cyclique : Utilisez la synchronisation (cyclique) par défaut. • Synchronisation à la demande : Permet à l'application d'automate d'implémenter des modifications locales sur la sortie binaire ou analogique. NOTE: L'activation d'un point Synchronisation à la demande modifie la structure de variable (hors du DDT d'équipement).
Mode de déclenchement-fermeture		✓		Sélectionnez une option : • Mode consécutif • Mode pair
Préfixe				Cette chaîne fait partie du nom de variable pour les points de sortie analogiques ou binaires lorsque vous sélectionnez Synchronisation à la demande comme Mode de synchronisation des données (page : 1 à 6). Remarques : • Utilisez des noms de préfixe uniques pour chaque module BMENOR2200H. Les noms en double entraînent l'écrasement des variables. • En mode Synchronisation à la demande, les points de routage côté client pour l'état de sortie analogique ou binaire ne prennent pas en charge le mappage côté serveur. • Un trait de soulignement (_) n'est pas un caractère de fin valide dans le Préfixe. • En mode Synchronisation à la demande, le Préfixe consomme 7 caractères. La longueur restante disponible pour le nom de variable est donc réduite à 23 caractères.
NOTE: 1 Les paramètres cochés dans la colonne <i>Indépendance des voies</i> peuvent être configurés indépendamment et respectivement sur chaque voie serveur, une fois que la fonction <i>session multiple</i> est activée.				

Mappage des objets de données DNP3

Introduction

En vue de faciliter les communications avec le module BMENOR2200H, créez des points de données pour le protocole de communication DNP3 dans l'onglet **MAPPAGES DE DONNEES** du DTM.

Accès à l'onglet Configuration

Accédez aux paramètres de configuration dans l'onglet **MAPPAGES DE DONNEES** de Control Expert :

Etape	Action
1	Accédez à la configuration DTM de votre module.
2	Vérifiez que vous avez déjà créé des voies client ou serveur.
3	Dans le menu CONFIGURATION , développez (+) le sous-menu Voies/Equipements .
4	Effectuez une sélection dans le sous-menu VoiesEquipements : • Serveur NET DNP3 • Client NET DNP3 • Serveur série DNP3 • Client série DNP3
5	Sélectionnez une voie spécifique dans le sous-menu.
6	Sélectionnez l'onglet MAPPAGES DE DONNEES pour la voie.
7	Configurez les paramètres de mappage de données.
8	• Sélectionnez Appliquer pour appliquer vos modifications de configuration. • Sélectionnez OK pour appliquer les modifications et fermer la boîte de dialogue.

Mappages de données DNP3

En utilisant une **Entrée binaire** comme exemple, modifiez la configuration des points de données dans l'onglet **MAPPAGES DE DONNEES** :

CONFIGURATION

Sélection de version

Communication

Configuration des voies

SNMP

Service de temps réseau

Port Ethernet

Port série

Voies / Equipements

Serveur NET DNP3

Journalisation des données

Général

Exporter / Importer

Informations module

SERVEURPARAMETRESÉVÉNEMENTSMAPPAGES DE DONNEES

MAPPAGES DE DONNEES

Sélectionner l'ID de type : Sélectionner un identificateur de typeAjouterSupprimer

Rechercher	Identification de type	Numéro de point	Quantité de données	Adresse de point CPU	Nom de variable
☐	Entrée binaire	0	1		BI_P0
☐	Entrée binaire	1	1		BI_P1
☐	Entrée analogique	0	1		AI_P0
☐	Entrée analogique	1	1		AI_P1

ENTREE BINAIRE

Numéro de point : 0

Nombre de points : 1

Nombre de points : BI_PO

Mapping des registres CPU : Valeur uniquement

Nom de point : Entrée binaire g1v1

Variation statique par défaut : Entrée binaire g1v1

Variation événementielle par défaut : Entrée binaire g2v1

Masque de classe d'événement : ☒ Class0

Etat automate : Qualité non impactée

☐ Class1

☐ Class2

☐ Class3

☐ Non sollicité

Etape	Action
1	Dans Sélectionner l'ID de type , sélectionnez un ID de type. NOTE: En l'occurrence, sélectionnez Entrée binaire .
2	Cliquez sur Ajouter pour voir le nom "Entrée binaire" dans la colonne Identification de type .
3	Sélectionnez la ligne correspondant à la nouvelle entrée binaire pour afficher les options de configuration correspondant au type ENTREE BINAIRE .
4	Modifiez les paramètres. NOTE: Lorsque la fenêtre Control Expert est active, vous pouvez déplacer le curseur sur n'importe quel champ pour afficher une description de la fonctionnalité correspondante et de la plage de valeurs disponible.
5	- Sélectionnez Appliquer pour appliquer vos changements de configuration. - Sélectionnez OK pour implémenter vos modifications et fermer la boîte de dialogue.

Objet de données Contrôleur échangeable

⚠

AVERTISSEMENT

FONCTIONNEMENT IMPREVU DE L'EQUIPEMENT

Ne créez pas une instance d'accès redondant aux données.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Implémentez le dictionnaire de données dans Control Expert :

Etape	Action
1	Ouvrez les Options du projet (Outils > Options du projet) .
2	Développez (+) le menu : Options du projet > Général
3	Sélectionnez le paramètre Données intégrées de l'automate pour afficher les colonnes Etiquette de propriété et Valeur de propriété .
4	Dans la colonne Etiquette de données, recherchez la ligne Dictionnaire de données et cochez la case correspondante dans la zone Valeur de propriété. NOTE: Cochez cette case lorsque vous programmez l'application de l'automate. Sinon, les variables non localisées risquent de ne pas être mappées en points de données RTU. Toutefois, une application compilée consomme davantage de mémoire lorsque le dictionnaire de données est inclus, ce qui peut avoir un impact sur les variables non localisées implémentées dans des solutions RTU.
5	- Sélectionnez Appliquer pour appliquer vos changements de configuration. - Sélectionnez OK pour implémenter vos modifications et fermer la boîte de dialogue.

Les variables non localisées peuvent être échangées entre le contrôleur et le module BMENOR2200H une fois que vous avez défini et géré le mappage mémoire du contrôleur pour échanger des données avec le module.

Les objets de données du contrôleur sont mappés et liés uniquement pour l'usage du module BMENOR2200H.

Echange de données

Pour maintenir un débit élevé d'échange de données, l'utilisateur peut définir la mémoire RTU du module BMENOR2200H pour les objets de données dans un type de données ARRAY séquentiel afin de regrouper les points présentant les mêmes paramètres.

Utilisez des numéros de points consécutifs (0, 1, 2, 3...) dans les fragments de requête DNP3. Une rupture dans la séquence des numéros entraînera l'indisponibilité de certains points DNP3.

Liste des commandes prédéfinies

Les champs de saisie requis sont nécessaires pour définir un élément de commande prédéfini pour client DNP3/client NET DNP3.

Nom de variation statique de DNP3

Type d'objet de données	Variation statique
Binary Input	g1v1 Binary In
	g1v2 Binary In Flag
Double Input	g3v1 Double In
	g3v2 Double In Flag
Binary Output	g10v1 Binary Out
	g10v2 Binary Out Flag
Binary Counter	g20v1 32bit Counter
	g20v2 16bit Counter
	g20v5 32bit Ctr No Flag
	g20v6 16bit Ctr No Flag
Frozen Counter	g21v1 32bit Frozen Ctr Flag
	g21v2 16bit Frozen Ctr Flag
	g21v5 32bit Frozen Ctr Flag Time
	g21v6 16bit Frozen Ctr Flag Time
	g21v9 32bit Frozen Counter
	g21v10 32bit Frozen Counter
Analog Input	g30v1 32bit Analog In
	g30v2 16bit Analog In
	g30v3 32bit AI No Flag
	g30v4 16bit AI No Flag
	g30v5 Short Float AI
Analog Input Deadband	g34v1 16bit AI Deadband
	g34v2 32bit AI Deadband
	g34v3 Short Float AI Deadband
Analog Input Dband_Ctrl	g34v1 16bit AI Deadband
	g34v2 32bit AI Deadband
	g34v3 Short Float AI Deadband
Analog Output	g40v1 32bit Analog Output
	g40v2 16bit Analog Output
	g40v3 Short Float AO
Read_Group	—
Read_Class	—
Write_Octet_String	—
Freeze_Counter	—
Unsolicited_Class	—
Time_Sync	—
Restart	—
Octet String	Chaînes d'octets g110
Integrity_Poll	—
Gen_Events	—
Clear_Events	—

Tables de mappage

Selon le type d'objet de données et le profil de protocole sélectionné, différents champs de configuration sont nécessaires pour définir un élément de mappage d'objets de données. Les tableaux ci-dessous décrivent les paramètres disponibles pour chaque sélection possible dans le menu déroulant **Sélectionner l'ID de type** des onglets **MAPPAGES DE DONNEES** client et serveur.

NOTE: Ces tableaux incluent de brèves descriptions de chaque paramètre de mappage de données. Lorsque la fenêtre Control Expert est active, vous pouvez déplacer le curseur sur n'importe quel champ pour voir une description de la fonctionnalité correspondante et la plage de valeurs disponible.

Entrée binaire

Le tableau suivant décrit les paramètres du client NET DNP3 qui apparaissent dans l'onglet **MAPPAGES DE DONNEES** lorsque vous sélectionnez une **Entrée binaire** dans l'onglet **MAPPAGES DE DONNEES** :

Paramètre client		Description
Numéro de point		Indique le numéro de début du point. NOTE: Vérifiez que les numéros de point DNP3 commencent à 0 et sont consécutifs en mode serveur. Si cette règle n'est pas appliquée, les points non consécutifs ne peuvent pas fonctionner normalement.
Nombre de points		Indique le nombre de points.
Enregistrer sur le contrôleur		Choisissez une source pour l'horodatage et l'indicateur d'événement : • Valeur uniquement : heure du module • Valeur avec heure : heure du registre contrôleur • Valeur avec indicateur : informations d'indicateur de point provenant des registres du contrôleur • Valeur avec indicateur et heure : indicateur et heure provenant des registres du contrôleur
Nom du point		Nom du registre non localisé
Variation statique		Sélectionnez la variation statique du point de données.
Routage d'événements	Voie de routage	• Désactiver : Désactiver le routage pour la voie. • Activer : Activer le routage pour la voie.
	Point de routage	Numéro de point à router. (Ce numéro de point apparaît côté serveur mais ne peut pas être modifié côté serveur.)
	Masque de classe d'événements	Définit la classe d'événements des points. <i>Unsolicited</i> n'est pas autorisé avec class 0 uniquement. Dans le client, <i>Channel</i> vaut 0.
	Variation événementielle par défaut	Indique la variation d'événement par défaut du point de données.
	Routage hors ligne	Spécifiez l'indicateur lorsque la voie de routage est hors ligne : • Qualité valide : Utiliser toute connexion de voie de routage disponible. • Qualité non valide sans événements : Définir l'indicateur de déconnexion lorsque la voie de routage est hors ligne. • Qualité non valide avec événement : ◦ Définir l'indicateur de non validité du point lorsque la voie de routage est hors ligne. ◦ Générer un événement avec la valeur d'indicateur reçue lorsque la voie de routage est en ligne. L'intégrité générale est tout d'abord démarrée (si l'intégrité générale est activée dans le client).

Le tableau suivant décrit les paramètres du serveur NET DNP3 qui apparaissent dans l'onglet **MAPPAGES DE DONNEES** lorsque vous sélectionnez une **Entrée binaire** dans l'onglet **MAPPAGES DE DONNÉES** :

Paramètre serveur	Description
Numéro de point	Indique le numéro de début du point. NOTE: Les numéros de point DNP3 commencent à 0 et sont consécutifs en mode serveur. Si cette règle n'est pas respectée, les points non consécutifs ne fonctionnent pas normalement.
Nombre de points	Indique le nombre de points.
Mappage des registres contrôleur	Choisissez une source pour l'horodatage et l'indicateur d'événement : • Valeur uniquement : heure du module • Valeur avec heure : heure du registre contrôleur • Valeur avec indicateur : informations d'indicateur de point provenant des registres du contrôleur • Valeur avec indicateur et heure : indicateur et heure provenant des registres du contrôleur NOTE: Sélectionnez l'une de ces valeurs pour implémenter SOE pour l'horodatage.
Nom du point	Nom du registre non localisé
Variation statique par défaut	Sélectionnez la variation statique par défaut du point de données.
Variation événementielle par défaut	Sélectionnez la variation d'événement par défaut pour le point de données.
Masque de classe d'événements	Définit la classe d'événements des points. <i>Unsolicited</i> n'est pas autorisé avec class 0 uniquement. Dans le client, <i>Channel</i> vaut 0.
Etat de l'automate	Spécifiez l'indicateur lorsque la voie de routage est hors ligne : • Qualité non impactée : La qualité est valide lorsque l'automate est en marche. • Qualité impactée : Si l'automate est arrêté ou retiré du rack, la qualité est non valide.

Entrée analogique

Ce tableau décrit les paramètres de mappage des données du client pour les types d'entrée analogiques :

Paramètre client		Description
Numéro de point		Indique le numéro de début du point. NOTE: Vérifiez que les numéros de point DNP3 commencent à 0 et sont consécutifs en mode serveur. Si cette règle n'est pas appliquée, les points non consécutifs ne peuvent pas fonctionner normalement.
Nombre de points		Indique le nombre de points.
Enregistrer sur le contrôleur		Choisissez une source pour l'horodatage et l'indicateur d'événement : • Valeur uniquement : heure du module • Valeur avec heure : heure du registre contrôleur • Valeur avec indicateur : informations d'indicateur de point provenant des registres du contrôleur • Valeur avec indicateur et heure : indicateur et heure provenant des registres du contrôleur
Variation statique		Sélectionnez la variation statique du point de données.
Nom du point		Nom du registre non localisé
Afficher la bande morte dans la variable		Spécifiez un nom de variable de zone morte.
Nom du point		Nom du registre non localisé lorsque l'option Afficher la bande morte dans la variable est sélectionnée.
Routage d'événements	Voie	Activez ou désactivez le routage du numéro de voie.
	Point de routage	Définissez le numéro de point à router.
	Masque de classe d'événements	Définit la classe d'événements des points. <i>Unsolicited</i> n'est pas autorisé avec class 0 uniquement. Dans le client, vérifiez que <i>Channel</i> est à 0 pour les opérations normales.
	Variation événementielle par défaut	Indique la variation d'événement par défaut du point de données.
	Routage hors ligne	Spécifiez l'indicateur lorsque la voie de routage est hors ligne : • Qualité valide : Utiliser toute connexion de voie de routage disponible. • Qualité non valide sans événements : Définir l'indicateur de déconnexion lorsque la voie de routage est hors ligne. • Qualité non valide avec événement : ◦ Définir l'indicateur de non validité dans l'événement lorsque la voie de routage est hors ligne. ◦ Générer un événement avec la valeur d'indicateur reçue lorsque la voie de routage est en ligne. L'intégrité générale est tout d'abord démarrée (si l'intégrité générale est activée dans le client).

Ce tableau décrit les paramètres de mappage des données du serveur pour les types d'entrée analogique :

Paramètre serveur	Description
Numéro de point	Indique le numéro de début du point. NOTE: Vérifiez que les numéros de point DNP3 commencent à 0 et sont consécutifs en mode serveur. Si cette règle n'est pas appliquée, les points non consécutifs ne peuvent pas fonctionner normalement.
Nombre de points	Indique le nombre de points.
Masque de classe d'événements	Définit la classe d'événements des points. Dans le client, vérifiez que <code>Channel</code> est à 0 pour les opérations normales.
Variation statique par défaut	Sélectionnez la variation statique par défaut du point de données.
Variation événementielle par défaut	Sélectionnez la variation d'événement par défaut pour le point de données.
Mappage des registres contrôleur	Choisissez une source pour l'horodatage et l'indicateur d'événement : • Valeur uniquement : heure du module • Valeur avec heure : heure du registre contrôleur • Valeur avec indicateur : informations d'indicateur de point provenant des registres du contrôleur • Valeur avec indicateur et heure : indicateur et heure provenant des registres du contrôleur NOTE: Sélectionnez l'une de ces valeurs pour implémenter SOE pour l'horodatage.
Bande morte	Valeur de bande morte de l'entrée analogique
Utiliser les données de pourcentage	Utiliser une plage basse et haute pour le pourcentage de calcul de la bande morte lorsque cette case est cochée.
Plage basse	Valeur la plus basse de la plage lorsque la case Utiliser les données de pourcentage est cochée.
Plage haute	Valeur la plus élevée de la plage lorsque la case Utiliser les données de pourcentage est cochée.
Nom du point	Nom du registre non localisé
Etat de l'automate	Spécifiez l'indicateur lorsque la voie de routage est hors ligne : • Qualité non impactée : La qualité est valide lorsque l'automate est en marche. • Qualité impactée : Si l'automate est arrêté ou retiré du rack, la qualité est non valide.
Afficher la bande morte dans la variable	Spécifiez un nom de variable de zone morte.
Nom du point	Nom du registre non localisé lorsque la case Afficher la bande morte dans la variable est cochée.

Sortie binaire

Le tableau suivant décrit les paramètres de mappage des données du client pour les types de sortie binaires :

Paramètre client	Description
Numéro de point	Indique le numéro de début du point. NOTE: Vérifiez que les numéros de point DNP3 commencent à 0 et sont consécutifs en mode serveur. Si cette règle n'est pas appliquée, les points non consécutifs ne peuvent pas fonctionner normalement.
Nombre de points	Indique le nombre de points.
Mode de fonctionnement	Mode de fonctionnement sélectionné
Type de code de contrôle	Spécifiez le code de contrôle utilisé par le CROB : • Latch_On_Off : Déclencher le CROB. • Pulse_On : Modifier la valeur. NOTE: Reportez-vous à la description du comportement des sorties binaires .
Durée d'impulsion	Spécifiez la largeur de l'impulsion (ms).
Nom du point	Nom du registre non localisé
Ajouter CMD_STATUS	Spécifiez le nom de la variable CMD_STATUS.

Paramètres de mappage des données du serveur pour les types de sortie binaires :

Paramètre serveur	Description
Numéro de point	Indique le numéro de début du point. NOTE: Vérifiez que les numéros de point DNP3 commencent à 0 et sont consécutifs en mode serveur. Si cette règle n'est pas appliquée, les points non consécutifs ne peuvent pas fonctionner normalement.
Nombre de points	Indique le nombre de points.
TCC	Utilisé pour créer le code TCC (Trip Close Control) des CROB. Si cette option est activée, le point impair de cette configuration est une sortie de fermeture et le point suivant est une sortie de déclenchement lorsque la station satellite reçoit une commande de fermeture ou de déclenchement. Dans ce cas, assurez-vous que le nombre de points est pair. La valeur par défaut est <i>Aucun</i>.
Durée d'impulsion courte	Indique la durée d'impulsion préconfigurée du serveur
Variation statique par défaut	Sélectionnez la variation statique par défaut du point de données.
Variation événementielle par défaut	Sélectionnez la variation d'événement par défaut pour le point de données.
Ajouter une variable d'indicateur	Indiquez le nom de la variable d'indicateur.
Nom du point	Nom du registre non localisé lorsque la case Ajouter une variable d'indicateur est cochée.
Etat de l'automate	Spécifiez l'indicateur lorsque la voie de routage est hors ligne : Qualité non impactée : La qualité est valide lorsque l'automate est en marche. Qualité impactée : Si l'automate est arrêté ou retiré du rack, la qualité est non valide.
Préfixe	Ce préfixe du nom de variable est suivi d'un trait de soulignement (_). Configurez le préfixe dans les paramètres avancés du serveur. Exemple : RTU001_Point1.
Type de registre du contrôleur	La seule option disponible pour la sortie binaire est %MW.
Adresse de registre du contrôleur	C'est l'adresse %MW de début dans le contrôleur. Ce champ ne s'applique qu'aux variables localisées. Pour créer une variable sans adresse %MW, utilisez la valeur -1. Remarques : - La valeur de sortie binaire (0 ou 1) est le bit 0 du %MW (INT) dans la liste de variables globales. Les données d'indicateur de sortie binaire restent dans le DDT d'équipement. - La plage de %MW dépend de la plage de registres %MW du contrôleur (2048 par défaut).

NOTE:

- Le paramètre **Binary_Output_Status** est appliqué dans le client, ce qui enregistre la valeur, l'état (indicateur) et l'horodatage les plus récents.

Sortie analogique

Ce tableau décrit les paramètres de mappage des données du client pour les types de sortie analogiques :

Paramètre client	Description
Numéro de point	Indique le numéro de début du point. NOTE: Vérifiez que les numéros de point DNP3 commencent à 0 et sont consécutifs en mode serveur. Si cette règle n'est pas appliquée, les points non consécutifs ne peuvent pas fonctionner normalement.
Nombre de points	Indique le nombre de points.
Mode de fonctionnement	Mode de fonctionnement sélectionné
Variation statique par défaut	Sélectionnez la variation statique par défaut pour le point de données.
Nom du point	Nom du registre non localisé
Ajouter CMD_STATUS	Spécifiez le nom de la variable CMD_STATUS.

Ce tableau décrit les paramètres de mappage des données du serveur pour les types de sortie analogiques :

Paramètre serveur	Description
Numéro de point	Indique le numéro de début du point. NOTE: Vérifiez que les numéros de point DNP3 commencent à 0 et sont consécutifs en mode serveur. Si cette règle n'est pas appliquée, les points non consécutifs ne peuvent pas fonctionner normalement.
Nombre de points	Indique le nombre de points.
Masque de classe d'événements	Définit la classe d'événements des points. <code>Unsolicited</code> n'est pas autorisé avec class 0 uniquement. Dans le client, vérifiez que <code>Channel</code> est à 0.
Variation statique par défaut	Sélectionnez la variation statique par défaut du point de données.
Variation événementielle par défaut	Sélectionnez la variation d'événement par défaut pour le point de données.
Bande morte	Valeur de bande morte du point analogique
Nom du point	Nom du registre non localisé
Ajouter une variable d'indicateur	Indiquez le nom de la variable d'indicateur.
Nom du point	Nom du registre non localisé lorsque la case Ajouter une variable d'indicateur est cochée.
Etat de l'automate	Spécifiez l'indicateur lorsque la voie de routage est hors ligne : • Qualité non impactée : La qualité est valide lorsque l'automate est en marche. • Qualité impactée : Si l'automate est arrêté ou retiré du rack, la qualité est non valide.
Préfixe	Le préfixe du nom de variable est suivi d'un trait de soulignement (<code>_</code>). Configurez le préfixe dans les paramètres avancés du serveur. Le nom de variable final présente le format suivant : <code>Prefix_VariableName.Pointx.value</code> Exemple : <code>RTU001_AO01.Point[10].value</code>
Type de registre du contrôleur	La seule option disponible pour la sortie analogique est %MW.
Adresse de registre CPU	C'est l'adresse %MW de début dans l'automate. Ce champ ne s'applique qu'aux variables localisées. Pour créer une variable sans adresse %MW, utilisez une adresse de début de type float/32 bits. Une valeur de type sortie analogique valide est un nombre pair. Utilisez l'adresse -1. Remarques : • La valeur de sortie analogique figure dans la liste de variables globales. Les données d'indicateur de sortie binaire restent dans le DDT d'équipement. • La plage de %MW dépend de la plage de registres %MW du contrôleur (2048 par défaut).

NOTE:

- Le paramètre **Analog_Output_Status** est appliqué dans le client, ce qui enregistre la valeur, l'état (indicateur) et l'horodatage les plus récents.
- Il est possible d'entrer des valeurs à virgule flottante (notation scientifique) pour la **Plage morte**.

Comportement d'une sortie binaire

Cette configuration dépend de la sélection effectuée pour le champ **Type de code de contrôle** dans les paramètres client de sortie binaire.

La configuration applique **latch on/off**, **pulse on**, et **Pulse/Trip close**.

Selon la situation, trois types de contrôle sont disponibles pour les sorties binaires. Le tableau suivant présente des exemples de numéros de point de déclenchement/fermeture côté client et côté serveur pour le module BMENOR2200H.

CROB envoyé dans le client DNP3	Numéro de point dans le client DNP3	Numéro de point dans le serveur DNP3
Close/Pulse on (mode double)	n	n
Trip/Pulse on (mode double)	n	$n + 1$
Close/Pulse on (mode simple)	n	premier élément de n
Trip/Pulse on (mode simple)		deuxième élément de n

Reportez-vous aux mécanismes de déclenchement suivants pour connaître le type de code de contrôle correspondant :

Op type field	Mécanisme de déclenchement	Description
Pulse_on	toute modification de valeur (0 à 65535)	impulsion en cas de modification de valeur
Latch_on	changement de valeur paire à impaire, par exemple : 0 à 1 2 à 3	mémorisation activée
Latch off	changement de valeur impaire à paire, par exemple : 1 à 0 3 à 2	mémorisation désactivée
Close/Pulse_on	changement de valeur paire à impaire, par exemple : 0 à 1 2 à 3	impulsion en cas de sortie fermeture
Trip/Pulse_on	changement de valeur impaire à paire, par exemple : 1 à 0 3 à 2	impulsion en cas de sortie déclenchement

Impulsions longue et courte des sorties binaires

Cette configuration dépend de la sélection que vous avez effectuée pour ces paramètres dans les paramètres client de sortie binaire :

- **Durée d'impulsion** : Il s'agit du réglage de durée d'impulsion du client.
- **Durée d'impulsion courte** : Indique la durée d'impulsion préconfigurée du serveur

NOTE: La station satellite utilise la **Durée d'impulsion** saisie. La valeur 0 signifie que l'équipement utilise une valeur préconfigurée.

Définition de la valeur mesurée

Appliquer la bande morte d'entrée analogique (**obj34**) pour définir la bande morte de la valeur mesurée. Les paramètres des points mesurés sont activés immédiatement après que le serveur DNP3 a reçu la requête du client DNP3.

Pour le **obj34**DNP3, aucun qualificatif n'est à définir car il applique uniquement le paramètre **deadband**. Définissez la variation statique et le numéro de point au même réglage de l'entrée analogique. La valeur **deadband** d'entrée analogique est appliquée à la fois sur le client DNP3 et le serveur DNP3. Le serveur DNP3 l'utilise pour stocker la valeur actuelle qui est indiquée dans la réponse aux requêtes de lecture ; le client DNP3 l'utilise pour afficher la valeur de **deadband** actuelle qui peut être contrôlée par le serveur via le bloc de contrôle **deadband** d'entrée analogique.

Cette configuration dépend des paramètres de bande morte que vous avez définis dans les champs suivants :

- **Numéro de point** (paramètres d'entrée analogique du client)
- **Numéro de point** (paramètres d'entrée analogique du serveur)
- **Variation statique par défaut** (paramètres d'entrée analogique du serveur)

NOTE: Reportez-vous à la description des paramètres d'entrée analogique du client et du serveur.

Mappage de chaînes d'octets pour DNP3

Dans DNP3, le type Chaîne d'octet s'applique au groupe 110. Il prend en charge les codes de fonction de lecture, d'écriture et de réponse.

Pour le module BMENOR2200H, la chaîne se divise en deux types de points : points d'entrée et points de sortie.

Le client utilise une commande Read_Group pour lire la chaîne d'octet.

Interprétation de la chaîne d'octet du point de vue du client :

- Les points de type **Chaîne d'octet** sont des points d'entrée.
- Les points de type **Chaîne d'octet d'écriture** sont des points de sortie.

Interprétation de la chaîne d'octet du point de vue du serveur :

- Les points de type **Chaîne d'octet** avec accès aux variables de **protocole** sont des points d'entrée pour le client DNP3.
- Les points de type **Chaîne d'octet** avec accès aux variables de **contrôleur** sont des points de sortie du contrôleur.

Longueur des types Chaîne d'octet :

- *maximum* : 255 caractères
- *par défaut* : 16 caractères

Génération d'événements

Accédez à la configuration de commande d'événement dans Control Expert :

Etape	Action
1	Suivez les instructions pour configurer une voie serveur.
2	Développez (+) Voies > Serveur DNP3 NET > <nom du serveur> .
3	Sélectionnez l'un de ces éléments dans le menu déroulant Sélectionner un ID de type de l'onglet MAPPAGES DE DONNEES : • Générer les événements • Effacer des événements
4	Cliquez sur le bouton Ajouter pour afficher les paramètres du type sélectionné : • Générer les événements : ◦ Numéro de point ◦ Nombre de points ◦ Groupe d'objets ◦ Nom du point ◦ Ajouter CMD_STATUS • Effacer des événements : ◦ Groupe d'objets ◦ Nom du point ◦ Ajouter CMD_STATUS NOTE: Lorsque la fenêtre Control Expert est active, vous pouvez déplacer le curseur sur n'importe quel champ pour afficher une description de la fonctionnalité correspondante et de la plage de valeurs disponible.
5	• Cliquez sur le bouton Appliquer pour appliquer vos changements de configuration. • Cliquez sur le bouton OK pour appliquer les modifications et fermer la boîte de dialogue.

NOTE: Les protocoles IEC60870-5-101/104 ne prennent pas en charge la génération d'événements.

Effacement d'événements sur le serveur

Clear_Events prend en charge un nouveau type de point qui efface le tampon d'événements dans les serveurs DNP3 et IEC60870-5-101/104. Cette opération peut être effectuée dans un système SCADA local ou distant, en mappant la mémoire.

Pour créer *Clear_Events* pour ces serveurs, sélectionnez Data Mapping.

Lorsque la valeur du registre *Clear_Events* change, le module BMENOR2200H efface les événements du groupe d'objets dans la configuration.

Paramètre	Portée de la valeur	Définition
<i>Groupe d'objets</i>	<i>All ObjectsBinary InputDouble InputBinary CounterAnalog InputBinary OutputAnalog Output</i>	Spécifie le groupe d'objets dont l'événement est effacé sur demande
<i>Nom de variable</i>	—	Indique le nom du registre localisé.

Paramètres d'événement DNP3

Les paramètres de génération d'événements décrits dans les tableaux suivants sont disponibles après la création d'une instance de l'ID de type correspondant. Sélectionnez l'instance *Générer les événements* ou *Effacer des événements* dans le tableau **Mappages de données** pour afficher les paramètres.

Paramètres pour *Générer les événements* :

Paramètre	Description
<i>Numéro de point</i>	Numéro de départ du point (min : 0, max : 65535, par défaut : 0)
<i>Nombre de points</i>	Nombre de points (min : 0, max : 7000, par défaut : 1)
<i>Groupe d'objets</i>	Groupe d'objets à lire (par défaut : entrée binaire)
<i>Nom du point</i>	Nom du registre localisé ou non localisé (par défaut : -, symbole interdit : {} " [], longueur maximum : 50), par défaut : CE_P0_P0
<i>Ajouter CMD_STATUS</i>	<i>sélectionné</i> : Spécifier un nom de variable CMD_STATUS.
	<i>désélectionné</i> : Aucun nom de variable CMD_STATUS n'est spécifié.

Paramètres pour *Effacer des événements* :

Paramètre	Description	
Groupe d'objets	Groupe d'objets à lire (par défaut : entrée binaire)	
Nom du point	Nom du registre localisé ou non localisé (par défaut : -, symbole interdit : {} " [], longueur maximum : 50), par défaut : CE_P0_P0	
Ajouter CMD_STATUS	sélectionné : Spécifier un nom de variable CMD_STATUS.	
	désélectionné : Aucun nom de variable CMD_STATUS n'est spécifié.	
Masque de voie	Voie principale	Cochez la case <i>Masque de voie</i> appropriée pour spécifier le numéro de voie en vue d'effacer un groupe d'objets. NOTE: Cette fonctionnalité dépend de la configuration.
	Voie virtuelle-1	
	Voie virtuelle-2	
	Voie virtuelle-3	

Page de définition d'une file d'attente d'événements

Configurez les paramètres de l'onglet **Evénements** pour mapper l'état de la file d'attente d'événements sur les registres de DDT d'équipement du contrôleur. Chaque état de la file d'attente d'événements consomme un registre de trois octets.

NOTE: Lorsque le nombre d'événements dépasse la taille de tampon configurée, les événements sont perdus ou remplacés.

Accédez à la configuration de la file d'événements dans Control Expert :

Etape	Action
1	Développez : Voies/équipements <Serveur DNP3 NET><Nom du serveur>
2	Effectuez une sélection dans le menu déroulant Sélectionner un ID de type de l'onglet EVENEMENTS
3	Cliquez sur le bouton Ajouter pour afficher les paramètres du type sélectionné : • Mode de conservation des événements • Nbre maxi. d'événements • Configuration de tampon • Nbre maxi. d'événements-1 • Nbre maxi. d'événements-2 • Nbre maxi. d'événements-3 • Sauvegarde des événements NOTE: Lorsque la fenêtre Control Expert est active, vous pouvez déplacer le curseur sur n'importe quel champ pour afficher une description de la fonctionnalité correspondante et de la plage de valeurs disponible.
4	• Cliquez sur le bouton Appliquer pour appliquer vos changements de configuration. • Cliquez sur le bouton OK pour implémenter les modifications et fermer la boîte de dialogue.

Événements DNP3

Introduction

Vous pouvez configurer l'onglet **Événements** pour les voies serveur NET DNP3.

Accès à l'onglet Configuration

Accédez aux paramètres de configuration dans l'onglet **EVENEMENTS** de Control Expert :

Etape	Action
1	Accédez à la configuration DTM de votre module.
2	Vérifiez que vous avez déjà créé des voies client ou serveur.
3	Dans le menu CONFIGURATION , développez (+) le sous-menu Voies/Equipements .
4	Sélectionnez Serveur DNP3 NET dans le sous-menu Voies/Equipements . NOTE: L'onglet EVENEMENTS n'est pas disponible pour les voies Client DNP3 NET .
5	Sélectionnez l'onglet EVENEMENTS .
6	Configurez les paramètres d'événement. NOTE: Les paramètres de l'onglet Événements sont similaires aux paramètres de mappage de données DNP3.
7	Cliquez sur le bouton OK ou Appliquer pour appliquer vos modifications de configuration.

NOTE: Configurez les événements de sécurité DNP3 SAV5 (objet 121/122) dans les pages web.

SEUILS DES STATISTIQUES SAV5

Masque de classe d'événements :

☒ Classe 0 ☐ Classe 1 ☐ Classe 2 ☐ Classe 3 ☐ Non sollicité

Variation événementielle par défaut :

16 bits avec drapeau

Nb max. d'événements par voie :

100

[1 - 10000]

Mode de conservation des événements :

Tout

Sauvegarde des événements :

☐ Classe 1 ☐ Classe 2 ☐ Classe 3

Configuration de voies IEC60870

Introduction

Configurez les communications IEC60870-5-101 et IEC60870-5-104 pour votre module dans le DTM Control Expert.

CONFIGURATION

Sélection de version

Communication

Configuration des voies

SNMP

Service de temps réseau

Ports Ethernet

Port série

Voies / Equipements

Server IEC104

Journalisation des données

Général

Exporter / Importer

Informations module

CLIENTSERVEUR

VOIES SERVEUR

	Non	Nom de la voie :	Protocole :	Type de réseau :	Filtre IP :	Redond	Modifier	Configuration groupée
☐	0	Server_PC	Serveur IEC60870-5-104	TCP-IP	192.168.10.127	1		
☐	1	Server_PC2[Virtual-1]	Serveur IEC60870-5-104	TCP-IP	10.10.10.127	1		
☐	2	Server_PC2[Virtual-2]	Serveur IEC60870-5-104	TCP-IP	192.168.10.128	Aucun		

MODIFIER LA VOIE

Nom de la voie :

Filtre IP :

Protocole :

Type de réseau :

Port local :

Groupe redondant :

Contrôle de liaison active :

Mettre à jourAnnuler

PARAMETRES AVANCEES

Période d'acquiescement T1 (ms) :

Période de test T3 (ms) :

Activer la sauvegarde d'événements :☐

Mode de restauration d'événement :

Attente premier caractère (ms) :

Période de détection de déconnexion (ms) :

Temporisation incrémentielle (ms) :

Période des trames S T2 (ms) :

Valeur K :

Valeur W :

Qualité de l'heure de l'événement :

Taille du tampon de réception :

Supprimer les trames à la déconnexion :☐

CONFIGURATION D'EQUIPEMENT

	Non	Nom de l'équipement	Adresse ASDU	Modifier
☐		Equipement 1	3	

Ajouter nouveauSupprimer

Configuration des paramètres de base

Configurez les voies CLIENT ou SERVEUR :

Etape	Action
1	Accédez à la configuration DTM de votre module.
2	Dans la fenêtre CONFIGURATION ouverte, développez (+) Communication et sélectionnez Configuration des voies . NOTE: L'option de menu Voies/Equipements ne peut pas être développée car aucune voie n'est configurée.
3	Sélectionnez l'onglet approprié : CLIENT : Ajoutez des voies client. SERVEUR : Ajoutez des voies serveur.
4	Cliquez sur le bouton Ajouter nouveau pour afficher les paramètres de configuration AJOUTER UNE NOUVELLE VOIE .
5	Configurez les paramètres conformément à la description des paramètres de configuration d'une nouvelle voie.
6	Cliquez sur le bouton Ajouter pour afficher la nouvelle voie configurée dans le tableau.

Etape	Action
	NOTE: Le menu Equipements peut désormais être développé car il existe au moins un équipement configuré. Tous les équipements configurés apparaissent dans ce menu.
7	Après avoir créé une voie <i>serveur</i> dans l'onglet SERVEUR , répétez les étapes 1 à 6 pour créer la voie <i>client</i> correspondante dans l'onglet CLIENT (ou inversement). NOTE: Un seul client et un seul serveur sont pris en charge.
8	• Cliquez sur le bouton Appliquer pour appliquer les modifications. • Cliquez sur OK pour appliquer les modifications et fermer la boîte de dialogue. NOTE: Lorsque vous créez la première voie, le sous-menu Voies/Equipements s'affiche sur l'écran CONFIGURATION .
9	Répétez les étapes 1 à 8 pour créer des voies supplémentaires en respectant les limites suivantes : • <i>client</i> : ◦ IEC60870-5-104 : 64 connexions ◦ IEC60870-5-101 : 32 connexions • <i>serveur</i> : 4 connexions

Description des paramètres de base

NOTE: Lorsque la fenêtre Control Expert est active, vous pouvez faire glisser le curseur sur n'importe quel champ pour afficher une description de la fonctionnalité correspondante et la plage de valeurs possibles.

Les champs suivants sont disponibles dans **AJOUTER UNE NOUVELLE VOIE** pour les configurations de voies IEC60870-5-101/104 client et serveur :

Champ	Client	Serveur	Description
Nom de la voie	✓	✓	Attribuez un nom au serveur. NOTE: Les pages Web utilisent le paramètre Nom de la voie pour identifier la configuration appliquée à la voie. Par conséquent, attribuez un nom de voie identique lorsque vous configurez les paramètres de cybersécurité.
Protocole	✓	✓	Client IEC60870-5-104 Serveur IEC60870-5-104 Client IEC60870-5-101 Serveur IEC60870-5-101
Adresse IP	✓		Entrez l'adresse IP du serveur avec lequel le client communique. NOTE: Ce champ s'applique à IEC60870-5-104 uniquement.
Port de dest.	✓		Définissez le port de destination. NOTE: Ce champ s'applique à IEC60870-5-104 uniquement.
Filtre IP		✓	Lorsque vous sélectionnez le champ Filtre IP , la boîte de dialogue IP Filter Panel s'ouvre. Entrez l'adresse IP de l'équipement distant. Sélectionnez le bouton OK . NOTE: Ce champ s'applique à IEC60870-5-104 uniquement.
Port local		✓	Définissez le port local pour les communications réseau. • Ce champ s'applique à IEC60870-5-104 uniquement. • La valeur par défaut est 2404.
Groupe redondant		✓	Sélectionnez Aucun, 1 ou 2 dans la liste déroulante. NOTE: Ce champ s'applique à IEC60870-5-104 uniquement.

Configuration des paramètres avancés

Une fois que vous avez créé une voie selon les instructions ci-dessus, la nouvelle voie apparaît dans le tableau de l'onglet **CLIENT** ou **SERVEUR**. Vous pouvez configurer des **PARAMETRES AVANCES** pour cette voie. Les paramètres avancés sont des paramètres globaux qui sont implémentés sur toutes les voies serveur ou client.

Etape	Action
1	Sélectionnez Configuration des voies dans le menu Communication .
2	Sélectionnez l'onglet approprié : • CLIENT : Affiche le tableau VOIE CLIENT. • SERVEUR : Affiche le tableau VOIE SERVEUR.
3	Sélectionnez une ligne dans le tableau.
4	Cliquez sur le bouton Paramètres avancés pour afficher le tableau PARAMÈTRES AVANCÉS . NOTE: Selon la taille de la fenêtre Control Expert, il se peut que vous deviez faire défiler l'onglet Client ou Serveur vers le bas pour afficher les champs des PARAMÈTRES AVANCÉS .
5	Configurez les paramètres conformément à la description des paramètres avancés ci-dessous.
6	• Cliquez sur le bouton Appliquer pour appliquer les modifications. • Cliquez sur OK pour appliquer les modifications et fermer la boîte de dialogue.

Description des paramètres avancés

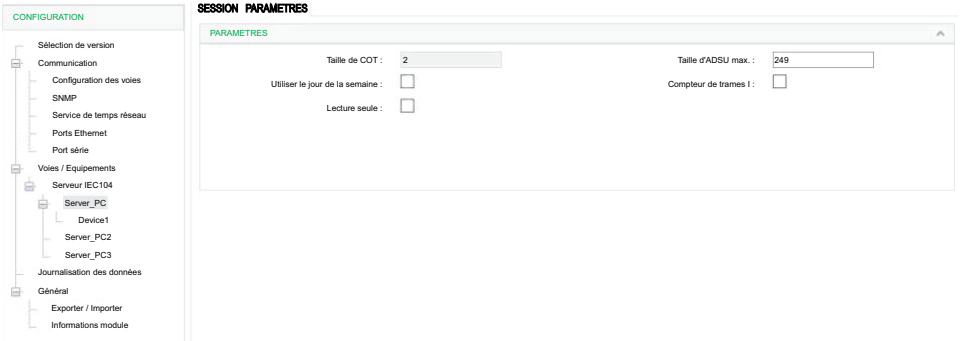
Champ	Client	Serveur	Description
Période d'acquiescement T1 (ms)	✓	✓	Entrez une valeur pour le délai d'attente d'accusé de réception ACK vers une APDU transmise. Le temps T1 du serveur doit être supérieur au temps T2 du client. • La plage de valeurs va de 0 à 4294967295. • La valeur par défaut est 15000.
Période des trames S T2 (ms)	✓	✓	Entrez une valeur de délai d'attente avant l'envoi de l'accusé de réception ACK de l'APDU de supervision. • La plage de valeurs va de 0 à 4294967295. • La valeur par défaut est 10000.
Période de test T3 (ms)	✓	✓	Entrez une valeur de temps d'activité avant l'envoi d'une APDU de test. • La plage de valeurs va de 0 à 4294967295. • La valeur par défaut est 20000.
Valeur K	✓	✓	Entrez une valeur pour le nombre maximum d'APDU transmises non acquittées. • La plage de valeurs va de 1 à 12. • La valeur par défaut est 12.
Attente premier caractère (ms)	✓	✓	Entrez une valeur pour le temps minimum entre réception et transmission. • La plage de valeurs va de 0 à 65535. • La valeur par défaut est 0.
Valeur W	✓	✓	Entrez une valeur pour le nombre maximum d'APDU reçues non acquittées. • La plage de valeurs va de 0 à 32767. • La valeur par défaut est 8.
Taille du tampon de réception	✓	✓	Entrez une valeur pour la taille du tampon de réception du port série (octets). • La plage de valeurs va de 0 à 256. • La valeur par défaut est 256.
Période de détection de déconnexion (ms)	✓	✓	Entrez une valeur pour la période de rétablissement du transfert d'une session déconnectée. • La plage de valeurs va de 0 à 4294967295. • La valeur par défaut est 10000.
Taille maxi file d'attente	✓		Entrez une valeur pour le nombre maximum de messages de requête avec un type ASDU (unité de données spécifique à l'application) et une destination spécifiques correspondant à une requête en attente qui sera mise en file d'attente sur un client. • La plage de valeurs va de 0 à 65535 (file d'attente illimitée). • La valeur par défaut est 0 (file d'attente désactivée).
Temporisation incrémentielle (ms)	✓	✓	Entrez une valeur pour la temporisation incrémentielle de la couche d'application. • La plage de valeurs va de 0 à 4294967295.

Champ	Client	Serveur	Description
			La valeur par défaut est 30000.
Inhibition en cas d'arrêt de l'UC	✓		Cochez cette case pour arrêter l'envoi de commandes lorsque le contrôleur s'arrête.
Activer la sauvegarde d'événements		✓	Indiquez si les événements doivent être sauvegardés en cas de coupure d'alimentation détectée. Par défaut, cette case est désélectionnée.
Event Buffer Sync Enable		✓	- Activer (valeur 1) - Le module NOR primaire synchronise les événements DNP/IEC sur le module NOR redondant pendant l'exécution. - Lorsque le système à redondance (HSBY) bascule, le SCADA peut récupérer les événements à partir du nouveau NOR primaire. Si le taux de génération d'événements lors de l'exécution ne dépasse pas le nombre maximal d'événements pris en charge, les événements ne seront pas perdus. - Désactiver (valeur 0) - Le module NOR primaire ne synchronise pas les événements DNP/IEC sur le module NOR redondant pendant l'exécution. - Le module NOR primaire synchronise l'heure et d'autres données sur le module NOR redondant pendant l'exécution. - Lorsque le système HSBY bascule : - Le module NOR redondant efface les événements générés. - Le module NOR primaire commence à générer des événements. - Si des événements ne sont pas signalés, ils sont perdus et le système SCADA ne peut pas les récupérer à partir du module NOR primaire.
Event Buffer Sync Ports		✓	Sélectionnez le chemin réseau pour transférer les données de synchronisation des événements. - Port d'embase (par défaut) En général, les données de synchronisation interne doivent être transférées via le port d'embase. - Port(s) de contrôle Dans les cas ci-dessous, le chemin de synchronisation peut être déplacé du port d'embase aux ports frontaux. - Le réseau d'embase n'est pas disponible entre le contrôleur/NOR primaire et le contrôleur/NOR secondaire. - L'anneau RIO est très chargé et tout trafic de données supplémentaire doit être évité.

Configuration de session / d'équipement IEC60870

Introduction

Pour faciliter les communications avec le module BMENOR2200H, configurez les paramètres des protocoles de communication IEC60870 dans l'onglet PARAMETRES DE SESSION ou PARAMETRES D'EQUIPEMENT du DTM.



Accès à l'onglet Configuration

Accédez aux paramètres de configuration dans Control Expert :

Etape	Action
1	Accédez à la configuration DTM de votre module.
2	Vérifiez que vous avez déjà créé des voies client ou serveur.
3	Dans le menu CONFIGURATION , développez (+) le sous-menu Voies/Equipements .
4	Effectuez une sélection dans le sous-menu Voies/Equipements : • Serveur IEC60870-5-104 • Client IEC60870-5-104 • Serveur IEC60870-5-101 • Client IEC60870-5-101
5	Sélectionnez une voie/un équipement spécifique dans le sous-menu pour afficher les paramètres de session ou d'équipement.
6	Sélectionnez l'onglet PARAMETRES DE SESSION ou PARAMETRES D'EQUIPEMENT correspondant à la voie.
7	Configurez les paramètres.
8	• Sélectionnez Appliquer pour appliquer vos modifications de configuration. • Sélectionnez OK pour implémenter vos modifications et fermer la boîte de dialogue.

Description des paramètres de session IEC60870

Accédez aux paramètres de session client et serveur.

Client : Sélectionnez les paramètres de session client dans le menu **CONFIGURATION (Voies/Équipements > Client IEC101/104 > Client)** :

Paramètre	Description
<i>Taille de COT</i>	Configurez les octets de COT.
<i>Adresse d'origine du COT</i>	Utilisez comme deuxième octet COT si la longueur de COT est de 2.
<i>Temporisation de réponse par défaut</i>	Il s'agit de la valeur du timeout pour les réponses supprimées. NOTE : Configurez cette valeur pour supprimer de la file d'attente les anciennes réponses qui ne sont plus pertinentes.
<i>Utiliser le jour de la semaine</i>	Désélectionnez cette case pour ignorer dayOfWeek dans IEC60870. NOTE : Certains équipements ne peuvent pas recevoir l'entrée dayOfWeek.
<i>Vérification stricte du COT</i>	Cochez cette case pour appliquer la vérification de COT.

Serveur : Sélectionnez les paramètres de session serveur dans le menu **CONFIGURATION (Voies/Équipements > Serveur IEC101/104 > Serveur)** :

Paramètre	Description
<i>Taille de COT</i>	Configurez les octets de COT.
<i>Utiliser le jour de la semaine</i>	Désélectionnez cette case pour ignorer dayOfWeek dans IEC60870. NOTE : Certains équipements ne peuvent pas recevoir l'entrée dayOfWeek.
<i>Taille d'ADSU max.</i>	Configurez la taille maximale d'une unité de données spécifique à l'application.
<i>Lecture seule</i>	Cochez cette case pour activer le mode lecture seule pour les voies de serveur IEC104.

Description des paramètres d'équipement IEC60870

Les tableaux ci-après décrivent les paramètres de client/serveur IEC60870 qui apparaissent dans l'onglet PARAMETRES CLIENT/SERVEUR.

NOTE: Lorsque la fenêtre Control Expert est active, vous pouvez déplacer le curseur sur n'importe quel champ pour afficher une description de la fonctionnalité correspondante et de la plage de valeurs disponible.

PARAMÈTRES :

Paramètre	Client	Serveur	Description
Adresse commune d'ASDU	✓	✓	Entrez une valeur pour l'adresse commune d'une ASDU. - La plage de valeurs va de 1 à 65535. 65535 est l'adresse de diffusion. - La valeur par défaut est 3. NOTE: L'adresse commune d'ASDU peut être configurée dans l'écran Configuration des voies > Configuration de l'équipement .
Intervalle entre messages cycliques (ms)		✓	Entrez le nombre de millisecondes entre les mises à jour cycliques. - La plage de valeurs va de 1 à 4294967295. - La valeur par défaut est 10000.
Première période cyclique (ms)		✓	Entrez une valeur pour la période de génération de la première réponse de données cyclique. - La plage de valeurs va de 1 à 4294937295. - La valeur par défaut est 500.
Période d'arrière-plan (ms)		✓	Entrez une valeur pour la période de génération des données de scrutation en arrière-plan sur un secteur particulier. - La plage de valeurs va de 1 à 4294967295. - La valeur par défaut est 20000.
Format de lecture de l'heure		✓	Sélectionnez dans la liste déroulante le format d'heure pour la réponse à C_RD_NA : - Néant - CP24 uniquement pour IEC60870-5-101 - CP56 La valeur par défaut est Aucun.

Paramètre	Client	Serveur	Description
Format de mesure et d'heure C_RD_NA		✓	Sélectionnez dans la liste déroulante le format de l'horodatage dans la réponse à la commande de lecture : - Néant - CP24 uniquement pour IEC60870-5-101 - CP56 REMARQUE : - Ce champ est utilisé pour les points mesurés. - La valeur par défaut est Aucun.
Format d'heure C_IC_NA		✓	Sélectionnez dans la liste déroulante le format de l'horodatage dans la réponse à la commande de lecture : - Néant - CP24 uniquement pour IEC60870-5-101 - CP56 REMARQUE : - Ce champ est utilisé pour les compteurs. - La valeur par défaut est Aucun.

NOTE: Lorsque le module reçoit une commande C_RD, il répond à l'objet d'information avec l'adresse IOA (adresse d'objet d'information) demandée. Lorsque plusieurs points de données ont la même IOA, le module renvoie le premier objet d'information dans l'ordre de priorité suivant : M_SP, M_DP, M_ST, M_BO, M_ME_A, M_ME_B, M_ME_C, P_ME_A, P_ME_B, P_ME_C, CUSTOM_M_IT_D. Tenez compte de ces points lorsque vous configurez les communications IEC60870-5-104 côté serveur.

PARAMETRES AVANCES :

Paramètre	Client	Serveur	Description
Temporisation de sélection (ms)		✓	Entrez une valeur pour la période au bout de laquelle une sélection reçue précédemment expire. Assurez-vous qu'une commande exécutée est reçue avant le timeout pour être valide. - La plage de valeurs va de 0 à 4294967295. - La valeur par défaut est 5000.
Temporisation de réponse par défaut (ms)		✓	Entrez une valeur pour la temporisation par défaut de la confirmation de requête. - La plage de valeurs va de 0 à 4294967295. - La valeur par défaut est 60000.
Profondeur du type CMD		✓	Entrez la taille d'une file d'attente de commandes à traiter en parallèle pour chaque type de point. - La plage de valeurs va de 1 à 128. - La valeur par défaut est 1.
Profondeur du secteur CMD		✓	Entrez une valeur pour le nombre total de commandes simultanées prises en charge par le secteur. - La plage de valeurs va de 1 à 128. - La valeur par défaut est 1.
ACTTERM avec consigne C_SE	✓	✓	Cochez la case pour transmettre ACT TERM une fois les commandes de consigne exécutées : C_SE_NA, C_SE_NB, C_SE_TA, C_SE_TB, C_SE_TC NOTE: Cette case est cochée par défaut.
ACTTERM avec commande	✓	✓	Cochez la case pour transmettre ACT TERM à l'achèvement de commandes autres que des commandes de consigne. NOTE: Cette case est cochée par défaut.
Période de validité de l'horloge (ms)		✓	Entrez une valeur pour la période pendant laquelle l'horloge système reste valide après une synchronisation d'horloge. Si cette période expire sans qu'une synchronisation d'horloge ait lieu, toutes les heures sont signalées comme non valides. - La plage de valeurs va de 0 à 4294967295. - La valeur par défaut est 86400000.
Age max. de la commande (ms)		✓	Entrez la valeur du décalage maximum avec lequel les commandes sont acceptées. L'étiquette d'horodatage de la commande est sélectionnée et, si le temps écoulé est supérieur à MAX Command Age (ms), la commande n'obtient aucune réponse. La valeur 0 indique que l'étiquette d'horodatage de la commande n'est pas sélectionnée.

Paramètre	Client	Serveur	Description
			- La plage de valeurs va de 0 à 600000. - La valeur par défaut est 30000.
Nombre max. de futures commandes		✓	Entrez la valeur du décalage de temps maximum avec lequel les commandes sont acceptées avec une heure future. Il existe un test de conformité qui pose qu'un décalage d'une heure dans le futur entraîne un échec. Si une commande horodatée est reçue avec une avance supérieure à l'heure actuelle plus <i>Max Command Future</i>, elle est ignorée et aucune réponse n'est envoyée. - La plage de valeurs va de 0 à 600000. - La valeur par défaut est 30000.
Événements d'envoi de synchronisation d'horloge		✓	Cochez cette case pour envoyer des événements de synchronisation d'horloge spontanés au client. NOTE: Par défaut, cette case n'est pas cochée.
Supprimer l'événement le plus ancien		✓	Indique si l'événement le plus ancien est supprimé de la file d'attente d'événements lorsque le tampon est plein et qu'un nouvel événement arrive. - Cochez cette case pour supprimer l'événement le plus ancien. - Désélectionnez la case pour ignorer le nouvel événement. - Par défaut, cette case n'est pas cochée.
Mode compteur		✓	Spécifiez le mode de gel du compteur : - Désactiver le gel local : gel par commande d'interrogation de compteur uniquement (mode C ou mode D). - Activer le gel local sans réinitialisation : active automatiquement le gel local du compteur (mode A ou mode B) et le gel par la commande d'interrogation de compteur (mode C ou mode D). - Activer le gel local avec réinitialisation : active automatiquement le gel local avec réinitialisation du compteur (mode A ou mode B) et le gel par commande d'interrogation de compteur (mode C ou mode D). - La valeur par défaut est <i>Désactiver le gel local</i> (mode C ou mode D).
Bit d'heure d'été		✓	Activez cette case à cocher pour gérer le bit d'heure d'été de l'horodatage provenant d'un équipement externe ou du contrôleur. - Cette fonctionnalité n'est effective que si l'option Heure d'été est activée. - Par défaut, cette case n'est pas cochée.
Mode de synchronisation des données		✓	Sélectionnez un mode de synchronisation des données : Synchronisation cyclique : Utilisez la synchronisation (cyclique) par défaut. Synchronisation à la demande : Autorisez l'application PAC à implémenter des modifications locales sur la sortie binaire ou analogique. NOTE: L'activation d'un point de synchronisation à la demande modifie la structure de variable (hors du DDT d'équipement).
M_EI_NA GI	✓		Cochez cette case pour effectuer une interrogation générale après la réception d'un message EOI M_EI_NA. NOTE: Cette case est cochée par défaut.
Synchronisation de l'heure M_EI_NA	✓		Cochez cette case pour indiquer qu'une synchronisation d'horloge est effectuée après la réception d'un message EOI M_EI_NA. NOTE: Cette case est cochée par défaut.
M_EI_NA CI	✓		Cochez cette case pour indiquer qu'une interrogation de compteur est effectuée après la réception d'un message EOI M_EI_NA. NOTE: Par défaut, cette case n'est pas cochée.
GI en ligne	✓		Cochez cette case pour indiquer qu'une interrogation générale est effectuée lorsqu'un équipement distant est entré en ligne et qu'il est disponible pour les équipements qui ne génèrent pas de message EOI M_EI_NA. NOTE: Cette case est cochée par défaut.
Synchronisation de l'heure en ligne	✓		Cochez cette case pour indiquer qu'une synchronisation d'horloge est effectuée lorsqu'un équipement distant est mis en ligne et qu'il est disponible pour les équipements qui ne génèrent pas de message EOI M_EI_NA. NOTE: Cette case est cochée par défaut.
CI en ligne	✓		Cochez cette case pour indiquer qu'une interrogation de compteur est effectuée lorsqu'un équipement distant est mis en ligne et qu'il est disponible pour les équipements qui ne génèrent pas de message EOI M_EI_NA. NOTE: Par défaut, cette case n'est pas cochée.
Commande avec balise horaire	✓		Cochez cette case pour indiquer que la commande de contrôle suit la balise horaire. NOTE: Par défaut, cette case n'est pas cochée.

Mappage d'objets de données IEC60870

Introduction

En vue de faciliter les communications avec le module BMENOR2200H, créez des points de données pour le protocole de communication IEC60870-5-101/104 dans l'onglet **MAPPAGES DE DONNEES** du DTM.

CONFIGURATION

Sélection de version

Communication

Configuration des voies

SNMP

Service de temps réseau

Ports Ethernet

Port série

Voies / Equipements

Serveur IEC104

Server_PC

Equipement 1

Server_PC2

Server_PC3

Journalisation des données

Général

Exporter / Importer

Informations module

EQUIPEMENTPARAMETRES

EVENEMENTS

DONNEES/MAPPAGES

MAPPAGES DE DONNEES

Sélectionner l'ID de type : Sélectionner un identificateur de type

AjouterSupprimer

Rechercher	Identification de type	IOA	Quantité de données	Adresse de point CPU	Nom de variable
☐	M_SP	1	1		M_SP_P1
☐	M_ME_A	2	1		M_ME_A_P2
☐	C_SE_A	3	1		C_SE_A_P3

Information à point unique M_SP

IOA1

Nombre de points1

Nom de variableM_SP_P1

Etat automatiqueQualité non impactée

Mapage des registres CPUValeur uniquement

Fonctions d'application

☒Scrutation en arrière-plan

☒Transmission cyclique de données

☒Génération d'événements

Groupes

☒Global

☒Group1

☐Group2

☐Group3

☐Group4

☐Group5

☐Group6

☐Group7

☐Group8

☐Group9

☐Group10

☐Group11

☐Group12

☐Group13

☐Group14

☐Group15

☐Group6

Accès à l'onglet Configuration

Accédez aux paramètres de configuration dans l'onglet **MAPPAGES DE DONNEES** de Control Expert :

Etape	Action
1	Accédez à la configuration DTM de votre module.
2	Vérifiez que vous avez déjà créé des voies client et/ou serveur.
3	Dans le menu CONFIGURATION , développez (+) le sous-menu Voies .
4	Effectuez l'une des sélections suivantes dans le sous-menu Voies/Equipements : • Client IEC104 • Serveur IEC104 • Client IEC101 • Serveur IEC101
5	Sélectionnez l'équipement souhaité dans le sous-menu.
6	Sélectionnez l'onglet MAPPAGES DE DONNEES pour la voie.
7	Configurez les paramètres de mappage de données.
8	• Sélectionnez Appliquer pour appliquer vos modifications de configuration. • Sélectionnez OK pour appliquer les modifications et fermer la boîte de dialogue.

Mappages de données IEC60870

Modifiez la configuration des points de données dans l'onglet **MAPPAGES DE DONNEES** :

Etape	Action
1	Sélectionnez un ID de type dans la liste déroulante Sélectionner un ID de type .
2	Cliquez sur le bouton Ajouter pour configurer le type d'objet de données.
3	Configurez le type d'objet de données. Selon le type d'objet de données et le profil de protocole sélectionné, différents champs de configuration sont nécessaires pour définir un élément de mappage d'objets de données.
4	- Sélectionnez Appliquer pour appliquer vos modifications de configuration. - Sélectionnez OK pour implémenter vos modifications et fermer la boîte de dialogue.

Paramètres de mappage de données IEC60870

NOTE: Lorsque la fenêtre Control Expert est active, vous pouvez déplacer le curseur sur n'importe quel champ pour afficher une description de la fonctionnalité correspondante et la plage de valeurs possibles.

Le tableau suivant décrit les paramètres qui apparaissent dans l'onglet MAPPAGES DE DONNEES pour le client et le serveur :

Paramètre client et serveur	Description
IOA	Indique l'adresse IOA (adresse d'objet d'information) de l'objet.
Nombre de points	Indique le nombre d'objets définis. Adresse IOA de chaque objet défini. Les adresses IOA sont séquentielles à partir de l'adresse du premier objet.
Nom de variable	Indique le nom de la variable.
Mappage des registres CPU	Indique le choix de l'heure ou de l'indicateur stocké ; suit la valeur de la variable DDT d'équipement du contrôleur : Valeur uniquement : heure du module Valeur avec heure : heure du registre contrôleur Valeur avec indicateur : informations d'indicateur de point provenant des registres du contrôleur Valeur avec indicateur et heure : indicateur et heure provenant des registres du contrôleur
Seuil	Indique la valeur de seuil par défaut pour que le point M_ME_A/M_ME_B déclenche l'événement.
	Indique la valeur de seuil par défaut pour que le point M_ME_C déclenche l'événement.
Limite basse	Indique la valeur limite inférieure pour que le point M_ME_A/M_ME_B déclenche l'événement.
	Indique la valeur limite inférieure pour que le point M_ME_C déclenche l'événement.
Limite haute	Indique la valeur limite supérieure pour que le point M_ME_C déclenche l'événement.
	Indique la valeur limite supérieure pour que le point M_ME_A/M_ME_B déclenche l'événement.
Ajouter CMD_STATUS	Indiquez le nom de la variable CMD_STATUS.

Le tableau suivant décrit les paramètres qui apparaissent dans l'onglet
MAPPAGES DE DONNEES pour le serveur :

Paramètre serveur	Portée de la valeur	Description
Numéro de point associé	104 max. : 16777215 101 max. : selon la taille de l'IOA	Numéro de départ du point.
Masque de voie	Cases à cocher	Pour chaque case à cocher, indiquez le numéro de voie pour effacer le groupe d'objets (dépend de la configuration de la voie).
Qualificateur par défaut	• Impulsion courte • Impulsion longue • Sortie persistante	Qualificatif par défaut de la commande si la station de contrôle ne spécifie pas de qualificatif.
Période de gel	0 à 4294967295	Spécifiez la largeur de l'impulsion (ms).
Numéro du point M_ME_X	1...16777215	Spécifiez le paramètre correspondant au point M_ME_X.
Etat de l'automate	Qualité non impactée Qualité impactée	Indiquez si la qualité des points de surveillance est affectée par l'état de l'automate.
Type	(types de commande)	Sélectionnez un type de commande.
Durée d'impulsion courte	0 à 4294967295 ms	Indique la durée d'impulsion courte pour le point de contrôle C_SC/C_DC/C_RC.
Durée d'impulsion longue	0 à 4294967295 ms	Indique la durée d'impulsion longue pour le point de contrôle C_SC/C_DC/C_RC.
Sélection nécessaire	Case à cocher	Indique si une sélection est nécessaire avant l'opération pour la commande de contrôle C_SC/C_DC/C_RC/C_SE_A/C_SE_B/C_SE_C.
Mode CDC	• Etat déterminé • Etat indéterminé	Indique l'état de récupération d'impulsion pour la commande C_DC. En mode Etat déterminé, retour à l'état activé (2)/désactivé (1) précédent. En mode Etat indéterminé, retour à l'état intermédiaire (0) fixe.
Global 1/2/3/4/5/6/7/8/9/10/11/12/13/14/15/16	Case à cocher	Définit le groupe d'objets de données répondant à la commande d'interrogation du client. Il peut s'agir d'une combinaison d'options.

Le tableau suivant décrit les paramètres qui apparaissent dans l'onglet
MAPPAGES DE DONNEES pour le client :

Paramètre client	Portée de la valeur	Description
Mode de fonctionnement	• Auto • Sélectionner • Exécution • Désélectionner	Indique le mode de fonctionnement de la commande de contrôle C_SC/C_DC/C_RC/C_SE_A/C_SE_B/C_SE_C.
	• Activation • Désactivation	Indique l'opération activer/désactiver pour le point C_IC/P_AC.
	• Lire • Geler • Gel avec réinitialisation • Réinitialiser	Indique le mode de fonctionnement de la commande de contrôle C_CI.
Qualificatif	• Par défaut • Impulsion courte • Impulsion longue • Sortie persistante	Indique le qualificatif de la commande de contrôle C_SC/C_DC/C_RC. Lors de la réception d'une commande C_SC/C_DC/C_RC avec "qualificatif par défaut", le serveur exécute la commande avec ce qualificatif configuré.
	G/1/2/3/4/5/6/7/8/9/10/11/12/13/14/15/16	Indique le groupe d'interrogation pour la commande de contrôle C_IC.
	1/2/3/4/G	Indique le groupe d'interrogation de compteur pour la commande de contrôle C_CI.
	• Général • Evénement	Indique une réinitialisation générale ou une suppression d'événement pour la commande de contrôle C_RP.
	• Seuil • Limites basses • Limites hautes	Indique le type de paramètre à définir pour le point P_ME_A/P_ME_B/P_ME_C.
Lire le numéro	1...16777215	Indique l'adresse IOA (adresse d'objet d'information) du point à lire.
Qualificatif	• Seuil • Limites basses	Indique le type de paramètre à définir pour le point P_ME_A/P_ME_B/P_ME_C.

Paramètre client		Portée de la valeur	Description
		Limites hautes	
Routage d'événements	Voie de routage	Désactiver/Activer	Indique si la fonction de routage d'événements est désactivée ou activée.
	Session de l'itinéraire	0	Indique le nombre de sessions à router.
	Secteur de l'itinéraire	Liste d'équipements serveur	Indique l'équipement à router.
	Point de routage	1...16777215	Indique l'adresse IOA (adresse d'objet d'information) à router.
	Routage hors ligne	Qualité valide	Utiliser toute connexion de voie de routage disponible.
		Qualité non valide sans événements	Définir l'indicateur de déconnexion lorsque la voie de routage est hors ligne.
		Qualité non valide avec événement :	- Définir l'indicateur de non validité dans l'événement lorsque la voie de routage est hors ligne. - Générer un événement avec la valeur d'indicateur reçue lorsque la voie de routage est en ligne. L'intégrité générale est tout d'abord démarrée (si l'intégrité générale est activée dans le client).
	Scrutation en arrière-plan	Case à cocher	Indique que la scrutation en arrière-plan est activée. (La case est cochée.)
	Transmission cyclique de données	Case à cocher	Indique que la transmission de données cyclique est activée. (La case est cochée.)
	Génération d'événements	Case à cocher	Indique que des événements associés aux points peuvent être configurés.

Effacement d'événements sur le serveur

Clear_Events prend en charge un nouveau type de point qui efface le tampon d'événements dans les serveurs DNP3 et IEC60870-5-101/104. Cette opération peut être effectuée dans un système SCADA local ou distant, en mappant la mémoire.

Pour créer *Clear_Events* pour ces serveurs, sélectionnez Data Mapping.

Lorsque la valeur du registre *Clear_Events* change, le module BMENOR2200H efface les événements du groupe d'objets dans la configuration.

Paramètre	Portée de la valeur	Définition
Groupe d'objets	<i>All Objects</i> <i>Binary</i> <i>InputDouble</i> <i>InputBinary</i> <i>CounterAnalog</i> <i>InputBinary</i> <i>OutputAnalog</i> <i>Output</i>	Spécifie le groupe d'objets dont l'événement est effacé sur demande
Nom de variable	—	Indique le nom du registre localisé.

Page de définition d'une file d'attente d'événements

Configurez les paramètres de l'onglet **Evénements** pour mapper l'état de la file d'attente d'événements sur les registres de DDT d'équipement du contrôleur. Chaque état de la file d'attente d'événements consomme un registre de trois octets.

NOTE: Lorsque le nombre d'événements dépasse la taille de tampon configurée, les événements sont perdus ou remplacés.

Accédez à la configuration de la file d'événements dans Control Expert :

Etape	Action
1	Développez : Serveur IEC10 <Nom du serveur><Nom d'équipement>
2	Effectuez une sélection dans le menu déroulant Sélectionner un ID de type de l'onglet EVENEMENTS
3	Cliquez sur le bouton Ajouter pour afficher les paramètres du type sélectionné : • Mode de conservation des événements • Nbre maxi. d'événements • Configuration de tampon • Nbre maxi. d'événements-1 • Nbre maxi. d'événements-2 • Nbre maxi. d'événements-3 • Sauvegarde des événements NOTE: Lorsque la fenêtre Control Expert est active, vous pouvez déplacer le curseur sur n'importe quel champ pour afficher une description de la fonctionnalité correspondante et de la plage de valeurs disponible.
4	• Cliquez sur le bouton Appliquer pour appliquer vos changements de configuration. • Cliquez sur le bouton OK pour implémenter les modifications et fermer la boîte de dialogue.

Evénements IEC60870

Accès à l'onglet Configuration

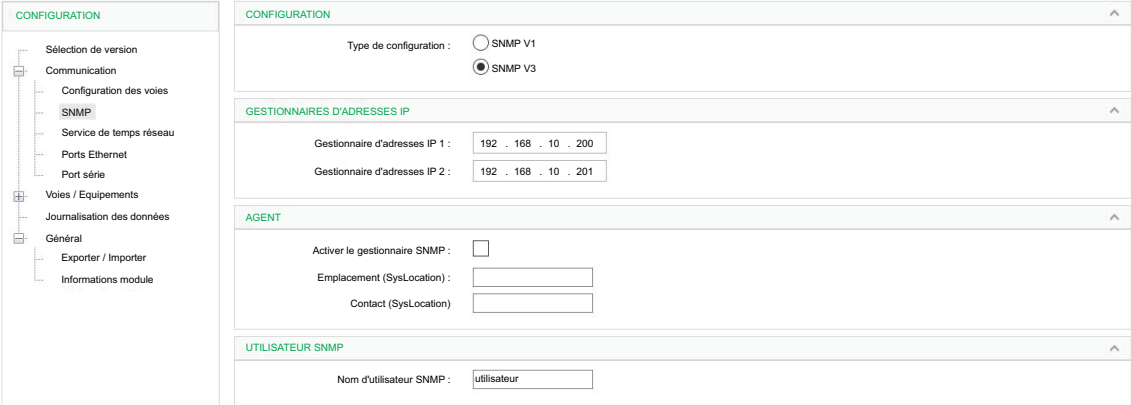
Accédez aux paramètres de configuration pour les événements IEC60870-5-101 et IEC60870-5-104 dans l'onglet **EVENEMENTS** de Control Expert :

Etape	Action
1	Accédez à la configuration DTM de votre module.
2	Vérifiez que vous avez déjà créé des voies client et/ou serveur pour les communications IEC60870.
3	Dans le menu CONFIGURATION , développez (+) le sous-menu Voies/Equipements .
4	Effectuez l'une des sélections suivantes dans le sous-menu Voies/Equipements : • Client IEC101/CEI104 • Serveur IEC101/CEI104
5	• Sélectionnez la voie spécifique dans le sous-menu. • Sélectionnez l'équipement dans le sous-menu.
6	Sélectionnez l'onglet EVENEMENTS .
7	Configurez les paramètres d'événement. NOTE: Les paramètres d'événement sont similaires aux paramètres de mappage de données.
8	• Sélectionnez Appliquer pour appliquer vos modifications de configuration. • Sélectionnez OK pour appliquer les modifications et fermer la boîte de dialogue.

Configuration de SNMP

Accès à la configuration SNMP

Accédez aux paramètres SNMP dans le DTM Control Expert :

Etape	Action
1	Accédez à la configuration DTM de votre module.
2	Dans le menu <i>CONFIGURATION</i> , développez (+) le sous-menu <i>Communication</i> .
3	Sélectionnez <i>SNMP</i> .
4	Configurez les paramètres SNMP.  NOTE: Ces paramètres sont décrits dans le tableau suivant.
5	• Cliquez sur le bouton <i>Appliquer</i> pour appliquer vos changements de configuration. • Cliquez sur le bouton <i>OK</i> pour implémenter vos modifications et fermer la boîte de dialogue.

Paramètres

Le tableau suivant présente les paramètres SNMP disponibles pour votre module.

NOTE: Lorsque la fenêtre Control Expert est active, vous pouvez déplacer le curseur sur n'importe quel champ pour afficher une description de la fonctionnalité correspondante et la plage de valeurs disponible.

Champ	Paramètre	Description
CONFIGURATION	SNMP V1	Cliquez sur le bouton d'option correspondant à la conception de votre application.
	SNMP V3	NOTE: Les versions SNMP ne sont pas compatibles entre elles.
GESTIONNAIRES D'ADRESSES IP	Gestionnaire d'adresses IP 1	Adresse IP du gestionnaire SNMP principal.
	Gestionnaire d'adresses IP 2	Adresse IP du gestionnaire SNMP secondaire.
AGENT	Activer le gestionnaire SNMP	<i>sélectionné</i> : Cochez cette case pour activer le gestionnaire SNMP. <i>désélectionné</i> : Laissez cette case vide pour désactiver le gestionnaire SNMP.
	Emplacement (SysLocation)	Indiquez l'emplacement physique du module lorsque le gestionnaire SNMP est activé.
	Contact (SysContact)	Entrez le nom d'un agent de maintenance à contacter lorsque le gestionnaire SNMP est activé.
NOMS DE COMMUNAUTÉ (SNMP V1 uniquement)	Set	Entrez le nom de communauté pour l'utilitaire <i>Set</i> .
	Get	Entrez le nom de communauté pour l'utilitaire <i>Get</i> .
	Trap	Entrez le nom de communauté pour l'utilitaire <i>Trap</i> . NOTE: - Les traps sont envoyés via le port UDP 162. - Vérifiez que les paramètres de trap que vous configurez sur le gestionnaire SNMP sont cohérents avec ceux du processeur.
SECURITE (SNMP V1 uniquement)	Activer le trap "Echec d'authentification"	<i>sélectionné</i> : L'agent SNMP envoie un message de déroutement (trap) au gestionnaire SNMP lorsqu'un gestionnaire non autorisé lui envoie une commande <i>Get</i> ou <i>Set</i> . <i>désélectionné</i> : Cette fonction est désactivée.
UTILISATEUR SNMP (SNMP V3 uniquement)	Nom d'utilisateur SNMP	Entrez un nom d'utilisateur pour SNMP version 3 (longueur maximale : 32 caractères).

NOTE: Les caractéristiques et les détails du service SNMP sont décrits dans le chapitre Services Ethernet.

Mode sécurisé

En mode sécurisé, SNMP v3 doit être configuré dans la page Web Cybersécurité. Sinon, le service SNMP ne démarrera pas.

Configuration du service de temps réseau

Introduction

Le module BMENOR2200H prend en charge la synchronisation d'horloge en tant que client SNTP et protocole RTU.

Lorsque le client SNTP est activé, le module synchronise l'horloge interne à partir du serveur de temps. Cette heure est la base de l'horodatage des événements RTU.

NOTE: Pour plus d'informations, reportez-vous à la description du module BMENOR2200H en tant que client SNTP.

Caractéristiques du service

La synchronisation d'horloge via SNTP offre les avantages suivants :

- corrections périodiques de l'heure obtenues auprès d'une source de référence telle qu'un serveur SNTP
- basculement automatique vers un serveur de temps de secours en cas d'événement anormal détecté sur le système de serveur normal
- un fuseau horaire local configurable et personnalisable (heure d'été comprise).

Les projets d'automate utilisent un bloc fonction pour lire l'horloge, une fonctionnalité qui permet d'horodater les événements ou les variables du projet.

L'horodatage est exact à :

- 5 ms près en général
- 10 ms près au pire

Accès à la configuration SNTP

Accédez aux paramètres SNTP dans le DTM Control Expert :

Etape	Action
1	Accédez à la configuration DTM de votre module.
2	Dans le menu CONFIGURATION , développez (+) le sous-menu Communication .
3	Sélectionnez Service de temps réseau .
4	Configurez les paramètres SNTP. NOTE: Ces paramètres sont décrits dans le tableau suivant.
5	• Cliquez sur le bouton Appliquer pour appliquer vos changements de configuration. • Cliquez sur le bouton OK pour appliquer les modifications et fermer la boîte de dialogue.

Paramètres de synchronisation horaire

Les paramètres SNTP suivants sont disponibles pour votre module :

CONFIGURATION

- Sélection de version
- Communication
 - Configuration des voies
 - SNMP
 - Service de temps réseau
 - Ports Ethernet
 - Port série
 - Voies / Equipements
 - Journalisation des données
 - Général
 - Exporter / Importer
 - Informations module

DEFINITION DE LA SOURCE HORAIRE

Source de synchronisation horaire : SNTp

SERVEUR SNTp

Adresse IP principale : 192 . 168 . 10 . 1

Adresse IP secondaire : 0 . 0 . 0 . 0

Période d'interrogation : 20 secondes

FUSEAU HORAIRE

Fuseau horaire : (GMT+08:00) Chine Décalage de fuseau horaire : 480 Minutes

Régler automatiquement l'horloge sur l'heure d'été : ☐

Début de l'heure d'été :

Mois : Mars Semaine : Dimanche

Occurrence : 1 Heure : 0

Fin de l'heure d'été :

Mois : Mars Semaine : Dimanche

Occurrence : 1 Heure : 0

HEURE D'APRES CPU

Alignement de l'horloge sur la CPU : ☐

Champ	Paramètre	Description
Définition de la source horaire	Source de synchronisation horaire	Sélectionnez une valeur dans la liste déroulante pour identifier la source horaire de la synchronisation : Protocole RTU : Si SCADA ou le client synchronise l'heure avec le module BMENOR2200H, sa source horaire est la station de contrôle. Serveur SNTp : Si le client NTP est activé et connecté au serveur NTP, sa source horaire est le serveur NTP lorsqu'il synchronise l'horloge du module BMENOR2200H.
Serveur SNTp	Adresse IP primaire	Entrez une adresse IP valide pour le serveur SNTp primaire.
	Adresse IP secondaire	Entrez une adresse IP valide pour le serveur SNTp secondaire.
	Période d'interrogation	Cette valeur représente le nombre de secondes entre les mises à jour provenant du serveur SNTp.
Fuseau horaire	Fuseau horaire	Sélectionnez un fuseau horaire dans le menu déroulant.
	Décalage horaire	Cette valeur représente la différence (en minutes) entre le fuseau horaire configuré et l'heure UTC.
	Régler automatiquement l'horloge sur l'heure d'été	<i>sélectionné</i> : Ajuster l'horloge pour l'heure d'été. <i>désélectionné</i> : L'horloge n'est pas ajustée pour l'heure d'été.
	Début de l'heure d'été	Configurez les heures de début et de fin de l'heure d'été dans les champs disponibles.
	Fin de l'heure d'été	
HEURE D'APRES CPU	Alignement de l'horloge sur la CPU	<i>sélectionné</i> : Mettre à jour l'horloge d'après le contrôleur. <i>désélectionné</i> : L'horloge n'est pas mise à jour d'après le contrôleur.

NOTE: Lorsque la fenêtre Control Expert est active, vous pouvez déplacer le curseur sur n'importe quel champ pour afficher une description de la fonctionnalité correspondante et la plage de valeurs disponible.

Termes liés à la synchronisation d'horloge

Termes SNTP :

Terme	Description du service
décalage de l'horloge locale	Des réglages précis de l'heure locale sont réalisés par le décalage de l'horloge locale. Le décalage de l'horloge locale est calculé comme suit : $((T2 - T1) + (T4 - T3)) / 2$ où : - T1 = heure à laquelle la requête SNTP est émise depuis le module - T2 = heure à laquelle le serveur SNTP reçoit la requête (indiquée par le module dans la réponse) - T3 = heure à laquelle le serveur SNTP transmet la réponse (indiquée au module dans la réponse) - T4 = heure à laquelle la réponse SNTP est reçue par le module
exactitude de l'heure	La marge horaire locale est inférieure à 10 ms par rapport à l'heure du serveur SNTP référencé. - typique : 5 ms - pire cas : <10 ms
temps de stabilisation	L'exactitude est optimale après 2 mises à jour depuis le serveur SNTP.
période d'interrogation	L'exactitude dépend de la période d'interrogation. Une marge inférieure à 10 ms est obtenue pour des périodes d'interrogation de 120 ms ou moins. Pour obtenir un niveau d'exactitude élevé (lorsque la bande passante de votre réseau le permet), définissez une période d'interrogation courte (par exemple, l'exactitude est meilleure avec une période d'interrogation de 5 s qu'avec une période d'interrogation de 30 s).
seconde intercalaire	Pour compenser la décélération de la rotation terrestre, le module insère automatiquement une seconde intercalaire dans le temps UTC tous les 18 mois, sur les instructions du Service international de la rotation terrestre et des systèmes de référence (IERS). Les secondes intercalaires sont insérées automatiquement lorsqu'elles sont nécessaires. Dans ce cas, elles sont insérées à la fin de la dernière minute de juin ou de décembre sur instruction du serveur SNTP.

Configuration du port série

Etape	Action
1	Accédez à la configuration DTM de votre module.
2	Dans le menu CONFIGURATION , développez (+) le sous-menu Communication .
3	Sélectionnez Port série .
4	Configurez les paramètres du port série. NOTE: Ces paramètres sont décrits dans le tableau suivant.
5	- Cliquez sur le bouton Appliquer pour appliquer vos changements de configuration. - Cliquez sur le bouton OK pour appliquer les modifications et fermer la boîte de dialogue.

Paramètres de port série



Les paramètres suivants s'appliquent au port série de votre module :

Paramètre	Description
Ligne physique	Sélectionnez le type de ligne physique du port.
Signaux	Sélectionnez le type de signal pris en charge par la ligne physique.
Débit en bauds	Sélectionnez une vitesse de transmission pour le port.
Bits de données	Ajustez le nombre de bits de données en fonction de l'équipement distant utilisé.
Bits d'arrêt	Sélectionnez le nombre de bits d'arrêt dans une seule transmission.
Parité	Configurez l'ajout (ou non) du bit de parité.

Obtention et maintien de l'exactitude

L'horloge du service de temps commence à la valeur 0 et s'incrémente jusqu'à la mise à jour réseau Ethernet per le module.

L'horloge du M580 est synchronisée au démarrage du module. Horodatage initial affiché par défaut :

Modèle	Date de début
M580	1er janvier 1980 00:00:00.00

Par la suite, le module va consulter la source d'heure SNTP ou attendre la commande de synchronisation d'horloge RTU du client. La date par défaut du M580 est la suivante.

Caractéristiques de l'horloge :

- L'exactitude de l'horloge n'est pas affectée par les commandes stop/run de l'automate.
- Les mises à jour de l'horloge ne sont pas affectées par les commandes stop/run de l'automate.
- Les transitions de mode n'ont aucun effet sur la précision du réseau Ethernet.

NOTE: Pour plus d'informations, consultez la description des sources horaires disponibles.

Terminologie générale liée à la synchronisation horaire

Termes généraux :

Terme	Description du service
fuseau horaire	La valeur par défaut est le temps universel coordonné (UTC). Vous pouvez éventuellement configurer le service pour utiliser un fuseau horaire local (par exemple, GMT+1 pour Barcelone ou Paris). <i>Reportez-vous à la remarque à la fin de ce tableau.</i>
heure d'été	Le module change automatiquement d'heure au printemps et à l'automne. <i>Reportez-vous à la remarque à la fin de ce tableau.</i>
alignement de l'horloge sur la CPU	Si aucune autre source horaire n'est configurée, le module BMENOR2200H envoie le signal de synchronisation d'horloge source au contrôleur via Xbus.

NOTE: Ce réglage est implémenté au niveau du module même s'il n'existe pas de configuration SNTP pour ce module. L'implémentation de ce paramètre est conditionnée par la prise en charge de plusieurs sources horaires (par exemple, DNP3) par le module BMENOR2200H. Ainsi, si vous utilisez DNP3 au lieu de SNTP pour la synchronisation horaire, le fuseau horaire est appliqué au module.

Configuration des ports de contrôle

Activation/désactivation des ports de contrôle

Lorsque la **Sélection de version** est *version de firmware* ≥ 4.0 , procédez comme suit pour activer les ports de contrôle :

Etape	Action
1	Accédez à la configuration DTM de votre module.
2	Dans le menu CONFIGURATION , développez (+) le sous-menu Communication .
3	Cliquez sur le sous-menu Ports Ethernet pour afficher les PARAMETRES : • ETH1 • ETH2 NOTE: Par défaut, les deux ports de contrôle frontaux sont désactivés. Le port d'embase doit obligatoirement être activé à 100 Mbits/s.
4	Activez les ports en cochant les cases correspondantes.
5	• Sélectionnez Appliquer pour appliquer vos changements de configuration. • Sélectionnez OK pour implémenter vos modifications et fermer la boîte de dialogue.

Réseau de contrôle (ETH1 & ETH2)

Les paramètres ci-dessous peuvent être configurés manuellement une fois que les ports de contrôle ont été activés :

Paramètres	Description
Adresse IP	Entrez l'adresse IP : deux ports de contrôle partagent la même adresse IP.
Masque de sous-réseau	Entrez un masque de sous-réseau correspondant à l'adresse IP pour les ports de contrôle.
Passerelle par défaut	Il s'agit de l'adresse IP de la passerelle par défaut pour les ports de contrôle / le port Ethernet d'embase à laquelle les messages destinés à d'autres réseaux sont transmis
Adresse IP + 1	Le champ Adresse IP + 1 est utilisé pour configurer un système redondant.
Utiliser la passerelle du port d'embase	Si cette case est cochée, la passerelle est définie dans le domaine du port d'embase.
• Cliquez sur le bouton Appliquer pour appliquer vos changements de configuration. • Cliquez sur le bouton OK pour implémenter les modifications et fermer la boîte de dialogue.	

NOTE: Il existe deux adresses MAC, mais une seule passerelle peut être configurée en vue de fonctionner soit pour les ports de contrôle frontaux (si elle est définie dans le domaine des ports de contrôle frontaux), soit pour les ports d'embase (si elle est définie dans le domaine des ports d'embase)

NOTE: La plage d'adresses IP des ports de contrôle ne peut pas être identique à celle du port d'embase, car cela entraînerait un état non valide pour l'exécution du module. (Voyant RUN éteint, voyant ERR rouge clignotant)

Réglage de la vitesse de transmission

Une fois les deux ports de contrôle fontaux sont activés, le réglage du débit en bauds est possible. Les options sont les suivantes :

- Auto 10/100/1000 Mbits/s
- 100 Mbits/s semi-duplex
- 100 Mbits/s duplex intégral
- 10 Mbits/s semi-duplex
- 10 Mbits/s duplex intégral

NOTE: *Auto 10/100/1000 Mbits/s* est l'option par défaut une fois que les ports sont activés.

Exportation et importation de fichiers .xml avec le DTM

Introduction

Un module BMENOR2200H stocke sa configuration dans un fichier .xml. Vous pouvez utiliser les fonctions d'importation et d'exportation du Control Expert DTM pour sauvegarder/récupérer et partager ce fichier entre différents modules afin d'implémenter la même configuration.

Utiliser la fonctionnalité **EXPORTER/IMPORTER** de Control Expert :

- *exporter* : Enregistrer les configurations de module et de protocole dans un fichier .xml.
- *importer* : Importer des fichiers .xml contenant les paramètres de configuration et le mappage de données vers un ou plusieurs modules.

Cas d'utilisation

Ces exemples pratiques représentent quelques implémentations courantes des fonctions d'importation et d'exportation :

Exemple d'utilisation	Action	
Sauvegarde/récupération et configuration par lots	1	Exporter le fichier de configuration .xml d'un module BMENOR2200H.
	2	Importer le fichier de configuration .xml vers un <i>ou plusieurs</i> modules BMENOR2200H.
	3	Réutiliser le fichier de configuration du module BMENOR2200H dans d'autres modules BMENOR2200H
Migration de projet	Migrer le fichier de configuration d'un module BMXNOR0200H vers un module BMENOR2200H. NOTE: Toutes les adresses localisées sont perdues après l'importation de fichiers .xml à partir du module BMXNOR0200H. Le type et la longueur du nom sont modifiés en fonction du nouveau format. Tenez compte des remplacements de type de données requis lors de la migration du fichier XML.	

Importer

Pour importer un fichier de configuration .xml :

Etape	Action
1	Accédez à la configuration DTM de votre module.
2	Dans le menu CONFIGURATION , développez (+) le sous-menu Général .
3	Sélectionnez Export / Import .
4	Dans la boîte de dialogue Importer/Exporter , cliquez sur le bouton Parcourir du champ Nom du fichier d'importation pour rechercher le chemin d'accès au fichier de configuration .xml à importer, situé sur votre lecteur local ou réseau.
5	Sélectionnez le fichier de configuration approprié et cliquez sur le bouton Ouvrir pour entrer le chemin d'accès du fichier dans le champ Nom du fichier d'importation .
6	Cochez ou désélectionnez la case Utiliser le mappage des noms de points de données défini par le système : • <i>sélectionné</i> : Ce paramètre d'importation vous permet d'importer des noms de point de mappage définis par l'utilisateur. • <i>désélectionné</i> : Le nom de point de mappage de données est affecté en fonction du type de point, du numéro de point et du nombre de points.

Etape	Action
7	Sélectionnez le bouton Importer . NOTE: Lorsque vous appliquerez la commande <i>importer</i> , toutes les données de configuration existantes seront remplacées et tous les fichiers de sauvegarde existants de cette table seront déplacés vers le dossier Archive.
8	Sélectionnez Appliquer pour enregistrer vos modifications ou cliquez sur OK pour enregistrer vos modifications et fermer la boîte de dialogue.

Exporter

Pour exporter un fichier de configuration .xml :

Etape	Action
1	Accédez à la configuration DTM de votre module.
2	Dans le menu CONFIGURATION , développez (+) le sous-menu Général .
3	Sélectionnez Export / Import .
4	Dans la boîte de dialogue Importer/Exporter , copiez/collez dans le champ Nom du fichier d'importation le chemin d'accès du fichier de configuration .xml enregistré à partir du module BMENOR et des paramètres de protocole que vous souhaitez exporter vers un lecteur local.
5	Cochez ou désélectionnez la case Utiliser le mappage des noms de points de données défini par le système : <i>sélectionné</i> : Ce paramètre d'importation vous permet d'importer des noms de point de mappage définis par l'utilisateur. <i>désélectionné</i> : Le nom de point de mappage de données est affecté en fonction du type de point, du numéro de point et du nombre de points.
6	Sélectionnez le bouton Exporter . NOTE: Le fichier de configuration .xml est exporté vers un emplacement prédéterminé de votre lecteur local ou réseau.
7	Sélectionnez Appliquer pour enregistrer vos modifications ou cliquez sur OK pour enregistrer vos modifications et fermer la boîte de dialogue.

Configuration groupée

Etape	Action
1	Accédez à la configuration DTM de votre module.
2	Dans le menu CONFIGURATION , développez (+) le sous-menu Communication .
3	Sélectionnez Configuration des voies .
4	Pour modifier, double-cliquez sur le crayon dans l'onglet Configuration groupée de la boîte de dialogue VOIES CLIENT . Résultat : Une boîte de dialogue Ouvrir apparaît et vous permet d'accéder au fichier de configuration groupée de votre choix.
5	Sélectionnez le fichier DataMapping_BulkConfiguration.xlsm dans le dossier demandé à l'étape 4 et ouvrez la feuille de calcul Excel ou le fichier CSV.
6	En fonction des besoins (points de données pour serveur et client IEC ou DNP3), copiez les données respectives dans la feuille Client IEC ou Serveur IEC.
7	Ouvrez le mappage de données correspondant. Les données devraient être importées correctement.
8	Enregistrez vos modifications et importez la feuille de calcul Excel ou le fichier CSV.

Détails de la feuille de calcul Excel :

- Serveur IEC : Feuille IECDataPoint_Ref vers IECServer
- Client IEC : Feuille IECDataPoint_Ref vers IECClient
- Serveur DNP3 : DNP3DataPoints_Ref vers DNP3Server
- Client DNP3 : DNP3DataPoints_Ref vers DNP3Client

Informations du module dans le DTM

Accès aux informations

Consultez la fonction **Informations du module** dans le DTM Control Expert :

Etape	Action
1	Accédez à la configuration DTM de votre module.
2	Dans le menu CONFIGURATION , développez (+) le sous-menu Général .
3	Sélectionnez Informations du module .

CONFIGURATION

Sélection de version

Communication

Configuration des voies

SNMP

Service de temps réseau

Ports Ethernet

Port série

Voies / Equipements

Journalisation des données

Général

Exporter / Importer

Informations module

INFORMATIONS D'ADRESSE IP

Adresse IP : 192 . 168 . 10 . 21

Lancer

Masque de sous-réseau : 255 . 255 . 0 . 0

Lancer

Adresse IP des ports de contrôle : 10 . 10 . 10 . 21

Lancer

Masque de sous-réseau des ports de contrôle : 255 . 255 . 0 . 0

Lancer

Passerelle par défaut : 192 . 168 . 10 . 1

Lancer

ETAT MEMOIRE

Taille de la configuration d'entrée : 124 /8192

Taille de la configuration de sortie : 26 /8192

Distribution de l'utilisation de la mémoire

Nom	Type	Nombre de points	Taille des entrées	Taille des sorties
Module	Module	9	124	22
Tête de section	Tête de section	0	3	0
Données de diagnostic	Diagnostic	0	62	0
Tête réservée	Tête réservée	0	16	16
Connexion	Connexion	9	53	6

Description

La page **Informations du module** affiche des informations en lecture seule :

- INFORMATIONS D'ADRESSE IP** : Ces champs contiennent les paramètres IP du module.
- ETAT MÉMOIRE** :
 - Entrée** : L'indicateur de niveau affiche l'utilisation de la mémoire (en octets) pour le type de mémoire d'entrée.
 - Sortie** : L'indicateur de niveau affiche l'utilisation de la mémoire (en octets) pour le type de mémoire de sortie.

Limites

Surveillez les ressources implicites consommées tout en respectant la taille totale des types d'entrée et de sortie comme suit :

Type	Mémoire
Entrée	8 Ko
Sortie	8 Ko

NOTE: Pour plus de détails, reportez-vous à la description de l'échange de données d'E/S avec le contrôleur.

Journalisation des données

A propos de la journalisation des données

Introduction

Le service de journalisation des données permet d'archiver les données d'application (événements, alarmes, données de processus, état des équipements, mesures, etc.) dans la mémoire interne du module. Ce service vous permet d'enregistrer des données dans des fichiers .csv au format ASCII. Ces fichiers sont stockés localement sur la carte mémoire SD du module.

Vous pouvez configurer le service de journalisation des données pour qu'il s'exécute dès que l'un des événements suivants est détecté :

- Un intervalle de temps configuré s'est écoulé.
- La CPU ou l'utilisateur déclenche un événement.

Format de fichier

Ce service de journalisation consigne les données dans des fichiers .csv (valeurs séparées par des virgules). Ces fichiers offrent une grande souplesse d'utilisation :

- Transportez le fichier directement vers une feuille de calcul Microsoft Excel ou un système de gestion de base de données (SGBD) à des fins d'analyse.
- Ces fichiers sont accessibles par les clients HTTPS.

Tables de journalisation des données

Une table de journalisation de données occupe une portion de la mémoire du module (RAM).

La valeur des variables journalisées y est consignée. Un nouvel enregistrement est inséré dans la table pour chaque événement consigné. L'enregistrement peut contenir un horodatage ou une valeur pour toutes les variables sélectionnées. Vous pouvez configurer le nombre d'enregistrements que peut contenir la table.

Lorsque l'événement de sauvegarde de la journalisation de données se produit, la table en mémoire RAM est enregistrée en tant que fichier de sauvegarde dans la carte SD et tous les enregistrements de la table sont effacés.

Bilan mémoire

Le service de journalisation des données peut gérer jusqu'à 10 tables indépendantes l'une de l'autre. Cela signifie que chaque table peut avoir une taille unique et un mécanisme de déclenchement différent. Le service peut également gérer jusqu'à 10 groupes de fichiers de journalisation de données (sauvegardes). Vous pouvez donc créer plusieurs tables de données différentes associées chacune à des périodes de journalisation différentes.

Par exemple, le dossier *Table_n* représente la sauvegarde correspondant à *table_n*. Les fichiers de sauvegarde de la table sur la carte mémoire SD peuvent être purgés (ou supprimés) comme configuré (événement n déclenché par la CPU). Lorsque le module connaît une coupure d'alimentation lors de la journalisation de données, les enregistrements de la table en mémoire RAM qui n'ont pas été sauvegardés sont perdus tandis que les fichiers de sauvegarde sont conservés.

Ces événements se produisent lorsque vous téléchargez un nouveau projet ou une nouvelle configuration sur l'automate :

- Les tables de journalisation de données en mémoire RAM sont effacées et expulsées.
- Les fichiers de sauvegarde correspondants sur carte SD sont archivés si la configuration de la table est modifiée.

Avant de commencer

Journalisation des données et DTM

Le service de journalisation des données est configuré dans Control Expert via le DTM correspondant au module BMENOR2200H.

Journalisation des données et carte SD

Vérifiez qu'une carte SD est insérée dans le logement situé à l'avant du module avant de télécharger sur le module le projet Control Expert qui inclut le service de journalisation des données.

NOTE: Le module reconnaît la carte SD sept secondes environ après son insertion dans le logement de carte mémoire.

NOTE: Ne retirez pas la carte SD pendant que le service de journalisation des données est en cours d'exécution.

L'utilisation du service de journalisation des données nécessite l'activation du dictionnaire de données dans les paramètres du projet.

Configuration de la journalisation des données dans Control Expert

Accès à la configuration

Accédez aux paramètres de journalisation des données :

Etape	Action
1	Accédez à la configuration DTM de votre module.
2	Dans le <i>Navigateur de DTM</i> , double-cliquez sur le DTM correspondant au module BMENOR2200H pour accéder à ses paramètres de configuration.
3	Dans le menu CONFIGURATION , sélectionnez Journalisation des données .

The screenshot shows the 'PARAMETRES DE JOURNALISATION DES DONNEES' window in Control Expert. On the left, a tree view under 'CONFIGURATION' has 'Journalisation des données' selected. The main area shows 'Chemin d'application' as 'C:\TEMPRTUS3_FT_IEC104.stu' and 'Nom de la table' as an empty field. Below this is a table titled 'TABLES DE JOURNALISATION' with two rows: 'Datalog_1' and 'Datalog_2'. Each row has 'Non' in the first column and 'Nom de la table' in the second. Action buttons (Modifier, Supprimer, Dupliquer) are on the right. The bottom of the window is empty.

Non	Nom de la table	Modifier	Supprimer	Dupliquer
0	Datalog_1			
1	Datalog_2			

Instructions de configuration

Configurez la journalisation des données dans les champs *PARAMÈTRES DE JOURNALISATION DES DONNÉES* :

Etape	Action
1	Entrez la destination du fichier .stu dans le champ <i>Chemin d'application</i> . NOTE: Vous pouvez utiliser le bouton Parcourir pour accéder à une destination de fichier.
2	Attribuez un nom dans le champ <i>Nom de la table</i> . NOTE: Ce champ peut contenir jusqu'à 31 caractères.
3	Appuyez sur le bouton Ajouter pour créer la table de journalisation.
4	Vérifiez que la nouvelle table de journalisation est créée : - La nouvelle table apparaît dans le champ <i>TABLES DE JOURNALISATION</i>. - Développez la structure (CONFIGURATION > Journalisation des données) pour faire apparaître le nom de la nouvelle table.
5	Cliquez sur le bouton OK ou Appliquer pour appliquer les modifications.

Paramètres de journalisation des données

CONFIGURATION

Sélection de version

Communication

Configuration des voies

SNMP

Service de temps réseau

Ports Ethernet

Port série

Voies / Équipements

Journalisation des données

Datalog_1

Datalog_2

Général

Exporter / Importer

Informations module

PARAMETRES DE JOURNALISATION

Nombre maximum d'enregistrements : 100

Sauvegarde à saturation : ☐

Période de journalisation : 1

Horodatage : ☒

Unité de temps de la période de journalisation : secondes

VARIABLES DE JOURNAL

☐	Nom de variable	Type
☐	PLC0_d0_r0_e5_ERT1604_2_MOD_HEALTH	BOOL
☐	BMEP58_ECPU_EXT_DROP_HEALTH[1]	BOOL
☐	RTUV2_CONN.Device1_M_SP_P1.Value	BYTE
☐	RTUV2_CONN.Device1_M_ME_A_P2.Value	INT
☐	RTUV2_CONN.Device1_C_SE_A_P3.Value	INT
☐	RTUV2_CONN.Device3_Error_Code	WORD

Ajouter

Supprimer

Importer

Exporter

Nombre total de variables : 6

PARAMETRES DE SAUVEGARDE

Période de sauvegarde : 30

Unité de temps de la période de sauvegarde : minutes

Temps de sauvegarde estimé : 300 minutes

Nombre maximum de fichiers : 10

Effacer au redémarrage : ☒

Taille maximum de la sauvegarde : 43.9 Ko

PARAMÈTRES DE JOURNALISATION : Développez (+) **Journalisation des données** dans le menu **CONFIGURATION** et sélectionnez une table pour accéder aux paramètres suivants :

Paramètre	Description
Nombre maximum d'enregistrements	Entrez le nombre maximum d'enregistrements pouvant être stockés dans une table de journalisation. NOTE: Lorsque le nombre d'enregistrements configuré est atteint, les enregistrements les plus récents remplacent les enregistrements les plus anciens.
Période de journalisation	Utilisez ces valeurs pour entrer un intervalle après lequel la sauvegarde est déclenchée : - Désactiver la sauvegarde de la période : 0 - Configurer l'intervalle. - Configurer l'unité de temps de la période de journalisation.
Unité de temps de la période de journalisation	Sélectionnez l'unité de temps à appliquer.
Sauvegarde à saturation	Activez cette case à cocher pour déclencher une sauvegarde lorsque la table de journalisation est pleine (d'après sa capacité maximale configurée).
Horodatage	Activez cette case à cocher pour ajouter un horodatage à chaque enregistrement de journal.

172

EIO0000004870.01

VARIABLES DE JOURNAL : Vous ne pouvez accéder à ces paramètres qu'après avoir créé une table de journalisation des données (voir ci-dessus).

Paramètre	Description
<i>Ajouter</i>	Cliquez sur ce bouton pour ouvrir la boîte de dialogue <i>Variables globales</i> et ajouter de nouvelles variables à la table <i>VARIABLES DE JOURNAL</i> .
<i>Nom de variable</i>	Cette colonne affiche le nom des variables ajoutées.
<i>Type</i>	Cette colonne indique le type correspondant aux variables configurées.
<i>Supprimer</i>	Cliquez sur ce bouton pour supprimer la variable sélectionnée de la table.
<i>Importer</i>	Importe la variable sélectionnée.
<i>Exporter</i>	Exporte la variable sélectionnée.
<i>Nombre total de variables</i>	Ce champ indique le nombre total de variables dans la table.

PARAMÈTRES DE SAUVEGARDE:

Paramètre	Description
<i>Période de sauvegarde</i>	Utilisez ces valeurs pour déclencher la sauvegarde de la table ou configurer un événement périodique. Dans ce cas, configurez la base de temps : - Désactiver la sauvegarde de la période : 0 - Configurez l'intervalle : 30 min à 100 jours
<i>Temps de sauvegarde estimé</i>	Il s'agit de la durée maximum estimée qui s'écoule avant la perte des données de sauvegarde (remplacées par de nouvelles données de sauvegarde).
<i>Effacer au redémarrage</i>	Cochez cette case pour supprimer les fichiers de la table de journalisation sur la carte SD lors d'un redémarrage du module.
<i>Unité de temps de la période de sauvegarde</i>	Sélectionnez l'unité de temps à appliquer.
<i>Nombre maximum de fichiers</i>	Utilisez ces valeurs pour définir le nombre maximal de fichiers de sauvegarde pour la table : - valeur par défaut : 10 - nombre maximum de fichiers de sauvegarde : 200
<i>Taille maximum de la sauvegarde</i>	Les fichiers de journalisation des données sont stockés dans la carte SD et la capacité maximale d'une carte SD est de 4 Go. Lorsque vous générez une nouvelle table de journalisation de données, la taille maximale de la table est fixe. Ce nombre provient du DTM, lequel utilise les évaluations suivantes pour calculer la taille maximum du dossier (dossier de sauvegarde en l'occurrence) : - type de données dans la table - nombre d'enregistreurs dans chaque fichier - nombre de fichiers sur la carte SD

Variables dans le DDT d'équipement

Pour accéder aux variables du DDT d'équipement du module, ouvrez l'onglet **Variables** dans le **Navigateur de projet (Projet > Variables et instances FB > Variables de DDT d'équipement)**.

Valeur	Action
1	Ouvrez l'onglet Variables dans le Navigateur de projet (Projet > Variables et instances FB > Variables de DDT d'équipement) .
2	Dans la colonne Nom , développez (+) le nom d'un module associé à une table de journalisation de données.
3	Recherchez le nom de la table et développez (+) le nœud pour accéder aux éléments structurels qui sont décrits dans le tableau suivant.

Eléments structurels :

Elément	Description
<i>Enable</i>	Cette valeur contrôle le service de journalisation des données pour la table sélectionnée : • 0 : désactivé • 1 : activé
<i>Records_count</i>	Cette valeur représente le nombre d'enregistrements dans la table sélectionnée.
<i>Backup_count</i>	Cette valeur représente le nombre de fichiers de sauvegarde dans la table sélectionnée.
<i>Last_Log_Status</i>	<i>octet 0</i> : valeur de déclenchement (action terminée sans détection d'erreur).
	<i>octet 1</i> : résultat du déclenchement (la carte SD n'est pas disponible).
<i>Last_Backup_Status</i>	<i>octet 0</i> : valeur de déclenchement (action terminée sans détection d'erreur).
	<i>octet 1</i> : résultat du déclenchement (la carte SD n'est pas disponible).
<i>Log</i>	Déclenchez une action de journal et affichez le résultat du déclenchement. NOTE: Reportez-vous à la description des valeurs d'octet pour <i>Trigger_S</i> ci-dessous.
<i>Backup</i>	Déclenchez une action de sauvegarde et affichez le résultat du déclenchement. NOTE: Reportez-vous à la description des valeurs d'octet pour <i>Trigger_S</i> ci-dessous.
<i>Purge</i>	Déclenchez une action de purge pour supprimer le fichier de sauvegarde et affichez le résultat du déclenchement. NOTE: Reportez-vous à la description des valeurs d'octet pour <i>Trigger_S</i> ci-dessous.

Trigger_S

Le type *Trigger_S* a deux variables lorsqu'il est associé aux variables *log*, *backup* ou *purge* :

- *Trigger* : Chaque changement de valeur déclenche l'action correspondante.
- *Status* : L'octet de poids fort de la variable *Status* contient le résultat de l'action exécutée, comme indiqué par les valeurs suivantes :

Octet	Description
0	L'exécution de l'action s'est terminée sans détection d'erreur :
1	La carte SD n'est pas disponible : ◦ <i>raison possible</i> : Le logement de carte ne contient pas de carte SD compatible. ◦ <i>action suggérée</i> : Insérez une carte SD compatible.
2	Une erreur du système de fichiers est détectée : ◦ <i>raison possible</i> : Il est impossible d'écrire des fichiers sur la carte SD. ◦ <i>action suggérée</i> : Vérifiez la protection en écriture de la carte, redémarrez le module ou remplacez la carte SD.
3	L'espace disponible sur la carte SD n'est pas suffisant pour exécuter l'action : ◦ <i>raison possible</i> : La carte SD est saturée. ◦ <i>action suggérée</i> : Remplacez la carte SD ou purgez les fichiers de la carte.
4	La mémoire RAM disponible ne suffit pas pour la journalisation ou la sauvegarde : ◦ <i>raison possible</i> : Trop de services ou de points de données sont configurés. ◦ <i>action suggérée</i> : Réduisez la taille de la configuration.
5	La variable n'est pas disponible : ◦ <i>raison possible</i> : Le dictionnaire de données n'est pas activé dans le projet ou une ou plusieurs variables configurées dans la table sont manquantes dans le projet de l'utilisateur. ◦ <i>action suggérée</i> : Activez le dictionnaire de données dans les paramètres du projet ou reconfigurez la table de journalisation de données pour supprimer les variables manquantes.
6	La table est pleine : ◦ <i>raison possible</i> : Il y a trop d'enregistrements de journal. ◦ L'octet de poids fort de la variable <i>Status</i> contient le résultat de l'action exécutée, comme indiqué par ces valeurs de <i>Status</i> : ◦ <i>action suggérée</i> : Déclenchez une action de sauvegarde.
7	La carte SD est occupée.
8	Une erreur système est détectée : ◦ <i>raison possible</i> : Le transfert de données entre le module et le contrôleur est interrompu. ◦ <i>action suggérée</i> : Vérifiez les connexions matérielles ou redémarrez l'ensemble du système.

- L'octet de poids faible de la variable *Status* identifie l'action entraînée par le résultat. Lorsque l'exécution d'une action est terminée, l'octet de poids faible est mis à jour pour prendre la valeur de l'octet *Trigger* qui a déclenché l'action.

NOTE:

Vérifiez que *Status* est mis à jour avant le déclenchement de l'action suivante.

1. Voici un exemple d'action de journalisation déclenchée avec vérification du résultat pour une table sélectionnée :
 - *BME_NOR_2200H_DATALOG.Table0.enable* = 1 (La table est activée.)
 - *BME_NOR_2200H_DATALOG.Table0.log.Trigger* = 0
 - *BME_NOR_2200H_DATALOG.Table0.log.Status* = 0
2. L'action est déclenchée par un changement de valeur de *BME_NOR_2200H_DATALOG.Table0.log.Trigger* de 0 à 1 pour démarrer cette séquence :
 - a. Le module ajoute un enregistrement de journal à la table.
 - b. Le module met à jour la valeur de *BME_NOR_2200H_DATALOG.Table0.log.Status*.
3. Le programme d'application de l'utilisateur continue à surveiller la valeur de *BME_NOR_2200H_DATALOG.Table0.log.Status* :
 - Si l'octet de poids faible passe à 1, l'action de journal termine son exécution.
 - Si l'octet de poids fort passe à 0, l'action de journal se termine avec succès.
 - Toute autre valeur indique un échec d'exécution.
4. Le programme d'application de l'utilisateur peut à nouveau modifier la valeur de *BME_NOR_2200H_DATALOG.Table0.log.Trigger* pour déclencher une autre action de journal.
5. Répétez ces étapes pour vérifier le résultat.

DDT d'équipement de diagnostic du module

Le DDT d'équipement de diagnostic du module inclut l'état de la carte SD (*SD_STATUS*) et le service de journalisation de données (*DATALOGING*). Voici les valeurs de bit possibles pour *SD_STATUS* :

- *bit 0 STATUS* : Ce bit est activé lorsque la carte SD est normale.
- *bit 1 BUSY* : Ce bit est activé lorsque la carte SD est occupée.
- *bit 2 LOW_SPACE_ALARM* : Ce bit est activé lorsque le pourcentage d'espace libre de la carte SD est inférieur à 20 %.

Sélection de variables

Vous pouvez ajouter des variables non localisées existantes (dans votre projet actuel) au tableau *Sélection de variables* lorsque vous configurez la table de journalisation de données. Le service de journalisation des données prend en charge les types de variable suivants :

Type de variable	Format de journalisation (fichiers de sauvegarde)
BOOL	0, 1
EBOOL	0, 1
BYTE	0 ... 255 (décimal)
INT	-32768 ... 32767 (décimal)
UINT	0 ... 65535 (décimal)
WORD	0 ... 65535 (décimal)
DINT	-2147483648 ... 2147483647 (décimal)
UDINT	0 ... 4294967295 (décimal)
DWORD	0 ... 4294967295 (décimal)
REAL	-1.2345678e-99 (notation scientifique)
TIME	49D_17H_20M_47S_295MS
DATE	02/02/1990
TOD	23:10:59

Lorsque vous cliquez sur le bouton **Ajouter** dans la section *Variable d'historique*, la fenêtre *Sélection de variables* s'ouvre. A partir de là, vous pouvez faire un choix parmi les variables définies dans le projet Control Expert.

Lorsqu'un nouvel événement de sauvegarde se produit (suite à un déclencheur ou à l'expiration d'une période), un nouvel enregistrement contenant toutes les valeurs des variables est ajouté à la table de journalisation (avec éventuellement un horodatage). Lorsque le nombre maximum d'enregistrements configuré par l'utilisateur est atteint, les enregistrements les plus récents remplacent les enregistrements les plus anciens.

Format du fichier de sauvegarde

Le service de journalisation des données prend en charge une carte SD d'une capacité de 4 Go. Les fichiers de sauvegarde sont stockés dans le dossier du journal de données à la racine de la carte. Chaque table comprend un sous-dossier dédié pour cette action de stockage. Le nom du sous-dossier est identique à celui de la table configurée par l'utilisateur.

Lorsqu'un nouvel événement de journal se produit (suite à un déclencheur ou à l'expiration d'une période), un nouveau fichier est généré dans ce dossier et les enregistrements de la table de journalisation sont stockés dans ce fichier. La table de journalisation se retrouve alors vide. Lorsque le nombre maximum de fichiers configuré par l'utilisateur est atteint, les fichiers de sauvegarde les plus anciens sont supprimés.

Le fichier généré prend l'horodatage de l'événement comme nom personnalisé au format suivant :

aaaa-mm-jj_hh-mm-ss

Le format de fichier est fixe. Vous ne pouvez pas le modifier.

Le fichier est codé au format ASCII pur dans un fichier texte portant l'extension .csv. Voici un exemple de contenu d'un fichier journal :

```
Date,plc.plc1.height,plc.plc1.length,plc.plc1.width,
2003-10-01 02:44:55,150,200,50,
2003-10-01 03:48:08,140,150,30,
2003-10-01 04:55:10,220,280,80,
2003-10-01 06:01:05,170,220,60,
```

Vous pouvez ouvrir le fichier .csv dans Microsoft Excel pour séparer les données en colonnes :

Date	plc.plc1.height	plc.plc1.length	plc.plc1.width
10/1/2003 2:44	150	200	50
10/1/2003 3:48	140	150	30
10/1/2003 4:55	220	280	80
10/1/2003 6:01	170	220	60

Purge

Une purge déclenchée par le contrôleur efface de la carte SD tous les fichiers de sauvegarde de la table. Dans ce cas, le dossier de la table est vidé.

Pour déclencher l'action de purge à chaque redémarrage du module, sélectionnez *Effacer au redémarrage*.

NOTE:

- Cette variable n'est disponible qu'une fois le service de journalisation configuré.
- La purge n'affecte pas la table de journalisation en mémoire.

Nom		Type	Description
Purge_Archive		Trigger_S	Effacer le fichier de sauvegarde archivé.
	Trigger	BYTE	Modifier la valeur de cet octet pour déclencher l'action.
	Status	WORD	0 : Valeur de déclenchement sans détection d'erreur.
			1 : La carte SD n'est pas disponible.
			2 : Une erreur du système de fichiers est détectée.
			3 : L'espace disponible sur la carte SD est insuffisant.
			4 : L'espace mémoire est insuffisant.
			5 : La variable n'est pas disponible.
			6 : La table est pleine.
			7 : La carte SD est occupée.
			8 : Une erreur système est détectée.
(nom de la table)		T_BME_NOR_2200H_TABLE	Le nom de table est attribué lorsque vous créez une table de journalisation de données.

Nom		Type	Description
	<i>Enable</i>	BOOL	0 : Désactiver le service de journalisation.
			1 : Activer le service de journalisation.
	<i>Records_count</i>	UINT	Nombre d'enregistrements dans cette table.
	<i>Backup_count</i>	UINT	Nombre d'enregistrements de sauvegarde de cette table.
	<i>Last_Log_Status</i>	BYTE	0 : Valeur de déclenchement sans détection d'erreur.
			1 : La carte SD n'est pas disponible.
			2 : Une erreur du système de fichiers est détectée.
			3 : L'espace disponible sur la carte SD est insuffisant.
			4 : L'espace mémoire est insuffisant.
			5 : La variable n'est pas disponible.
			6 : La table est pleine.
			7 : La carte SD est occupée.
			8 : Une erreur système est détectée.
	<i>Last_Backup_Status</i>	BYTE	0 : Valeur de déclenchement sans détection d'erreur.
			1 : La carte SD n'est pas disponible.
			2 : Une erreur du système de fichiers est détectée.
			3 : L'espace disponible sur la carte SD est insuffisant.
			4 : L'espace mémoire est insuffisant.
			5 : La variable n'est pas disponible.
			6 : La table est pleine.
			7 : La carte SD est occupée.
			8 : Une erreur système est détectée.

Journalisation des données et Hot Standby

Le service de journalisation des données du module s'exécute dans les modes primaire et redondant au sein d'un système à redondance d'UC (Hot Standby). Les deux modules répondent lorsque vous déclenchez une action de journalisation, de sauvegarde ou de purge.

Le DDT d'équipement affiche toujours le résultat du déclenchement pour le module jouant le rôle primaire. Lors d'une permutation Hot Standby, l'état du module qui assume le rôle primaire est remplacé.

Vous pouvez télécharger les fichiers de journalisation de données de sauvegarde des modules primaire et redondant depuis le Web. Les deux modules ne présentent pas nécessairement les mêmes données de journalisation, d'horodatage et d'état de carte SD.

Diagnostics des pages Web et des DDT d'équipement

Introduction

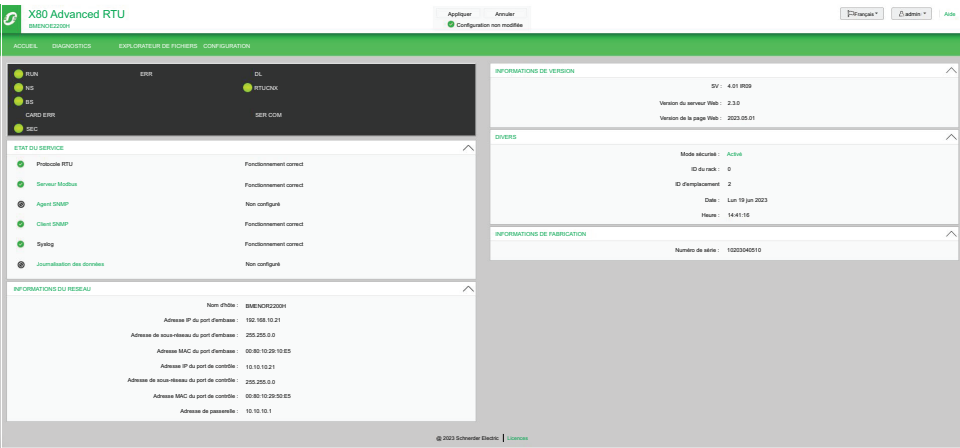
Ce chapitre décrit les diagnostics du BMENOR2200H dans les pages Web et le DDT d'équipement tels que configurés dans une application Control Expert.

Accès aux pages Web

Introduction

Le module BMENOR2200H intègre un serveur Web qui fournit diverses pages Web offrant des fonctions de configuration, de diagnostic, de cybersécurité et de surveillance.

Accédez aux pages Web du module BMENOR2200H en saisissant l'adresse IP ou l'URL du module dans un navigateur Web.



Voici les principaux onglets de la page **Accueil** :

- **DIAGNOSTICS**, page 180: Cet onglet permet de configurer les diagnostics pour les pages Web du BMENOR2200H et le DDT d'équipement tels qu'ils sont configurés dans une application Control Expert.
- **EXPLORATEUR DE FICHIERS**: Accédez aux informations de journalisation des données via l'explorateur de fichiers.
- **CONFIGURATION**, page 202: Accédez à cet onglet pour définir la sécurité et les droits d'accès associés au module.

Navigateurs pris en charge

Respectez les exigences suivantes concernant les versions de navigateur requises pour utiliser les pages Web :

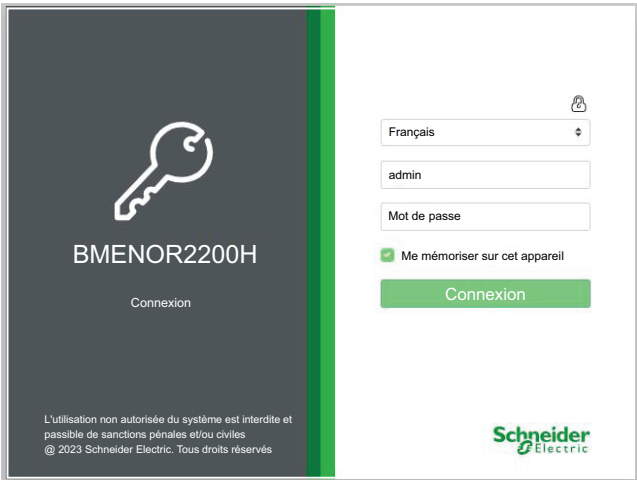
Navigateur	Version requise
Google Chrome	50+ (recommandation)
Mozilla Firefox	40+
Microsoft Edge	14+
Internet Explorer	11

Connexion via le protocole HTTPS

Si votre application rencontre des problèmes de connexion, vérifiez auprès de votre service informatique local que votre configuration réseau et vos règles de sécurité sont cohérentes avec l'accès HTTPS (port 443) à l'adresse IP du module BMENOR2200H.

Le module BMENOR2200H accepte les connexions HTTPS avec le protocole TLS (Transport Layer Security) de version 1.2 ou ultérieure. Par exemple, Windows 7 peut nécessiter une mise à jour pour activer TLS 1.2 en vue de mettre à niveau le micrologiciel du module BMENOR2200H ou d'accéder à son site Web.

Accès aux pages Web

Etape	Action
1	Saisissez l'adresse IP ou l'URL (https://...) du module dans un navigateur Web pour ouvrir la page Accueil du module.  NOTE: • L'accès Web via l'URL n'est pas pris en charge par le module BMENOR2200H, mais il peut être implémenté par l'intégration système. • Il se peut qu'un message s'affiche pour indiquer que les pages Web ne sont pas sécurisées. Ignorez ce message et ouvrez la page Web. • Lorsque le module traite une charge de communication importante, il se peut que la page Web ne s'ouvre pas immédiatement. Dans ce cas, exécutez la fonction d'actualisation du navigateur.
2	Dans le menu déroulant, sélectionnez la langue appropriée.
3	Entrez le nom d'utilisateur et le mot de passe par défaut correspondant au mode de cybersécurité sélectionné lorsque vous accédez au Web pour la première fois : • Mode de cybersécurité Advanced : ◦ <i>nom d'utilisateur</i> : admin ◦ <i>mot de passe</i> : password • Mode de cybersécurité Standard : ◦ <i>nom d'utilisateur</i> : installer ◦ <i>mot de passe</i> : Inst@ller1
4	Cliquez sur le bouton Connexion .
5	Modifiez votre nom d'utilisateur et votre mot de passe lorsque vous y êtes invité.

Diagnostics des pages Web

Introduction

Cette section décrit les diagnostics des pages Web du BMENOR2200H tels que configurés dans une application Control Expert.

Diagnostics des pages Web

Accès aux diagnostics

Accédez aux informations de diagnostic du module BMENOR2200H via les pages Web :

Etape	Action
1	Sélectionnez Outils > Navigateur de DTM pour ouvrir votre DTM de projet.
2	Double-cliquez sur le DTM du module BMENOR2200H.
3	Dans la boîte de dialogue Configuration du DTM, développez Général et sélectionnez Informations du module .
4	Dans le volet de droite, faites défiler la page jusqu'en bas de la boîte de dialogue pour afficher la zone des diagnostics Web .
5	Cliquez sur le bouton Adresse IP pour accéder aux pages Web de diagnostic.
6	Sélectionnez l'onglet Diagnostics .
7	Développez le MENU pour afficher les pages de diagnostic disponibles : • MODULE ◦ Récapitulatif des états ◦ Etat HSBY ◦ Etat du tampon d'événements ◦ Statistiques des ports • EQUIPEMENTS CONNECTES ◦ Protocole RTU ◦ Messagerie • SERVICES ◦ SNTP ◦ Horloge ◦ Journalisation des données ◦ SNMP

Diagnostics du module

Récapitulatif des états

Surveillez l'état du module à l'aide des paramètres suivants :

Champ	Description
RUN, ERR	<i>vert</i> <i>rouge</i> NOTE: Les informations de diagnostic sont décrites dans la section relative à l'activité et la signification des voyants.
ETAT DU SERVICE	Surveillez les performances de chaque service répertorié sur la liaison de communication : <i>vert</i> : Le service fonctionne normalement. <i>rouge</i> : Une erreur est détectée pour le service. <i>noir</i> : Le service est absent ou n'est pas configuré.
INFORMATIONS DU RESEAU	Nom d'hôte : Ce champ indique le nom d'hôte du module (BMENOR2200H).
	Adresse IP du port d'embase : Ce champ indique l'adresse IP du port d'embase.
	Adresse de sous-réseau du port d'embase : Ce champ indique l'adresse de sous-réseau du port d'embase.
	Adresse MAC du port d'embase : Ce champ indique l'adresse MAC du port d'embase.
	Adresse IP du port de contrôle : Ce champ indique l'adresse IP du port de contrôle. NOTE: Lorsque les deux ports sont désactivés ou que le câble n'est pas connecté au port activé, l'adresse IP est 0.0.0.0.
	Adresse de sous-réseau du port de contrôle : Ce champ indique l'adresse de sous-réseau du port de contrôle.
	Adresse MAC du port de contrôle : Ce champ indique l'adresse MAC du port de contrôle.
INFORMATIONS DE VERSION	Adresse de la passerelle : Ce champ indique l'adresse de passerelle du port de contrôle.
	Affiche les versions logicielles qui s'exécutent sur le module : SV Version de serveur Web Version de page Web
DIVERS	Mode de cybersécurité : L'état du service de sécurité (activé ou désactivé) est indiqué.
	ID de rack : Ce champ identifie le rack local (0).
	ID d'emplacement : Ce champ indique le numéro d'emplacement dans lequel le module BMENOR2200H est installé.
	Date : Ce champ indique la date du module BMENOR2200H.
	Heure : Ce champ indique l'heure du module BMENOR2200H.
INFORMATIONS DE FABRICATION	Affiche le numéro de série de l'appareil.

Diagnostic de la redondance d'UC (Hot Standby)

Ces champs figurent dans la page de diagnostic des performances du mode de redondance d'UC (Hot Standby - HSBY) :

- **ÉTAT DU SERVICE** : Définit si le service HSBY fonctionne correctement.
- **ÉTAT DE SYNCHRONISATION** : Définit si l'état de redondance d'UC se synchronise correctement.
 - NOTE:** Si aucune voie client ou serveur RTU n'est configurée dans le DTM du module, page 113, cet état de synchronisation reste à *En cours* et le voyant ERR (erreur détectée) clignote.
- **VALIDITÉ DES PARAMÈTRES** : Définit si des équipements partenaires sont valides dans un système de redondance d'UC.
- **COMPTEUR DE SYNCHRONISATION** : Décrit la valeur numérique du compteur de synchronisation.
- **DERNIÈRE SYNCHRONISATION** : Dernière synchronisation de l'état HSBY, au format date/heure.
- **STATISTIQUES SUR LES PAQUETS** : Définit l'état de chaque ensemble de paquets :
 - Paquets entrants
 - Paquets sortants
 - Paquets entrants contenant des erreurs
 - Paquets sortants contenant des erreurs
- **ERREURS DÉTECTÉES** : Décrit les codes d'erreur détectés dans le système HSBY.
- **ÉTAT DE SYNCHRONISATION DES ÉVÉNEMENTS** : Définit si la synchronisation des événements est activée pour les modules BMENOR2200H du système HSBY.
- **MODULE LOCAL/MODULE DISTANT** : Définit l'état de ces paramètres pour les modules locaux et distants :
 - Rôle : Primaire ou Redondant
 - Adresse IP
 - Version de micrologiciel

Etat du tampon d'événements

Afficher l'état du tampon d'événements du module pour la mise en service des communications :

Paramètre	Description
UTILISATION DU TAMPON D'ÉVÉNEMENTS	Indique le pourcentage du tampon d'événements consommé.
DEPASSEMENT DU NOMBRE D'ÉVÉNEMENTS	Ce champ indique si la capacité du tampon d'événements est dépassée.
UTILISATION DES RESSOURCES D'ÉVÉNEMENT	Indique le pourcentage de ressources d'événement consommées.
SAUVEGARDE DES ÉVÉNEMENTS	Activé : Les événements sont sauvegardés.
	Désactivé : Les événements ne sont pas sauvegardés.
ÉTAT DE L'ÉVÉNEMENT DE VOIE/POINT	N° : Ce numéro représente la séquence des connexions d'équipement.
	Nom de la voie : Il s'agit du nom de voie DNP3 configuré.
	% d'utilisation du tampon d'événements actuel : Indique le pourcentage du tampon d'événements qui est consommé.
	Nombre d'événements actuels : Nombre d'événements en mémoire tampon.
	Nombre d'événements configurés : Taille configurée du tampon d'événements.
	Nombre d'événements actuellement en excès : Nombre d'événements qui ne se trouvent pas en mémoire tampon en raison d'un débordement de capacité de celle-ci.
	Débordement total actuel : Nombre total d'événements de débordement pour le module.
	NOTE : Cliquez sur le signe plus (+) ou moins (-) pour développer ou réduire une voie dans la page État du tampon d'événements afin d'afficher l'état détaillé du point de vue du module.

Statistiques des ports

La page **Statistiques des ports** fournit les statistiques relatives à la connexion Ethernet frontale et à la connexion d'embase du module :

Paramètre	Description
Ports	vert : Le port est actif.
Vitesse	Ce champ indique la vitesse du port configurée (0, 100, 1000 Mbps/s).
Duplex, Semi	Le mode duplex est composé d'une combinaison des éléments suivants : • TP/Fibre • -Intégral/-Semi/-Aucun • Liaison/(aucun mot) • Néant NOTE : Lorsque le treizième bit du mot dans la réponse Modbus est à 1, " Liaison " est ajouté à la chaîne du mode duplex (TP-Intégral Liaison , TP-Semi Liaison , etc.).
Total erreurs	Ce champ indique le nombre d'erreurs détectées.
Taux de réussite	Ce champ indique le pourcentage de requêtes qui ont abouti par rapport au nombre total de requêtes.
Activer/désactiver la vue détaillée	Cliquez sur ce bouton pour développer ou réduire la liste des statistiques des ports.

Ce tableau décrit les paramètres des statistiques de port :

Paramètre	Description
Trames transmises	Ce champ indique le nombre de trames correctement transmises à partir du port.
Trames reçues	Ce champ indique le nombre de trames reçues depuis le port.
Collisions excessives	Ce champ indique le nombre de fois où la transmission d'une trame Ethernet sur ce port a échoué en raison d'un excès de collisions (plus de 16 tentatives par paquet).
Collisions tardives	Ce champ indique le nombre de collisions détectées après l'expiration du délai lié à l'emplacement de la voie. NOTE: Ce champ n'est renseigné que si le matériel fournit les informations correspondantes.
Erreurs CRC	Ce champ indique le nombre de trames reçues pour lesquelles le contrôle de redondance cyclique (CRC) n'est pas valide. Une erreur de CRC détectée est une statistique RMON qui combine les valeurs des paramètres Erreurs FCS et Erreurs d'alignement .
Octets reçus	Ce champ indique le nombre d'octets reçus sur le port.
Paquets entrants contenant des erreurs	Ce champ indique le nombre de paquets reçus sur le port pour lesquels des erreurs sont détectées. NOTE: Les Sortants ignorés ne sont pas comptabilisés.
Paquets entrants ignorés	Ce champ indique le nombre de paquets entrants reçus sur le port mais ignorés.
Octets émis	Ce champ indique le nombre d'octets envoyés sur le port.
Paquets sortants contenant des erreurs	Ce champ indique le nombre de paquets envoyés sur le port pour lesquels des erreurs sont détectées. NOTE: Les Sortants ignorés ne sont pas comptabilisés.
Paquets sortants ignorés	Ce champ indique le nombre de paquets sortants envoyés sur le port mais ignorés.
Erreurs de détection de porteuse	Ce champ indique le nombre de fois où la condition de détection de porteuse a été perdue ou n'a jamais été confirmée lors d'une tentative d'émission de trame sur ce port.
Erreurs FCS	Ce champ indique le nombre de trames reçues sur ce port qui comprennent un nombre entier d'octets mais ont été rejetées par la vérification FCS.
Erreurs d'alignement	Ce champ indique le nombre de trames reçues sur ce port qui ne comprennent pas un nombre entier d'octets et qui ont été rejetées par la vérification FCS.
Erreurs émission MAC internes	Ce champ indique le nombre de trames que le port ne transmet pas correctement en raison d'une erreur de transmission de la sous-couche MAC interne.
Erreurs réception MAC internes	Ce champ indique le nombre de trames que le port ne reçoit pas correctement en raison d'une erreur de réception de la sous-couche MAC interne.
Erreurs de test SQE	Ce champ indique le nombre de réceptions d'erreur de test SQE sur le port. NOTE: Ce compteur ne s'incrémente pas sur les ports qui fonctionnent à des débits supérieurs à 10 Mbits/s, ni sur les ports en mode duplex intégral.

La page **Statistiques des ports** fournit les statistiques de connexion des ports série du module après activation :

Paramètre	Description
Etat du port RJ45 série	Vert : le port est actif.
	Noir : le port est inactif
Débit en bauds	Ce champ indique le débit en bauds configuré du port série (300 à 115200).
Ligne physique	Ce champ indique la configuration de l'interface physique (RS485 ou RS232).
Octets reçus	Ce champ indique le nombre de trames reçues.
Octets émis	Ce champ indique le nombre de trames transmises.
Error Frame Counter	Ce champ indique le nombre de trames d'erreur détectées.

Diagnostics des équipements connectés

Protocole RTU

Le tableau suivant indique l'état de la connexion RTU des équipements client et des unités RTU serveur :

Paramètre	Description
Nombre d'appareils déconnectés/en cours de connexion	Cette valeur représente le nombre d'équipements connectés.
Nombre d'appareils déconnectés	Cette valeur représente le nombre d'équipements déconnectés.
CONNEXIONS RTU - SERVEURS / CLIENTS	N° : Ce numéro représente la séquence des connexions d'équipement.
	Nom de la voie : Il s'agit du nom de voie DNP3/IEC60870 configuré.
	Protocole : Ce champ indique le protocole de connexion implémenté.
	Mode de voie : Ce champ indique le mode de voie (Lecture seule ou Standard) du serveur IEC60870-5-104.
	Groupe redondant : Ce champ indique le numéro d'ID du groupe redondant.
	Etat : Etat de la connexion (Connecté , Connexion en cours , Déconnecté).
	Adresse distante : Adresse IP distante.
	Port distant : Port TCP distant.
	Port local : Port TCP local.
	Statistiques sécurisées : Voir Statistiques détaillées pour plus d'informations sur une version d'authentification sécurisée spécifique.
	Code d'erreur : Voir Code d'erreur pour plus d'informations sur une erreur détectée spécifique.

Messagerie

Ce tableau contient des informations sur l'échange de données en termes de statistiques Modbus :

Paramètre	Description
STATISTIQUES DE MESSAGERIE	Consultez le nombre total de messages envoyés et reçus sur le port 502 : • Messages envoyés : Ce champ indique le nombre de messages envoyés à partir du port 502. • Messages reçus : Ce champ indique le nombre de messages reçus par le port 502. • Taux de réussite : Ce champ indique le pourcentage de requêtes qui ont abouti par rapport au nombre total de requêtes. NOTE: Ces valeurs ne sont pas réinitialisées lorsque la connexion du port 502 se ferme. Les valeurs tiennent donc compte du nombre de messages échangés depuis le dernier redémarrage du module.
CONNEXIONS ACTIVES	Affiche les connexions qui sont en activité au moment de l'actualisation de la page Messagerie : • Adresse distante : Cette colonne indique l'adresse IP distante. • Port local : Cette colonne indique le port TCP local. • Type : Cette colonne indique le type de connexion. • Envoyés : Cette colonne indique le nombre de messages envoyés à partir de cette connexion. • Reçus : Cette colonne indique le nombre de messages reçus par cette connexion. • Erreurs : Cette colonne indique le nombre d'erreurs détectées concernant cette connexion.

Diagnostics des services

Introduction

Développez le nœud **MENU** de l'onglet **DIAGNOSTICS** pour consulter et configurer les paramètres **SERVICES** suivants :

- SNTP
- Horloge
- Journalisation des données
- SNMP

Diagnostics du service SNTP

Le tableau suivant décrit les paramètres SNTP utilisés pour le diagnostic du service :

Paramètre	Description
ETAT DU SERVICE	Marche : Le service correctement configuré est en cours d'exécution.
	Désactivé : Le service est désactivé.
	Inconnu : L'état du service est inconnu.
TYPE DE SERVEUR	Primaire : Un serveur primaire interroge un serveur de temps client pour connaître l'heure actuelle.
	Secondaire : Un serveur secondaire interroge un serveur de temps client pour connaître l'heure actuelle.
DATE ACTUELLE	Ce champ affiche la date actuelle dans le fuseau horaire sélectionné.
ETAT DU SERVEUR	<i>vert</i> : Le serveur est connecté et en cours d'exécution.
	<i>rouge</i> : Une erreur de serveur est détectée.
	<i>gris</i> : L'état du serveur est inconnu.
HEURE D'ETE	Activé : La gestion de l'heure d'été et configurée et active.
	Désactivé : La gestion de l'heure d'été est désactivée.
	Inconnu : L'état du service d'heure d'été est inconnu.
HEURE ACTUELLE	Ce champ indique l'heure du jour.
FUSEAU HORAIRE	Ce champ indique le fuseau horaire associé au module.

Diagnostics du service d'horloge

Le tableau suivant décrit les paramètres d'horloge utilisés pour diagnostiquer le service :

Paramètre	Description
DATE ET HEURE ACTUELLES	Date (date du module)
	Heure (heure du module)
FUSEAU HORAIRE	(fuseau horaire du module)
DERNIERE SYNCHRONISATION HORAIRE	Date (horodatage de synchronisation)
	Heure (horodatage de synchronisation)
	Source horaire (horodatage de synchronisation) : • CPU : Si le protocole RTU est configuré, le RTU peut obtenir son heure initiale auprès du contrôleur lorsque le protocole RTU démarre ou redémarre. • RTU : Ce champ indique la source horaire lorsqu'un système SCADA ou un client synchronise son heure avec RTU. • SNTP : Si le client SNTP est activé et connecté au serveur SNTP, sa source horaire provient d'un serveur SNTP qui s'aligne sur l'horloge interne du module BMENOR2200H.

Diagnostics du service de journalisation des données

Le tableau suivant décrit les paramètres de journalisation des données utilisés pour diagnostiquer le service :

Paramètre	Description
ETAT DU SERVICE	<i>Activé</i> : Le service de journalisation des données est activé.
	<i>Fonctionnement correct</i> : Le service de journalisation des données est activé et fonctionne normalement.
	<i>Désactivé</i> : Le service de journalisation des données n'est pas activé.
	<i>Non configuré</i> : Le service de journalisation des données n'est pas configuré.
	<i>Au moins une connexion est incorrecte</i> : Une connexion matérielle incorrecte arrête le service de journalisation des données.
	<i>Activé (allumé)</i> : Le service de journalisation des données est activé.
	<i>Activé (éteint)</i> : Le service de journalisation des données est désactivé.
ETAT DE LA CARTE SD	<i>Carte présente</i> : La carte SD est présente dans le module et elle peut être utilisée pour les fonctions de journalisation des données.
	<i>Alarme de manque d'espace</i> : L'espace libre sur la carte SD est inférieur à 20 %.
	<i>Carte occupée</i> : La carte SD est occupée.
	<i>Carte manquante</i> : La carte SD n'est pas disponible.
ESPACE LIBRE SD	Quantité d'espace disponible en Ko sur la carte SD.

La table de journalisation des données contient les colonnes suivantes :

Colonne	Description
<i>Nom de la table</i>	Cette colonne indique les noms des tables créées. NOTE: Le nom de la table est généré par la réponse Modbus.
<i>Etat de la table</i>	<i>Activé</i> : La table est activée.
	<i>Désactivé</i> : La table est désactivée.
<i>Nombre de sauvegardes (carte SD)</i>	Lorsque ce nombre est atteint, les nouvelles données écrasent les anciennes données sur la carte SD.
<i>Nombre d'enregistrements</i>	Cette valeur représente le nombre d'enregistrements pris en compte pour établir le résultat.
<i>Etat de la dernière journalisation</i>	<i>Réussite</i> : Aucune erreur n'a été détectée lors de la dernière exécution du service de journalisation des données.
	<i>Manque d'espace mémoire</i> : La mémoire disponible n'était pas suffisante pour exécuter le service de journalisation des données.
	<i>Variable non disponible</i> : Le service de journalisation des données nécessite une variable qui n'est pas disponible.
	<i>Table saturée</i> : La fonction de journalisation continue d'enregistrer lorsque la table atteint la capacité indiquée par cette valeur.
	<i>Erreur système</i> : La détection d'une erreur système a bloqué l'exécution du service de journalisation des données.
<i>Etat de la dernière sauvegarde</i>	<i>Réussite</i> : Aucune erreur n'a été détectée lors de la dernière sauvegarde des fichiers de journalisation des données.
	<i>Aucune carte SD compatible</i> : La carte SD n'est pas compatible avec la sauvegarde des données journalisées.
	<i>Erreur du système de fichiers</i> : La détection d'une erreur du système de fichiers a bloqué l'exécution de la sauvegarde.
	<i>Espace insuffisant sur la carte SD</i> : La mémoire disponible sur la carte SD n'était pas suffisante pour exécuter la sauvegarde.
	<i>Carte SD occupée</i> : La carte SD est verrouillée ou protégée en écriture.
	<i>Erreur système</i> : La sauvegarde n'a pas été possible en raison de la détection d'une erreur de traitement.
<i>Dernière sauvegarde réussie</i>	Cette colonne indique la date et l'heure de la dernière sauvegarde réussie du fichier journal de données.

Diagnostics du service SNMP

Ce tableau indique les états possibles pour le diagnostic du service SNMP :

Paramètre	Description
ETAT DU SERVICE	<i>fonctionnement correct</i> : L'agent SNMP est activé pour les services réseau et fonctionne correctement.
	<i>désactivé</i> : L'agent SNMP est désactivé pour les services réseau.
	<i>non configuré</i> : La version configurée dans le DTM ne correspond pas à celle de la configuration Web.
VERSION SNMP	V1 : Sélectionner la version 1 (SNMPv1).
	V3 : Sélectionner la version 3 (SNMPv3).
	<i>Inconnu</i> : La version de SNMP est inconnue.
DIAGNOSTIC	<i>Paquets entrants</i> : Cette valeur représente le nombre de paquets SNMP reçus.
	<i>Paquets sortants</i> : Cette valeur représente le nombre de paquets SNMP envoyés.
	<i>Versions incorrectes reçues</i> : Cette valeur représente le nombre de paquets SNMP reçus d'une version de SNMP non prise en charge.
	<i>Stats USM - Noms d'utilisateur inconnus</i> (SNMPv3 uniquement) : Cette valeur représente le nombre de paquets pour lesquels la fonction SNMPv3 est interrogée par un utilisateur qui n'est pas reconnu d'après le modèle de sécurité utilisateur (USM).
	<i>Stats USM - Abrégés incorrects</i> (SNMPv3 uniquement) : Cette valeur représente le nombre de paquets pour lesquels la fonction d'interrogation SNMPv3 utilise un mot de passe ou un algorithme de synthèse qui est incorrect d'après le modèle de sécurité utilisateur (USM).
	<i>USM - Modèles de sécurité inconnus</i> (SNMPv3 uniquement) : Cette valeur représente le nombre de paquets SNMP demandés à partir d'un niveau de sécurité inconnu d'après le modèle de sécurité utilisateur (USM).

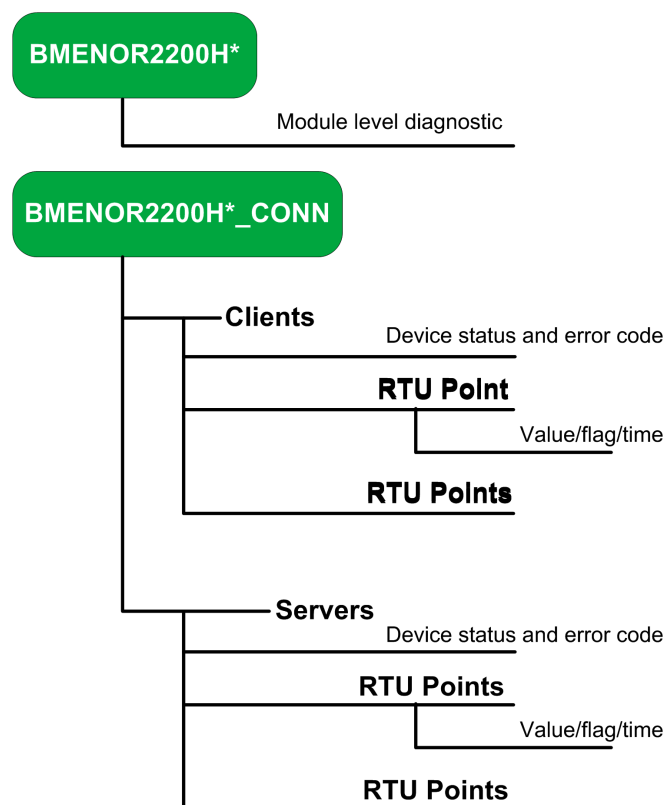
Diagnostic de DDT d'équipement

Introduction

Cette section décrit les diagnostics du DDT d'équipement pour le module BMENOR2200H dans une configuration de redondance d'UC (Hot Standby).

Structure des DDT d'équipement

Représentation graphique



* *customer-defined name*

Dans l'onglet de configuration de DTM du serveur, la structure de DDT d'équipement (variable non localisée) se présente comme suit :

Name	Type
BME_NOR_2200H	T_BME_N...
BME_NOR_2200H_CONN	T_BME_N...
Client00	T_BME_N...
Device_State	BYTE
Error_Code	WORD
AI_P0_P0	ARRAY[0...
BOST_P0_P0	Bin_Outpu...
BI_P0_P0	Binary_Inp...
TmSync_0000_CB	Time_Sync
BCnt_P0_P0	Counter_...
Server00	T_BME_N...
Device_State	BYTE
Error_Code	WORD
BI_P0_P0	ARRAY[0...
DI_P0_P0	ARRAY[0...
AI_P0_P0	Analog_In...
Flags	BYTE
Timestamp	CP56Time...
Value	DINT
AO_P0_P0	Analog_O...
BI_P10_P10	Binary_Inp...
Event_STAT_BinaryInput	EVENT_S...
Event_STAT_BinaryOutput	EVENT_S...
Event_STAT_AnalogInput	EVENT_S...

Correspondances

Ces correspondances s'appliquent à la structure et à la représentation graphique de DDT ci-dessus :

- Le nom de variable défini par le client correspond au type T_BME_NOR.
- Le client correspond aux points RTU suivants :
 - Device_State : type BYTE
 - Error_Code : type WORD
 - AI_Px : type Analog_input_xxx
NOTE: Lorsque le nombre de points est inférieur à 1, le type de point utilise le format de tableau ARRAY.
 - BOST_P0_P0 : type Bin_Output_xxx
 - BI_P0_P0 : type Binary_Input_xxx
 - TmSync_0000_CB : type Time_Sync
 - BCnt_P0_P0 : type Counter_...
- Le serveur correspond aux points RTU suivants :
 - Device_State : type BYTE
 - Error_Code : type WORD
 - BI_P0_P0 : type Binary_Input_xxx
 - DI_P0_P0 : type Double_Input_xxx
 - AI_P0_P0 : type Analog_Input (Drapeaux, Horodatage, Valeur)
 - AO_P0_P0 : type Analog_Output
 - BI_P10_P10 : type Binary_Input_xxx
 - Event_STAT_BinaryInput : type WORD (compteur) ; type BYTE (débordement)
 - Event_STAT_BinaryOutput : type WORD (compteur) ; type BYTE (débordement)
 - Event_STAT_AnalogInput : type WORD (compteur) ; type BYTE (débordement)

Diagnostic de DDT d'équipement

Accès aux diagnostics

Afficher les diagnostics de DDT d'équipement pour le module BMENOR2200H :

1. Accédez à l'onglet **Variables** de l'éditeur de données (**Navigateur de projet > Projet > Variables et instances FB**).
2. Cochez la case **DDT d'équipement**.

NOTE: La colonne **Nom** affiche le nom attribué lorsque vous ajoutez le module au projet.

Diagnostics du module

Affichez le DDT d'équipement pour les diagnostics du module BMENOR2200H :

Nom du diagnostic		Commentaire
ETH_STATUS		Etat Ethernet
	ETH_BKP_PORT_LINK	Liaison établie/interrompue pour le port d'embase Ethernet
	SCANNER_OK	Scrutateur OK et scrutation d'au moins un équipement (si au moins un équipement est configuré)
	GLOBAL_STATUS	0 : Un ou plusieurs services ne fonctionnent pas normalement.
		1 : tous opérationnels
	NETWORK_HEALTH	1 : Aucune surcharge de trafic détectée.
		0 : Surcharge de trafic détectée (par exemple, tempête de diffusion) NOTE: Vérifiez la topologie et la configuration de votre réseau.
	PORT1_LINK	Liaison établie/interrompue pour le port de contrôle 1
	PORT2_LINK	Liaison établie/interrompue pour le port de contrôle 2
IN_PACKETS		Nombre de paquets reçus sur l'interface
IN_ERRORS		Nombre de paquets entrants contenant des erreurs
OUT_PACKETS		Nombre de paquets envoyés sur l'interface
OUT_ERRORS		Nombre de paquets sortants contenant des erreurs
SERVICE_STATUS		Un bit pour chaque caractéristique observable par l'utilisateur
	PORT502_SERVICE	0 : Le service ne fonctionne pas normalement.
		1 : Le service fonctionne normalement ou est désactivé
	SNMP_SERVICE	0 : Le service ne fonctionne pas normalement.
		1 : Le service fonctionne normalement ou est désactivé.
	IP_ADDRESS_STATUS	Etat de l'adresse IP (0 en cas d'adresse IP en double ou d'absence d'adresse IP attribuée)
	SNTP_CLIENT	0 : Le service ne fonctionne pas normalement.
		1 : Le service fonctionne normalement ou est désactivé
	WEB_SERVER	0 : Le service ne fonctionne pas normalement.
		1 : Le service fonctionne normalement ou est désactivé
	FIRMWARE_UPGRADE	0 : Le service ne fonctionne pas normalement.
		1 : Le service fonctionne normalement ou est désactivé
	CONTROL_NETWORK_MAIN_IP_ADDR	Etat de l'adresse IP principale (0 en cas d'adresse IP en double ou non attribuée)
	TIME_VALID	0 : Heure non valide
		1 : Heure valide
	LLDP_SERVICE	Etat de l'adresse IP A/B (0 en cas d'adresse IP en double ou d'absence d'adresse IP attribuée)
	SYSLOG_STATUS	0 : Le service Syslog ne fonctionne pas normalement
		1 : Le service Syslog fonctionne normalement ou est désactivé
	SYSLOG_SERVER_NOT_REACHABLE	1 : Aucun acquittement reçu du serveur Syslog

Nom du diagnostic		Commentaire
		0 : autres cas
	SMTP_SERVICE	0 : Le service ne fonctionne pas normalement. 1 : Le service fonctionne normalement ou est désactivé
	DATALOGING	0 : Le service ne fonctionne pas normalement. 1 : Le service fonctionne normalement ou est désactivé
	RTU_DNP3	0 : Le service ne fonctionne pas normalement. 1 : Le service fonctionne normalement ou est désactivé
	RTU_IEC60870	0 : Le service ne fonctionne pas normalement. 1 : Le service fonctionne normalement ou est désactivé
	SD_STATUS	Bit 0 (STATUS) : Défini lorsque la carte est normale Bit 1 (BUSY) : Défini lorsque la carte est occupée Bit 2 (LOW_SPACE_ALARM) : Défini lorsque l'espace libre sur la carte est inférieur à 2 %
	FIRMWARE_VERSION	Octet de poids fort : Révision majeure [HEX] Octet de poids faible : Révision mineure [HEX]
	HW_VERSION	Version du matériel [HEX]
	ETH_PORT1_2_STATUS	Etat des ports de contrôle 1 et 2
	PROTOCOL_STATUS	Variable générale pour l'état du protocole RTU
	EVENT_OVERFLOW_COUNT	Nombre total d'événements en débordement
	EVENT_BUFFER_USAGE	Pourcentage du tampon d'événements utilisé dans la taille configurée
	DNP3_CLIENT_CONNECTION_COUNT	Nombre total de connexions client DNP3
	DNP3_SERVER_CONNECTION_COUNT	Nombre total de connexions serveur DNP3
	IEC60870_CLIENT_CONNECTION_COUNT	Nombre total de connexions client IEC60870
	IEC60870_SERVER_CONNECTION_COUNT	Nombre total de connexions serveur IEC60870
	MODBUS_CLIENT_CONNECTION_COUNT	Nombre total de connexions client Modbus
	MODBUS_SERVER_CONNECTION_COUNT	Nombre total de connexions serveur Modbus
CS_STATUS		—
	SECURE_MODE	Etat de la roue de codage : 0 : Standard 1 : Avancé
	CS_LED_STATUS	Etat des voyants de cybersécurité

Diagnostics de la redondance d'UC (Hot Standby)

Vous ne pouvez voir tous les diagnostics de DDT d'équipement dédiés pour un module BMENOR2200H d'un système Hot Standby qu'après avoir configuré au moins une voie RTU dans le DTM :

Diagnostic		Valeur	Type	Commentaire
HTSB_DIAG			T_HTSB_DIAG	—
	SERVICE_STATE	0	BYTE	Etat du service HTSB : 0 : Problème détecté 1 : En cours d'exécution
	SYNC_STATE	0	BYTE	Etat de synchronisation HTSB : 0 : En cours 1 : OK
	INTERNAL_STATE	0	BYTE	Etat HTSB interne : 0 : Init 1 : Liaison établie 2 : Réserve 3 : Intégrité 4 : Attente de synchronisation 5 : Synchronisé
	PARTNER_VALIDITY	0	BYTE	Validité du partenaire : 0 : Injoignable 1 : OK
	ERROR_CODE	0	WORD	Bit 0 : Micrologiciel non concordant
				Bit 1 : Configuration de DTM non concordante
				Bit 2 : Mode de sécurité non concordant
				Bit 3 : Erreur de certification DTLS
				Bit 4 : Non-concordance de configuration CS (réserve)
				Bits 5 à 15 : Réserve
	FW_VERSION_MISMATCH	0	BOOL	Les applications des modules primaire et redondant fonctionnent avec une version de micrologiciel différente
	DTM_CFG_MISMATCH	0	BOOL	Les applications des modules primaire et redondant fonctionnent avec une configuration DTM différente
	CS_CFG_MISMATCH	0	BOOL	Les applications des modules primaire et redondant s'exécutent avec une configuration CS différente
	CERTIFICATION_ERROR	0	BOOL	Erreur de certification DTLS
	SYNC_COUNT	0	UDINT	Compteur de synchronisation HTSB
	DIN_PACKETS	0	UDINT	Compteur de paquets d'entrée HTSB
	N_ERRORS	0	UDINT	Compteur de paquets d'erreurs d'entrée HTSB
	OUT_PACKETS	0	UDINT	Compteur de paquets de sortie HTSB
	OUT_ERRORS	0	UDINT	Compteur de paquets d'erreurs de sortie HTSB

Diagnostics RTU

Vous ne pouvez afficher le DDT d'équipement pour les diagnostics de communication RTU BMENOR2200H qu'après avoir configuré au moins une voie RTU dans le DTM :

Nom du diagnostic		Valeur	Type	Commentaire		
Diagnostics du protocole RTU						
Freshness		0	BOOL	Toutes les variables DDT d'équipement du module sont actuelles		
Scan_State		0	BYTE	0 : Inactif		
				1 : Occupé		
HSBY_Event_Index		0	UDINT	Numéro d'index de l'événement actuel généré dans le module		
HSBY_EventSync_Index		0	UDINT	Numéro d'index de l'événement actuel synchronisé sur le module redondant		
Diagnostics des voies/équipements						
<voie_client>		—	—	Le nom de la voie (<voie_client>, <voie_serveur>) correspond au nom attribué lors de la phase de configuration des voies.		
<voie_serveur>		—	—			
	Device_state		0	BYTE	0 : Non connecté	
					1 : Connecté	
	Error_Code		0	WORD	Bit 0 (security_not_configured) : Sécurité non configurée.	
					Bit 1 (variable_initialize_error) : Erreur d'initialisation de variable	
					Bit 2 (internal_error) : Erreur interne	
					Bit 3 (authentication_failed) : Problème d'authentification détecté	
					Bit 4 (unexpected_response) : Réponse inattendue	
					Bit 5 (no_response) : Pas de réponse	
					Bit 6 (aggressive_mode_not_supported) : Mode agressif non pris en charge	
					Bit 7 (MAC_algorithm_not_supported) : Algorithme MAC non pris en charge	
					Bit 8 (key Wrap_algorithm_not_supported) : Algorithme d'enveloppe de clé non pris en charge	
					Bit 9 (authorization_failed) : Problème d'autorisation détecté	
					Bit 10 (update_key_change_method_not_permitted) : Méthode de modification de clé de mise à jour non autorisée	
					Bit 11 (invalid_signature) : Signature non valide	
					Bit 12 (invalid_certification_data) : Données de certification non valides	
					Bit 13 (unknown_user) : Utilisateur inconnu	
					Bit 14 (max_session_key_status_requests_exceed) : Nombre maximum de requêtes d'état de clé de session dépassé	
	Bit 15 (TLS_error) : Erreur TLS					
	Unsol_Enabled (voie serveur uniquement)		—	BYTE	0 : Désactivation non sollicitée	
					1 : Activation non sollicitée	
	Event_STAT_AuthSecStats (voie serveur uniquement)		—	—		
		Count		0	WORD	
		Overflow		0	BYTE	0 : Normal
	1 : Débordement					

Explorateur de fichiers

Introduction

Accédez à l'onglet **EXPLORATEUR DE FICHIERS** du module pour accéder aux informations de journalisation des données via la page Web BMENOR2200H.

L'**EXPLORATEUR DE FICHIERS** contient deux onglets :

- **JOURNAUX DE DONNÉES** : Cet onglet affiche la liste des fichiers de journalisation de données enregistrés.
- **ARCHIVES** : Lorsque le module reçoit sa configuration, il compare la somme de contrôle à celle figurant sur la carte SD. Si les valeurs diffèrent, le module archive les anciens fichiers (y compris les tables modifiées ou non configurées) dans ce dossier d'archive dédié.

Journaux de données

Le tableau suivant décrit les colonnes du tableau de l'onglet **JOURNAUX DE DONNEES** :

Paramètre	Description
<i>Nom</i>	Cette colonne indique les noms des tables créées. NOTE: Le nom de la table est généré par la réponse Modbus.
<i>Date de modification</i>	Cette colonne indique le jour, la date et l'heure de la dernière modification de la table.
<i>Taille</i>	Cette colonne indique la taille (Ko) de la table sélectionnée.

NOTE: Cliquez sur le bouton plus (+) à la fin d'une ligne pour développer et afficher les fichiers .csv composant la table journalisée.

Archives

Le tableau suivant décrit les paramètres de l'onglet **ARCHIVES** :

Paramètre	Description
<i>Nom</i>	Cette colonne indique les noms des tables créées. NOTE: Le nom de la table est généré par la réponse Modbus.
<i>Date de modification</i>	Cette colonne indique le jour, la date et l'heure de la dernière modification de la table.
<i>Taille</i>	Cette colonne indique la taille (kilo-octets) de la table sélectionnée.

Boutons

Le tableau suivant décrit les boutons des onglets **JOURNAUX DE DONNEES** et **ARCHIVES** présentés précédemment dans ce chapitre :

Bouton	Description
Supprimer	Appuyez sur ce bouton et suivez les invites pour supprimer la table sélectionnée.
Télécharger	Appuyez sur ce bouton et suivez les invites pour télécharger la table sélectionnée.
Télécharger et supprimer	Appuyez sur ce bouton et suivez les invites pour télécharger et supprimer la table sélectionnée.

Configuration de la cybersécurité

Présentation des pages Web de cybersécurité

Introduction

Le module BMENOR2200H intègre un serveur Web HTTPS (Hyper Text Transfer Protocol Secure) qui permet d'accéder à diverses pages Web sécurisées. Utilisez ces pages pour surveiller l'état du module sans installer Control Expert ou le DTM correspondant du module.

Ces pages Web permettent d'importer, d'exporter ou de supprimer des fichiers de gestion de la cybersécurité cryptés.

Vous pouvez surveiller la sécurité des communications à l'aide du voyant **SEC**.

NOTE: L'accès aux pages Web n'est possible que lorsque le module est en mode avancé. Reportez-vous aux instructions de réglage du niveau de cybersécurité à l'aide du commutateur rotatif, page 28.

Avant de commencer

Utilisez les pages Web décrites dans ce chapitre pour appliquer les fonctions de cybersécurité au module BMENOR2200H

Les fonctionnalités de cybersécurité peuvent être appliquées au module lorsque les conditions suivantes sont remplies :

- Si vous souhaitez configurer la cybersécurité sur le protocole RTU, vous devez avoir configuré au moins une voie de communications pour le module dans le DTM Control Expert.
- Vous avez réglé convenablement (**Advanced**) le commutateur rotatif, page 28.

Connexion

La première fois que vous vous connectez au mode avancé, le fichier de cybersécurité n'est pas valide. Pour configurer ce fichier, procédez comme suit :

Etape	Description
1	Connectez-vous aux pages Web en tant qu'administrateur.
2	Accédez à la page de configuration de la cybersécurité.
3	Configurez le journal des événements avec une adresse IP valide (ou désactivez la journalisation d'événements), page 205.
4	Configurez une clé prépartagée valide ou désactivez DTLS dans HSBY.
5	Appliquez la configuration au module.

Pages Web de configuration

Introduction

Utilisez les pages Web de configuration pour communiquer avec un serveur Web du module BMENOR2200H afin de définir tous les aspects de la configuration de cybersécurité de l'équipement.



Navigation dans la page

Accédez aux liens vers les pages Web suivantes lorsque vous développez (+) **MENU** dans l'onglet **CONFIGURATION** :

- **DEVICE SECURITY SETTING** :
 - Stratégie des comptes utilisateur, page 204
 - Journaux d'événements, page 205
 - Services réseau, page 206
 - HSBY, page 208
 - SNMP, page 209
- **CERTIFICATES MANAGEMENT** :
 - Configuration PKI, page 212
 - Gestion de la liste de confiance, page 216
 - Gestion de l'AC racine, page 218

- **RTU PROTOCOL CONFIGURATION :**
 - Gestion des clés DNP3, page 220
 - Configuration du client DNP3, page 222
 - Configuration du serveur DNP3, page 223
 - Pages Web client et serveur IEC60870, page 227
- **GESTION :**
 - Gestion des utilisateurs, page 228
 - Gestion de la configuration, page 229

Page Web Stratégie des comptes utilisateur

Accès à la page

Accédez à la page Web **Stratégie des comptes utilisateur** via l'onglet **CONFIGURATION** du module BMENOR2200H (**CONFIGURATION > MENU > PARAMETRES DE SECURITE DE L'APPAREIL > Stratégie des comptes utilisateur**).

Paramètres

Configurez les paramètres suivants dans la page Web **Stratégie des comptes utilisateur** :

Paramètre		Description
PARAMETRES DE COMPTE UTILISATEUR	Inactivité maximum de session	Temporisation (minutes) des sessions inactives pour les connexions HTTPS. NOTE: Si une connexion reste inactive pendant cette durée, la session utilisateur est automatiquement fermée.
	Nombre maximum de tentatives de connexion	Cette valeur représente le nombre de tentatives de connexion infructueuses autorisées. NOTE: Lorsque cette limite est atteinte, aucune connexion supplémentaire n'est autorisée pour la période configurée.
	Minuteur de tentative de connexion	Cette valeur représente la durée maximale (minutes) allouée à la procédure de connexion.
	Durée de verrouillage du compte	Cette valeur représente la période (en minutes) pendant laquelle aucune tentative de connexion supplémentaire n'est autorisée après que le nombre maximum de tentatives configuré a été atteint. A l'expiration de cette période, un compte utilisateur verrouillé est automatiquement déverrouillé.
Envoyer		Cliquez sur ce bouton pour appliquer les nouveaux paramètres.

Exécuter les modifications

Après avoir configuré ces paramètres, appuyez sur le bouton **Appliquer** dans le bandeau de la page pour appliquer vos modifications.

NOTE: Les boutons **Appliquer** et **Annuler** sont désactivés (grisés) lorsque la configuration n'est pas valide.

Page Web Journaux d'événements

Introduction

Le module BMENOR2200H fournit le service de cybersécurité Syslog lorsque le mode Etendu est activé.

Configurez le client syslog dans le module. Les journaux sont stockés localement dans le module et échangés avec un serveur Syslog distant.

Accès à la page

Accédez à la page Web **Journaux d'événements** via l'onglet **CONFIGURATION** du module BMENOR2200H (**CONFIGURATION > MENU > PARAMETRES DE SECURITE DE L'APPAREIL > Journaux d'événements**).

Paramètres

La page Web **Journaux d'événements** contient les paramètres et réglages suivants :

Paramètre	Description
<i>Activation du service</i>	Cliquez sur ces boutons pour activer et désactiver les services de client Syslog. NOTE: Ce service est <i>activé</i> par défaut. Entrez une adresse IP valide la première fois que le module fonctionne en mode avancé pour <i>désactiver</i> le service de journalisation des événements. Sinon, le module reste en mode "configuration non valide".
<i>Adresse IP du serveur Syslog</i>	Ce champ contient l'adresse IPv4 du serveur Syslog distant. NOTE: Si vous configurez le serveur Syslog, tous les événements sont transférés vers cette adresse IP.
<i>Port du serveur Syslog</i>	Ce champ indique le numéro de port utilisé par le service client Syslog.
<i>Soumettre</i>	Cliquez sur ce bouton pour appliquer les nouveaux paramètres.

NOTE: Reportez-vous aux instructions de configuration d'un audit de cybersécurité pour la journalisation des événements dans le document Plates-formes automate Modicon - Cybersécurité, Manuel de référence.

Exécuter les modifications

Après avoir configuré ces paramètres, appuyez sur le bouton **Appliquer** dans le bandeau de la page pour appliquer vos modifications.

NOTE: Les boutons **Appliquer** et **Annuler** sont désactivés (grisés) lorsque la configuration n'est pas valide.

Page Web Services Réseau

Introduction

Les services réseau SNMP, Syslog et Modbus ne sont pas des protocoles sécurisés par nature. Ils sont sécurisés lorsqu'ils sont installés sur des équipements VPN externes.

La synergie de ces services réseau constitue un pare-feu qui autorise ou refuse le passage des communications à travers le module BMENOR2200H.

Accès à la page

Accédez à la page Web **Services réseau** via l'onglet **CONFIGURATION** du module BMENOR2200H (**CONFIGURATION > MENU > PARAMETRES DE SECURITE DE L'APPAREIL > Services réseau**).

Paramètres

Paramètre		Description
STRATEGIE GLOBALE	Appliquer la sécurité	Cliquez sur ce bouton pour désactiver tous les services réseau, sauf IPsec qui est activé.
	Déverrouiller la sécurité	Cliquez sur ce bouton pour activer tous les services réseau, sauf IPsec qui est désactivé.
ACTIVATION DES SERVICES RÉSEAU	Agent SNMP	Utilisez le menu déroulant pour activer et désactiver les communications avec l'agent SNMP.
	Serveur Modbus TCP	Utilisez le menu déroulant pour activer et désactiver le serveur Modbus TCP.
	Serveur DNP3	Utilisez le menu déroulant pour activer et désactiver le serveur DNP3.
	Serveur IEC60870	Utilisez le menu déroulant pour activer et désactiver le serveur IEC60870.
Envoyer		Cliquez sur ce bouton pour appliquer les nouveaux paramètres.

Exécuter les modifications

Après avoir configuré ces paramètres, appuyez sur le bouton **Appliquer** dans le bandeau de la page pour appliquer vos modifications.

NOTE: Les boutons **Appliquer** et **Annuler** sont désactivés (grisés) lorsque la configuration n'est pas valide.

Page Web Bannière de sécurité

Accès à la page

Cette page contient le texte modifiable qui s'affiche lorsqu'un utilisateur accède aux pages Web du module BMENOR2200H :

Accédez à la page Web **Bannière de sécurité** via l'onglet **CONFIGURATION** du module (**CONFIGURATION > MENU > PARAMETRES DE SECURITE DE L'APPAREIL > Bannière de sécurité**).

Paramètres

Vous trouverez les paramètres et réglages suivants dans la page Web **Bannière de sécurité** :

Paramètre		Description
<i>BANNIERE DE SECURITE LEGALE</i>	<i>Texte de la bannière</i>	Une chaîne de caractères s'affiche sur la page de connexion d'un utilisateur. Ce texte modifiable s'affiche par défaut : <i>L'utilisation non autorisée du système est interdite et passible de sanctions pénales et/ou civiles.</i> NOTE: La longueur maximale de la chaîne est de 128 caractères.
<i>Envoyer</i>		Cliquez sur ce bouton pour appliquer les nouveaux paramètres.

Exécuter les modifications

Après avoir configuré ces paramètres, appuyez sur le bouton **Appliquer** dans le bandeau de la page pour appliquer vos modifications.

NOTE: Les boutons **Appliquer** et **Annuler** sont désactivés (grisés) lorsque la configuration n'est pas valide.

Page Web HSBY

Introduction

Dans un système de redondance d'UC (Hot Standby), le module BMENOR2200H prend en charge la sécurité de la couche de transport des datagrammes (DTLS - Datagram Transport Layer Security). Cette fonction de cybersécurité assure une défense contre les attaques en cachant la communication de redondance d'UC dans du trafic crypté. Utilisez les paramètres suivants :

- *Activer DTLS*
- *Clé prépartagée*

Vous pouvez activer ou désactiver le protocole DTLS pour chaque module. Cette fonction est activée par défaut lorsque le module est en mode avancé. Entrez la clé prépartagée ou désactivez DTLS lors du démarrage initial du module BMENOR2200H (comme la fonction Syslog).

Accès à la page

Accédez à la page Web **HSBY** via l'onglet **CONFIGURATION** du module BMENOR2200H (**CONFIGURATION > MENU > PARAMETRES DE SECURITE DE L'APPAREIL > HSBY**).

Paramètres

Paramètre	Description
<i>Activer DTLS</i>	Sélectionnez (cochez) cette case pour activer DTLS.
	Désélectionnez cette case pour désactiver DTLS.
	NOTE: La fonction DTLS de la redondance d'UC est activée par défaut. La première fois que vous utilisez le module en mode avancé, entrez une clé prépartagée valide ou désactivez la fonction. Sinon, le module reste en mode "configuration non valide".
<i>Clé prépartagée</i>	Entrez une valeur (hexadécimale) de clé. NOTE: Il n'existe aucune valeur par défaut pour la <i>Clé prépartagée</i> . L'utilisateur doit enregistrer cette clé manuellement ou sauvegarder la configuration de cybersécurité après toute modification appliquée.
<i>Générer</i>	Cliquez sur ce bouton pour utiliser une clé générée aléatoirement.
<i>Soumettre</i>	Cliquez sur ce bouton pour appliquer les nouveaux paramètres.

Exécuter les modifications

Après avoir configuré ces paramètres, appuyez sur le bouton **Appliquer** dans le bandeau de la page pour appliquer vos modifications.

NOTE: Les boutons **Appliquer** et **Annuler** sont désactivés (grisés) lorsque la configuration n'est pas valide.

Page Web SNMP

Accès à la page

Vous pouvez accéder à la page Web **SNMP** via l'onglet **CONFIGURATION** du module BMENOR2200H (**CONFIGURATION > MENU > PARAMETRES DE SECURITE DE L'APPAREIL > SNMP**).

Paramètres

Vous trouverez les paramètres et réglages suivants dans la page Web **SNMP** :

Paramètre	Description
Version SNMP	SNMPv1
	SNMPv3
Niveau de sécurité (SNMPv3 uniquement)	Pas d'authentification, Pas de confidentialité
	Authentification, Pas de confidentialité
	Authentification, Confidentialité : Cette sélection active deux champs de mot de passe obligatoires : - Mot de passe d'authentification - Mot de passe de confidentialité

Exécuter les modifications

Après avoir configuré ces paramètres, appuyez sur le bouton **Appliquer** dans le bandeau de la page pour appliquer vos modifications.

NOTE: Les boutons **Appliquer** et **Annuler** sont désactivés (grisés) lorsque la configuration n'est pas valide.

Gestion des certificats

Présentation de l'authentification

Un module BMENOR2200H peut être authentifié de deux manières :

- Certificat auto-signé
- Autorité de certification (CA)

Le module BMENOR2200H crée un certificat auto-signé aux fins suivantes :

- Configuration des paramètres de cybersécurité via les pages Web du module
- Diagnostic du module via ses pages Web
- Mise à niveau du micrologiciel

Limites des certificats

Pour prendre en charge la communication avec le module BMENOR2200H, notez les limites suivantes des certificats auto-signés et des certificats d'autorité de certification (CA) :

Certificats auto-signés :

- Utilisation des clés (marqué comme critique) :
 - Signature numérique
 - Chiffrement de clé (pas d'utilisation pour la suite TLS basée sur des clés éphémères telles que TLS_ECDHE_xxxx ; utilisation pour TLS_RSA_xxxx)
 - Signature des certificats de clé : lorsque la clé publique du sujet est utilisée pour vérifier les signatures sur les certificats de clé publique (valeur TRUE)
 - Non-répudiation
 - Chiffrement des données
- Autre nom du sujet : Ce champ accepte les valeurs suivantes : Adresse IP V4/V6, URI
- Contraintes de base :
 - le champ CA indique si la clé publique certifiée peut être utilisée pour vérifier les signatures de certificat (valeur TRUE) et la contrainte de longueur de chemin 0
- Identificateur de la clé du sujet :
 - moyen d'identifier les certificats qui contiennent un hachage public SHA-1 160 bits particulier de la valeur de la chaîne de bits de la clé publique du sujet (à l'exclusion de la balise, de la longueur et du nombre de bits inutilisés).
- Extension de l'utilisation améliorée des clés :
 - id-kp-serverAuth en cas d'authentification du serveur Web TLS
 - id-kp-clientAuth en cas d'authentification du client Web TLS

Certificats d'autorité de certification (CA) :

- Utilisation des clés (marqué comme critique) :
 - Signature numérique
 - Chiffrement de clé (pas d'utilisation pour la suite TLS basée sur des clés éphémères telles que TLS_ECDHE_xxxx ; utilisation pour TLS_RSA_xxxx)
 - Signature des certificats de clé : lorsque la clé publique du sujet est utilisée pour vérifier les signatures sur les certificats de clé publique (valeur FALSE)
 - Non-répudiation
 - Chiffrement des données
- Autre nom du sujet : Ce champ accepte les valeurs suivantes : Adresse IP V4/V6, URI
- Contraintes de base :
 - Champ CA : indique si la clé publique certifiée peut être utilisée pour vérifier les signatures de certificat (valeur FALSE)
- Extension de l'utilisation améliorée des clés :
 - id-kp-serverAuth en cas d'authentification du serveur Web TLS
 - id-kp-clientAuth en cas d'authentification du client Web TLS
- Points de distribution de liste de certificats de confiance
- Identificateur de clé de l'autorité :
 - Identification de la clé publique correspondant à la clé privée utilisée pour signer un certificat.

Page Web de configuration de PKI

Gestion des certificats et PKI

NOTE: Avant de commencer à travailler sur la page Web **Configuration PKI**, familiarisez-vous avec la description générale de la gestion des certificats, page 212.

Le module BMENOR2200H s'appuie sur des certificats pour l'authentification. Pour assurer la cybersécurité, chaque entité gère une liste de confiance de tous les certificats d'équipements et d'applications qui communiquent avec elle. La méthode de gestion des certificats dépend de la conception du système, qui peut appliquer ou non une infrastructure de clé publique (PKI) avec une autorité de certification (CA) :

- **Gestion de certificats sans PKI :** Utilisez cette méthode de gestion des certificats si votre système n'inclut pas d'autorité de certification. Gérez les certificats dans les pages Web de gestion des certificats comme suit :
 - Le mode PKI par défaut du système est le mode autosigné uniquement.
 - Vous ne pouvez régler le mode de réinitialisation d'usine de l'équipement que sur le mode auto-signé.
 - Gérez la liste de certificats de confiance à l'aide des fonctions Ajouter et Supprimer pour créer une liste autorisée à communiquer avec le module BMENOR2200H.
 - Cliquez sur le bouton **Télécharger** pour exporter le certificat du module BMENOR2200H vers les équipements communicants.
- **Gestion des certificats avec PKI :** Accédez à la page Web **Configuration PKI** et configurez les paramètres comme indiqué ci-dessous.

Accès à la page

Vous accédez à la page Web **Configuration PKI** via l'onglet **CONFIGURATION** du module BMENOR2200H (**CONFIGURATION > MENU > GESTION DES CERTIFICATS > Configuration PKI**).

Paramètres PKI

Gérez l'attribution et l'acceptation de certificats avec les paramètres PKI suivants si votre système inclut une autorité de certification.

Paramètres *PUBLIC KEY INFRASTRUCTURE SETTINGS* :

Paramètre	Description
PKI Mode	<i>Self-Signed only</i> : Il s'agit du mode PKI par défaut du système.
	<i>CA only</i> : Tous les équipements installés prennent en charge PKI. Inscrivez manuellement chaque module BMENOR2200H auprès de l'autorité de certification.
	<i>Self-Signed & CA</i> : Certains équipements installés ne prennent pas en charge PKI. Remarques : - Le certificat du module BMENOR2200H est émis par une autorité de certification. - Les certificats des équipements qui prennent en charge PKI sont émis par une autorité de certification. - Les certificats des équipements qui ne prennent pas en charge PKI sont auto-signés. Inscrivez manuellement chaque module BMENOR2200H auprès de l'autorité de certification. Gérez la liste de confiance pour créer une liste autorisée à communiquer avec le module BMENOR2200H. NOTE: Seuls les certificats de la liste Gestion de la liste de confiance ont besoin d'être gérés.
Submit	Cliquez sur ce bouton pour attribuer le mode PKI.

Paramètres *DEVICE CERTIFICATION* :

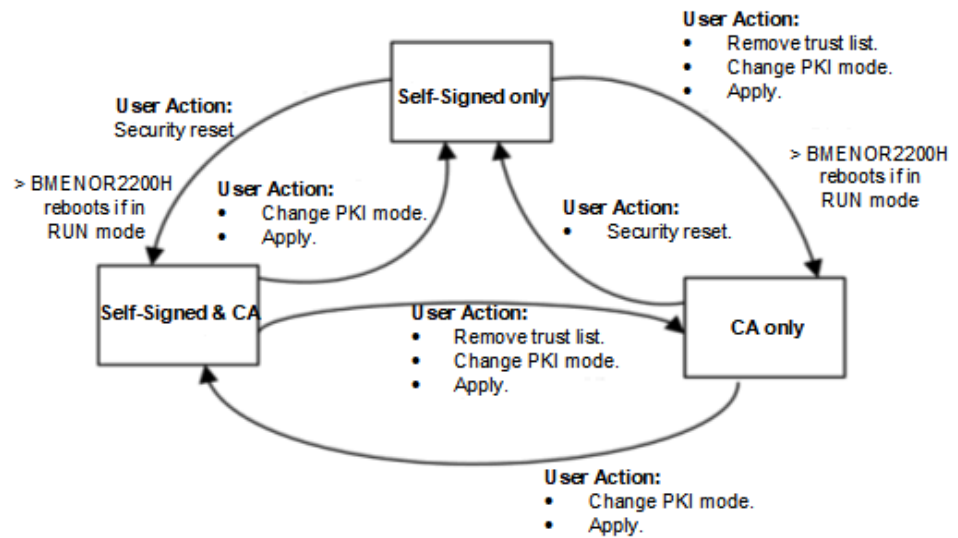
Paramètre	Description
Subject	Cette ligne identifie l'hôte ou la partie qui contrôle la certification par clé privée.
Subject Alternative Name	Le nom structuré indiqué dans ce champ inclut les noms de domaine et de sous-domaine ainsi que les adresses IP sécurisées par le certificat.
Issuer	Ce champ indique l'entité qui a émis le certificat.
Expiration Date	Ce champ indique la date d'expiration du certificat.
Download	Cliquez sur ce bouton pour exporter le certificat du module BMENOR2200H pour HTTPS sur votre PC.

Paramètres *ENROLLMENT* :

Paramètre	Description
1. Generate CSR	Cliquez sur ce bouton pour télécharger sur votre PC une demande de signature de certificat (CSR) au format .pem (Privacy Enhanced Mail).
2. Select the certificate file to upload	Entrez un certificat X.509v3 codé en ASN.1 (DER). Une autorité de certification installée dans l'équipement a produit ce certificat à partir du fichier CSR téléchargé pour l'équipement. NOTE: Vous pouvez utiliser le bouton Parcourir pour accéder au fichier.
Upload	Cliquez sur ce bouton pour charger sur le module un fichier hors ligne contenant une configuration pour les communications avec l'autorité de certification en recevant le certificat via la CSR.
NOTE: Reportez-vous à la description du processus manuel d'inscription de certificats.	

Logigramme de configuration du mode PKI

Ce schéma illustre les événements et actions utilisateur liés à la modification du mode PKI :



Exécuter les modifications

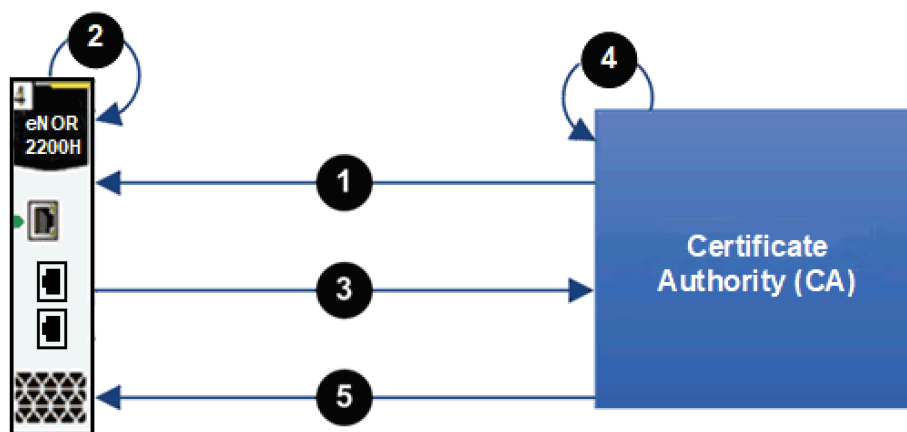
Après avoir configuré ces paramètres, appuyez sur le bouton **Appliquer** dans le bandeau de la page pour appliquer vos modifications.

NOTE: Les boutons **Appliquer** et **Annuler** sont désactivés (grisés) lorsque la configuration n'est pas valide.

Inscription manuelle

Après avoir configuré le module BMENOR2200H dans Control Expert, vous pouvez utiliser la section ENROLLMENT du menu de configuration PKI pour *obtenir* un fichier CSR à soumettre à une autorité de certification (CA). Après avoir envoyé le fichier CSR, vous pouvez extraire le certificat CA correspondant. Par la suite, vous pouvez insérer ce certificat CA dans le module BMENOR2200H. Les opérations combinées d'extraction et d'insertion inscrivent manuellement un certificat émis par une autorité de certification tierce. Une fois le certificat inséré, le serveur l'applique pour signer et crypter sa communication avec le client.

Vous trouverez ci-après une vue d'ensemble du processus d'inscription manuelle d'un certificat :



1 Le BMENOR2200H importe un MENU de Gestion d'autorité de certification racine à partir de l'autorité de certification (CA).

2 Le BMENOR2200H génère une demande de signature de certificat (CSR).

3 Le BMENOR2200H exporte la CSR vers l'autorité de certification.

4 L'autorité de certification exécute la demande CSR et génère un certificat.

5 Le BMENOR2200H importe le certificat émis par l'autorité de certification.

Page Web de gestion de la liste de confiance

Introduction

Pour fournir le niveau requis de cybersécurité, chaque module BMENOR2200H d'entité gère une liste de confiance de tous les certificats d'équipement/application qui communiquent avec lui.

Seuls les équipements qui ont fourni au module BMENOR2200H un certificat d'instance d'application peuvent communiquer avec RTU. Le module met en œuvre une gestion locale (basée sur un module) des certificats d'instance d'application, lesquels sont stockés dans une liste de confiance. Utilisez les commandes des pages Web **Gestion des certificats** pour ajouter, télécharger ou supprimer un certificat.

NOTE:

- Les certificats d'instance d'application de la liste de confiance sont codés en ANSI CRT.
- Avant de commencer à travailler sur la page Web **Configuration PKI**, familiarisez-vous avec la description générale de la gestion des certificats, page 212.

Accès à la page

Accédez à la page Web **Gestion de la liste de confiance** via l'onglet **CONFIGURATION** du module BMENOR2200H (**CONFIGURATION > MENU > GESTION DES CERTIFICATS > Gestion de la liste de confiance**).

Paramètres

Utilisez les paramètres et réglages suivants de la page Web **Gestion de la liste de confiance** pour créer une liste de confiance :

Paramètre	Description
<i>Nom (CN)</i>	Ce champ indique le nom du certificat.
<i>Nom distinctif (DN)</i>	Ce champ correspond au nom du certificat.
<i>Date d'expiration</i>	Ce champ indique la date d'expiration du certificat. NOTE: Les dates d'expiration des certificats approuvés sont définies par rapport aux paramètres internes de date et d'heure du module BMENOR2200H. Pour éviter toute incohérence, utilisez le service NTP pour mettre à jour les paramètres de date et d'heure du module RTU et vérifiez que le serveur NTP est accessible et qu'il dispose de réglages de date et d'heure à jour. Le module BMENOR2200H ne gère pas automatiquement les dates d'expiration des certificats. • Pour un fichier de certificat auto-signé, ce paramètre est déterminé par l'équipement. • Pour un fichier de certificat d'autorité de certification, il dépend de l'agent d'autorité de certification.
<i>Parcourir</i>	Cliquez sur ce bouton pour accéder au certificat que vous souhaitez ajouter à la liste et le sélectionner.
<i>Soumettre</i>	Cliquez sur ce bouton pour ajouter le fichier sélectionné à la liste.
<i>Appliquer</i>	Cliquez sur ce bouton pour enregistrer vos modifications de configuration.

Exécuter les modifications

Après avoir configuré ces paramètres, appuyez sur le bouton **Appliquer** dans le bandeau de la page pour appliquer vos modifications.

NOTE: Les boutons **Appliquer** et **Annuler** sont désactivés (grisés) lorsque la configuration n'est pas valide.

Page Web de gestion d'autorité de certification racine

Introduction

Le certificat d'autorité de certification est un certificat de clé publique qui identifie l'autorité de certification (AC) dans une infrastructure de clé publique (PKI). Utilisez la page **Gestion de l'AC racine** pour insérer des certificats d'autorité de certification dans l'équipement.

NOTE: Avant de commencer à travailler sur la page Web **Configuration PKI**, familiarisez-vous avec la description générale de la gestion des certificats, page 212.

Accès à la page

Accédez à la page Web **Gestion de l'AC racine** via l'onglet **CONFIGURATION** du module BMENOR2200H (**CONFIGURATION > MENU > GESTION DES CERTIFICATS > Gestion de l'AC racine**).

Paramètres

Vous trouverez les paramètres et réglages suivants dans la page Web **Gestion de l'AC racine** :

Paramètre	Description
<i>Nom (CN)</i>	Cette colonne indique le nom du certificat.
<i>Nom distinctif (DN)</i>	Cette colonne correspond au nom du certificat.
<i>Date d'expiration</i>	Ce champ indique la date d'expiration du certificat. NOTE: - Les dates d'expiration des certificats approuvés sont définies par rapport aux paramètres internes de date et d'heure du module BMENOR2200H. Pour éviter toute incohérence, utilisez le service NTP pour mettre à jour les paramètres de date et d'heure du module BMENOR2200H et vérifiez que le serveur NTP est accessible et qu'il dispose d'un réglage de date et d'heure à jour. - Le module BMENOR2200H ne gère pas automatiquement les dates d'expiration des certificats. - Pour un fichier de certificat auto-signé, ce paramètre est déterminé par l'équipement. - Pour un fichier de certificat d'autorité de certification, il dépend de l'agent d'autorité de certification.
<i>Parcourir</i>	Cliquez sur ce bouton pour accéder au certificat que vous souhaitez ajouter à la liste et le sélectionner.
<i>Soumettre</i>	Cliquez sur ce bouton pour ajouter le fichier sélectionné à la liste.
<i>Appliquer</i>	Cliquez sur ce bouton pour enregistrer vos modifications de configuration.

NOTE: Vous pouvez ajouter jusqu'à 10 certificats d'autorité de certification.

Exécuter les modifications

Après avoir configuré ces paramètres, appuyez sur le bouton **Appliquer** dans le bandeau de la page pour appliquer vos modifications.

NOTE: Les boutons **Appliquer** et **Annuler** sont désactivés (grisés) lorsque la configuration n'est pas valide.

Page Web Gestion des clés DNP3

Accès à la page

Accédez aux onglets **CLIENT** et **SERVEUR** de la page Web **Gestion des clés DNP3** via l'onglet **CONFIGURATION** du module BMENOR2200H (**CONFIGURATION > MENU > GESTION > Gestion des clés DNP3**).

Paramètres du client

Vous trouverez les paramètres et réglages suivants dans l'onglet **CLIENT** de la page Web **Gestion des clés DNP3** :

Paramètre	Description
<i>Numéro d'utilisateur</i>	Ce numéro correspond à l'utilisateur DNP3 actuel.
<i>Nom d'utilisateur</i>	Ce nom correspond à l'utilisateur DNP3 actuel.
<i>Envelope de clé</i>	Sélectionnez AES-128 ou AES-256 dans le menu déroulant.
<i>Clé de mise à jour</i>	Cette colonne contient la valeur de la clé prépartagée.
<i>Générer</i>	Pour le champ de clé pré-partagée (<i>Clé de mise à jour</i>), vous avez la possibilité de cliquer sur le bouton Générer pour utiliser une clé générée aléatoirement.
<i>Soumettre</i>	Cliquez sur ce bouton pour appliquer les modifications à la voie sélectionnée.
<i>Ajouter un utilisateur</i>	Cliquez sur ce bouton pour ouvrir la boîte de dialogue Ajouter un utilisateur . Cet écran vous permet de configurer les paramètres ci-dessus pour créer un utilisateur supplémentaire avec des rôles définis puis de cliquer sur le bouton OK pour ajouter l'utilisateur au tableau de la page principale GESTION DES CLÉS > CLIENT .

Paramètres du serveur

Les paramètres serveur ne sont visibles qu'après la création d'un tableau dans l'onglet **SERVEUR** de la page Web **Gestion des clés DNP3** :

Etape	Action
1	Cliquez sur le bouton Créer un tableau pour ouvrir la boîte de dialogue Créer un tableau d'utilisateurs .
2	Attribuez un nom au tableau dans le champ Nom du tableau .
3	Cliquez sur le bouton OK pour afficher le nouveau tableau dans la liste GESTION DES CLES . NOTE: Le nom du tableau figure désormais dans le menu déroulant en regard du bouton Supprimer le tableau .
4	Etapas supplémentaires : - Pour ajouter d'autres tableaux à la liste GESTION DES CLES, répétez les étapes ci-dessus. - Pour supprimer ce tableau, sélectionnez-le dans la liste déroulante, cliquez sur le bouton Supprimer le tableau et suivez les invites pour terminer l'opération. NOTE: Le bouton Supprimer le tableau n'est visible qu'après la création d'au moins un tableau. - Pour supprimer des utilisateurs spécifiques d'un tableau, sélectionnez celui-ci dans la liste GESTION DES CLES, cliquez sur l'icône de la corbeille et suivez les invites pour supprimer les utilisateurs voulus.

Description des paramètres :

Paramètre	Description
Numéro d'utilisateur	Ce numéro correspond à l'utilisateur DNP3 actuel.
Nom d'utilisateur	Ce nom correspond à l'utilisateur DNP3 actuel.
Rôle d'utilisateur	Sélectionnez un rôle pour l'utilisateur en fonction des descriptions de rôle, page 231.
Envelope de clé	Sélectionnez l'algorithme d'enveloppe approprié (AES-128 ou AES-256).
Clé de mise à jour	Cette colonne contient la valeur de la clé prépartagée.
Générer	Pour le champ de clé pré-partagée (<i>Clé de mise à jour</i>), vous avez la possibilité de cliquer sur le bouton Générer pour utiliser une clé générée aléatoirement.
Ajouter un utilisateur	Cliquez sur ce bouton pour ouvrir la boîte de dialogue Ajouter un utilisateur . Cet écran vous permet de configurer les paramètres ci-dessus pour créer un utilisateur supplémentaire avec des rôles définis puis de cliquer sur le bouton OK pour ajouter l'utilisateur au tableau de la page principale GESTION DES CLES > SERVEUR .
Soumettre	Cliquez sur ce bouton pour appliquer les modifications à la voie sélectionnée.

Exécuter les modifications

Après avoir configuré ces paramètres, appuyez sur le bouton **Appliquer** dans le bandeau de la page pour appliquer vos modifications.

NOTE: Les boutons **Appliquer** et **Annuler** sont désactivés (grisés) lorsque la configuration n'est pas valide.

Page Web de configuration de client DNP3

Accès à la page

Accédez à la page Web **Configuration du client DNP3** via l'onglet **CONFIGURATION** du module BMENOR2200H (**CONFIGURATION > MENU > CONFIGURATION DU PROTOCOLE RTU > Configuration du client DNP3**).

Paramètres

Vous trouverez les paramètres et réglages suivants dans la page Web **Configuration du client DNP3** :

Paramètre	Description
<i>Nom de la voie</i>	Nom de la voie sélectionnée.
<i>Activer TLS</i>	Cochez cette case pour activer TLS.
	Désélectionnez cette case pour désactiver TLS.
<i>Authentification sécurisée</i>	SAv2
	SAv5
	Désactivé
<i>Activer le mode agressif</i>	Cochez cette case pour activer le mode agressif.
	Désélectionnez cette case pour désactiver le mode agressif.
<i>Utilisateur actuel</i>	Cliquez sur le bouton Sélectionner pour ouvrir la boîte de dialogue Utilisateur actuel et définir l'utilisateur actif. NOTE: Vous pouvez cliquer sur le lien Gestion des clés dans la boîte de dialogue Utilisateur actuel pour accéder directement à la page Web de gestion des clés DNP3, page 220.
<i>Paramètres avancés</i>	Cliquez sur le bouton Configurer pour ouvrir la boîte de dialogue Paramètres avancés et configurer les paramètres suivants : - PARAMETRES D'AUTHENTIFICATION GENERAUX - PARAMETRES SAV2/SAV5 NOTE: La boîte de dialogue Paramètres avancés contient plusieurs paramètres. Cliquez sur l'icône d'information (i) à droite d'un champ de paramètre pour afficher la description des valeurs acceptables.
<i>Soumettre</i>	Cliquez sur ce bouton pour appliquer les modifications à la voie sélectionnée.
<i>Ajouter une voie</i>	Cliquez sur ce bouton pour ouvrir la boîte de dialogue Ajouter une voie dans laquelle vous pouvez créer une voie supplémentaire à l'aide des paramètres répertoriés ci-dessus. Cliquez sur le bouton OK pour ajouter une entrée au tableau (avec le nouveau Nom d'utilisateur).

Exécuter les modifications

Après avoir configuré ces paramètres, appuyez sur le bouton **Appliquer** dans le bandeau de la page pour appliquer vos modifications.

NOTE: Les boutons **Appliquer** et **Annuler** sont désactivés (grisés) lorsque la configuration n'est pas valide.

Page Web de configuration du serveur DNP3

Accès à la page

Accédez à la page Web **Configuration du serveur DNP3** via l'onglet **CONFIGURATION** du module BMENOR2200H (**CONFIGURATION > MENU > CONFIGURATION DU PROTOCOLE RTU > Configuration du serveur DNP3**).

Paramètres

Vous trouverez les paramètres et réglages suivants dans la page Web **Configuration du serveur DNP3** :

Paramètre	Description
<i>Nom de la voie</i>	Nom de la voie sélectionnée.
<i>TLS activé</i>	Cochez cette case pour activer TLS pour toutes les voies serveur.
	Désélectionnez cette case pour désactiver TLS pour toutes les voies serveur.
<i>Authentification sécurisée activée</i>	SAv2
	SAv5
<i>Algorithme MAC (HMAC)</i>	Sélectionnez l'algorithme MAC à appliquer aux défis.
<i>Tableau des clés/ comptes</i>	Ce tableau répertorie les options de client/serveur suivantes : • <i>Numéro d'utilisateur</i> • <i>Nom d'utilisateur</i> • <i>Rôle d'utilisateur</i> utilisateur (opérateur, visualiseur, utilisateur unique) • <i>Envelope de clé</i> : Sélectionnez AES-128 ou AES-256. • <i>Clé</i> : Entrez l'algorithme d'enveloppe de clé (format hexadécimal). • <i>Appliquer</i> : Cliquez sur ce bouton pour enregistrer vos modifications.
<i>Activer le mode agressif</i>	Cochez cette case pour activer le mode agressif.
	Désélectionnez cette case pour désactiver le mode agressif.
<i>Paramètres avancés</i>	Cliquez sur le bouton Configurer pour accéder aux paramètres avancés suivants pour la voie sélectionnée : • <i>PARAMETRES D'AUTHENTIFICATION GENERAUX</i> • <i>PARAMETRES SAV2/SAV5</i> NOTE: Cliquez sur une icône d'information (i) pour afficher la description du paramètre correspondant.
<i>Soumettre</i>	Cliquez sur ce bouton pour appliquer les modifications à la voie sélectionnée.
<i>Ajouter une voie</i>	Cliquez sur ce bouton pour créer une voie avec cette configuration.

Exécuter les modifications

Après avoir configuré ces paramètres, appuyez sur le bouton **Appliquer** dans le bandeau de la page pour appliquer vos modifications.

NOTE: Les boutons **Appliquer** et **Annuler** sont désactivés (grisés) lorsque la configuration n'est pas valide.

Configuration de l'authentification sécurisée DNP3

Accès aux paramètres

Accédez à la page **AUTHENTIFICATION SÉCURISÉE DNP3** à partir de la page Web **CONFIGURATION** :

Etape	Action
1	Accédez aux pages Web de cybersécurité concernant le module.
2	Sélectionnez l'onglet CONFIGURATION dans la bannière de la page.
3	Développez l'arborescence de navigation MENU .
4	Développez AUTHENTIFICATION SÉCURISÉE DNP3 dans la bannière de l'arborescence de navigation pour afficher les paramètres suivants : • Configuration du client • Configuration du serveur • Gestion des clés NOTE: Ces paramètres de sécurité sont décrits plus loin.

Reportez-vous aux sujets suivants :

- Page Web de configuration de voie client DNP3, page 222
- Page Web de configuration de voie serveur DNP3, page 223

NOTE: Le paramètre HMAC implémenté représente la principale différence entre l'authentification DNP3 réseau et série :

Protocole de communication	Paramètre HMAC
série	HMAC SHA-1 (8 octets)
	HMAC SHA-256 (8 octets)
réseau	HMAC SHA-1 (10 octets)
	HMAC SHA-256 (16 octets)

Gestion des clés

Créez une liste d'utilisateurs autorisés à accéder à votre module :

Etape	Description
1	Dans la page Web Gestion des clés , appuyez sur le bouton Créer un tableau et suivez les instructions pour attribuer un nom au tableau. NOTE: Les tableaux que vous créez s'affichent dans un menu déroulant en regard du bouton Créer un tableau .
2	Appuyez sur le bouton Ajouter un utilisateur pour ajouter une liste d'utilisateurs autorisés dans l'environnement de supervision (SCADA). NOTE: Vous pouvez configurer jusqu'à 64 utilisateurs pour l'authentification sécurisée DNP3.
3	Renseignez les champs de la boîte de dialogue Ajouter un utilisateur . NOTE: Lorsque la fenêtre Control Expert est active, vous pouvez faire glisser le pointeur de la souris sur le cercle bleu (i) à côté de la fonction pour afficher la description de chaque champ.
4	<i>étape facultative</i> : Pour le champ de clé pré-partagée (Clé de mise à jour), vous pouvez cliquer sur le bouton Générer pour utiliser une clé générée de manière aléatoire.
5	<i>étape facultative</i> : Vous pouvez copier les informations de Clé de mise à jour en cliquant sur l'icône de copie à côté du bouton Générer . NOTE: Vous pouvez copier la clé pour la partager plus facilement avec le système SCADA.
6	Appuyez sur le bouton Appliquer pour ajouter l'utilisateur au tableau des utilisateurs autorisés.
7	Répétez ces étapes pour ajouter d'autres utilisateurs. NOTE: La norme DNP3 limite le nombre d'utilisateurs à 64.

NOTE: Respectez les limites maximales suivantes pour le nombre d'utilisateurs DNP3 pouvant participer à la configuration de gestion des clés :

- DNP3 SAV2 : 10
- DNP3 SAV5 : 64

Les utilisateurs mentionnés dans votre tableau pourront accéder à votre module à partir de l'environnement SCADA.

Le tableau suivant décrit les paramètres de **Gestion des clés** :

Paramètre	Description
CLIENT (onglet)	Numéro d'utilisateur : Ce numéro correspond à l'utilisateur DNP3 actuel. NOTE: Utilisez la valeur 1 lorsque SAV5 est affecté à cet utilisateur.
	Nom d'utilisateur : Ce champ indique l'utilisateur actuel. NOTE: Comme le module BMENOR2200H joue le rôle de concentrateur de données, le rôle d'utilisateur actuel côté CLIENT est UTILISATEUR UNIQUE.
	Enveloppe de clé : Sélectionnez l'algorithme d'enveloppe approprié (AES-128, AES-256). Norme de cryptage. NOTE: AES-256 ne fonctionne pas avec SAV2. Dans ce cas, la valeur de Clé de mise à jour est 32 hex.
	Clé : Cette colonne affiche le contenu de la valeur de Clé de mise à jour .
SERVEUR (onglet)	Numéro d'utilisateur : Ce numéro correspond à l'utilisateur DNP3 actuel.
	Nom d'utilisateur : Ce champ indique l'utilisateur actuel.
	Rôle d'utilisateur : Ce champ indique le rôle joué par l'utilisateur (OPERATEUR, INGENIEUR, INSTALLATEUR, ADMINISTRATEUR DE SECURITE, VISUALISEUR, UTILISATEUR UNIQUE).
	Enveloppe de clé : Sélectionnez l'algorithme d'enveloppe approprié (AES-128, AES-256). Norme de cryptage. NOTE: AES-256 ne fonctionne pas avec SAV2. Dans ce cas, la valeur de Clé de mise à jour est 32 hex.
	Clé : Cette colonne affiche le contenu de la valeur de Clé de mise à jour .

Pages Web client et serveur IEC60870

Accès à la page

Accédez aux pages Web client et serveur pour la norme IEC60870 via l'onglet **CONFIGURATION** du module BMENOR2200H.

Paramètres du client

Affichez la configuration du client IEC60870 (**CONFIGURATION > MENU > CONFIGURATION DU PROTOCOLE RTU > Configuration du client IEC60870**) :

Paramètre	Description
<i>Nom de la voie</i>	Nom de la voie sélectionnée.
<i>Activer TLS</i>	<i>activé</i> : Cochez cette case pour activer TLS.
	<i>désactivé</i> : Désélectionnez cette case pour désactiver TLS.
<i>Envoyer</i>	Cliquez sur ce bouton pour appliquer les modifications à la voie sélectionnée.
<i>Ajouter une voie</i>	Cliquez sur ce bouton pour créer une voie supplémentaire.

Paramètres du serveur

Affichez la configuration du serveur IEC60870 (**CONFIGURATION > MENU > CONFIGURATION DU PROTOCOLE RTU > Configuration du serveur IEC60870**) :

Paramètre	Description
<i>TLS activé</i>	<i>activé</i> : Cochez cette case pour activer TLS.
	<i>désactivé</i> : Désélectionnez cette case pour désactiver TLS.
<i>Envoyer</i>	Cliquez sur ce bouton pour appliquer les modifications à la voie sélectionnée.

Exécuter les modifications

Après avoir configuré ces paramètres, appuyez sur le bouton **Appliquer** dans le bandeau de la page pour appliquer vos modifications.

NOTE: Les boutons **Appliquer** et **Annuler** sont désactivés (grisés) lorsque la configuration n'est pas valide.

Page Web Gestion des utilisateurs

Accès à la page

Accédez à la page Web **Gestion des utilisateurs** via l'onglet **CONFIGURATION** du module BMENOR2200H (**CONFIGURATION > MENU > MANAGEMENT > Gestion des utilisateurs**).

Paramètres

Paramètre		Description
GESTION DES UTILISATEURS	Nom d'utilisateur	Ce champ indique l'utilisateur actuel.
	Rôles	Ce champ indique le rôle de l'utilisateur actuel.
RÔLES		Sélectionnez le rôle joué par l'utilisateur (OPERATEUR, INGENIEUR, INSTALLATEUR, ADMINISTRATEUR DE LA SECURITE) NOTE: Un même utilisateur peut remplir plusieurs rôles.
CHANGEMENT DU MOT DE PASSE	Nouveau mot de passe	Saisissez le nouveau mot de passe.
	Confirmation du mot de passe	Saisissez à nouveau le nouveau mot de passe.
	Soumettre	Appliquez le nouveau mot de passe.
	NOTE: - Il n'existe aucune valeur par défaut pour le MOT DE PASSE. L'utilisateur doit enregistrer le mot de passe manuellement ou sauvegarder la configuration de cybersécurité après toute modification appliquée. - Si l'utilisateur oublie le mot de passe, utilisez la réinitialisation d'usine pour effacer toute la configuration de cybersécurité. Pour plus d'informations, voir Réglage du commutateur, page 29	
Ajouter un utilisateur	Cliquez sur ce bouton pour créer d'autres utilisateurs avec des rôles définis. NOTE: Vous pouvez créer jusqu'à 15 nouveaux utilisateurs.	

Cliquez sur l'icône en forme de crayon pour modifier ces paramètres, puis cliquez sur le bouton **Appliquer**.

Exécuter les modifications

Après avoir configuré ces paramètres, appuyez sur le bouton **Appliquer** dans le bandeau de la page pour appliquer vos modifications.

NOTE: Les boutons **Appliquer** et **Annuler** sont désactivés (grisés) lorsque la configuration n'est pas valide.

Page Web Gestion de la configuration

Introduction

Vous pouvez utiliser la page Web **Gestion de la configuration** pour exporter les paramètres de cybersécurité d'un module BMENOR2200H en vue d'importer cette configuration dans un autre module.

NOTE: Seul un administrateur de la sécurité disposant d'identifiants SECADM peut effectuer ces tâches de gestion de configuration.

Accès à la page

Accédez à la page Web **Gestion de la configuration** via l'onglet **CONFIGURATION** du module BMENOR2200H (**CONFIGURATION > MENU > GESTION > Gestion de la configuration**).

Exportation de la configuration

Exportez le fichier de configuration de la cybersécurité avec les paramètres **CONFIGURATION DE L'EXPORTATION** de l'onglet **Gestion de la configuration**. Les paramètres appliqués remplacent immédiatement les paramètres existants.

Configurez les paramètres suivants pour l'action d'exportation :

Paramètre	Description
<i>Mot de passe</i>	Saisissez votre mot de passe, qui est une clé de cryptage pour archiver le fichier de configuration exporté. NOTE: Ce même mot de passe est utilisé pour archiver un fichier de configuration importé.
<i>Confirmation du mot de passe</i>	Saisissez à nouveau votre mot de passe.
<i>Exporter</i>	Cliquez sur ce bouton pour exporter la configuration.

Importation de la configuration

Importez la configuration de gestion de la cybersécurité et appliquez-la au module à l'aide des paramètres **CONFIGURATION DE L'IMPORTATION** de l'onglet **Gestion de la configuration**.

Configurez les paramètres suivants pour l'action d'importation :

Paramètre	Description
<i>Archive de configuration</i>	Sélectionnez le fichier de configuration à importer et suivez les invites pour confirmer votre sélection. NOTE: Vous pouvez utiliser le bouton Parcourir pour accéder au fichier approprié.
<i>Mot de passe</i>	Entrez le mot de passe du fichier de configuration qui a été attribué lors de l'exportation.
<i>Enregistrer</i>	Cochez cette case pour appliquer automatiquement la configuration importée immédiatement après son chargement.
<i>Importer</i>	Cliquez sur ce bouton pour importer la configuration.

Réinitialisation de la configuration

Cliquez sur le bouton **Réinitialiser** dans le champ *REINITIALISER LA CONFIGURATION* pour rétablir les paramètres de cybersécurité par défaut du module.

NOTE: Redémarrez le module pour mettre en œuvre l'action de réinitialisation.

Exécuter les modifications

Après avoir configuré ces paramètres, appuyez sur le bouton **Appliquer** dans le bandeau de la page pour appliquer vos modifications.

NOTE: Les boutons **Appliquer** et **Annuler** sont désactivés (grisés) lorsque la configuration n'est pas valide.

RBAC

Introduction

Le contrôle d'accès basé sur les rôles (RBAC) est une méthode permettant de réduire le risque d'attaques de cybersécurité en attribuant différents niveaux d'accès basés sur les privilèges d'accès associés à un rôle défini de l'utilisateur.

Le module BMENOR2200H utilise la méthode RBAC pour fournir des niveaux d'accès définis aux utilisateurs. RBAC est prédéfini conformément à la norme IEC 62351-2, mais également configurable en fonction des besoins de l'utilisateur.

La norme IEC 62351-2 définit les menaces suivantes :

- usurpation d'adresse (spoofing)
- modification
- replay
- écoute (sur échange de clés cryptographiques)

Limites

Le nombre maximum de connexions utilisateur actives au serveur Web est de cinq.

Fonctionnalités disponibles

Le tableau suivant présente les fonctions disponibles pour chaque valeur et le nom correspondant :

Valeur	Nom	DNP3 SAV2/v5		Micrologiciel	Page Web (HTTPS)			
		Surveillance des données	Contrôle opérateur	Mise à niveau	Paramètres de cybersécurité	Diagnostic	Téléchargement de la journalisation des données	Journalisation des données : Supprimer
1	OPERATEUR	✓	✓			✓	✓	
2	INGENIEUR	✓				✓	✓	✓
3	INSTALLATEUR	✓		✓		✓	✓	
4	SECADM				✓	✓	✓	
32768	MONOUTILISATEUR (COMMUN)	✓	✓					
	NOTE: La fonctionnalité MONOUTILISATEUR est dédiée aux fonctions d'authentification de sécurité DNP3 et non à l'accès Web.							

Annexes

Interopérabilité

A propos de ce chapitre

Ce chapitre décrit la mise en œuvre spécifique des protocoles avec le module BMXNOR0200H.

Il aborde les sujets suivants :

- Profil d'équipement serveur DNP3, page 234
- Profil d'équipement client DNP3, page 238
- Tableau d'implémentation de profil d'équipement DNP3, page 242
- Profil d'équipement serveur IEC60870-5-104, page 252
- Profil d'équipement client IEC60870-5-104, page 262
- Profils d'équipement client et serveur IEC60870-5-101, page 273

Interopérabilité DNP3

Introduction

Cette section décrit la mise en oeuvre spécifique du protocole DNP3 (Distributed Network Protocol) dans le module BMENOR2200H utilisé comme client et serveur.

En conjonction avec le jeu de documents DNP3 Basic 4 et le document contenant les définitions de sous-ensemble DNP3, ces informations détaillent la manière de communiquer avec le module BMENOR2200H utilisé en tant que client via le protocole DNP3.

Cette mise en oeuvre de DNP3 est entièrement conforme au niveau 3 de définition de sous-ensemble DNP3.

Cette section traite des sujets suivants :

- DNP3 profil d'équipement serveur, page 234
- DNP3 profil d'équipement client, page 238
- DNP3 tableau d'implémentation de profil d'équipement, page 242

Profil d'équipement serveur DNP3

Paramètres de profil

Ce tableau fournit un *document de profil d'équipement* dans le format standard défini dans le Document des définitions de sous-ensemble DNP3. Bien qu'il soit mentionné dans la section Définitions de sous-ensemble DNP3 en tant que *document*, il s'agit en fait d'une partie d'un guide d'interopérabilité plus complet. Ce tableau utilise un module BMENOR2200H comme exemple de client. (Votre module peut être différent.)

Paramètre	Fonctionnalités	Valeur
Identification d'équipement		
Fonction de l'équipement	Serveur	Serveur
Nom du fabricant	—	Schneider Electric Industries SAS
Nom d'équipement	—	BMENOR2200H
Version matérielle du fabricant de l'équipement	—	1.0
Version logicielle du fabricant de l'équipement	—	1.0
Numéro de version du document de profil d'équipement	—	1
Niveaux DNP3 pris en charge	Pour les requêtes et les réponses : Aucun, niveau 1, niveau 2, niveau 3	Niveau 3
Blocs fonction pris en charge	Prise en charge de l'auto-adressage	Authentification sécurisée
	Authentification sécurisée	
Ajouts notables	—	—
Méthodes de réglage des paramètres configurables	Logiciel	Logiciels (EcoStruxure Control Expert)
	Protocole, défini via DNP3	
Fichiers XML DNP3 disponibles en ligne	N/A	N/A
Fichiers XML DNP3 disponibles hors ligne	dnpDP.xml (lecture)	dnpDP.xml (lecture)
Connexions prises en charge	Série	Réseau IP
	Réseau IP	
Test de conformité	Testé indépendamment	—
Connexions série		
Nom du port	—	Port série
Paramètres de connexion série	Asynchrone - 8 bits de données, 1 bit de démarrage, 1 bit d'arrêt, pas de parité	Asynchrone
	Autre	
Débit en baud	Configurable, sélectionnable parmi les valeurs 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200	19200
Contrôle de flux matériel (dialogue d'établissement de liaison)	Options RS-232/V.24/V.28 : Déclarations : - RTS avant Rx - DTR avant RX Requiert avant Tx : - CTS (déclaré) - DCD (déclaré)	Options RS-232/V.24/V.28 : - Déclare RTS avant Rx - Déclare DTR avant Rx - Avant Tx, requiert CTS déclaré - Avant Tx, requiert DCD déclaré
	Options RS-485 : Requiert Rx inactif avant Tx	
		Options RS-485 : Requiert Rx inactif avant Tx
Intervalle de demande d'état de liaison	Configurable, plage de 0 à 4294967295 ms	2500 ms
Prend en charge l'évitement de collision DNP3	Non	Non
Timeout entre caractères côté récepteur	Non coché	Non coché
Ecart entre caractères dans l'émission	Néant	Néant
Réseau IP		
Nom du port	—	Ethernet
Type de point final	Ecoute TCP	Ecoute TCP
	Datagramme TCP	

Paramètre	Fonctionnalités	Valeur
Adresse IP de cet équipement	—	0.0.0.0
Masque de sous-réseau	—	255.255.255.0
Adresse IP de passerelle	—	0.0.0.0
Accepte les connexions TCP ou les datagrammes UDP depuis	Autorise tout (*. *.*.*)	Autorise tout
	Limites basées sur l'adresse IP	
	Limites basées sur une liste d'adresses IP	
Adresses IP depuis lesquelles les connexions TCP ou les datagrammes UDP sont acceptés	—	*.*.*
Numéro de port d'écoute TCP	Configurable, plage de 1 à 65536	20000
Numéro de port d'écoute TCP de l'équipement distant	N/A	N/A
Temporisateur de maintien de connexion TCP	Fixe à 75000 ms	75000 ms
Port UDP local	Configurable, plage de 1 à 65535	20000
Port UDP de destination pour les requêtes DNP3	Configurable, plage de 1 à 65535	20000
Port UDP de destination pour les réponses nulles non sollicitées initiales	Fixé à 20000	20000
Port UDP de destination pour les réponses DNP3	Configurable, plage de 1 à 65536	20000
Connexions serveur multiples	N/A	N/A
Connexions client multiples	Prend en charge plusieurs clients	Adresse IP
	Méthode 1 (basée sur l'adresse IP)	
Prise en charge de la synchronisation horaire	Procédure LAN DNP3 (code de fonction 24)	Procédure LAN
	Temps d'écriture DNP3	
	Autre	
Couche liaison		
Adresse de liaison de données	Configurable, plage de 0 à 65519	4
Validation d'adresse source DNP3	Jamais	Jamais
	Toujours, adresse unique	
Adresses source DNP3 attendues lorsque la validation est activée	Configurable, plage de 0 à 65519	3
Prise en charge de l'auto-adressage à l'aide de l'adresse 0xFFFFC	Oui	Non
Envoie des trames de données utilisateur confirmées	Jamais	Jamais
	Toujours	
	Parfois	
Temporisation de confirmation de la couche de liaison de données	Configurable, plage de 0 à 4294977295 ms	2000 ms
Nombre maximum de tentatives de liaison de données	Configurable, plage de 0 à 255	3
Nombre maximum d'octets transmis dans une trame de liaison de données	Configurable, plage de 24 à 292	292
Nombre maximum d'octets pouvant être reçus dans une trame de liaison de données	Configurable, plage de 24 à 292	292
Couche application		
Nombre maximum d'octets transmis dans un fragment de couche application hors transfert de fichier	Configurable, plage de 0 à 2048	2048
Nombre maximum d'octets transmis dans un fragment de couche application avec transfert de fichier	—	—
Nombre maximum d'octets pouvant être reçus dans un fragment de couche application	Configurable, plage de 0 à 2048	2048
Délai d'attente d'un fragment de couche application complet	Configurable, plage de 0 à 2147483647	15000 ms
Nombre maximum d'objets autorisés dans une seule requête de contrôle CROB (groupe 12)	Configurable, plage de 1 à 10	10
Nombre maximum d'objets autorisés dans une seule requête de contrôle pour sorties analogiques (groupe 31)	Configurable, plage de 1 à 10	10
Nombre maximum d'objets autorisés dans une seule requête de contrôle pour ensembles de données (groupes 85, 86, 87)	—	—

Paramètre	Fonctionnalités	Valeur
Prend en charge des groupes d'objets mixtes (AOB, CROB et ensembles de données) dans la même requête de contrôle	Oui	Oui
	Non	
Codes d'état de contrôle pris en charge	1 Temporisation	—
	2 Aucune sélection	
	3 Erreur de format	
	4 Non pris en charge	
	5 Déjà actif	
	6 Erreur de matériel	
	7 Local	
	8 Trop d'objets	
	9 Non autorisé	
	10 Inhibition d'automatisation	
	11 Traitement limité	
	12 Hors plage	
	13 Aval local	
	14 Déjà effectué	
	15 Bloqué	
	16 Annulé	
	17 Bloqué autre client	
	18 Aval échec	
	126 Réserve	
127 Non défini		
Propriétés de serveur uniquement		
Délai d'attente de confirmation d'application pour le message de réponse sollicité	Configurable, plage de 0 à 2147483647 ms	10000 ms
Fréquence de synchronisation horaire requise du client	Heure jamais nécessaire	Périodiquement, toutes les 1800 s
	entre 0 et 4294967295 secondes	
Bit de problème d'équipement IIN1.6	Jamais utilisé	Jamais utilisé
Délai d'expiration de descripteur de fichier	Non applicable	Non applicable
Comportement sur débordement du tampon d'événements	Supprimer l'événement le plus ancien	Supprimer l'événement le plus récent
	Supprimer l'événement le plus récent	
Organisation du tampon d'événements	Par groupe d'objets	Par groupe d'objets
Envoie des réponses multiframe	Oui	Oui
Confirmation du dernier fragment	Parfois	Parfois
Paramètres de commande DNP préservés lors d'un redémarrage de l'équipement	—	—
Prend en charge la signature de configuration	Pas de prise en charge	Pas de prise en charge
Demande la confirmation de l'application	Pour les réponses aux événements : Oui	Oui
	Pour les fragments non finaux : Configurable	Oui
Prise en charge de la gestion d'horloge DNP3	Oui	Oui
	Non	
Propriétés de prise en charge des réponses serveur non sollicitées		
Prend en charge les rapports non sollicités	Configurable (activé/désactivé)	Activé
Adresse de liaison de données client	Configurable, plage de 0 à 65519	3
Temporisation de confirmation de réponse non sollicitée	Configurable, plage de 0 à 2147483647	5000 ms
Nombre de tentatives non sollicitées	Configurable, plage de 0 à 65535	3
Conditions de déclenchement de réponse serveur non sollicitée		
Nombre d'événements de classe 1	Configurable, plage de 0 à 255	5
Nombre d'événements de classe 2	Configurable, plage de 0 à 255	5
Nombre d'événements de classe 3	Configurable, plage de 0 à 255	5

Paramètre	Fonctionnalités	Valeur
Nombre total d'événements de toutes classes	Nombre total d'événements non utilisés pour déclencher des réponses non sollicitées	—
Temps de maintien après événement de classe 1	Configurable, plage de 0 à 4294967295 ms	5000 ms
Temps de maintien après événement de classe 2	Configurable, plage de 0 à 4294967295 ms	5000 ms
Temps de maintien après événement de classe 3	Configurable, plage de 0 à 4294967295 ms	5000 ms
Temps de maintien après événement affecté à une classe quelconque	Fixe à 0 ms	0 ms
Redéclenchement du temps de maintien	Le temporisateur de temps de maintien n'est pas redéclenché pour chaque nouvel événement détecté (temps de mise à jour activé)	Non redéclenché
Autres conditions de déclenchement de réponse non sollicitée	—	N/A
Propriétés des performances du serveur		
Dérive maximum de la base de temps	—	—
Quand le serveur définit IIN1.4	Jamais	Jamais
	Déclaré au démarrage jusqu'à la réception de la première demande de synchronisation horaire	
	Plage de 1 à 4294967 secondes après la dernière synchronisation horaire	
Erreur de référence horaire interne maximum avec DNP	Autre	Autre
Erreur de mesure de délai maximum	Autre	Autre
Temps de réponse maximum	Autre	Autre
Temps maximum entre le démarrage et la déclaration IIN 1.4	Autre	Autre
Erreur d'horodatage d'événement maximum pour les E/S binaires et double bit locales	Autre	Autre
Erreur d'horodatage d'événement maximum pour les E/S locales autres que les types de données Binaire et Double bit	Autre	Autre
Paramètres pour un serveur donné		
Nom d'emplacement ou chaîne de code attribué (e) par l'utilisateur (identique à g0v245)	—	—
Code/chaîne numérique d'identification attribué(e) par l'utilisateur (identique à g0v246)	—	—
Chaîne de nom attribuée par l'utilisateur au serveur (identique à g0v247)	—	—
Chaîne de numéro de série de l'équipement (identique à g0v248)	—	—
Nom d'opérateur secondaire (identique à g0v206)	—	—
Nom d'opérateur principal (identique à g0v207)	—	—
Nom du système (identique à g0v208)	—	—
Nom du propriétaire (identique à g0v244)	—	—
Paramètres de sécurité		
Prise en charge de l'authentification sécurisée par l'équipement DNP3	Version 2 (IEEE 1815-2010)	v 2 5
	Version 5 (IEEE 1815-2012)	
Nombre maximum d'utilisateurs	Configurable, plage de 1 à 300	Nombre maximum d'utilisateurs pris en charge : 0
Temporisation de réponse des messages de sécurité	Configurable, plage de 1 à 640 ms	2 ms
Mode de fonctionnement agressif (réception)	—	Oui
Mode de fonctionnement agressif (émission)	—	Non
Intervalle de modification de clé de session	Configurable, plage de 60 à 604800 s (si activé)	Activé à 900 s
Nombre de messages de modification de clé de session	Configurable, plage de 0 à 65535	1000
Nombre maximum d'erreurs (SAV2 uniquement)	Configurable, plage de 0 à 255	2

Paramètre	Fonctionnalités	Valeur
Algorithme MAC demandé dans un échange défi-réponse	SHA-1 (tronqué aux 4 octets les plus à gauche)	SHA-256 (16)
	SHA-1 (tronqué aux 8 octets les plus à gauche)	
	SHA-1 (tronqué aux 10 octets les plus à gauche)	
	SHA-256 (tronqué aux 8 octets les plus à gauche)	
	SHA-256 (tronqué aux 16 octets les plus à gauche)	
Algorithme d'enveloppe de clé pour crypter les clés de session	AES-128	AES-128
	AES-256	
Suites de chiffrement utilisées avec les implémentations DNP utilisant TLS	TLS_RSA crypté avec AES-128	TLS_RSA crypté avec AES-128
Temporisation des requêtes de modification de chiffrement	Fixé à 30 s	30 s
Nombre d'autorités de certification prises en charge	—	Aucune limite
Temps de vérification de la révocation de certificat	Non pertinent - fonctionnalité CRL non utilisée	Non pertinent
Codes de fonctions critiques supplémentaires	Néant	Néant
Autres fragments critiques	Néant	N/A
Prise en charge des modifications de clé de mise à jour à distance	Néant	N/A
Les identifiants utilisateur par défaut sont autorisés à expirer	Non	Non
Authentification sécurisée activée	Configurable : Activé ou désactivé	Désactivé
Longueur des données de défi	Configurable, plage de 4 à 60 octets	4 octets
Nombre maximum de statistiques (SAv5) :		
Nb max. d'échecs d'authentification détectés	Configurable, plage de 4 à 60	4
Nb max. de timeouts de réponse	Configurable, plage de 1 à 65535	3
Nb max. de nouvelles tentatives d'authentification	Configurable, plage de 1 à 65535	3
Nb max. de messages d'erreur envoyés	Configurable, plage de 1 à 65535	3
Fonctionnalité de diffusion		
Désactivée, non configurable	—	—

Profil d'équipement client DNP3

Paramètres du profil

Ce tableau fournit un *document de profil d'équipement* dans le format standard défini dans le document des définitions de sous-ensemble DNP3. Bien qu'il soit mentionné comme un *document* dans les définitions de sous-ensemble DNP3, il s'agit en fait d'une composante d'un guide d'interopérabilité plus complet. Ce tableau utilise un module BMENOR2200H comme exemple de client. (Votre module peut être différent.)

Paramètre	Fonctionnalités	Valeur
Identification de l'appareil		
Fonction d'appareil	Client	Client
Nom du fabricant	—	Schneider Electric Industries SAS
Nom de l'équipement	Nom de l'équipement	BMENOR2200H
Version matérielle du fabricant de l'équipement	—	1.0
Version logicielle du fabricant de l'équipement	—	1.0
Numéro de version du document de profil d'équipement	—	1
Niveaux DNP3 pris en charge	Pour les requêtes et les réponses : Aucun, niveau 1, niveau 2, niveau 3	Pour les requêtes : niveau 3
		Pour les réponses : niveau 3

Paramètre	Fonctionnalités	Valeur
Blocs fonction pris en charge	Prise en charge de l'auto-adressage	Authentification sécurisée
	Authentification sécurisée	
Ajouts notables	Reportez-vous au tableau d'implémentation DNP3 , page 242.	
Méthodes de réglage des paramètres configurables	Logiciel	Logiciel (EcoStruxure Control Expert)
	Fichier propriétaire chargé via un autre mécanisme de transport	
Fichiers XML DNP3 disponibles en ligne	Sans objet	Logiciel (EcoStruxure Control Expert)
Fichiers XML DNP3 externes disponibles hors ligne	dnpDP.xml (lecture)	dnpDP.xml (lecture)
Connexions prises en charge	Série	Réseau IP
	Réseau IP	
Test de conformité	Testé indépendamment	—
Connexions série		
Nom du port	—	Port série
Paramètres de connexion série	Asynchrone - 8 bits de données, 1 bit de démarrage, 1 bit d'arrêt, pas de parité	Asynchrones
	Autres, expliquer <i>configurable</i>	
Débit en bauds	Configurable, sélectionnable parmi les valeur 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200	19200
Contrôle de flux matériel (dialogue d'établissement de liaison)	Options RS-232/V.24/V.28 : Déclarations : - RTS avant Rx - DTR avant RX Requiert avant Tx : - CTS (déclaré) - DCD (déclaré)	Options RS-232/V.24/V.28 : - Déclare RTS avant Rx - Déclare DTR avant Rx - Avant Tx, requiert CTS déclaré - Avant Tx, requiert DCD déclaré
	Options RS-485 : Requiert Rx inactif avant Tx	Options RS-485 : Requiert Rx inactif avant Tx
Intervalle de demande d'état de liaison	Configurable de 0 à 4294967295 ms	2500 ms
Prend en charge l'évitement de collision DNP3	Non	Non
Timeout entre caractères côté récepteur	Not checked	Not checked
Ecart entre caractères dans l'émission	Aucun	Aucun
Réseau IP		
Nom du port	—	Ethernet
Type de point final	Init TCP	Init TCP
	Datagramme TCP	
Adresse IP de cet équipement	—	0.0.0.0
Masque de sous-réseau	—	255.255.255.0
Adresse IP de passerelle	—	0.0.0.0
Accepte les connexions TCP ou les datagrammes UDP depuis	Limites basées sur l'adresse IP	Adresse IP
Adresses IP depuis lesquelles les connexions TCP ou les datagrammes UDP sont acceptés	—	192.168.0.1
Numéro de port d'écoute TCP	Sans objet	Sans objet
Numéro de port d'écoute TCP de l'équipement distant	Plage configurable de 1 à 65535	20000
Temporisateur de maintien de connexion TCP	Fixe à 75000 ms	75000 ms
Port UDP local	Plage configurable de 1 à 65535	20000
	Laisser le système choisir (client uniquement)	
Port UDP de destination pour les requêtes DNP3	Plage configurable de 1 à 65535	20000
Port UDP de destination pour les réponses nulles non sollicitées initiales	Aucun	Aucun
Port UDP de destination pour les réponses DNP3	Plage configurable de 1 à 65536	20000

Paramètre	Fonctionnalités	Valeur
Connexions serveur multiples	Prend en charge plusieurs serveurs	TRUE
Connexions client multiples	Non pris en charge	Non pris en charge
Prise en charge de la synchronisation horaire	Procédure de LAN DNP3 (code de fonction 24)	Procédure LAN
	Temps d'écriture DNP3	
	Autre	
Couche de liaison		
Adresse de liaison de données	Plage configurable de 0 à 65519	4
Validation d'adresse source DNP3	Toujours, une seule adresse autorisée	Toujours, adresse unique
Adresses source DNP3 attendues lorsque la validation est activée	Plage configurable de 0 à 65519	3
Prise en charge de l'auto-adressage à l'aide de l'adresse 0xFFFC	Oui	Non
	Non	
Envoi des trames de données utilisateur confirmées	Jamais	Jamais
	Toujours	
	Parfois	
Temporisation de confirmation de la couche de liaison de données	Plage configurable 0 à 2147483647 ms	2000 ms
Nombre maximum de tentatives de liaison de données	Plage configurable de 0 à 255	3
Nombre maximum d'octets transmis dans une trame de liaison de données	Plage configurable de 24 à 292	292
Nombre maximum d'octets pouvant être reçus dans une trame de liaison de données	Plage configurable de 24 à 292	292
Couche application		
Nombre maximum d'octets transmis dans un fragment de couche application hors transfert de fichier	Plage configurable de 0 à 2048	2048
Nombre maximum d'octets transmis dans un fragment de couche application avec transfert de fichier	Fixé à 0	0
Nombre maximum d'octets pouvant être reçus dans un fragment de couche application	Plage configurable de 0 à 2048	2048
Délai d'attente d'un fragment de couche application complet	Aucun	Aucun
Nombre maximum d'objets autorisés dans une seule requête de contrôle CROB (groupe 12)	Fixé à 10	10
Nombre maximum d'objets autorisés dans une seule requête de contrôle pour sorties analogiques (groupe 31)	Plage configurable de 1 à 512	10
Nombre maximum d'objets autorisés dans une seule requête de contrôle pour ensembles de données (groupes 85, 86, 87)	Plage configurable de 1 à 128	8
Prend en charge des groupes d'objets mixtes (AOB, CROB et ensembles de données) dans la même requête de contrôle	Oui	Oui
	Non	
Codes d'état de contrôle pris en charge	4 Non pris en charge	—
	8 Trop d'objets	
Propriétés spécifiques au client		
Délai d'attente de réponses complètes de la couche application (ms)	Plage configurable de 0 à 4294967295 ms	30000 ms
Nombre maximum de tentatives de la couche application pour les messages de requête	Aucun	Aucun
Délai d'attente du premier ou prochain fragment d'une réponse de la couche application	Plage configurable de 0 à 4294967295 ms	10000 ms
Emission de commandes vers des équipements hors ligne	Non	Non
Emission de commandes vers des équipements hors scrutation	Non	Non
Nombre maximum de tentatives de la couche application pour les messages de sélection de contrôle (même numéro de séquence)	Aucun	Aucun
Nombre maximum de tentatives de la couche application pour les messages de sélection de contrôle (nouveau numéro de séquence)	Aucun	Aucun

Paramètre	Fonctionnalités	Valeur
Paramètres de sécurité		
Prise en charge de l'authentification sécurisée par l'équipement DNP3	Configurable, sélectionnable depuis 2, 5	v 2 5
Nombre maximum d'utilisateurs	Plage configurable de 1 à 300	Nombre maximum d'utilisateurs pris en charge : 0
Temporisation de réponse des messages de sécurité	Plage configurable de 1 à 640 ms	2 ms
Mode de fonctionnement agressif (réception)	—	Oui
Mode de fonctionnement agressif (émission)	—	Non
Intervalle de modification de clé de session	Plage configurable de 60 à 604800 s (si activé)	Activé à 900 s
Nombre de messages de modification de clé de session	Plage configurable de 0 à 65535	1000
Nombre maximum d'erreurs (SAv2 uniquement)	Plage configurable de 0 à 255	2
Algorithme MAC demandé dans un échange défi-réponse	SHA-1 (tronqué aux 4 octets les plus à gauche)	SHA-256 (16)
	SHA-1 (tronqué aux 8 octets les plus à gauche)	
	SHA-1 (tronqué aux 10 octets les plus à gauche)	
	SHA-256 (tronqué aux 8 octets les plus à gauche)	
	SHA-256 (tronqué aux 16 octets les plus à gauche)	
Algorithme d'enveloppe de clé pour crypter les clés de session	AES-128	AES-128
	AES-256	
Suites de chiffrement utilisées avec les implémentations DNP utilisant TLS	TLS_RSA crypté avec AES-128	TLS_RSA crypté avec AES-128
Temporisation des requêtes de modification de chiffrement	Fixé à 30 s	30 s
Nombre d'autorités de certification prises en charge	—	Aucune limite
Temps de vérification de la révocation de certificat	Non pertinent - fonctionnalité CRL non utilisée	Non pertinent
Codes de fonctions critiques supplémentaires	Aucun	Aucun
Autres fragments critiques	Aucun	Aucun
Prise en charge des modifications de clé de mise à jour à distance	Aucun	Aucun
Les identifiants utilisateur par défaut sont autorisés à expirer	Non	Non
Authentification sécurisée activée	Configurable : Activé ou désactivé	Désactivé
Longueur des données de défi	Plage configurable de 4 à 60 octets	4 octets
Nombre maximum de statistiques (SAv5) :		
Nb max. d'échecs d'authentification	Plage configurable de 4 à 60	4
Nb max. de timeouts de réponse	Plage configurable de 1 à 65535	3
Nb max. de nouvelles tentatives d'authentification	Plage configurable de 1 à 65535	3
Nb max. de messages d'erreur envoyés	Plage configurable de 1 à 65535	3
Fonctionnalité de diffusion		
Désactivée, non configurable	—	—

Implémentation du profil d'équipement DNP3

Tableau d'implémentation

Ce tableau identifie les groupes d'objets, les variations, les codes de fonction et les qualificatifs pris en charge par le module BMENOR2200H dans les requêtes et les réponses. Les colonnes *Requête* identifient toutes les requêtes qui peuvent être envoyées par un client ou toutes les requêtes analysées par un serveur. Les colonnes *Réponse* identifient toutes les réponses analysées par un client ou toutes les réponses qui peuvent être envoyées par un serveur :

GROUPE D'OBJETS DNP ET VARIATION			REQUETE		REPONSE	
			Pouvant être émise par le client		Analysée par le client	
			Analysée par le serveur		Pouvant être émise par le serveur	
Numéro de groupe d'objets	Numéro de variation	Description	Codes de fonction (déc.)	Codes qualificatifs (hex.)	Codes de fonction (déc.)	Codes qualificatifs (hex.)
1	0	Entrée binaire - toute variation	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)		
1	0	Entrée binaire - toute variation		00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)		
1	1	Entrée binaire - bit simple compact	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)
1	2	Entrée binaire - bit simple avec drapeau	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)
2	0	Événement de modification d'entrée binaire - toute variation	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)		
2	1	Événement de modification d'entrée binaire - sans heure	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
2	1	Événement de modification d'entrée binaire - sans heure			(Rép. non sollicitée)	17, 28 (index)
2	2	Événement de modification d'entrée binaire - avec heure absolue	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
2	2	Événement de modification d'entrée binaire - avec heure absolue			(Rép. non sollicitée)	17, 28 (index)
2	3	Événement de modification d'entrée binaire - avec heure relative	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
2	3	Événement de modification d'entrée binaire - avec heure relative			(Rép. non sollicitée)	17, 28 (index)
3	0	Entrée double bit - toute variation	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)		
3	0	Entrée double bit - toute variation		00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)		
3	1	Entrée double bit - double bit compressé	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)

GROUPE D'OBJETS DNP ET VARIATION			REQUETE		REPONSE	
			Pouvant être émise par le client		Analysée par le client	
			Analysée par le serveur		Pouvant être émise par le serveur	
Numéro de groupe d'objets	Numéro de variation	Description	Codes de fonction (déc.)	Codes qualificatifs (hex.)	Codes de fonction (déc.)	Codes qualificatifs (hex.)
3	2	Entrée double bit - avec drapeau	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)
4	0	Événement de modification d'entrée double bit - toute variation	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)		
4	1	Événement de modification d'entrée double bit - sans heure	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
4	1	Événement de modification d'entrée double bit - sans heure			(Rép. non sollicitée)	17, 28 (index)
4	2	Événement de modification d'entrée double bit - avec heure absolue	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
4	2	Événement de modification d'entrée double bit - avec heure absolue			(Rép. non sollicitée)	17, 28 (index)
4	3	Événement de modification d'entrée double bit - avec heure relative	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
4	3	Événement de modification d'entrée double bit - avec heure relative			(Rép. non sollicitée)	17, 28 (index)
10	0	Sortie binaire - toute variation	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)		
10	0	Sortie binaire - toute variation		00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)		
10	1	Sortie binaire - format compressé	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)
10	1	Sortie binaire - format compressé	2(écriture)	00, 01 (départ-arrêt)		
10	2	Contrôle continu - état des sorties avec drapeaux	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)
11	0	Événement de modification de sortie binaire - toute variation	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)		
11	1	Événement de modification de sortie binaire - état sans heure	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
11	1	Événement de modification de sortie binaire - état sans heure			(Rép. non sollicitée)	17, 28 (index)
11	2	Événement de modification de sortie binaire - état avec heure	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
11	2	Événement de modification de sortie binaire - état avec heure			(Rép. non sollicitée)	17, 28 (index)

GROUPE D'OBJETS DNP ET VARIATION			REQUETE		REPONSE	
			Pouvant être émise par le client		Analysée par le client	
			Analysée par le serveur		Pouvant être émise par le serveur	
Numéro de groupe d'objets	Numéro de variation	Description	Codes de fonction (déc.)	Codes qualificatifs (hex.)	Codes de fonction (déc.)	Codes qualificatifs (hex.)
12	0	Commande de sortie binaire (CROB) - toute variation		00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)		
12	1	Commande de sortie binaire (CROB) - bloc de sortie relais de contrôle	3(sélection)	17, 28 (index)	(Réponse)	écho de requête
12	1	Commande de sortie binaire (CROB) - bloc de sortie relais de contrôle	4(opération)	17, 28 (index)	(Réponse)	écho de requête
12	1	Commande de sortie binaire (CROB) - bloc de sortie relais de contrôle	5(op. directe)	17, 28 (index)	(Réponse)	écho de requête
12	1	Commande de sortie binaire (CROB) - bloc de sortie relais de contrôle	6(op. directe, pas d'acq.)	17, 28 (index)		écho de requête
20	0	Compteur - toute variation	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)		
20	0	Compteur - toute variation		00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)		
20	0	Compteur - toute variation	7(arrêt)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)		
20	0	Compteur - toute variation	8(gel, pas d'acq.)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)		
20	0	Compteur - toute variation	9(gel et effacement)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)		
20	0	Compteur - toute variation	10(gel et eff. pas d'acq.)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)		
20	1	Compteur - 32 bits avec drapeau	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)
20	2	Compteur - 16 bits avec drapeau	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)
20	5	Compteur - 32 bits sans drapeau	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)
20	6	Compteur - 16 bits sans drapeau	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)
21	0	Compteur gelé - toute variation	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)		
21	0	Compteur gelé - toute variation		00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)		

GROUPE D'OBJETS DNP ET VARIATION			REQUETE		REPONSE	
			Pouvant être émise par le client		Analysée par le client	
			Analysée par le serveur		Pouvant être émise par le serveur	
Numéro de groupe d'objets	Numéro de variation	Description	Codes de fonction (déc.)	Codes qualificatifs (hex.)	Codes de fonction (déc.)	Codes qualificatifs (hex.)
21	1	Compteur gelé - 32 bits avec drapeau	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)
21	2	Compteur gelé - 16 bits avec drapeau	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)
21	5	Compteur gelé - 32 bits avec drapeau et heure	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)
21	6	Compteur gelé - 16 bits avec drapeau et heure	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)
21	9	Compteur gelé - 32 bits sans drapeau	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)
21	10	Compteur gelé - 16 bits sans drapeau	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)
22	0	Événement de modification de compteur - toute variation	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)		
22	1	Événement de modification de compteur - 32 bits avec drapeau	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
22	1	Événement de modification de compteur - 32 bits avec drapeau			(Rép. non sollicitée)	17, 28 (index)
22	2	Événement de modification de compteur - 16 bits avec drapeau	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
22	2	Événement de modification de compteur - 16 bits avec drapeau			(Rép. non sollicitée)	17, 28 (index)
22	5	Événement de modification de compteur - 32 bits avec drapeau et heure	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
22	5	Événement de modification de compteur - 32 bits avec drapeau et heure			(Rép. non sollicitée)	17, 28 (index)
22	6	Événement de modification de compteur - 16 bits avec drapeau et heure	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
22	6	Événement de modification de compteur - 16 bits avec drapeau et heure			(Rép. non sollicitée)	17, 28 (index)
23	0	Événement de modification de compteur gelé - toute variation	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)		
23	1	Événement de modification de compteur gelé - 32 bits avec drapeau	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)

GROUPE D'OBJETS DNP ET VARIATION			REQUETE		REPONSE	
			Pouvant être émise par le client		Analysée par le client	
			Analysée par le serveur		Pouvant être émise par le serveur	
Numéro de groupe d'objets	Numéro de variation	Description	Codes de fonction (déc.)	Codes qualificatifs (hex.)	Codes de fonction (déc.)	Codes qualificatifs (hex.)
23	1	Événement de modification de compteur gelé - 32 bits avec drapeau			(Rép. non sollicitée)	17, 28 (index)
23	2	Événement de modification de compteur gelé - 16 bits avec drapeau	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
23	2	Événement de modification de compteur gelé - 16 bits avec drapeau			(Rép. non sollicitée)	17, 28 (index)
23	5	Événement de modification de compteur gelé - 32 bits avec drapeau et heure	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
23	5	Événement de modification de compteur gelé - 32 bits avec drapeau et heure			(Rép. non sollicitée)	17, 28 (index)
23	6	Événement de modification de compteur gelé - 16 bits avec drapeau et heure	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
23	6	Événement de modification de compteur gelé - 16 bits avec drapeau et heure			(Rép. non sollicitée)	17, 28 (index)
30	0	Entrée analogique - toute variation	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)		
30	0	Entrée analogique - toute variation		00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)		
30	3	Entrée analogique - 32 bits sans drapeau	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)
30	1	Entrée analogique - 32 bits avec drapeau	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt) 17, 28 (index)
30	2	Entrée analogique - 16 bits avec drapeau	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt) 17, 28 (index)
30	3	Entrée analogique - 32 bits avec drapeau	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt) 17, 28 (index)
30	4	Entrée analogique - 16 bits sans drapeau	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt) 17, 28 (index)
30	5	Entrée analogique - simple précision, virgule flottante avec drapeau	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt) 17, 28 (index)
32	0	Événement de modification d'entrée analogique - toute variation	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)		
32	1	Événement de modification d'entrée analogique - 32 bits sans heure	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)

GROUPE D'OBJETS DNP ET VARIATION			REQUETE		REPONSE	
			Pouvant être émise par le client		Analysée par le client	
			Analysée par le serveur		Pouvant être émise par le serveur	
Numéro de groupe d'objets	Numéro de variation	Description	Codes de fonction (déc.)	Codes qualificatifs (hex.)	Codes de fonction (déc.)	Codes qualificatifs (hex.)
32	1	Événement de modification d'entrée analogique - 32 bits sans heure			(Rép. non sollicitée)	17, 28 (index)
32	2	Événement de modification d'entrée analogique - 16 bits sans heure	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
32	2	Événement de modification d'entrée analogique - 16 bits sans heure			(Rép. non sollicitée)	17, 28 (index)
32	3	Événement de modification d'entrée analogique - 32 bits avec heure	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
32	3	Événement de modification d'entrée analogique - 32 bits avec heure			(Rép. non sollicitée)	17, 28 (index)
32	4	Événement de modification d'entrée analogique - 16 bits avec heure	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
32	4	Événement de modification d'entrée analogique - 16 bits avec heure			(Rép. non sollicitée)	17, 28 (index)
32	5	Événement de modification d'entrée analogique - précision simple, virgule flottante sans heure	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
32	5	Événement de modification d'entrée analogique - précision simple, virgule flottante sans heure			(Rép. non sollicitée)	17, 28 (index)
32	7	Événement de modification d'entrée analogique - précision simple, virgule flottante avec heure	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
32	7	Événement de modification d'entrée analogique - précision simple, virgule flottante avec heure			(Rép. non sollicitée)	17, 28 (index)
34	0	Bande morte d'entrée analogique - toute variation	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)		
34	1	Bande morte d'entrée analogique - 16 bits	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)
34	1	Bande morte d'entrée analogique - 16 bits	2(écriture)	00, 01 (départ-arrêt) 17, 28 (index)		
34	2	Bande morte d'entrée analogique - 32 bits	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)
34	2	Bande morte d'entrée analogique - 32 bits	2(écriture)	00, 01 (départ-arrêt) 17, 28 (index)		
34	3	Bande morte d'entrée analogique - simple précision, virgule flottante	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt) 17, 28 (index)

GROUPE D'OBJETS DNP ET VARIATION			REQUETE		REPONSE	
			Pouvant être émise par le client		Analysée par le client	
			Analysée par le serveur		Pouvant être émise par le serveur	
Numéro de groupe d'objets	Numéro de variation	Description	Codes de fonction (déc.)	Codes qualificatifs (hex.)	Codes de fonction (déc.)	Codes qualificatifs (hex.)
34	3	Bande morte d'entrée analogique - simple précision, virgule flottante	2(écriture)	00, 01 (départ-arrêt) 17, 28 (index)		
40	0	Etat de sortie analogique - toute variation	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)		
40	0	Etat de sortie analogique - toute variation	22(affectation de classe)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)		
40	1	Etat de sortie analogique - 32 bits avec drapeau	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)
40	2	Etat de sortie analogique - 16 bits avec drapeau	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)
40	3	Etat de sortie analogique - simple précision, virgule flottante avec drapeau	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)
41	0	Bloc de sortie analogique - toute variation		00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)		
41	1	Bloc de sortie analogique - 32 bits	3(sélection)	17, 27, 28 (index)	(Réponse)	écho de requête
41	1	Bloc de sortie analogique - 32 bits	4(opération)	17, 27, 28 (index)	(Réponse)	écho de requête
41	1	Bloc de sortie analogique - 32 bits	5(op. directe)	17, 27, 28 (index)	(Réponse)	écho de requête
41	1	Bloc de sortie analogique - 32 bits	6(op. directe, pas d'acq.)	17, 27, 28 (index)	(Réponse)	écho de requête
41	2	Bloc de sortie analogique - 16 bits	3(sélection)	17, 27, 28 (index)	(Réponse)	écho de requête
41	2	Bloc de sortie analogique - 16 bits	4(opération)	17, 27, 28 (index)	(Réponse)	écho de requête
41	2	Bloc de sortie analogique - 16 bits	5(op. directe)	17, 27, 28 (index)	(Réponse)	écho de requête
41	2	Bloc de sortie analogique - 16 bits	6(op. directe, pas d'acq.)	17, 27, 28 (index)	(Réponse)	écho de requête
41	3	Bloc de sortie analogique - simple précision, virgule flottante	3(sélection)	17, 27, 28 (index)	(Réponse)	écho de requête
41	3	Bloc de sortie analogique - simple précision, virgule flottante	4(opération)	17, 27, 28 (index)	(Réponse)	écho de requête
41	3	Bloc de sortie analogique - simple précision, virgule flottante	5(op. directe)	17, 27, 28 (index)	(Réponse)	écho de requête
41	3	Bloc de sortie analogique - simple précision, virgule flottante	6(op. directe, pas d'acq.)	17, 27, 28 (index)	(Réponse)	écho de requête

GROUPE D'OBJETS DNP ET VARIATION			REQUETE		REPONSE	
			Pouvant être émise par le client		Analysée par le client	
			Analysée par le serveur		Pouvant être émise par le serveur	
Numéro de groupe d'objets	Numéro de variation	Description	Codes de fonction (déc.)	Codes qualificatifs (hex.)	Codes de fonction (déc.)	Codes qualificatifs (hex.)
42	0	Événement de modification de sortie analogique - toute variation	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)		
42	1	Événement de modification de sortie analogique - 32 bits sans heure	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
42	1	Événement de modification de sortie analogique - 32 bits sans heure			(Rép. non sollicitée)	17, 28 (index)
42	2	Événement de modification de sortie analogique - 16 bits sans heure	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
42	2	Événement de modification de sortie analogique - 16 bits sans heure			(Rép. non sollicitée)	17, 28 (index)
42	3	Événement de modification de sortie analogique - 32 bits avec heure	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
42	3	Événement de modification de sortie analogique - 32 bits avec heure			(Rép. non sollicitée)	17, 28 (index)
42	4	Événement de modification de sortie analogique - 16 bits avec heure	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
42	4	Événement de modification de sortie analogique - 16 bits avec heure			(Rép. non sollicitée)	17, 28 (index)
42	5	Événement de modification de sortie analogique - précision simple, virgule flottante sans heure	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
42	5	Événement de modification de sortie analogique - précision simple, virgule flottante sans heure			(Rép. non sollicitée)	17, 28 (index)
42	7	Événement de modification de sortie analogique - précision simple, virgule flottante avec heure	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
42	7	Événement de modification de sortie analogique - précision simple, virgule flottante avec heure			(Rép. non sollicitée)	17, 28 (index)
50	1	Heure et date - heure absolue	1(lecture)	07 (qté limitée = 1)	(Réponse)	07 (qté limitée = 1)
50	1	Heure et date - heure absolue	2(écriture)	07 (qté limitée = 1)		
50	3	Heure et date - heure absolue lors du dernier relevé horaire	2(écriture)	07 (qté limitée = 1)		
51	1	Heure et date CTO - heure absolue, synchronisée			(Réponse)	07 (qté limitée = 1)
51	1	Heure et date CTO - heure absolue, synchronisée			(Rép. non sollicitée)	07 (qté limitée = 1)

GROUPE D'OBJETS DNP ET VARIATION			REQUETE		REPONSE	
			Pouvant être émise par le client		Analysée par le client	
			Analysée par le serveur		Pouvant être émise par le serveur	
Numéro de groupe d'objets	Numéro de variation	Description	Codes de fonction (déc.)	Codes qualificatifs (hex.)	Codes de fonction (déc.)	Codes qualificatifs (hex.)
51	2	Heure et date CTO - heure absolue, non synchronisée			(Réponse)	07 (qté limitée = 1)
51	2	Heure et date CTO - heure absolue, non synchronisée			(Rép. non sollicitée)	07 (qté limitée = 1)
52	1	Temporisation - grossière			(Réponse)	07 (qté limitée = 1)
52	2	Temporisation - fine			(Réponse)	07 (qté limitée = 1)
60	1	Objets de classe - données de la classe 0	1(lecture)	06 (aucune plage, ou toutes)		
60	1	Objets de classe - données de la classe 0		06 (aucune plage, ou toutes)		
60	2	Objets de classe - données de la classe 1	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)		
60	2	Objets de classe - données de la classe 1	20(activation rép. non soll.)	06 (aucune plage, ou toutes)		
60	2	Objets de classe - données de la classe 1	21 (désactivation rép. non soll.)	06 (aucune plage, ou toutes)		
60	2	Objets de classe - données de la classe 1		06 (aucune plage, ou toutes)		
60	3	Objets de classe - données de la classe 2	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)		
60	3	Objets de classe - données de la classe 2	20(activation rép. non soll.)	06 (aucune plage, ou toutes)		
60	3	Objets de classe - données de la classe 2	21 (désactivation rép. non soll.)	06 (aucune plage, ou toutes)		
60	3	Objets de classe - données de la classe 2		06 (aucune plage, ou toutes)		
60	4	Objets de classe - données de la classe 3	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)		
60	4	Objets de classe - données de la classe 3	20(activation rép. non soll.)	06 (aucune plage, ou toutes)		
60	4	Objets de classe - données de la classe 3	21 (désactivation rép. non soll.)	06 (aucune plage, ou toutes)		
60	4	Objets de classe - données de la classe 3		06 (aucune plage, ou toutes)		
80	1	Indications internes - format compressé	1(lecture)	00, 01 (départ-arrêt)	(Réponse)	00, 01 (départ-arrêt)
80	1	Indications internes - format compressé	2(écriture)			
110	longueur de chaîne	Chaîne d'octet	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes)	(Réponse)	00, 01 (départ-arrêt)
110	longueur de chaîne	Chaîne d'octet	2(écriture)	00, 01 (départ-arrêt) 17, 28 (index)		
120	1	Authentification - Défi	32(auth req)	5B	(Rép. auth.)	5B
120	2	Authentification - Réponse	32(auth req)	5B	(Rép. auth.)	5B
120	3	Authentification - Mode agressif	de 1 à 31	07 (qté limitée = 1)	(Réponse)	07 (qté limitée = 1)

GROUPE D'OBJETS DNP ET VARIATION			REQUETE		REPONSE	
			Pouvant être émise par le client		Analysée par le client	
			Analysée par le serveur		Pouvant être émise par le serveur	
Numéro de groupe d'objets	Numéro de variation	Description	Codes de fonction (déc.)	Codes qualificatifs (hex.)	Codes de fonction (déc.)	Codes qualificatifs (hex.)
120	3	Authentification - Mode agressif			(Rép. non sollicitée)	07 (qté limitée = 1)
120	4	Authentification - Demande d'état de clé de session	32(auth req)	07 (qté limitée = 1)		
120	5	Authentification - État de clé de session			(Rép. auth.)	5B
120	6	Authentification - Modification de clé de session	32(auth req)	5B		
120	7	Authentification - Erreur	33(auth req, pas d'acq.)	5B	(Rép. auth.)	5B
121	1	Statistique de sécurité	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes) 17, 28 (index)	(Réponse)	00, 01 (départ-arrêt) 17, 28 (index)
122	0	Événement statistique de sécurité - 32 bits avec drapeau	1(lecture)	00, 01 (départ-arrêt) 06 (aucune plage, ou toutes) 17, 28 (index)		
122	1	Événement statistique de sécurité - 32 bits avec drapeau	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
122	1	Événement statistique de sécurité - 32 bits avec drapeau et heure			(Rép. non sollicitée)	17, 28 (index)
122	2	Événement statistique de sécurité - 32 bits avec drapeau et heure	1(lecture)	06 (aucune plage, ou toutes) 07, 08 (qté limitée)	(Réponse)	17, 28 (index)
122	2	Événement statistique de sécurité - 32 bits avec drapeau et heure			(Rép. non sollicitée)	17, 28 (index)

Interopérabilité IEC60870-5-104

Profils de serveur IEC60870-5-104

Introduction

Cette norme d'accompagnement présente des ensembles de paramètres et de variantes parmi lesquels vous devez sélectionner des sous-ensembles pour mettre en œuvre des systèmes de téléconduite particuliers. Certaines valeurs de paramètres, telles que le choix de champs *structurés* ou *non structurés* de l'adresse d'objet d'information des ASDU, représentent des choix qui s'excluent mutuellement. Autrement dit, une seule valeur des paramètres définis est admise par système. D'autres paramètres, tels que l'ensemble répertorié d'informations de processus différentes dans les directions de commande et de surveillance, permettent de spécifier l'ensemble complet ou des sous-ensembles en fonction des besoins des applications. Cette clause récapitule les paramètres des clauses précédentes afin de faciliter la sélection pour une application donnée. Si un système est composé d'équipements de différents fabricants, il est nécessaire que tous les partenaires s'accordent sur les paramètres sélectionnés.

Cette liste d'interopérabilité est définie conformément à la norme IEC60870-5-101 et étendue par des paramètres utilisés dans cette norme. Les descriptions textuelles des paramètres qui ne sont pas applicables à cette norme d'accompagnement sont occultées (la case correspondante est noire).

Les paramètres sélectionnés doivent être marqués dans les cases blanches :

- ☐ La fonction ou l'ASDU n'est pas utilisée.
- ☒ La fonction ou l'ASDU est utilisée en standard (par défaut).
- ☐ La fonction ou l'ASDU est utilisée en mode inverse.
- ☐ La fonction ou l'ASDU est utilisée en modes standard et inverse.

La sélection possible (*vide*, **X**, **R** ou **B**) est spécifiée pour chaque clause ou paramètre spécifique.

NOTE: Une case à cocher noire indique que l'option ne peut pas être sélectionnée dans cette norme d'accompagnement.

Système ou équipement

Les paramètres spécifiques au système indiquent la définition d'un système ou d'un équipement en remplissant ces cases avec un **X** :

- ☐ définition du système
- ☐ définition de la station de contrôle (client)
- ☒ définition de la station de contrôle (serveur)

Couche application

Pour toutes les fonctions de la couche application, marquez chaque paramètre en conséquence :

- **X** : Le paramètre est utilisé uniquement dans le sens standard.
- **C** : Le paramètre est utilisé uniquement dans le sens inverse.
- **B** : Le paramètre est utilisé dans les deux sens.
- (*vide*) : La fonction n'est pas disponible dans cette norme d'accompagnement.

Mode de transmission des données d'application

Le mode 1 (octet de poids faible en premier), tel que défini dans la section 4.10 de la norme IEC60870-5-4, est utilisé de manière exclusive dans cette norme d'accompagnement.

Adresse commune d'ASDU

Pour les paramètres spécifiques au système, toutes les configurations implémentées sont marquées d'un **X** :

☒ deux octets

Adresse d'objet d'information

Pour les paramètres spécifiques au système, toutes les configurations implémentées sont marquées d'un **X** :

☐ structuré

☒ trois octets

☐ structuré

Cause d'émission

Pour les paramètres spécifiques au système, toutes les configurations implémentées sont marquées d'un **X** :

☒ deux octets (avec adresse de l'émetteur)

NOTE: Si elle n'est pas utilisée, l'adresse de l'émetteur est définie sur 0.

Longueur de l'APDU : Pour les paramètres spécifiques au système, indiquez la longueur maximale de l'APDU par système.

NOTE: La longueur maximale de l'APDU est de 253 pour les deux sens. Il s'agit d'un paramètre système fixe.

Informations de processus dans le sens de surveillance

Pour les paramètres spécifiques à la station, marquez chaque ID de type de manière appropriée (**X**, **R**, **B**) :

☒	<1>	:=	informations de signalisation simple	M_SP_NA_1
☒	<3>	:=	informations de de signalisation double	M_DP_NA_1
☒	<5>	:=	informations de position d'étape	M_ST_NA_1
☒	<7>	:=	chaîne de 32 bits	M_BO_NA_1
☒	<9>	:=	valeur mesurée, valeur normalisée	M_ME_NA_1
☒	<11>	:=	valeur mesurée, valeur mise à l'échelle	M_ME_NB_1
☒	<13>	:=	valeur mesurée, valeur à virgule flottante courte	M_ME_NC_1
☒	<14>	:=	valeur mesurée, valeur à virgule flottante courte avec horodatage	M_ME_TC_1

☒	<15>	:=	totaux intégrés	M_IT_NA_1
☐	<20>	:=	paquet d'informations de signalisation simple avec détection de changement d'état	M_PS_NA_1
☐	<21>	:=	valeur mesurée, valeur normalisée sans descripteur de qualité	M_ME_ND_1
☒	<30>	:=	informations de signalisation simple avec horodatage CP56Time2a	M_SP_TB_1
☒	<31>	:=	informations de signalisation double avec horodatage CP56Time2a	M_DP_TB_1
☒	<32>	:=	informations de position d'étape avec horodatage CP56Time2a	M_ST_TB_1
☒	<33>	:=	chaîne de 32 bits avec horodatage CP56Time2a	M_BO_TB_1
☒	<34>	:=	valeur mesurée, valeur normalisée avec horodatage CP56Time2a	M_ME_TD_1
☒	<35>	:=	valeur mesurée, valeur mise à l'échelle avec horodatage CP56Time2a	M_ME_TE_1
☒	<36>	:=	valeur mesurée, valeur à virgule flottante courte avec horodatage CP56Time2a	M_ME_TF_1
☒	<37>	:=	totaux intégrés avec horodatage CP56Time2a	M_IT_TB_1
☐	<38>	:=	événement d'équipement de protection avec horodatage CP56Time2a	M_EP_TD_1
☐	<39>	:=	paquet d'événements de démarrage d'équipement de protection avec horodatage CP56Time2a	M_EP_TE_1
☐	<40>	:=	paquet d'informations de circuit de sortie d'équipement de protection avec horodatage CP56Time2a	M_EP_TF_1

NOTE: Cette norme d'accompagnement utilise uniquement le jeu de <30> à <40> pour les ASDU avec balises horaires autorisées.

Informations de processus dans le sens du contrôle

Pour les paramètres spécifiques à la station, marquez chaque ID de type de manière appropriée (X, R, B) :

☒	<45>	:=	commande simple	C_SC_NA_1
☒	<46>	:=	commande double	C_DC_NA_1
☒	<47>	:=	commande d'étape de régulation	C_RC_NA_1
☒	<48>	:=	commande de consigne, valeur normalisée	C_SE_NA_1
☒	<49>	:=	commande de consigne, valeur mise à l'échelle	C_SE_NB_1
☒	<50>	:=	commande de consigne, valeur à virgule flottante courte	C_SE_NC_1
☒	<51>	:=	chaîne de 32 bits	C_BO_NA_1
☒	<58>	:=	commande simple avec horodatage CP56Time2a	C_SC_TA_1
☒	<59>	:=	commande double avec horodatage CP56Time2a	C_DC_TA_1
☒	<60>	:=	commande d'étape de régulation avec horodatage CP56Time2a	C_RC_TA_1
☒	<61>	:=	commande de consigne, valeur normalisée avec horodatage CP56Time2a	C_SE_TA_1
☒	<62>	:=	commande de consigne, valeur mise à l'échelle avec horodatage CP56Time2a	C_SE_TB_1

☒	<63>	:=	commande de consigne, valeur à virgule flottante courte avec horodatage CP56Time2a	C_SE_TC_1
☒	<64>	:=	chaîne de 32 bits avec horodatage CP56Time2a	C_BO_TA_1

NOTE: Cette norme d'accompagnement utilise l'un des jeux ASDU suivants :

- <45> ... <50>
- <58> ... <64>

Informations système dans le sens de la surveillance

Marquez chaque paramètre spécifique à la station de manière appropriée (X, R, B) : M_EI_NA_1

☒	<70>	:=	fin de l'initialisation

Informations système dans le sens du contrôle

Pour les paramètres spécifiques à la station, marquez chaque ID de type de manière appropriée (X, R, B) :

☒	<100>	:=	commande d'interrogation	
☒	<101>	:=	commande d'interrogation de compteur	C_CI_NA_1
☒	<102>	:=	commande de lecture	C_RD_NA_1
☒	<103>	:=	commande de synchronisation d'horloge	C_CS_NA_1
☒	<105>	:=	commande de réinitialisation de processus	C_RP_NA_1
☒	<107>	:=	commande de test avec horodatage CP56Time2a	C_TS_TA_1

Paramètre dans le sens du contrôle

Pour les paramètres spécifiques à la station, marquez chaque ID de type de manière appropriée (X, R, B) :

☒	<110>	:=	Il s'agit du paramètre de la valeur mesurée, valeur normalisée.	P_ME_NA_1
☒	<111>	:=	Il s'agit du paramètre de la valeur mesurée, valeur mise à l'échelle.	P_ME_NB_1
☒	<112>	:=	Il s'agit du paramètre de la valeur mesurée, valeur à virgule flottante courte.	P_ME_NC_1
☒	<113>	:=	Il s'agit de l'activation du paramètre.	P_AC_NA_1

Transfert de fichier

Pour les paramètres spécifiques à la station, marquez chaque ID de type de manière appropriée (X, R, B) :

☐	<120>	:=	fichier prêt	
☐	<121>	:=	section prête	F_SR_NA_1
☐	<122>	:=	appel de répertoire, sélection de fichier, appel de fichier, appel de section	F_SC_NA_1
☐	<123>	:=	dernière section, dernier segment	F_LS_NA_1
☐	<124>	:=	accusé de réception de fichier, accusé de réception de section	F_AF_NA_1
☐	<125>	:=	segment	F_SG_NA_1

☐	<126>	:=	répertoire {vide ou X, disponible uniquement dans le sens de la surveillance (standard)}	F_DR_TA_1
☐	<127>	:=	journal de requêtes — journal d'archivage des requêtes	F_SC_NB_1

Affectations des identifiant de type et causes d'émission (paramètres spécifiques à la station)

- (*grisé*) : Ces cases ne sont pas nécessaires.
- (*noir*) : Cette option n'est pas autorisée dans cette norme d'accompagnement.
- (*vide*) : La fonction ou l'ASDU n'est pas utilisée.

Marquez correctement chaque combinaison type d'identifiant/cause d'émission (X, R, B) :

Identification de type		Cause de la transmission																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 ... 36	37 ... 41	44	45	46	47
<1>	M_SP_NA_1		X	X		X									X					
<3>	M_DP_NA_1		X	X		X									X					
<5>	M_ST_NA_1		X	X		X									X					
<7>	M_BO_NA_1		X	X		X									X					
<9>	M_ME_NA_1	X	X	X		X									X					
<11>	M_ME_NB_1	X	X	X		X									X					
<13>	M_ME_NC_1	X	X	X		X									X					
<15>	M_IT_NA_1			X												X				
<20>	M_PS_NA_1																			
<21>	M_ME_ND_1																			
<30>	M_SP_TB_1			X		X														
<31>	M_DP_TB_1			X		X														
<32>	M_ST_TB_1			X		X														
<33>	M_BO_TB_1			X		X														
<34>	M_ME_TD_1			X		X														
<35>	M_ME_TE_1			X		X														
<36>	M_ME_TF_1			X		X														
<37>	M_IT_TB_1			X																
<38>	M_EP_TD_1																			
<39>	M_EP_TE_1																			
<40>	M_EP_TF_1																			
<45>	C_SC_NA_1						X	X	X	X	X						X	X	X	X
<46>	C_DC_NA_1						X	X	X	X	X						X	X	X	X
<47>	C_RC_NA_1						X	X	X	X	X						X	X	X	X
<48>	C_SE_NA_1						X	X	X	X	X						X	X	X	X
<49>	C_SE_NB_1						X	X	X	X	X						X	X	X	X
<50>	C_SE_NC_1						X	X	X	X	X						X	X	X	X
<51>	C_BO_NA_1						X	X			X						X	X	X	X
<58>	C_SC_TA_1						X	X	X	X	X						X	X	X	X
<59>	C_DC_TA_1						X	X	X	X	X						X	X	X	X
<60>	C_RC_TA_1						X	X	X	X	X						X	X	X	X
<61>	C_SE_TA_1						X	X	X	X	X						X	X	X	X
<62>	C_SE_TB_1						X	X	X	X	X						X	X	X	X
<63>	C_SE_TC_1						X	X	X	X	X						X	X	X	X
<64>	C_BO_TA_1						X	X			X						X	X	X	X
<70>	M_EI_NA_1 Voir la remarque (ci-dessous).				X															
<100>	C_IC_NA_1						X	X	X	X	X						X	X	X	X
<101>	C_CI_NA_1						X	X			X						X	X	X	X
<102>	C_RD_NA_1					X											X	X	X	X
<103>	C_CS_NA_1						X	X									X	X	X	X
<105>	C_RP_NA_1						X	X									X	X	X	X
<107>	C_TS_TA_1						X	X									X	X	X	X

Identification de type		Cause de la transmission																		
<110>	P_ME_NA_1						X	X							X		X	X	X	X
<111>	P_ME_NB_1						X	X							X		X	X	X	X
<112>	P_ME_NC_1						X	X							X		X	X	X	X
<113>	P_AC_NA_1						X	X	X	X							X	X	X	X
<120>	F_FR_NA_1																			
<121>	F_SR_NA_1																			
<122>	F_SC_NA_1																			
<123>	F_LS_NA_1																			
<124>	F_AF_NA_1																			
<125>	F_SG_NA_1																			
<126>	F_DR_TA_1 Voir la remarque (ci-dessous).																			
<127>	F_SC_NB_1 Voir la remarque (ci-dessous).																			

NOTE: Vide ou X uniquement.

Fonctions d'application élémentaire

Marquez chaque fonction d'application élémentaire en conséquence :

- **X** : Le paramètre est utilisé uniquement dans le sens standard.
- **C** : Le paramètre est utilisé uniquement dans le sens inverse.
- **B** : Le paramètre est utilisé dans les deux sens.
- (*vide*) : La fonction n'est pas disponible dans cette norme d'accompagnement.

Initialisation de station

Pour les paramètres propres à la station, toutes les fonctions implémentées sont marquées d'un X :

☒ initialisation à distance

Transmission cyclique de données

Pour les paramètres spécifiques à la station, marquez chaque fonction de manière appropriée (X, R, B) :

☒ transmission cyclique de données

Procédure de lecture

Pour les paramètres spécifiques à la station, marquez chaque fonction de manière appropriée (X, R, B) :

☒ procédure de lecture

Transmission Spontanée

Pour les paramètres spécifiques à la station, marquez chaque fonction de manière appropriée (X, R, B) :

☒ transmission spontanée

Transmission double d'objets d'information avec cause de transmission spontanée

Pour les paramètres spécifiques à la station, marquez chaque fonction d'un X lorsqu'un ID de type sans heure et un ID de type correspondant avec heure sont tous les deux émis en réponse à un seul changement spontané d'un objet surveillé :

- ☐ informations de signalisation simple (M_SP_NA_1, M_SP_TA_1, M_SP_TB_1, M_PS_NA_1)
- ☐ informations de signalisation double (M_DP_NA_1, M_DP_TA_1, M_DP_TB_1)
- ☐ informations de position d'étape (M_ST_NA_1, M_ST_TA_1, M_ST_TB_1)
- ☐ chaîne de 32 bits (M_BO_NA_1, M_BO_TA_1, M_BO_TB_1) si définie pour un projet spécifique.
- ☐ valeur mesurée, valeur normalisée (M_ME_NA_1, M_ME_TA_1, M_ME_ND_1, M_ME_TD_1)
- ☐ valeur mesurée, valeur mise à l'échelle (M_ME_NB_1, M_ME_TB_1, M_ME_TE_1)
- ☐ valeur mesurée, nombre à virgule flottante court (M_ME_NC_1, M_ME_TC_1, M_ME_TF_1)

Interrogation de station

Pour les paramètres spécifiques à la station, marquez chaque fonction de manière appropriée (X, R, B) :

- ☒ global
- ☒ groupe 1 ☒ groupe 7 ☒ groupe 13
- ☒ groupe 2 ☒ groupe 8 ☒ groupe 14
- ☒ groupe 3 ☒ groupe 9 ☒ groupe 15
- ☒ groupe 4 ☒ groupe 10 ☒ groupe 16
- ☒ groupe 5 ☒ groupe 11
- ☒ groupe 6 ☒ groupe 12

NOTE: Affichez les adresses d'objet d'information affectées à chaque groupe dans un tableau distinct.

Synchronisation d'horloge

Pour les paramètres spécifiques à la station, marquez chaque fonction de manière appropriée (X, R, B) :

- ☒ synchronisation de l'horloge
- ☒ jour de la semaine utilisé
- ☒ RES1, GEN (horodatage remplacé / non remplacé) utilisé
- ☒ bit SU (heure d'été) utilisé

Transmission des totaux intégrés

Pour les paramètres spécifiques à la station ou à l'objet, marquez chaque fonction de manière appropriée (X, R, B) :

- ☒ Mode A : gel local avec transmission spontanée
- ☒ Mode B : gel local avec interrogation de compteur
- ☒ Mode C : geler et transmettre par des commandes d'interrogation de compteur
- ☐ Mode D : gel par commande d'interrogation de compteur, valeurs gelées signalées de façon spontanée
- ☒ lecture de compteur
- ☒ gel de compteur sans réinitialisation
- ☒ gel de compteur avec réinitialisation
- ☒ réinitialisation de compteur
- ☒ compteur de requêtes général
- ☒ compteur de requêtes groupe 1
- ☒ compteur de requêtes groupe 2
- ☒ compteur de requêtes groupe 3
- ☒ compteur de requêtes groupe 4

Chargement des paramètres

Pour les paramètres spécifiques à un objet, marquez chaque fonction de manière appropriée (X, R, B) :

- ☒ valeur de seuil
- ☐ facteur de lissage
- ☒ limite basse pour la transmission de valeur mesurée
- ☒ limite haute pour la transmission de valeur mesurée

Activation des paramètres

Pour les paramètres spécifiques à un objet, marquez chaque fonction de manière appropriée (X, R, B) :

- ☒ activer/désactiver la transmission périodique ou cyclique persistante de l'objet adressé

Procédure de test

Pour les paramètres spécifiques à la station, marquez chaque fonction de manière appropriée (X, R, B) :

- ☒ procédure de test

Transfert de fichier

Pour les paramètres spécifiques à la station, marquez X lorsque la fonction est utilisée.

Transfert de fichiers dans le sens de la surveillance :

- ☐ fichier transparent
- ☐ transmission de données de perturbation de l'équipement de protection
- ☐ transmission de séquences d'événements
- ☐ transmission de séquences de valeurs analogiques enregistrées

Transfert de fichiers dans le sens du contrôle :

- ☐ fichier transparent

Scrutation en arrière-plan

Pour les paramètres spécifiques à la station, marquez chaque fonction de manière appropriée (X, R, B) :

☒ scrutation en arrière-plan

Définition des timeouts

Paramètre	Valeur par défaut	Remarques	Valeur sélectionnée
t_0	30 s	délai d'établissement de la connexion	configurable
t_1	15 s	délai d'envoi ou de test des APDU	configurable
t_2	10 s	délai d'acquittement en cas d'absence de messages de données $t_2 < t_1$	configurable
t_3	20 s	délai d'envoi des trames de test en cas d'état d'inactivité prolongé	configurable
Plages : - plage maximale pour les timeouts t_0 à t_2 : 1 à 255 s (précision : 1 s) - plage maximale pour le timeout t_3 : 1 à 48 heures (résolution : 1 s) - des délais longs peuvent être nécessaires pour t_3 dans des cas particuliers où des liaisons par satellite ou des connexions par réseau commuté sont utilisées (par exemple, pour établir une connexion et collecter des valeurs seulement une fois par jour ou par semaine)			

Nombre maximal d'APDU de format I en attente (k) et dernières APDU acquittées (w)

Paramètre	Valeur par défaut	Remarques	Valeur sélectionnée
k	12 APDU	différence maximale entre le nombre de la séquence reçue et le nombre à envoyer	configurable
w	8 APDU	dernier accusé de réception après réception de w APDU de format I	configurable
Plage de valeurs : k : 1 à 12 APDU (précision : 1 APDU) w : 1 à 32767 APDU (précision : 1 APDU) (w ne doit pas dépasser les deux tiers de k). NOTE: Dans la plupart des cas, la valeur de w ne dépasse pas les deux tiers de k.			

Numéro de port

Paramètre	Valeur	Remarques
<i>Portnumber</i>	2404	configurable

Connexions redondantes

☐ **4** nombre N de connexions de groupe redondant utilisées

Suite RFC 2200

RFC 2200 est une norme Internet officielle qui décrit l'état de normalisation des protocoles utilisés sur Internet conformément aux spécifications du IAB (Internet Architecture Board). Elle offre un large éventail de normes actuellement utilisées sur Internet. Les documents RFC 2200 appropriés définis dans cette norme pour des projets donnés doivent être sélectionnés par l'utilisateur de la norme.

- ☐ Ethernet 802.3
- ☐ interface série X.21
- ☐ autre sélection de RFC 2200

Profils client IEC60870-5-104

Introduction

Cette norme d'accompagnement présente des ensembles de paramètres et de choix parmi lesquels vous devez sélectionner des sous-ensembles pour mettre en œuvre des systèmes de téléconduite particuliers. Certaines valeurs de paramètres, telles que le choix de champs *structurés* ou *non structurés* de l'adresse d'objet d'information des ASDU, représentent des solutions qui s'excluent mutuellement. Autrement dit, une seule valeur des paramètres définis est admise par système. D'autres paramètres, tels que l'ensemble répertorié d'informations de processus différentes dans les directions de contrôle et de surveillance, permettent de spécifier l'ensemble complet ou des sous-ensembles en fonction des besoins des applications. Cette clause récapitule les paramètres des clauses précédentes afin de faciliter la sélection pour une application donnée. Si un système est composé d'équipements provenant de différents fabricants, il est nécessaire que tous les partenaires soient d'accord sur les paramètres sélectionnés.

Cette liste d'interopérabilité est définie conformément à la norme IEC60870-5-101 et étendue par des paramètres utilisés dans cette norme. Les descriptions textuelles des paramètres qui ne sont pas applicables à cette norme d'accompagnement sont occultées (la case correspondante est noire).

Les paramètres sélectionnés doivent être marqués dans les cases blanches :

- ☐ La fonction ou l'ASDU n'est pas utilisée.
- ☒ La fonction ou l'ASDU est utilisée en standard (par défaut).
- ☐ La fonction ou l'ASDU est utilisée en mode inverse.
- ☐ La fonction ou l'ASDU est utilisée en modes standard et inverse.

La sélection possible (*vide*, **X**, **R** ou **B**) est spécifiée pour chaque clause ou paramètre spécifique.

NOTE: Une case à cocher noire indique que l'option ne peut pas être sélectionnée dans cette norme d'accompagnement.

Système ou équipement

Les paramètres spécifiques au système indiquent la définition d'un système ou d'un équipement en remplissant ces cases avec un **X** :

- ☐ définition du système
- ☒ définition de la station de contrôle (client)
- ☐ définition de la station de contrôle (serveur)

Couche application

Pour toutes les fonctions de la couche application, marquez chaque paramètre en conséquence :

- **X** : Le paramètre est utilisé uniquement dans le sens standard.
- **C** : Le paramètre est utilisé uniquement dans le sens inverse.
- **B** : Le paramètre est utilisé dans les deux sens.
- (*vide*) : La fonction n'est pas disponible dans cette norme d'accompagnement.

Mode de transmission des données d'application

Le mode 1 (octet de poids faible en premier), tel que défini dans la section 4.10 de la norme IEC60870-5-4, est utilisé de manière exclusive dans cette norme d'accompagnement.

Adresse commune d'ASDU

Pour les paramètres spécifiques au système, toutes les configurations implémentées sont marquées d'un X :

☒ deux octets

Adresse d'objet d'information

Pour les paramètres spécifiques au système, toutes les configurations implémentées sont marquées d'un X :

☐ structuré

☒ trois octets

☐ structuré

Cause d'émission

Pour les paramètres spécifiques au système, toutes les configurations implémentées sont marquées d'un X :

☒ deux octets (avec adresse de l'émetteur)

NOTE: Si elle n'est pas utilisée, l'adresse de l'émetteur est définie sur 0.

Longueur de l'APDU : Pour les paramètres spécifiques au système, indiquez la longueur maximale de l'APDU par système.

NOTE: La longueur maximale de l'APDU est de 253 pour les deux sens. Il s'agit d'un paramètre système fixe.

Informations de processus dans le sens de surveillance

Pour les paramètres spécifiques à la station, marquez chaque ID de type de manière appropriée (X, R, B) :

☒	<1>	:=	informations de signalisation simple	M_SP_NA_1
☒	<3>	:=	informations de de signalisation double	M_DP_NA_1
☒	<5>	:=	informations de position d'étape	M_ST_NA_1
☒	<7>	:=	chaîne de 32 bits	M_BO_NA_1
☒	<9>	:=	valeur mesurée, valeur normalisée	M_ME_NA_1
☒	<11>	:=	valeur mesurée, valeur mise à l'échelle	M_ME_NB_1
☒	<13>	:=	valeur mesurée, valeur à virgule flottante courte	M_ME_NC_1
☒	<15>	:=	totaux intégrés	M_IT_NA_1
☐	<20>	:=	paquet d'informations de signalisation simple avec détection de changement d'état	M_PS_NA_1
☐	<21>	:=	valeur mesurée, valeur normalisée sans descripteur de qualité	M_ME_ND_1
☒	<30>	:=	information de signalisation simple avec horodatage CP56Time2a	M_SP_TB_1
☒	<31>	:=	information de signalisation double avec horodatage CP56Time2a	M_DP_TB_1
☒	<32>	:=	informations de position d'étape avec horodatage CP56Time2a	M_ST_TB_1

☒	<33>	:=	chaîne de 32 bits avec horodatage CP56Time2a	M_BO_TB_1
☒	<34>	:=	valeur mesurée, valeur normalisée avec horodatage CP56Time2a	M_ME_TD_1
☒	<35>	:=	valeur mesurée, valeur mise à l'échelle avec horodatage CP56Time2a	M_ME_TE_1
☒	<36>	:=	valeur mesurée, valeur à virgule flottante courte avec horodatage CP56Time2a	M_ME_TF_1
☒	<37>	:=	totaux intégrés avec horodatage CP56Time2a	M_IT_TB_1
☐	<38>	:=	événement d'équipement de protection avec horodatage CP56Time2a	M_EP_TD_1
☐	<39>	:=	paquet d'événements de démarrage d'équipement de protection avec horodatage CP56Time2a	M_EP_TE_1
☐	<40>	:=	paquet d'informations de circuit de sortie d'équipement de protection avec horodatage CP56Time2a	M_EP_TF_1

NOTE: Cette norme d'accompagnement utilise uniquement le jeu <30> à <40> pour les ASDU avec balises horaires autorisées.

Informations de processus dans le sens du contrôle

Pour les paramètres spécifiques à la station, marquez chaque ID de type de manière appropriée (X, R, B) :

☒	<45>	:=	commande simple	C_SC_NA_1
☒	<46>	:=	commande double	C_DC_NA_1
☒	<47>	:=	commande d'étape de régulation	C_RC_NA_1
☒	<48>	:=	commande de consigne, valeur normalisée	C_SE_NA_1
☒	<49>	:=	commande de consigne, valeur mise à l'échelle	C_SE_NB_1
☒	<50>	:=	commande de consigne, valeur à virgule flottante courte	C_SE_NC_1
☒	<51>	:=	chaîne de 32 bits	C_BO_NA_1
☒	<58>	:=	commande simple avec horodatage CP56Time2a	C_SC_TA_1
☒	<59>	:=	commande double avec horodatage CP56Time2a	C_DC_TA_1
☒	<60>	:=	commande d'étape de régulation avec horodatage CP56Time2a	C_RC_TA_1
☒	<61>	:=	commande de consigne, valeur normalisée, avec horodatage CP56Time2a	C_SE_TA_1
☒	<62>	:=	commande de point de consigne, valeur mise à l'échelle, avec horodatage CP56Time2a	C_SE_TB_1
☒	<63>	:=	commande de consigne, valeur à virgule flottante courte, avec horodatage CP56Time2a	C_SE_TC_1
☒	<64>	:=	chaîne de 32 bits avec horodatage CP56Time2a	C_BO_TA_1

NOTE: Cette norme d'accompagnement utilise l'un des jeux ASDU suivants :

- <45> ... <50>
- <58> ... <64>

Informations système dans le sens de la surveillance

Marquez chaque paramètre spécifique à la station de manière appropriée (X, R, B) : M_EI_NA_1

☒ <70> := fin de l'initialisation

Informations système dans le sens du contrôle

Pour les paramètres spécifiques à la station, marquez chaque ID de type de manière appropriée (X, R, B) : C_IC_NA_1

☒ <100> := commande d'interrogation

☒ <101> := commande d'interrogation de compteur C_CI_NA_1

☒ <102> := commande de lecture C_RD_NA_1

☒ <103> := commande de synchronisation d'horloge C_CS_NA_1

☒ <105> := commande de réinitialisation de processus C_RP_NA_1

☒ <107> := commande de test avec horodatage CP56Time2a C_TS_TA_1

Paramètre dans le sens du contrôle

Pour les paramètres spécifiques à la station, marquez chaque ID de type de manière appropriée (X, R, B) :

☒ <110> := Il s'agit du paramètre de la valeur mesurée, valeur normalisée. P_ME_NA_1

☒ <111> := Il s'agit du paramètre de la valeur mesurée, valeur mise à l'échelle. P_ME_NB_1

☒ <112> := Il s'agit du paramètre de la valeur mesurée, valeur à virgule flottante courte. P_ME_NC_1

☒ <113> := Il s'agit de l'activation du paramètre. P_AC_NA_1

Transfert de fichier

Pour les paramètres spécifiques à la station, marquez chaque ID de type de manière appropriée (X, R, B) :

☐ <120> := fichier prêt

☐ <121> := section prête F_SR_NA_1

☐ <122> := appel de répertoire, sélection de fichier, appel de fichier, appel de section F_SC_NA_1

☐ <123> := dernière section, dernier segment F_LS_NA_1

☐ <124> := accusé de réception de fichier, accusé de réception de section F_AF_NA_1

☐ <125> := segment F_SG_NA_1

☐ <126> := répertoire {vide ou X, disponible uniquement dans le sens de la surveillance (standard)} F_DR_TA_1

☐ <127> := journal de requêtes — journal d'archivage des requêtes F_SC_NB_1

Affectations des identifiant de type et causes d'émission (paramètres spécifiques à la station)

- (grisé) : Ces cases ne sont pas nécessaires.
- (noir) : Cette option n'est pas autorisée dans cette norme d'accompagnement.
- (vide) : La fonction ou l'ASDU n'est pas utilisée.

Marquez correctement chaque combinaison type d'identifiant/cause d'émission (X, R, B) :

Identification de type		Cause d'émission																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 ...	37 ...	44	45	46	47
															36	41				
<1>	M_SP_NA_1		X	X		X						X	X		X					
<3>	M_DP_NA_1		X	X		X						X	X		X					
<5>	M_ST_NA_1		X	X		X						X	X		X					
<7>	M_BO_NA_1		X	X		X									X					
<9>	M_ME_NA_1	X	X	X		X									X					
<11>	M_ME_NB_1	X	X	X		X									X					
<13>	M_ME_NC_1	X	X	X		X									X					
<15>	M_IT_NA_1			X												X				
<20>	M_PS_NA_1																			
<21>	M_ME_ND_1																			
<30>	M_SP_TB_1			X		X						X	X							
<31>	M_DP_TB_1			X		X						X	X							
<32>	M_ST_TB_1			X		X						X	X							
<33>	M_BO_TB_1			X		X														
<34>	M_ME_TD_1			X		X														
<35>	M_ME_TE_1			X		X														
<36>	M_ME_TF_1			X		X														
<37>	M_IT_TB_1			X																
<38>	M_EP_TD_1																			
<39>	M_EP_TE_1																			
<40>	M_EP_TF_1																			
<45>	C_SC_NA_1						X	X	X	X	X						X	X	X	X
<46>	C_DC_NA_1						X	X	X	X	X						X	X	X	X
<47>	C_RC_NA_1						X	X	X	X	X						X	X	X	X
<48>	C_SE_NA_1						X	X	X	X	X						X	X	X	X
<49>	C_SE_NB_1						X	X	X	X	X						X	X	X	X
<50>	C_SE_NC_1						X	X	X	X	X						X	X	X	X
<51>	C_BO_NA_1						X	X			X						X	X	X	X
<58>	C_SC_TA_1						X	X	X	X	X						X	X	X	X
<59>	C_DC_TA_1						X	X	X	X	X						X	X	X	X
<60>	C_RC_TA_1						X	X	X	X	X						X	X	X	X
<61>	C_SE_TA_1						X	X	X	X	X						X	X	X	X
<62>	C_SE_TB_1						X	X	X	X	X						X	X	X	X
<63>	C_SE_TC_1						X	X	X	X	X						X	X	X	X
<64>	C_BO_TA_1						X	X			X						X	X	X	X
<70>	M_EI_NA_1 Voir la remarque (ci- dessous).				X															
<100- >	C_IC_NA_1						X	X	X	X	X						X	X	X	X
<101- >	C_CI_NA_1						X	X			X						X	X	X	X
<102- >	C_RD_NA_1					X											X	X	X	X
<103- >	C_CS_NA_1						X	X									X	X	X	X

Identification de type		Cause d'émission																		
<105->	C_RP_NA_1						X	X									X	X	X	X
<107->	C_TS_TA_1						X	X									X	X	X	X
<110->	P_ME_NA_1						X	X							X		X	X	X	X
<111>	P_ME_NB_1						X	X							X		X	X	X	X
<112->	P_ME_NC_1						X	X							X		X	X	X	X
<113->	P_AC_NA_1						X	X	X	X							X	X	X	X
<120->	F_FR_NA_1																			
<121->	F_SR_NA_1																			
<122->	F_SC_NA_1																			
<123->	F_LS_NA_1																			
<124->	F_AF_NA_1																			
<125->	F_SG_NA_1																			
<126->	F_DR_TA_1 Voir la remarque (ci- dessous).																			
<127->	F_SC_NB_1 Voir la remarque (ci- dessous).																			

NOTE: Vide ou X uniquement.

Fonctions d'application élémentaire

Marquez chaque fonction d'application élémentaire en conséquence :

- **X** : Le paramètre est utilisé uniquement dans le sens standard.
- **C** : Le paramètre est utilisé uniquement dans le sens inverse.
- **B** : Le paramètre est utilisé dans les deux sens.
- (*vide*) : La fonction n'est pas disponible dans cette norme d'accompagnement.

Initialisation de station

Pour les paramètres propres à la station, toutes les fonctions implémentées sont marquées d'un X :



initialisation à distance

Transmission cyclique de données

Pour les paramètres spécifiques à la station, marquez chaque fonction de manière appropriée (X, R, B) :



transmission cyclique de données

Procédure de lecture

Pour les paramètres spécifiques à la station, marquez chaque fonction de manière appropriée (X, R, B) :



procédure de lecture

Transmission Spontanée

Pour les paramètres spécifiques à la station, marquez chaque fonction de manière appropriée (X, R, B) :

☒ transmission spontanée

Transmission double d'objets d'information avec cause de transmission spontanée

Pour les paramètres spécifiques à la station, marquez chaque fonction d'un X lorsqu'un ID de type sans heure et un ID de type correspondant avec heure sont tous les deux émis en réponse à un seul changement spontané d'un objet surveillé :

☒ informations de signalisation simple (M_SP_NA_1, M_SP_TA_1, M_SP_TB_1, M_PS_NA_1)

☒ informations de signalisation double (M_DP_NA_1, M_DP_TA_1, M_DP_TB_1)

☒ informations de position d'étape (M_ST_NA_1, M_ST_TA_1, M_ST_TB_1)

☒ chaîne de 32 bits (M_BO_NA_1, M_BO_TA_1, M_BO_TB_1) si définie pour un projet spécifique.

☒ valeur mesurée, valeur normalisée (M_ME_NA_1, M_ME_TA_1, M_ME_ND_1, M_ME_TD_1)

☒ valeur mesurée, valeur mise à l'échelle (M_ME_NB_1, M_ME_TB_1, M_ME_TE_1)

☒ valeur mesurée, nombre à virgule flottante court (M_ME_NC_1, M_ME_TC_1, M_ME_TF_1)

Interrogation de station

Pour les paramètres spécifiques à la station, marquez chaque fonction de manière appropriée (X, R, B) :

☒ global

☒ groupe 1

☒ groupe 7

☒ groupe 13

☒ groupe 2

☒ groupe 8

☒ groupe 14

☒ groupe 3

☒ groupe 9

☒ groupe 15

☒ groupe 4

☒ groupe 10

☒ groupe 16

☒ groupe 5

☒ groupe 11

☒ groupe 6

☒ groupe 12

NOTE: Affichez les adresses d'objet d'information affectées à chaque groupe dans un tableau distinct.

Synchronisation d'horloge

Pour les paramètres spécifiques à la station, marquez chaque fonction de manière appropriée (X, R, B) :

☒ synchronisation de l'horloge

☒ jour de la semaine utilisé

☒ RES1, GEN (horodatage remplacé / non remplacé) utilisé

☒ bit SU (été) utilisé

Transmission de commande

☒ transmission de commande directe

☒ transmission de commande de consigne directe

☒ sélectionner et exécuter une commande

☒ sélectionner et exécuter une commande de consigne

☒ C_SE ACTTERM utilisé

☒ aucune définition supplémentaire

☒	durée d'impulsion courte (déterminée par un paramètre système dans le serveur)
☒	durée d'impulsion longue (déterminée par un paramètre système dans le serveur)
☒	sortie persistante
☐	supervision du délai maximum, dans le sens de contrôle, des commandes et des commandes de consigne

Configurable délai maximum admissible des commandes et des commandes de consigne

Transmission des totaux intégrés

Pour les paramètres spécifiques à la station ou à l'objet, marquez chaque fonction de manière appropriée (X, R, B) :

☒	Mode A : gel local avec transmission spontanée
☒	Mode B : gel local avec interrogation de compteur
☒	Mode C : geler et transmettre par des commandes d'interrogation de compteur
☐	Mode D : gel par commande d'interrogation de compteur, valeurs gelées signalées de façon spontanée
☒	lecture de compteur
☒	gel de compteur sans réinitialisation
☒	gel de compteur avec réinitialisation
☒	réinitialisation de compteur
☒	compteur de requêtes général
☒	compteur de requêtes groupe 1
☒	compteur de requêtes groupe 2
☒	compteur de requêtes groupe 3
☒	compteur de requêtes groupe 4

Chargement des paramètres

Pour les paramètres spécifiques à un objet, marquez chaque fonction de manière appropriée (X, R, B) :

☒	valeur de seuil
☐	facteur de lissage
☒	limite basse pour la transmission de valeur mesurée
☒	limite haute pour la transmission de valeur mesurée

Activation des paramètres

Pour les paramètres spécifiques à un objet, marquez chaque fonction de manière appropriée (X, R, B) :

☒	activer/désactiver la transmission périodique ou cyclique persistante de l'objet adressé

Procédure de test

Pour les paramètres spécifiques à la station, marquez chaque fonction de manière appropriée (X, R, B) :

☒	procédure de test

Transfert de fichier

Pour les paramètres spécifiques à la station, marquez X lorsque la fonction est utilisée.

Transfert de fichiers dans le sens de la surveillance :

☐	fichier transparent
☐	transmission de données de perturbation de l'équipement de protection

- ☐ transmission de séquences d'événements
- ☐ transmission de séquences de valeurs analogiques enregistrées

Transfert de fichiers dans le sens du contrôle :

- ☐ fichier transparent

Scrutation en arrière-plan

Pour les paramètres spécifiques à la station, marquez chaque fonction de manière appropriée (X, R, B) :

- ☒ scrutation en arrière-plan

Définition des timeouts

Paramètre	Valeur par défaut	Remarques	Valeur sélectionnée
t_0	30 s	délai d'établissement de la connexion	configurable
t_1	15 s	délai d'envoi ou de test des APDU	configurable
t_2	10 s	délai d'acquiescement en cas d'absence de messages de données $t_2 < t_1$	configurable
t_3	20 s	délai d'envoi des trames de test en cas d'état d'inactivité prolongé	configurable

Plages :

- plage maximale pour les timeouts t_0 à t_2 : 1 à 255 s (précision : 1 s)
- plage maximale pour le timeout t_3 : 1 à 48 heures (résolution : 1 s)
- des délais longs peuvent être nécessaires pour t_3 dans des cas particuliers où des liaisons par satellite ou des connexions par réseau commuté sont utilisées (par exemple, pour établir une connexion et collecter des valeurs seulement une fois par jour ou par semaine)

Nombre maximal d'APDU de format I en attente (k) et dernières APDU acquittées (w)

Paramètre	Valeur par défaut	Remarques	Valeur sélectionnée
k	12 APDU	différence maximale entre le nombre de la séquence reçue et le nombre à envoyer	configurable
w	8 APDU	dernier accusé de réception après réception de w APDU de format I	configurable

Plage de valeurs :

- k : 1 à 12 APDU (précision : 1 APDU)
- w : 1 à 32767 APDU (précision : 1 APDU) (w ne doit pas dépasser les deux tiers de k).

NOTE: Dans la plupart des cas, la valeur de w ne dépasse pas les deux tiers de k .

Numéro de port

Paramètre	Valeur	Remarques
<i>Portnumber</i>	2404	configurable

Connexions redondantes

- ☒ 4 nombre N de connexions de groupe redondant utilisées

Suite RFC 2200

RFC 2200 est une norme Internet officielle qui décrit l'état de normalisation des protocoles utilisés sur Internet conformément aux spécifications du IAB (Internet Architecture Board). Elle offre un large éventail de normes actuellement utilisées sur Internet. Les documents RFC 2200 appropriés définis dans cette norme pour des projets donnés doivent être sélectionnés par l'utilisateur de la norme.

- ☒ Ethernet 802.3

-
- ☐ interface série X.21
 - ☐ autre sélection de RFC 2200

Serveur IEC60870-5-101 et profils d'équipement client

Introduction

Cette section contient des informations permettant de configurer les équipements d'autres fournisseurs à des fins d'interopérabilité. Elle s'appuie sur le modèle d'interopérabilité de la norme IEC60870-5-101 (*IEC60870-5-101:2003, Clause 8*).

Cette norme d'accompagnement présente des ensembles de paramètres et de variantes parmi lesquels vous devez sélectionner des sous-ensembles pour mettre en oeuvre des systèmes de téléconduite particuliers. Certaines valeurs de paramètres, notamment le nombre d'octets dans l'adresse commune des ASDU, représentent des variantes qui s'excluent mutuellement. Autrement dit, une seule valeur des paramètres définis est admise par système. D'autres paramètres, tels que l'ensemble répertorié d'informations de processus différentes dans les directions de commande et de surveillance, permettent de spécifier l'ensemble complet ou des sous-ensembles en fonction des besoins des applications. Cette clause récapitule les paramètres des clauses précédentes afin de faciliter la sélection pour une application donnée. Si un système est composé d'équipements de différents fabricants, il est nécessaire que tous les partenaires s'accordent sur les paramètres sélectionnés.

Les paramètres sélectionnés doivent être marqués dans les cases blanches :

- ☐ La fonction ou l'ASDU n'est pas utilisée.
- ☒ La fonction ou l'ASDU est utilisée en standard (par défaut).
- ☒ La fonction ou l'ASDU est utilisée en mode inverse.
- ☒ La fonction ou l'ASDU est utilisée en modes standard et inverse.

La sélection possible (*vide*, **X**, **R** ou **B**) est spécifiée pour chaque clause ou paramètre spécifique.

NOTE: En outre, la spécification complète d'un système peut nécessiter la sélection individuelle de certains paramètres pour certaines parties du système, par exemple des facteurs d'échelle pour des valeurs mesurées adressables individuellement.

Système ou équipement

Les paramètres spécifiques au système indiquent la définition d'un système ou d'un équipement en remplissant ces cases avec un **X** :

- ☐ définition du système
- ☒ définition de la station de contrôle (client)
- ☒ définition de la station de contrôle (serveur)

Configuration réseau

Pour les paramètres propres au réseau, toutes les configurations implémentées sont marquées d'un **X** :

☒ point à point	☐ ligne de partage multipoint
☒ point à point multiple	☐ multipoint étoile

Couche physique

Pour les paramètres propres au réseau, toutes les interfaces et tous les débits de données implémentés sont marqués d'un X :

Vitesse de transmission (sens du contrôle) :

Circuit d'échange déséquilibré V.24/V.28 standard	Circuit d'échange déséquilibré V.24/V.28 recommandé si >1200 bits/s	Circuit d'échange équilibré V.24/V.27	
☐ 100 bits/s	☒ 2400 bits/s	☒ 2400 bits/s	☒ 57600 bits/s
☐ 200 bits/s	☒ 4800 bits/s	☒ 4800 bits/s	☒ 115200 bits/s
☒ 300 bits/s	☒ 9600 bits/s	☒ 9600 bits/s	
☒ 600 bits/s		☒ 19200 bits/s	
☒ 1200 bits/s		☒ 38400 bits/s	

Vitesse de transmission (sens de surveillance) :

Circuit d'échange déséquilibré V.24/V.28 standard	Circuit d'échange déséquilibré V.24/V.28 recommandé si >1200 bits/s	Circuit d'échange équilibré V.24/V.27	
☐ 100 bits/s	☒ 2400 bits/s	☒ 2400 bits/s	☒ 57600 bits/s
☐ 200 bits/s	☒ 4800 bits/s	☒ 4800 bits/s	☒ 115200 bits/s
☒ 300 bits/s	☒ 9600 bits/s	☒ 9600 bits/s	
☒ 600 bits/s		☒ 19200 bits/s	
☒ 1200 bits/s		☒ 38400 bits/s	

Couche de liaison

Pour les paramètres propres au réseau, toutes les options implémentées sont marquées d'un X. Indiquez la longueur de trame maximum. Si une affectation non standard de messages de classe 2 est implémentée pour une transmission non équilibrée, indiquez l'ID de type et le COT de tous les messages affectés à la classe 2.

Le format de trame FT 1.2, le caractère unique 1 et l'intervalle de temporisation fixe sont utilisés de manière mutuellement exclusive dans cette norme d'accompagnement.

Procédure de transmission de liaison

- ☒ transmission équilibrée
- ☒ transmission non équilibrée

Longueur de trame

longueur maximale L (sens du contrôle)

longueur maximale L (sens de surveillance)

temps pendant lequel les répétitions sont autorisées (Trp) ou nombre de répétitions

Champ d'adresse de la liaison

☐ non présent (transmission équilibrée uniquement)

☒ un octet

☒ deux octets

☐ structuré

☐ non structuré

Lors de l'utilisation d'une couche de liaison déséquilibrée, ces types ASDU sont renvoyés dans des messages de classe 2 (priorité faible) avec les causes de transmission indiquées (X).

☒ Affectation standard des ASDU aux messages de classe 2 :

Identification de type	Cause des transmissions
9, 11, 13, 21	<1>

☒ Affectation spéciale des ASDU aux messages de classe 2 :

Identification de type	Cause des transmissions
1, 3, 5, 7, 9, 11, 13	<2>

NOTE: En réponse à une interrogation de classe 2, une station contrôlée peut répondre avec des données de classe 1 lorsqu'aucune donnée de classe 2 n'est disponible.

Couche application

Mode de transmission des données d'application

Le mode 1 (octet de poids faible en premier), tel que défini dans la section 4.10 de la norme IEC60870-5-4, est utilisé de manière exclusive dans cette norme d'accompagnement.

Adresse commune d'ASDU

Pour les paramètres spécifiques au système, toutes les configurations implémentées sont marquées d'un X :

☒ un octet

☒ deux octets

Adresse d'objet d'information

Pour les paramètres spécifiques au système, toutes les configurations implémentées sont marquées d'un X :

☒ un octet	☐ structuré
☒ deux octets	☐ non structuré
☒ trois octets	

Cause de la transmission

Pour les paramètres spécifiques au système, toutes les configurations implémentées sont marquées d'un X :

☒ un octet	☒ deux octets (avec adresse de l'émetteur)

NOTE: Si elle n'est pas utilisée, l'adresse de l'émetteur est définie sur 0.

Sélection d'ASDU standard**Informations de processus dans le sens de surveillance**

Pour les paramètres spécifiques à la station, marquez chaque ID de type en conséquence :

- **X** : Le paramètre est utilisé uniquement dans le sens standard.
- **R** : Le paramètre est utilisé uniquement dans le sens inverse.
- **B** : Le paramètre est utilisé dans les deux sens.

☒	<1>	:= informations de signalisation simple	M_SP_NA_1
☒	<2>	:= informations de signalisation simple avec horodatage	M_SP_TA_1
☒	<3>	:= informations de de signalisation double	M_DP_NA_1
☒	<4>	:= informations de position d'étape	M_ST_NA_1
☒	<5>	:= chaîne de 32 bits	M_BO_NA_1
☒	<6>	:= informations de position d'étape avec horodatage	M_ST_TA_1
☒	<7>	:= chaîne de 32 bits	M_BO_NA_1
☒	<8>	:= chaîne de 32 bits avec horodatage	M_BO_TA_1
☒	<9>	:= valeur mesurée, valeur normalisée	M_ME_NA_1
☒	<10>	:= valeur mesurée, valeur normalisée avec horodatage	M_ME_TA_1
☒	<11>	:= valeur mesurée, valeur mise à l'échelle	M_ME_NB_1
☒	<12>	:= valeur mesurée, valeur mise à l'échelle avec horodatage	M_ME_TB_1
☒	<13>	:= valeur mesurée, valeur à virgule flottante courte	M_ME_NC_1
☒	<14>	:= valeur mesurée, valeur à virgule flottante courte avec horodatage	M_ME_TC_1
☒	<15>	:= totaux intégrés	M_IT_NA_1
☒	<16>	:= totaux intégrés avec horodatage	M_IT_TA_1
☐	<17>	:= événement d'équipement de protection avec horodatage	M_EP_TA_1
☐	<18>	:= paquet d'événements de démarrage d'équipement de protection avec horodatage	M_EP_TB_1

☐	<19>	:=	paquet de sortie de circuit d'informations d'équipement de protection avec horodatage	M_EP_TC_1
☐	<20>	:=	paquet d'informations de signalisation simple avec détection de changement d'état	M_PS_NA_1
☐	<21>	:=	valeur mesurée, valeur normalisée sans descripteur de qualité	M_ME_ND_1
☒	<30>	:=	informations de signalisation simple avec horodatage CP56Time2a	M_SP_TB_1
☒	<31>	:=	informations de signalisation double horodatage CP56Time2a	M_DP_TB_1
☒	<32>	:=	informations de position d'étape avec horodatage CP56Time2a	M_ST_TB_1
☒	<33>	:=	chaîne de 32 bits avec horodatage CP56Time2a	M_BO_TB_1
☒	<34>	:=	valeur mesurée, valeur normalisée avec horodatage CP56Time2a	M_ME_TD_1
☒	<35>	:=	valeur mesurée, valeur mise à l'échelle avec horodatage CP56Time2a	M_ME_TE_1
☒	<36>	:=	valeur mesurée, valeur à virgule flottante courte avec horodatage CP56Time2a	M_ME_TF_1
☒	<37>	:=	totaux intégrés avec horodatage CP56Time2a	M_IT_TB_1
☐	<38>	:=	événement d'équipement de protection avec horodatage CP56Time2a	M_EP_TD_1
☐	<39>	:=	paquet d'événements de démarrage d'équipement de protection avec horodatage CP56Time2a	M_EP_TE_1
☐	<40>	:=	paquet d'informations de sortie de circuit d'équipement de protection avec horodatage CP56Time2a	M_EP_TF_1

Les ASDU associées à l'un de ces ensembles sont utilisées :

- <2>, <4>, <6>, <8>, <10>, <12>, <14>, <16>, <18>, <19>
- <30>...<40>

Informations de processus dans le sens du contrôle

Pour les paramètres spécifiques à la station, marquez chaque ID de type en conséquence :

- **X** : Le paramètre est utilisé uniquement dans le sens standard.
- **R** : Le paramètre est utilisé uniquement dans le sens inverse.
- **B** : Le paramètre est utilisé dans les deux sens.

☒	<45>	:=	commande simple	C_SC_NA_1
☒	<46>	:=	commande double	C_DC_NA_1
☒	<47>	:=	commande d'étape de régulation	C_RC_NA_1
☒	<48>	:=	commande de consigne, valeur normalisée	C_SE_NA_1
☒	<49>	:=	commande de consigne, valeur mise à l'échelle	C_SE_NB_1
☒	<50>	:=	commande de consigne, valeur à virgule flottante courte	C_SE_NC_1
☒	<51>	:=	chaîne de 32 bits	C_BO_NA_1

Informations système dans le sens de la surveillance

Marquez chaque paramètre spécifique à la station de manière appropriée (X, R, B) : M_EI_NA_1

☒ <70> := fin de l'initialisation

Informations système dans le sens du contrôle

Pour les paramètres spécifiques à la station, marquez chaque ID de type de manière appropriée (X, R, B) :

C_IC_NA_1

☒ <100> := commande d'interrogation

☒ <101> := commande d'interrogation de compteur

C_CI_NA_1

☒ <102> := commande de lecture

C_RD_NA_1

☒ <103> := commande de synchronisation d'horloge

C_CS_NA_1

☒ <105> := commande de réinitialisation de processus

C_RP_NA_1

☒ <107> := commande de test avec horodatage CP56Time2a

C_TS_TA_1

Paramètres dans le sens du contrôle

Pour les paramètres spécifiques à la station, marquez chaque ID de type de manière appropriée (X, R, B) :

☒ <110> := Il s'agit du paramètre de la valeur mesurée, valeur normalisée.

P_ME_NA_1

☒ <111> := Il s'agit du paramètre de la valeur mesurée, valeur mise à l'échelle.

P_ME_NB_1

☒ <112> := Il s'agit du paramètre de la valeur mesurée, valeur à virgule flottante courte.

P_ME_NC_1

☒ <113> := Il s'agit de l'activation du paramètre.

P_AC_NA_1

Transfert de fichier

Pour les paramètres spécifiques à la station, marquez chaque ID de type de manière appropriée (X, R, B) :

☐ <120> := fichier prêt

☐ <121> := section prête

F_SR_NA_1

☐ <122> := appel de répertoire, sélection de fichier, appel de fichier, appel de section

F_SC_NA_1

☐ <123> := dernière section, dernier segment

F_LS_NA_1

☐ <124> := accusé de réception de fichier, accusé de réception de section

F_AF_NA_1

☐ <125> := segment

F_SG_NA_1

☐ <126> := répertoire {vide ou X, disponible uniquement dans le sens de la surveillance (standard)}

F_DR_TA_1

Affectations des identifiants de type et causes d'émission (paramètres spécifiques à la station) :

- (grisé) : Ces cases ne sont pas nécessaires.
- (vide) : La fonction ou l'ASDU n'est pas utilisée.

Marquez correctement chaque combinaison type d'identifiant/cause d'émission (X, R, B) :

Identification de type		Cause d'émission																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 ... 36	37 ... 41	44	45	46	47
<1>	M_SP_NA_1		X	X		X									X					
<2>	M_SP_TA_1			X		X														
<3>	M_DP_NA_1		X	X		X									X					
<4>	M_DP_TA_1			X		X														
<5>	M_ST_NA_1		X	X		X									X					
<6>	M_ST_TA_1			X		X														
<7>	M_BO_NA_1		X	X		X									X					
<8>	M_BO_TA_1			X		X														
<9>	M_ME_NA_1	X	X	X		X									X					
<10>	M_ME_TA_1			X		X														
<11>	M_ME_NB_1	X	X	X		X									X					
<12>	M_ME_TB_1			X		X														
<13>	M_ME_NC_1	X	X	X		X									X					
<14>	M_ME_TC_1			X		X														
<15>	M_IT_NA_1			X												X				
<16>	M_IT_TA_1			X																
<17>	M_EP_TA_1																			
<18>	M_EP_TB_1																			
<19>	M_EP_TC_1																			
<20>	M_PS_NA_1																			
<21>	M_ME_ND_1																			
<30>	M_SP_TB_1			X		X														
<31>	M_DP_TB_1			X		X														
<32>	M_ST_TB_1			X		X														
<33>	M_BO_TB_1			X		X														
<34>	M_ME_TD_1			X		X														
<35>	M_ME_TE_1			X		X														
<36>	M_ME_TF_1			X		X														
<37>	M_IT_TB_1			X																
<38>	M_EP_TD_1																			
<39>	M_EP_TE_1																			
<40>	M_EP_TF_1																			
<45>	C_SC_NA_1						X	X	X	X	X						X	X	X	X
<46>	C_DC_NA_1						X	X	X	X	X						X	X	X	X
<47>	C_RC_NA_1						X	X	X	X	X						X	X	X	X
<48>	C_SE_NA_1						X	X	X	X	X						X	X	X	X
<49>	C_SE_NB_1						X	X	X	X	X						X	X	X	X
<50>	C_SE_NC_1						X	X	X	X	X						X	X	X	X
<51>	C_BO_NA_1						X	X			X						X	X	X	X
<70>	M_EI_NA_1				X															
<100>	C_IC_NA_1						X	X	X	X	X						X	X	X	X
<101>	C_CI_NA_1						X	X			X						X	X	X	X
<102>	C_RD_NA_1					X											X	X	X	X
<103>	C_CS_NA_1						X	X									X	X	X	X

Identification de type		Cause d'émission																		
<104>	C_TS_NA_1						X	X									X	X	X	X
<105>	C_RP_NA_1						X	X									X	X	X	X
<106>	C_CD_NA_1						X	X									X	X	X	X
<110>	P_ME_NA_1						X	X							X		X	X	X	X
<111>	P_ME_NB_1						X	X							X		X	X	X	X
<112>	P_ME_NC_1						X	X							X		X	X	X	X
<113>	P_AC_NA_1						X	X	X	X							X	X	X	X
<120>	F_FR_NA_1																			
<121>	F_SR_NA_1																			
<122>	F_SC_NA_1																			
<123>	F_LS_NA_1																			
<124>	F_AF_NA_1																			
<125>	F_SG_NA_1																			
<126>	F_DR_TA_1																			
	Voir la remarque (ci-dessous).																			

NOTE: Vide ou X uniquement.

Fonctions élémentaires d'application

Marquez chaque fonction d'application élémentaire en conséquence :

- **X** : Le paramètre est utilisé uniquement dans le sens standard.
- **R** : Le paramètre est utilisé uniquement dans le sens inverse.
- **B** : Le paramètre est utilisé dans les deux sens.
- (*vide*) : La fonction n'est pas disponible dans cette norme d'accompagnement.

Initialisation de station

Pour les paramètres propres à la station, toutes les fonctions implémentées sont marquées d'un X :

☒ initialisation à distance

Transmission cyclique de données

Pour les paramètres spécifiques à la station, marquez chaque fonction de manière appropriée (X, R, B) :

☒ transmission cyclique de données

Procédure de lecture

Pour les paramètres spécifiques à la station, marquez chaque fonction de manière appropriée (X, R, B) :

☒ procédure de lecture

Transmission spontanée

Pour les paramètres spécifiques à la station, marquez chaque fonction de manière appropriée (X, R, B) :

☒ transmission spontanée

Transmission double d'objets d'information avec cause de transmission spontanée

Pour les paramètres spécifiques à la station, marquez chaque fonction d'un X lorsqu'un ID de type sans heure et un ID de type correspondant avec heure sont tous les deux émis en réponse à un seul changement spontané d'un objet surveillé :

- ☐ informations de signalisation simple (M_SP_NA_1, M_SP_TA_1, M_SP_TB_1, M_PS_NA_1)
- ☐ informations de signalisation double (M_DP_NA_1, M_DP_TA_1, M_DP_TB_1)
- ☐ informations de position d'étape (M_ST_NA_1, M_ST_TA_1, M_ST_TB_1)
- ☐ chaîne de 32 bits (M_BO_NA_1, M_BO_TA_1, M_BO_TB_1) si défini pour un projet spécifique.
- ☐ valeur mesurée, valeur normalisée (M_ME_NA_1, M_ME_TA_1, M_ME_ND_1, M_ME_TD_1)
- ☐ valeur mesurée, valeur mise à l'échelle (M_ME_NB_1, M_ME_TB_1, M_ME_TE_1)
- ☐ valeur mesurée, nombre à virgule flottante court (M_ME_NC_1, M_ME_TC_1, M_ME_TF_1)

Interrogation de station

Pour les paramètres spécifiques à la station, marquez chaque fonction de manière appropriée (X, R, B) :

☒ global		
☒ groupe 1	☒ groupe 7	☒ groupe 13
☒ groupe 2	☒ groupe 8	☒ groupe 14
☒ groupe 3	☒ groupe 9	☒ groupe 15
☒ groupe 4	☒ groupe 10	☒ groupe 16
☒ groupe 5	☒ groupe 11	
☒ groupe 6	☒ groupe 12	

NOTE: Affichez les adresses d'objet d'information affectées à chaque groupe dans un tableau distinct.

Synchronisation d'horloge

Pour les paramètres spécifiques à la station, marquez chaque fonction de manière appropriée (X, R, B) :

- ☒ synchronisation d'horloge
- ☒ jour de la semaine utilisé
- ☒ RES1, GEN (horodatage remplacé / non remplacé) utilisé
- ☒ Bit SU (été) utilisé

Transmission de commande

- ☒ transmission de commande directe
- ☒ transmission de commande de consigne directe
- ☒ sélectionner et exécuter une commande
- ☒ sélectionner et exécuter une commande de consigne
- ☒ C_SE ACTTERM utilisé
- ☒ aucune définition supplémentaire
- ☒ durée d'impulsion courte (déterminée par un paramètre système dans le serveur)
- ☒ durée d'impulsion longue (déterminée par un paramètre système dans le serveur)
- ☒ sortie persistante

Transmission des totaux intégrés

Pour les paramètres spécifiques à la station ou à l'objet, marquez chaque fonction de manière appropriée (X, R, B) :

- ☒ Mode A : gel local avec transmission spontanée

-
- ☒ Mode B : gel local avec interrogation de compteur
 - ☒ Mode C : geler et transmettre par des commandes d'interrogation de compteur
 - ☐ Mode D : gel par commande d'interrogation de compteur, valeurs gelées signalées de façon spontanée
 - ☒ lecture de compteur
 - ☒ gel de compteur sans réinitialisation
 - ☒ gel de compteur avec réinitialisation
 - ☒ réinitialisation de compteur
 - ☒ compteur de requêtes général
 - ☒ compteur de requêtes groupe 1
 - ☒ compteur de requêtes groupe 2
 - ☒ compteur de requêtes groupe 3
 - ☒ compteur de requêtes groupe 4

Chargement de paramètres

Pour les paramètres spécifiques à un objet, marquez chaque fonction de manière appropriée (X, R, B) :

- ☒ valeur de seuil
- ☐ facteur de lissage
- ☒ limite basse pour la transmission de valeur mesurée
- ☒ limite haute pour la transmission de valeur mesurée

Activation de paramètres

Pour les paramètres spécifiques à un objet, marquez chaque fonction de manière appropriée (X, R, B) :

- ☒ activer/désactiver la transmission périodique ou cyclique persistante de l'objet adressé

Procédure de test

Pour les paramètres spécifiques à la station, marquez chaque fonction de manière appropriée (X, R, B) :

- ☒ procédure de test

Transfert de fichier

Pour les paramètres spécifiques à la station, marquez X lorsque la fonction est utilisée.

Transfert de fichiers dans le sens de la surveillance :

- ☐ fichier transparent
- ☐ transmission de données de perturbation de l'équipement de protection
- ☐ transmission de séquences d'événements
- ☐ transmission de séquences de valeurs analogiques enregistrées

Transfert de fichiers dans le sens du contrôle :

- ☐ fichier transparent

Scrutation en arrière-plan

Pour les paramètres spécifiques à la station, marquez chaque fonction de manière appropriée (X, R, B) :

- ☒ scrutation en arrière-plan

Acquisition de données de transmission

Pour les paramètres spécifiques à la station, marquez chaque fonction de manière appropriée (X, R, B) :

- ☒ acquisition de délai de transmission

Migration de projet

Introduction

Respectez les consignes de cette section lorsque vous migrez un fichier de configuration depuis un module BMXNOR0200H d'un réseau M340 vers un module BMENOR2200H d'un réseau M580.

Migration de fichiers XML

Introduction

Vous pouvez migrer le fichier de configuration d'un module BMXNOR0200H vers un module BMENOR2200H.

NOTE: Consultez les instructions générales pour exporter et importer .xml des fichiers avec le DTM Control Expert.

Migration de projet - Cas d'utilisation

Migrer le fichier de configuration d'un module BMXNOR0200H vers un module BMENOR2200H :

Etape	Description
1	Exportez le fichier de configuration .xml à partir d'un module BMXNOR0200H dans une application de contrôleur PAC M340.
2	Importez le fichier de configuration .xml vers un module BMENOR2200H dans une application de contrôleur PAC M580.

NOTE: Toutes les adresses localisées sont perdues après l'importation de fichiers .xml à partir du module BMENOR2200H. Le type et la longueur du nom sont modifiés selon le nouveau format.

Migration des types de données DNP3

Introduction

Lorsque vous migrez une application RTU d'un module BMXNOR0200H vers un module BMENOR2200H, certains types de données et noms de variables sont convertis.

Tableaux ci-après :

- Serveur - Migration des types de données DNP3 de point RTU
- Client - Migration des types de données DNP3 de point RTU

Appliquez ces informations lorsque vous configurez les communications DNP3 dans le DTM du BMENOR2200H.

Serveur - Migration des types de données DNP3 de point RTU

Les types de données qui changent lors de la migration sont indiqués en **red** :

Type d'objet (nom de variable par défaut)	Élément d'objet	BMXNOR0200H		BMENOR2200H	
		Paramètre	Type de données	Paramètre	Type de données
Binary Input (BI_Px)	Valeur	.value	WORD	.value	BYTE
	Indicateur	.flags	WORD	.flags	BYTE
	Heure	.timestamp	CP56	.Timestamp	CP56
Double_Input (DI_Px)	Valeur	.value	WORD	.value	BYTE
	Indicateur	.flags	WORD	.flags	BYTE
	Heure	.timestamp	CP56	.Timestamp	CP56
Binary_Output (BO_Px)	Valeur	.value	WORD	.value	BYTE
					INT (mode Synchronisation à la demande uniquement)
Binary_Counter (BCnt_Px)	Valeur - 16 bits	.value	DWORD	.value	INT
	Valeur - 32 bits	.value	DWORD	.value	DINT
	Indicateur	.flags	DWORD	.flags	BYTE
	Heure	.timestamp	CP56	.Timestamp	CP56
Analog_Input (AI_Px)	Valeur - 16 bits	.value	INT	.Value	INT
	Valeur - 32 bits	.value	DINT	.Value	DINT
	Valeur - Courte	.value	REAL	.Value	REAL
	Indicateur - 16 bits	.flags	WORD	.Flags	BYTE
	Indicateur - 32 bits/Court	.flags	DWORD	.Flags	BYTE
	Heure	.timestamp	CP56	.Timestamp	CP56
Analog_Output (AO_Px)	Valeur - 16 bits	.value	INT	.Value	INT
	Valeur - 32 bits	.value	DINT	.Value	DINT
	Valeur - Courte	.value	REAL	.Value	REAL
Analog_Input_Deadband (AI_Px_Dband)	Valeur	.Value	DWORD	.Value	DWORD
Binary_Output_Flags (BO_Px_Flag)	—	— None Structure	WORD	.Flag	BYTE
Analog_Output_Flags	—	— None Structure	WORD	.Flag	BYTE

Type d'objet (nom de variable par défaut)	Élément d'objet	BMXNOR0200H		BMENOR2200H	
		Paramètre	Type de données	Paramètre	Type de données
(AO_Px_Flag)					
Gen_Event	—	.Command	WORD	.Command	BYTE
(GE_xxxx)	—	.Status	WORD	.Status	WORD
Clear_Event	—	.Command	WORD	.Command	BYTE
(CE_xxxx_CB)	—	.Status	WORD	.Status	WORD
Octet String		—	—	.Value	STRING
(Str_Px)					[0-255]

Client - Migration des types de données DNP3 de point RTU

Les types de données qui changent lors de la migration sont indiqués en **red** :

Type d'objet (nom de variable par défaut)	Élément d'objet	BMXNOR0200H		BMENOR2200H	
		Paramètre	Type de données	Paramètre	Type de données
Binary_Input (BI_Px)	Valeur	.value	WORD	.value	BYTE
	Indicateur	.flags	WORD	.flags	BYTE
	Heure	.timestamp	CP56	.Timestamp	CP56
Double_Input (DI_Px)	Valeur	.value	WORD	.value	BYTE
	Indicateur	.flags	WORD	.flags	BYTE
	Heure	.timestamp	CP56	.Timestamp	CP56
Binary_Output (BO_Px)	—	.value	WORD	.value	BYTE
	État de commande	.Status	WORD	.Status	WORD
Binary_Output_Status (BO_Px_Sts)	Valeur	.value	WORD	.value	BYTE
	Indicateur	.flags	WORD	.flags	BYTE
	Heure	.timestamp	CP56	.Timestamp	CP56
Octet String (Str_Px)		—	—	.Value	STRING
Write Octet String (WOctStr_I_Px) (Str_Px_Wrt)		—	—	.Value	STRING
		—	—	.Status	WORD
Binary_Counter (BCnt_Px)	Valeur - 16 bits	.value	DWORD	.counter	WORD
	Valeur - 32 bits	.value	DWORD	.counter	DWORD
	Indicateur - 16 bits/32 bits	.flags	DWORD	.flags	BYTE
	Heure	.timestamp	CP56	.timestamp	CP56
Frozen_Counter (FrozCnt_xxxx)	Valeur - 16 bits	.value	DWORD	.counter	WORD
	Valeur - 32 bits	.value	DWORD	.counter	DWORD
	Indicateur - 16 bits/32 bits	.flags	DWORD	.flags	BYTE
	Heure	.timestamp	CP56	.timestamp	CP56
Analog_Input (AI_Px)	Valeur - 16 bits	.value	INT	.Value	INT
	Valeur - 32 bits	.value	DINT	.Value	DINT
	Valeur - Courte	.value	REAL	.Value	REAL
	Indicateur - 16 bits	.flags	WORD	.Flags	BYTE

Type d'objet (nom de variable par défaut)	Élément d'objet	BMXNOR0200H		BMENOR2200H	
		Paramètre	Type de données	Paramètre	Type de données
	Indicateur - 32 bits/Court	.flags	DWORD	.Flags	BYTE
	Heure	.timestamp	CP56	.Timestamp	CP56
Analog_Input_Deadband (AI_Px_Dband)	Valeur - 16 bits	.value	WORD	.Value	WORD
	Valeur - 32 bits	.value	DWORD	.Value	DWORD
Analog_Input_Deadband_Control (AIDBCtrl_Px)	Valeur - 16 bits	.Value	WORD	.Value	WORD
	Valeur - 32 bits	.Value	DWORD	.Value	DWORD
	Valeur - Courte	.Value	REAL	.Value	REAL
	Etat de commande	.Status	WORD	.Status	WORD
	Etat de commande	.Status	DWORD	.Status	WORD
Analog_Output (AO_Px)	Valeur - 16 bits	.Value	INT	.Value	INT
	Valeur - 32 bits	.Value	DINT	.Value	DINT
	Valeur - courte	.Value	REAL	.Value	REAL
	Etat de commande	.Status	WORD	.Status	WORD
	Etat de commande	.Status	DWORD	.Status	WORD
Analog_Output_Status (AO_Px_Sts)	Valeur - 16 bits	.value	INT	.Value	INT
	Valeur - 32 bits	.value	DINT	.Value	DINT
	Valeur - courte	.value	REAL	.Value	REAL
	Indicateur - 16 bits	.flags	WORD	.Flags	BYTE
	Indicateur - 32 bits	.flags	DWORD	.Flags	BYTE
	Heure	.timestamp	CP56	.Timestamp	CP56
Read_Class (RC_xxxx)	—	.Value	WORD	.Value	BYTE
	Etat de commande	.Status	WORD	.Status	WORD
Freeze_Counter (FrezCnt_xxxx)	—	.Value	WORD	.Value	BYTE
	Etat de commande	.Status	WORD	.Status	WORD
Unsolicited_Class (UnsC_xxxx)	—	.Value	WORD	.Value	BYTE
	Etat de commande	.Status	WORD	.Status	WORD
Time_Sync (TS_xxxx)	—	.Value	WORD	.Value	BYTE
	Etat de commande	.Status	WORD	.Status	WORD
Restart (Rst_xxxx)	—	.Value	WORD	.Value	BYTE
	Etat de commande	.Status	WORD	.Status	WORD
Integrity_Poll (IP_xxxx)	—	.Value	WORD	.Value	BYTE
	Etat de commande	.Status	WORD	.Status	WORD
Read_Group (RG_xxxx)	—	.Value	WORD	.Value	BYTE
	Etat de commande	.Status	WORD	.Status	WORD
Connect Status		.Status	DWORD	Device_ State	BYTE

Migration des types de données IEC60870

Introduction

Lorsque vous migrez une application RTU d'un module BMXNOR0200H vers un module BMENOR2200H, certains types de données et noms de variables sont convertis.

Tableaux ci-après :

- Serveur - Migration des types de données IEC60870-5-104 de point RTU
- Client - Migration des types de données IEC60870-5-104 de point RTU

Appliquez ces informations lorsque vous configurez les communications IEC60870-5-104 dans le module BMENOR2200H.

Client - Migration des types de données IEC60870 de point RTU

Types de données de point RTU côté client pouvant changer lors de la migration :

Type d'objet	Type de registre CPU	Type de données	Nom du paramètre	Type de données dans BMXNOR0200	Nom du paramètre dans BMENOR2200H	Type de données dans BMENOR2200H
M_SP	%M	Valeur	.value	WORD	.value	BYTE
	%MW	Indicateur	.quality	WORD	.flags	BYTE
	Non localisée	Heure	.timestamp	CP56	.timestamp	CP56
M_DP	%MW	Valeur	.value	WORD	.value	BYTE
	Non localisée	Indicateur	.quality	WORD	.flags	BYTE
		Heure	.timestamp	CP56	.timestamp	CP56
M_ST	%MW	Valeur	.value	WORD	.value	BYTE
	Non localisée	Indicateur	.quality	WORD	.flags	BYTE
		Heure	.timestamp	CP56	.timestamp	CP56
M_BO	%MW	Valeur	.value	DWORD	.value	DWORD
	Non localisée	Indicateur	.quality	DWORD	.flags	BYTE
		Heure	.timestamp	CP56	.timestamp	CP56
M_ME_A	%MW	Valeur	.value	INT	.value	INT
	Non localisée	Indicateur	.quality	WORD	.flags	BYTE
		Heure	.timestamp	CP56	.timestamp	CP56
M_ME_B	%MW	Valeur	.value	INT	.value	INT
	Non localisée	Indicateur	.quality	WORD	.flags	BYTE
		Heure	.timestamp	CP56	.timestamp	CP56
M_ME_C	%MW	Valeur	.value	REAL	.value	REAL
	Non localisée	Indicateur	.quality	DWORD	.flags	BYTE
		Heure	.timestamp	CP56	.timestamp	CP56
M_IT	%MW	Valeur	.value	DINT	.value	DINT
	Non localisée	Indicateur	.quality	DWORD	.flags	BYTE
		Heure	.timestamp	CP56	.timestamp	CP56
C_SC	%MW	Valeur	.value	WORD	.value	BYTE
		Indicateur	.status	WORD	.status	BYTE

Type d'objet	Type de registre CPU	Type de données	Nom du paramètre	Type de données dans BMXNOR0200	Nom du paramètre dans BMENOR2200H	Type de données dans BMENOR2200H
C_DC	%MW		.value	WORD	.value	BYTE
			.status	WORD	.status	WORD
C_RC	%MW		.value	WORD	.value	BYTE
			.status	WORD	.status	WORD
C_SE_A	%MW		.value	INT	.value	INT
			.status	WORD	.status	WORD
C_SE_B	%MW		.value	INT	.value	INT
			.status	WORD	.status	WORD
C_SE_C	%MW		.value	REAL	.value	REAL
			.status	DWORD	.status	WORD
C_BO	%MW		.value	DWORD	.value	DWORD
			.status	DWORD	.status	WORD
C_IC	%MW		.value	WORD	.value	BYTE
			.status	WORD	.status	WORD
C_CI	%MW		.value	WORD	.value	BYTE
			.status	WORD	.status	WORD
C_RD	%MW		.value	WORD	.value	BYTE
			.status	WORD	.status	WORD
C_CS	%MW		.value	WORD	.value	BYTE
			.status	WORD	.status	WORD
C_TS	%MW		.value	WORD	.value	BYTE
			.status	WORD	.status	WORD
C_RP	%MW		.value	WORD	.value	BYTE
			.status	WORD	.status	WORD
P_ME_A	%MW		.value	WORD	.value	INT
			.status	WORD	.status	WORD
P_ME_B	%MW		.value	WORD	.value	INT
			.status	WORD	.status	WORD
P_ME_C	%MW		.value	REAL	.value	REAL
			.status	DWORD	.status	WORD
P_AC	%MW		.value	WORD	.value	BYTE
			.status	WORD	.status	WORD
M_IT_D			.value0	INT	.value0	INT
			.value1	INT	.value1	INT
			.value2	INT	.value2	INT
			.value3	INT	.value3	INT
			.flag	BYTE	.flags	BYTE
			.timestamp	CP56	.timestamp	CP56

NOTE: Lorsque le module reçoit une commande C_RD, il répond à l'objet d'information avec l'adresse IOA (adresse d'objet d'information) demandée. Lorsque plusieurs points de données ont la même IOA, le module renvoie le premier objet d'information dans l'ordre de priorité suivant : M_SP, M_DP, M_ST, M_BO, M_ME_A, M_ME_B, M_ME_C, P_ME_A, P_ME_B, P_ME_C, CUSTOM_M_IT_D. Tenez compte de ces points lorsque vous configurez les communications IEC60870-5-104 côté serveur.

Serveur - Migration des types de données IEC60870 de point RTU

Types de données de point RTU côté serveur qui peuvent changer lors de la migration :

Type d'objet	Type de registre CPU	Type de données	Nom du paramètre	Type de données dans BMXNOR0200	Nom du paramètre dans BMENOR2200H	Type de données dans BMENOR2200H
M_SP	%M	Valeur	.value	WORD	.value	BYTE
	%M	Indicateur	.quality	WORD	.flags	BYTE
	%S	Heure	.timestamp	CP56	.timestamp	CP56
	Non localisée					
M_DP	%MW	Valeur	.value	WORD	.value	BYTE
	Non localisée	Indicateur	.quality	WORD	.flags	BYTE
		Heure	.timestamp	CP56	.timestamp	CP56
M_ST	%MW	Valeur	.value	WORD	.value	BYTE
	Non localisée	Indicateur	.quality	WORD	.flags	BYTE
		Heure	.timestamp	CP56	.timestamp	CP56
M_BO	%MW	Valeur	.value	DWORD	.value	DWORD
	Non localisée	Indicateur	.quality	DWORD	.flags	BYTE
		Heure	.timestamp	CP56	.timestamp	CP56
M_ME_A	%MW	Valeur	.value	INT	.value	INT
	%SW	Indicateur	.quality	WORD	.Flags	BYTE
	Non localisée	Heure	.timestamp	CP56	.timestamp	CP56
M_ME_B	%MW	Valeur	.value	INT	.value	INT
	Non localisée	Indicateur	.quality	WORD	.Flags	BYTE
		Heure	.timestamp	CP56	.timestamp	CP56
M_ME_C	%MW	Valeur	.value	REAL	.value	REAL
	Non localisée	Indicateur	.quality	DWORD	.Flags	BYTE
		Heure	.timestamp	CP56	.timestamp	CP56
M_IT	%MW	Valeur	.value	DINT	.value	DINT
	Non localisée	Heure	.timestamp	CP56	.timestamp	CP56
C_SC	%MW %M Non localisée	—	.value	WORD	.value	BYTE
C_DC	%MW Non localisée	Valeur	.value	WORD	.value	BYTE
C_RC	%MW Non localisée	Valeur	.value	WORD	.value	BYTE
C_SE_A	%MW Non localisée	Valeur	.value	INT	.value	INT
C_SE_B	%MW Non localisée	Valeur	.value	INT	.value	INT
C_SE_C	%MW Non localisée	Valeur	.value	REAL	.value	REAL
C_BO	%MW Non localisée	Valeur	.value	DWORD	.value	DWORD

Type d'objet	Type de registre CPU	Type de données	Nom du paramètre	Type de données dans BMXNOR0200	Nom du paramètre dans BMENOR2200H	Type de données dans BMENOR2200H
P_ME_A	%MW Non localisée	Valeur	—	WORD	.value	INT
P_ME_B	%MW Non localisée	Valeur	—	WORD	.value	INT
P_ME_C	%MW Non localisée	Valeur	—	REAL	.value	REAL
P_AC	%MW Non localisée	Valeur	—	WORD	.value	BYTE
M_IT_D			.value0	INT	.value0	INT
			.value1	INT	.value1	INT
			.value2	INT	.value2	INT
			.value3	INT	.value3	INT
			.flag	BYTE	.flags	BYTE
			.timestamp	CP56	.timestamp	CP56
Effacer des événements	%MW	—	.cmd	WORD	.cmd	BYTE
			.status	WORD	.status	WORD
CUSTOM_CMD	%MW Non localisée	Gel cyclique (gel automatique)	Cmd	WORD	cmd	BYTE
			Etat	WORD	.status	WORD
		Gel déclenché (gel local)	Cmd	WORD	.cmd	BYTE
			Etat	WORD	.status	WORD
CMD_QUALITY	%MW Non localisée				.cmd	byte

Événements journalisés

Introduction

Pour plus d'informations sur les événements journalisés et les statistiques sécurisées concernant le module BMENOR2200H, vous pouvez vous reporter au chapitre *How to Help Secure the Architecture* dans le document *Modicon Controllers Platform - Cyber Security - Reference Manual*.

Codes de diagnostic Modbus

Mappage de données pour le code de fonction Modbus 3 avec ID d'unité 100

Code de fonction 3

Certains diagnostics de module (connexion d'E/S, intégrité étendue, état de redondance, serveur FDR, etc.) sont disponibles pour les clients Modbus qui lisent la zone du serveur Modbus local. Utilisez le code de fonction Modbus 3 avec l'ID d'unité 100 pour le mappage de registres :

Type	Décalage d'adresse Modbus	Taille (mots)
Données de diagnostic de réseau de base	0	39
Données de diagnostic du port Ethernet (interne)	39	103
Données de diagnostic du port Ethernet (Eth 1)	142	103
Données de diagnostic du port Ethernet (Eth 2)	245	103
Données de diagnostic du port Ethernet (Eth 3)	348	103
Données de diagnostic du port Ethernet (port d'embase Eth 4)	451	103
Données de diagnostic Modbus TCP/Port 502	554	114
Données de table de connexion Modbus TCP/Port 502	668	515
Données de diagnostic SMTP	1183	130
Diagnostics SNTP	1313	43
Informations de connexion DNP/IEC	1356	6
Diagnostic du serveur DNP/IEC	1362	1141
Diagnostic du client DNP/IEC	2503	1281
Diagnostic de sécurité du serveur DNP	3784	157
Diagnostic de sécurité du client DNP	3961	2497
Diagnostic de l'horloge	6458	13
Diagnostic SNMP	6471	1
Diagnostic du service Web	6472	1
Diagnostic du service LLDP	6473	1
Diagnostic du service de mise à niveau du micrologiciel	6474	1
Diagnostic du service Syslog	6475	1
Diagnostic SD	6476	1
Diagnostic IPAddrStatus	6477	1
Réservé	6478	13
Diagnostic HSBY	6491	35
Diagnostic général de la table de journalisation des données	6526	171
Diagnostic du service de journalisation des données	6697	230
Diagnostic du service SNMP	6927	23
Diagnostic du module	6950	15
Données de diagnostic des réseaux de base (port de face avant)	6965	39
Données de diagnostic du port série	7004	20

Données de diagnostic des réseaux de base (offset 0)

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset	Octet de poids fort	Octet de poids faible	Validité du diagnostic réseau de base
Offset + 1	Octet de poids fort	Octet de poids faible	
Offset + 2	Octet de poids fort	Octet de poids faible	Etat global des communications
Offset + 3	Octet de poids fort	Octet de poids faible	Services de communication pris en charge
Offset + 4	Octet de poids fort	Octet de poids faible	Etat des services de communication
Offset + 5	IP 1	IP 2	Adresse IP
Offset + 6	IP 3	IP 4	
Offset + 7	Masque SR 1	Masque SR 2	Masque de sous-réseau
Offset + 8	Masque SR 3	Masque SR 4	
Offset + 9	Passerelle IP 1	Passerelle IP 2	Passerelle par défaut
Offset + 10	Passerelle IP 3	Passerelle IP 4	
Offset + 11	MAC 00	MAC 01	Adresse MAC
Offset + 12	MAC 02	MAC 03	
Offset + 13	MAC 04	MAC 05	
Offset + 14	Octet de poids fort 00	01	Format de trame Ethernet - fonction/configuration/fonctionnement
Offset + 15	02	03	
Offset + 16	04	Octet de poids faible 05	
Offset + 17	C00	C01	Trames Ethernet reçues OK
Offset + 18	C02	C03	
Offset + 19	C00	C01	Trames Ethernet émises OK
Offset + 20	C02	C03	
Offset + 21	Octet de poids fort	Octet de poids faible	Nombre de connexions client ouvertes
Offset + 22	Octet de poids fort	Octet de poids faible	Nombre de connexions serveur ouvertes
Offset + 23	C00	C01	Nombre de messages d'erreur Modbus envoyés
Offset + 24	C02	C03	
Offset + 25	C00	C01	Nombre de messages Modbus envoyés
Offset + 26	C02	C03	
Offset + 27	C00	C01	Nombre de messages Modbus reçus
Offset + 28	C02	C03	
Offset + 29	Car. 1	Car. 2	Nom de l'équipement
Offset + 30	Car. 3	Car. 4	
Offset + 31	Car. 5	Car. 6	
Offset + 32	Car. 7	Car. 8	
Offset + 33	Car. 9	Car. 10	
Offset + 34	Car. 11	Car. 12	
Offset + 35	Car. 13	Car. 14	
Offset + 36	Car. 15	Car. 16	
Offset + 37	Octet de poids fort 00	01	Fonctionnalité de mode d'affectation d'adresse IP/opérationnel
Offset + 38	02	Octet de poids faible 03	

Données de diagnostic du port Ethernet (Offset 39)

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset	Octet de poids fort	Octet de poids faible	Validité des données de diagnostic de port
Offset + 1	Octet de poids fort	Octet de poids faible	Numéro de port logique/physique
Offset + 2	Octet de poids fort	Octet de poids faible	Capacité de contrôle Ethernet
Offset + 3	Octet de poids fort	Octet de poids faible	Capacité de vitesse de liaison
Offset + 4	Octet de poids fort	Octet de poids faible	Configuration de contrôle Ethernet
Offset + 5	Octet de poids fort	Octet de poids faible	Configuration de la vitesse de liaison
Offset + 6	Octet de poids fort	Octet de poids faible	Contrôle Ethernet opérationnel
Offset + 7	Octet de poids fort	Octet de poids faible	Vitesse de liaison opérationnelle
Offset + 8	MAC 00	MAC 01	Adresse MAC du port
Offset + 9	MAC 02	MAC 03	
Offset + 10	MAC 04	MAC 05	
Offset + 11	MSB - C00	C01	Validité des données des compteurs de supports
Offset + 12	C02	LSB - C03	
Offset + 13	MSB - C00	C01	Nombre d'octets transmis OK
Offset + 14	C02	LSB - C03	
Offset + 15	MSB - C00	C01	Nombre d'octets reçus OK
Offset + 16	C02	LSB - C03	
Offset + 17	MSB - C00	C01	Nombre de collisions Ethernet
Offset + 18	C02	LSB - C03	
Offset + 19	MSB - C00	C01	Erreurs de détection de porteuse
Offset + 20	C02	LSB - C03	
Offset + 21	MSB - C00	C01	Nombre de collisions Ethernet en excès
Offset + 22	C02	LSB - C03	
Offset + 23	MSB - C00	C01	Erreurs de CRC
Offset + 24	C02	LSB - C03	
Offset + 25	MSB - C00	C01	Erreurs de FSC
Offset + 26	C02	LSB - C03	
Offset + 27	MSB - C00	C01	Erreurs d'alignement
Offset + 28	C02	LSB - C03	
Offset + 29	MSB - C00	C01	Nombre d'erreurs de transmission MAC internes
Offset + 30	C02	LSB - C03	
Offset + 31	MSB - C00	C01	Collisions tardives
Offset + 32	C02	LSB - C03	
Offset + 33	MSB - C00	C01	Nombre d'erreurs de réception MAC internes
Offset + 34	C02	LSB - C03	
Offset + 35	MSB - C00	C01	Collisions multiples
Offset + 36	C02	LSB - C03	
Offset + 37	MSB - C00	C01	Collisions simples
Offset + 38	C02	LSB - C03	
Offset + 39	MSB - C00	C01	Transmissions différées
Offset + 40	C02	LSB - C03	
Offset + 41	MSB - C00	C01	Trames trop longues
Offset + 42	C02	LSB - C03	
Offset + 43	MSB - C00	C01	Trames trop courtes
Offset + 44	C02	LSB - C03	
Offset + 45	MSB - C00	C01	Erreur de test SQE
Offset + 46	C02	LSB - C03	

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset + 47	Octet de poids fort	Octet de poids faible	Longueur d'étiquette de l'interface
Offset + 48	IL_char64	IL_char63	Caractères d'étiquette d'interface
Offset + ...			Caractères d'étiquette d'interface
Offset + 79	IL_char2	IL_char1	Caractères d'étiquette d'interface
Offset + 80	Octet de poids fort	Octet de poids faible	Validité du diagnostic des compteurs d'interface
Offset + 81	MSB - C00	C01	Nombre d'octets reçus
Offset + 82	C02	LSB - C03	
Offset + 83	MSB - C00	C01	Nombre de paquets de monodiffusion reçus
Offset + 84	C02	LSB - C03	
Offset + 85	MSB - C00	C01	Nombre de paquets non monodiffusion reçus
Offset + 86	C02	LSB - C03	
Offset + 87	MSB - C00	C01	Nombre de paquets entrants rejetés
Offset + 88	C02	LSB - C03	
Offset + 89	MSB - C00	C01	Nombre de paquets d'erreurs entrants
Offset + 90	C02	LSB - C03	
Offset + 91	MSB - C00	C01	Nombre de paquets entrants inconnus
Offset + 92	C02	LSB - C03	
Offset + 93	MSB - C00	C01	Nombre d'octets envoyés
Offset + 94	C02	LSB - C03	
Offset + 95	MSB - C00	C01	Nombre de paquets de monodiffusion envoyés
Offset + 96	C02	LSB - C03	
Offset + 97	MSB - C00	C01	Nombre de paquets non monodiffusion envoyés
Offset + 98	C02	LSB - C03	
Offset + 99	MSB - C00	C01	Nombre de paquets sortants rejetés
Offset + 100	C02	LSB - C03	
Offset + 101	MSB - C00	C01	Nombre de paquets d'erreurs sortants
Offset + 102	C02	LSB - C03	
Offset + 103			Port 2
			103 mots par port
Offset + 206			Port 3
			103 mots par port
Offset + 309			Port 4
			103 mots par port

Données de diagnostic Modbus TCP/Port 502 (Offset 554)

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset	Octet de poids fort	Octet de poids faible	Validité des données de diagnostic Modbus TCP/Port 502
Offset + 1	Octet de poids fort	Octet de poids faible	
Offset + 2	Octet de poids fort	Octet de poids faible	Etat du port 502
Offset + 3	Octet de poids fort	Octet de poids faible	Nombre de connexions ouvertes
Offset + 4	MSB - C00	C01	Nombre de messages Modbus envoyés
Offset + 5	C02	LSB - C03	
Offset + 6	MSB - C00	C01	Nombre de messages Modbus reçus
Offset + 7	C02	LSB - C03	
Offset + 8	Octet de poids fort	Octet de poids faible	Nombre de connexions de client Modbus ouvertes
Offset + 9	Octet de poids fort	Octet de poids faible	Nombre de connexions de serveur Modbus ouvertes
Offset + 10	Octet de poids fort	Octet de poids faible	Nombre maximum de connexions
Offset + 11	Octet de poids fort	Octet de poids faible	Nombre maximum de connexions client
Offset + 12	Octet de poids fort	Octet de poids faible	Nombre maximum de connexions serveur
Offset + 13	MSB - C00	C01	Nombre de messages d'erreur Modbus envoyés
Offset + 14	C02	LSB - C03	
Offset + 15	Octet de poids fort	Octet de poids faible	Nombre de connexions prioritaires ouvertes
Offset + 16	Octet de poids fort	Octet de poids faible	Nombre maximum de connexions prioritaires
Offset + 17	Octet de poids fort	Octet de poids faible	Nombre d'entrées dans un tableau non autorisé
Offset + 18	MSB - IP1	IP2	Adresse IP distante 1
Offset + 19	IP3	LSB - IP4	
Offset + 20	Octet de poids fort	Octet de poids faible	Nombre de tentatives d'ouverture d'une connexion non autorisée 1
...			
Offset + 111	MSB - IP1	IP2	Adresse IP distante 32
Offset + 112	IP3	LSB - IP4	
Offset + 113	Octet de poids fort	Octet de poids faible	Nombre de tentatives d'ouverture d'une connexion non autorisée 32

Données de table de connexion Modbus TCP/Port 502 (Offset 668)

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset	Octet de poids fort	Octet de poids faible	Validité de la table de connexion
Offset + 1	Octet de poids fort	Octet de poids faible	Nombre d'entrées
Offset + 2	Octet de poids fort	Octet de poids faible	Index d'entrée de départ
Offset + 3	Octet de poids fort	Octet de poids faible	Index de connexion
Offset + 4	IP 1	IP 2	Adresse IP distante
Offset + 5	IP 3	IP 4	
Offset + 6	Octet de poids fort	Octet de poids faible	Numéro de port distant
Offset + 7	Octet de poids fort	Octet de poids faible	Numéro de port local
Offset + 8	Octet de poids fort	Octet de poids faible	Nombre de messages Modbus envoyés sur la connexion
Offset + 9	Octet de poids fort	Octet de poids faible	Nombre de messages Modbus reçus sur la connexion
Offset + 10	Octet de poids fort	Octet de poids faible	Nombre de messages d'erreur Modbus envoyés sur la connexion
...			
Offset + 3 + (8 * (N-1))	Octet de poids fort	Octet de poids faible	Index de connexion
Offset + 4 + (8 * (N-1))	IP 1	IP 2	Adresse de port distant
Offset + 5 + (8 * (N-1))	IP 3	IP 4	
Offset + 6 + (8 * (N-1))	Octet de poids fort	Octet de poids faible	Numéro de port distant
Offset + 7 + (8 * (N-1))	Octet de poids fort	Octet de poids faible	Numéro de port local
Offset + 8 + (8 * (N-1))	Octet de poids fort	Octet de poids faible	Nombre de messages Modbus envoyés sur la connexion
Offset + 9 + (8 * (N-1))	Octet de poids fort	Octet de poids faible	Nombre de messages Modbus reçus sur la connexion
Offset + 10 + (8 * (N-1))	Octet de poids fort	Octet de poids faible	Nombre de messages d'erreur Modbus détectée envoyés sur la connexion

Données de diagnostic SNTP (offset 1313)

Adresse	Octet de poids fort	Octet de poids faible	Type de CIP	Commentaires
Offset	MSW - MSB	MSW - LSB	UDINT	Activé/désactivé
Offset + 1	LSW - MSB	LSW - LSB		
Offset + 2	MSW - MSB	MSW - LSB	UDINT	Adresse IP du serveur NTP principal
Offset + 3	LSW - MSB	LSW - LSB		
Offset + 4	MSW - MSB	MSW - LSB	UDINT	Adresse IP du serveur NTP secondaire
Offset + 5	LSW - MSB	LSW - LSB		
Offset + 6	Inutilisé	Octet de poids faible	USINT	Période d'interrogation
Offset + 7	Inutilisé	Octet de poids faible	USINT	Réglage automatique de l'heure d'été
Offset + 8	Inutilisé	Octet de poids faible	USINT	Mettre à jour le contrôleur avec l'heure du module
Offset + 9	Inutilisé	Octet de poids faible	USINT	Réservé
Offset + 10	MSW - MSB	MSW - LSB	UDINT	Fuseau horaire
Offset + 11	LSW - MSB	LSW - LSB		
Offset + 12	Octet de poids fort	Octet de poids faible	INT	Décalage du fuseau horaire
Offset + 13	Inutilisé	Inutilisé	USINT	Réservé
Offset + 14	Inutilisé	Inutilisé	USINT	Réservé
Offset + 15	Inutilisé	Octet de poids faible	USINT	Date de début en heure d'été - mois
Offset + 16	Inutilisé	Octet de poids faible	USINT	Date de début de l'heure d'été - numéro de semaine, jour de la semaine
Offset + 17	Inutilisé	Octet de poids faible	USINT	Date de fin de l'heure d'été - mois
Offset + 18	Inutilisé	Octet de poids faible	USINT	Date de fin de l'heure d'été - numéro de semaine, jour de la semaine
Offset + 19	MSW - MSB	MSW - LSB	UDINT	Etat du service de temps réseau
Offset + 20	LSW - MSB	LSW - LSB		
Offset + 21	MSW - MSB	MSW - LSB	UDINT	Etat de la liaison vers le serveur NTP
Offset + 22	LSW - MSB	LSW - LSB		
Offset + 23	MSW - MSB	MSW - LSB	UDINT	Adresse IP du serveur NTP actuel
Offset + 24	LSW - MSB	LSW - LSB		
Offset + 25	MSW - MSB	MSW - LSB	UDINT	Type de serveur NTP
Offset + 26	LSW - MSB	LSW - LSB		
Offset + 27	MSW - MSB	MSW - LSB	UDINT	Qualité du temps serveur NTP
Offset + 28	LSW - MSB	LSW - LSB		
Offset + 29	MSW - MSB	MSW - LSB	UDINT	Nombre de requêtes NTP envoyées
Offset + 30	LSW - MSB	LSW - LSB		
Offset + 31	MSW - MSB	MSW - LSB	UDINT	Nombre d'erreurs de communication détectées
Offset + 32	LSW - MSB	LSW - LSB		
Offset + 33	MSW - MSB	MSW - LSB	UDINT	Nombre de réponses NTP reçues
Offset + 34	LSW - MSB	LSW - LSB		
Offset + 35	Octet de poids fort	Octet de poids faible	UINT	Dernière erreur détectée
Offset + 36	MSW - MSB	MSW - LSB	UDINT	Heure actuelle
Offset + 37	LSW - MSB	LSW - LSB		
Offset + 38	Octet de poids fort	Octet de poids faible		Date actuelle
Offset + 39	MSW - MSB	MSW - LSB	UDINT	Etat de l'heure d'été
Offset + 40	LSW - MSB	LSW - LSB		
Offset + 41	MSW - MSB	MSW - LSB	UINT	Temps depuis la dernière mise à jour
Offset + 42	LSW - MSB	LSW - LSB		

Informations de connexion DNP/IEC (offset 1356)

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset	Client Connecté Décompte	Client Configuré Décompte	Client DNP3/IEC Décompte
Offset + 1	Serveur Connecté Décompte	Serveur Configuré Décompte	Serveur DNP3/IEC Décompte
Offset + 2			Réservé
Offset + 3			Réservé
Offset + 4			Réservé
Offset + 5			Réservé

Diagnostic de connexion serveur DNP/IEC (offset 1362)

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset	Octet de poids fort	Octet de poids faible	Nombre d'entrées
Offset + 1	Octet de poids fort	Octet de poids faible	Octet de poids fort : Evénement UTILISÉ/CONFIGURÉ 0-100 % Octet de poids faible : CONFIGURÉ/TOTAL 0-100 %
Offset + 2	MSB - C03	C02	Total du module
Offset + 3	C01	LSB - C00	Evénement configuré Taille du tampon
Offset + 4	MSB - C03	C02	Total du module
Offset + 5	C01	LSB - C00	Utilisation du tampon d'événements actuelle
Offset + 6	MSB - C03	C02	Débordement actuel total du module
Offset + 7	C01	LSB - C00	
Offset + 8	Octet de poids fort	Octet de poids faible	Octet de poids fort : Débordement du tampon d'événements Octet de poids faible : Etat de la sauvegarde d'événements
Offset + 9	Octet de poids fort	Octet de poids faible	Index de voie
Offset + 10	Octet de poids fort réservé	Octet de poids faible 1 : DNP3 série 3 : DNP3 NET 5 : IEC 101 7 : IEC 104	Protocole : Serveur série DNP3 Serveur NET DNP3 Serveur IEC 101 Serveur IEC 104

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset + 11	Octet de poids fort	Octet de poids faible	Etat de connexion octet de poids faible 0 : déconnecté 1 : connecté 2 : connexion en cours 3 : actif 4 : inactif Type d'authentification octet de poids fort 0 : aucun 1 : SAV2 2 : SAV5 3 : TLS_ONLY 4 : TLS_SAV2 5 : TLS_SAV5
Offset + 12	Car. 1	Car. 2	Nom de voie
Offset + 13	Car. 3	Car. 4	
Offset + 14	Car. 5	Car. 6	
Offset + 15	Car. 7	Car. 8	
Offset + 16	Car. 9	Car. 10	
Offset + 17	Car. 11	Car. 12	
Offset + 18	Car. 13	Car. 14	
Offset + 19	Car. 15	Car. 16	Adresse IP distante
Offset + 20	IP 1	IP 2	
Offset + 21	IP 3	IP 4	
Offset + 22	Octet de poids fort	Octet de poids faible	Numéro de port distant
Offset + 23	Octet de poids fort	Octet de poids faible	Numéro de port local
Offset + 24	Octet de poids fort	Octet de poids faible	Code d'erreur : Bit 0 : Sécurité de la voie non configurée Bit 1 : Erreur d'initialisation de variable non localisée Bit 2 : Erreur interne (erreur de création de tuyau, erreur d'initialisation d'IPC, etc.) Bits 3-14 : Réservé Bit 15 : Erreur TLS
Offset + 25	C03	C02	Total voie
Offset + 26	C01	C00	Evénement configuré Taille du tampon
Offset + 27	C03	C02	Total voie
Offset + 28	C01	C00	Evénement actuel Tampon utilisé
Offset + 29	C03	C02	Total voie
Offset + 30	C01	C00	Débordement actuel
Offset + 31	Octet de poids fort	Octet de poids faible	Octet de poids fort : Réservé Octet de poids faible : Débordement du tampon d'événements
Offset + 32	C01	C00	Code d'erreur TLS
Offset + 33	Octet de poids fort	Octet de poids faible	Réservé 2
Offset + 34	Octet de poids fort	Octet de poids faible	Réservé 3

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset + 35	Octet de poids fort	Octet de poids faible	Nombre de types de données Etat d'événement Toujours 16
Offset + 36	Octet de poids fort	Octet de poids faible	Octet de poids fort Bit 0 : Validité Bit 1 : Débordement du tampon d'événements Bits 2-7 : Réserve Octet de poids faible : Index
Offset + 37	Octet de poids fort	Octet de poids faible	Type de données DNP : 1. Entrée binaire 2. Entrée double 3. Sortie binaire 4. Compteur binaire 5. Compteur gelé 6 : Entrée analogique 7. Sortie analogique 8-16. Pour type de données IEC étendu : 1. M_SP 2. M_DP 3. M_ST 4. M_BO 5. M_ME_A 6. M_ME_B 7. M_ME_C 8. M_IT 9. Custom_M_IT_D 10-16. Pour étendu
Offset + 38	Car. 1	Car. 2	Nom de type de données
Offset + 39	Car. 3	Car. 4	
Offset + 40	Car. 5	Car. 6	
Offset + 41	Car. 7	Car. 8	
Offset + 42	Car. 9	Car. 10	
Offset + 43	Car. 11	Car. 12	
Offset + 44	Car. 13	Car. 14	
Offset + 45	Car. 15	Car. 16	
Offset + 46	C03	C02	Evénement configuré
Offset + 47	C01	C00	Taille du tampon
Offset + 48	C03	C02	Evénement actuel
Offset + 49	C01	C00	Tampon utilisé
Offset + 50	C03	C02	Débordement actuel
Offset + 51	C01	C00	

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset + 36 + (X-1) *16	Octet de poids fort	Octet de poids faible	Octet de poids fort : Bit 0 : Validité Bit 1 : Débordement du tampon d'événements Bits 2-7 : Réservé Octet de poids faible : Index
Offset + 37 + (X-1) *16	Octet de poids fort	Octet de poids faible	Type de données DNP : 1. Entrée binaire 2. Entrée double 3. Sortie binaire 4. Compteur binaire 5. Compteur gelé 6. Entrée analogique 7. Sortie analogique 8-16. Pour type de données IEC étendu : 1. M_SP 2. M_DP 3. M_ST 4. M_BO 5. M_ME_A 6. M_ME_B 7. M_ME_C 8. M_IT 9. Custom_M_IT_D 10-16. Pour étendu
Offset + 38 + (X-1) *16	Car. 1	Car. 2	Nom de type de données
Offset + 39 + (X-1) *16	Car. 3	Car. 4	
Offset + 40 + (X-1) *16	Car. 5	Car. 6	
Offset + 41 + (X-1) *16	Car. 7	Car. 8	
Offset + 42 + (X-1) *16	Car. 9	Car. 10	
Offset + 43 + (X-1) *16	Car. 11	Car. 12	
Offset + 44 + (X-1) *16	Car. 13	Car. 14	
Offset + 45 + (X-1) *16	Car. 15	Car. 16	
Offset + 46 + (X-1) *16	Car. 03	Car. 02	Evénement configuré
Offset + 47 + (X-1) *16	Car. 01	Car. 00	Taille du tampon
Offset + 48 + (X-1) *16	Car. 03	Car. 02	Evénement actuel
Offset + 49 + (X-1) *16	Car. 01	Car. 00	Tampon utilisé
Offset + 50 + (X-1) *16	Car. 03	Car. 02	Débordement actuel
Offset + 51 + (X-1) *16	Car. 01	Car. 00	
...			
Offset + 09 + (N-1) *(27 + 16*16)	Octet de poids fort	Octet de poids faible	Index de voie

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset + (N-1)*283 + 10	Octet de poids fort réservé	Octet de poids faible : 1 : DNP3 série 3 : DNP3 NET 5 : IEC 101 7 : IEC 104	Protocole : Serveur série DNP3 Serveur NET DNP3 Serveur IEC 101 Serveur IEC 104
Offset + (N-1)*283 + 11	Octet de poids fort	Octet de poids faible	Etat de connexion octet de poids faible : 0 : Déconnecté 1 : Connecté 2 : Connexion en cours 3 : Actif 4 : Inactif Type d'authentification octet de poids fort : 5 : Néant 6 : SAV2 7 : SAV5 8 : TLS_ONLY 9 : TLS_SAV2 10 : TLS_SAV5
Offset + (N-1)*283 + 12	Car. 1	Car. 2	Nom de voie
Offset + (N-1)*283 + 13	Car. 3	Car. 4	
Offset + (N-1)*283 + 14	Car. 5	Car. 6	
Offset + (N-1)*283 + 15	Car. 7	Car. 8	
Offset + (N-1)*283 + 16	Car. 9	Car. 10	
Offset + (N-1)*283 + 17	Car. 11	Car. 12	
Offset + (N-1)*283 + 18	Car. 13	Car. 14	
Offset + (N-1)*283 + 19	Car. 15	Car. 16	
Offset + (N-1)*283 + 20	IP 1	IP 2	Adresse IP distante
Offset + (N-1)*283 + 21	IP 3	IP 4	
Offset + (N-1)*283 + 22	Octet de poids fort	Octet de poids faible	Numéro de port distant
Offset + (N-1)*283 + 23	Octet de poids fort	Octet de poids faible	Numéro de port local
Offset + (N-1)*283 + 24	Octet de poids fort	Octet de poids faible	Code d'erreur : Bit 0 : Sécurité de la voie non configurée Bit 1 : Erreur d'initialisation de variable non localisée Bit 2 : Erreur interne (erreur de création de tuyau, erreur d'initialisation d'IPC, etc.) Bits 3-14 : Réserve Bit 15 : Erreur TLS
Offset + (N-1)*283 + 25	C03	C02	Total voie
Offset + (N-1)*283 + 26	C01	C00	Evénement configuré Taille du tampon
Offset + (N-1)*283 + 27	C03	C02	Total voie
Offset + (N-1)*283 + 28	C01	C00	Evénement actuel Tampon utilisé

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset + (N-1)*283 + 29	C03	C02	Total voie
Offset + (N-1)*283 + 30	C01	C00	Débordement actuel
Offset + (N-1)*283 + 31	Octet de poids fort	Octet de poids faible	Octet de poids fort : Réservé Octet de poids faible : Débordement du tampon d'événements
Offset + (N-1)*283 + 32	C01	C00	Code d'erreur TLS
Offset + (N-1)*283 + 33	Octet de poids fort	Octet de poids faible	Réservé 2
Offset + (N-1)*283 + 34	Octet de poids fort	Octet de poids faible	Réservé 3
Offset + (N-1)*283 + 35	Octet de poids fort	Octet de poids faible	Nombre de types de données Etat d'événement Toujours 16
Offset + (N-1)*283 + 36	Octet de poids fort	Octet de poids faible	Octet de poids fort : Bit 0 : Validité Bit 1 : Débordement du tampon d'événements Bits 2-7 : Réservé Octet de poids faible : Index
Offset + (N-1)*283 + 37	Octet de poids fort	Octet de poids faible	Type de données DNP : Type de données DNP : 1. Entrée binaire 2. Entrée double 3. Sortie binaire 4. Compteur binaire 5. Compteur gelé 6 : Entrée analogique 7. Sortie analogique 8-16. Pour type de données IEC étendu : 1. M_SP 2. M_DP 3. M_ST 4. M_BO 5. M_ME_A 6. M_ME_B 7. M_ME_C 8. M_IT 9. Custom_M_IT_D 10-16. Pour étendu

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset + (N-1)*283 + 38	Car. 1	Car. 2	Nom de type de données
Offset + (N-1)*283 + 39	Car. 3	Car. 4	
Offset + (N-1)*283 + 40	Car. 5	Car. 6	
Offset + (N-1)*283 + 41	Car. 7	Car. 8	
Offset + (N-1)*283 + 42	Car. 9	Car. 10	
Offset + (N-1)*283 + 43	Car. 11	Car. 12	
Offset + (N-1)*283 + 44	Car. 13	Car. 14	
Offset + (N-1)*283 + 45	Car. 17	Car. 16	
Offset + (N-1)*283 + 46	C03	C02	Evénement configuré
Offset + (N-1)*283 + 47	C01	C00	Taille du tampon
Offset + (N-1)*283 + 48	C03	C02	Evénement actuel
Offset + (N-1)*283 + 49	C01	C00	Tampon utilisé
Offset + (N-1)*283 + 50	C03	C02	Débordement actuel
Offset + (N-1)*283 + 51	C01	C00	
...			
Offset + (N-1)*283 + 36 + (X-1)*16	Octet de poids fort	Octet de poids faible	Octet de poids fort : Bit 0 : Validité Bit 1 : Débordement du tampon d'événements Bits 2-7 : Réserve Octet de poids faible : Index
Offset + (N-1)*283 + 37 + (X-1)*16	Octet de poids fort	Octet de poids faible	Type de données DNP : 1. Entrée binaire 2. Entrée double 3. Sortie binaire 4. Compteur binaire 5. Compteur gelé 6. Sortie analogique 7. Sortie analogique 8-16. Pour type de données IEC étendu : 1. M_SP 2. M_DP 3. M_ST 4. M_BO 5. M_ME_A 6. M_ME_B 7. M_ME_C 8. M_IT 9. Custom_M_IT_D 10-16. Pour étendu

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset + (N-1)*283 + 38 + (X-1)*16	Car. 1	Car. 2	Nom de type de données
Offset + (N-1)*283 + 39 + (X-1)*16	Car. 3	Car. 4	
Offset + (N-1)*283 + 40 + (X-1)*16	Car. 5	Car. 6	
Offset + (N-1)*283 + 41 + (X-1)*16	Car. 7	Car. 8	
Offset + (N-1)*283 + 42 + (X-1)*16	Car. 9	Car. 10	
Offset + (N-1)*283 + 43 + (X-1)*16	Car. 11	Car. 12	
Offset + (N-1)*283 + 44 + (X-1)*16	Car. 13	Car. 14	
Offset + (N-1)*283 + 45 + (X-1)*16	Car. 15	Car. 16	
Offset + (N-1)*283 + 46 + (X-1)*16	C03	C02	Événement configuré
Offset + (N-1)*283 + 47 + (X-1)*16	C01	C00	Taille du tampon
Offset + (N-1)*283 + 48 + (X-1)*16	C03	C02	Événement actuel
Offset + (N-1)*283 + 49 + (X-1)*16	C01	C00	Tampon utilisé
Offset + (N-1)*283 + 50 + (X-1)*16	C03	C02	Débordement actuel
Offset + (N-1)*283 + 51 + (X-1)*16	C01	C00	

Diagnostic de connexion client DNP/IEC (offset 2503)

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset	Octet de poids fort	Octet de poids faible	Nombre d'entrées
Offset + 1	Octet de poids fort	Octet de poids faible	Index de voie
Offset + 2	Octet de poids fort réservé	Octet de poids faible 2 : DNP3 série 4 : DNP3 NET 6 : IEC 101 8 : IEC 104	Protocole : Client DNP3 série Client DNP3 NET Client IEC 101 Client IEC 104
Offset + 3	Octet de poids fort	Octet de poids faible	État de connexion octet de poids faible : 0 : Déconnecté 1 : Connecté 2 : Connexion en cours 3 : Actif 4 : Inactif Type d'authentification octet de poids fort : 5 : Néant 6 : SAV2 7 : SAV5 8 : TLS_ONLY 9 : TLS_SAV2 10 : TLS_SAV5

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset + 4	Car. 1	Car. 2	Nom de voie
Offset + 5	Car. 3	Car. 4	
Offset + 6	Car. 5	Car. 6	
Offset + 7	Car. 7	Car. 8	
Offset + 8	Car. 9	Car. 10	
Offset + 9	Car. 11	Car. 12	
Offset + 10	Car. 13	Car. 14	
Offset + 11	Car. 15	Car. 16	Adresse IP distante
Offset + 12	IP 1	IP 2	
Offset + 13	IP 3	IP 4	Numéro de port distant
Offset + 14	Octet de poids fort	Octet de poids faible	
Offset + 15	Octet de poids fort	Octet de poids faible	Numéro de port local
Offset + 16	Bits 15~8	Bits 7~0	Code d'erreur Bit 0 : Sécurité de la voie non configurée Bit 1 : Erreur d'initialisation de variable non localisée Bit 2 : Erreur interne (erreur de création de tuyau, erreur d'initialisation d'IPC, etc.) Bit 3 : authentification non effectuée Bit 4 : Réponse inattendue Bit 5 : Pas de réponse Bit 6 : Mode agressif non pris en charge Bit 7 : Algorithme MAC non pris en charge Bit 8 : Algorithme d'enveloppe de clé non pris en charge Bit 9 : Autorisation non effectuée Bit 10 : Méthode de modification de clé de mise à jour non autorisée Bit 11 : Signature non valide Bit 12 : Données de certification non valides Bit 13 : Utilisateur inconnu Bit 14 : Nombre maximum de requêtes d'état de clé de session dépassé Bit 15 : Erreur TLS
Offset + 17	C01	C02	Code d'erreur TLS
Offset + 18	Octet de poids fort	Octet de poids faible	Réservé 1
Offset + 19	Octet de poids fort	Octet de poids faible	Réservé 2
Offset + 20	Octet de poids fort	Octet de poids faible	Réservé 3
...			
Offset + 01 + (N-1)*20	Octet de poids fort	Octet de poids faible	Index de voie
Offset + 02 + (N-1)*20	Octet de poids fort réservé	Octet de poids faible : 2 : DNP3 série 4 : DNP3 NET 6 : IEC 101 8 : IEC 104	Protocole : Client DNP3 série Client DNP3 NET Client IEC 101 Client IEC 104

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset + 03 + (N-1)*20	Octet de poids fort	Octet de poids faible	Etat de connexion octet de poids faible : 0 : Déconnecté 1 : Connecté 2 : Connexion en cours 3 : Actif 4 : Inactif Type d'authentification octet de poids fort : 5 : Néant 6 : SAV2 7 : SAV5 8 : TLS_ONLY 9 : TLS_SAV2 10 : TLS_SAV5
Offset + 04 + (N-1)*20	Car. 1	Car. 2	Nom de voie
Offset + 05 + (N-1)*20	Car. 3	Car. 4	
Offset + 06 + (N-1)*20	Car. 5	Car. 6	
Offset + 07 + (N-1)*20	Car. 7	Car. 8	
Offset + 08 + (N-1)*20	Car. 9	Car. 10	
Offset + 09 + (N-1)*20	Car. 11	Car. 12	
Offset + 10 + (N-1)*20	Car. 13	Car. 14	
Offset + 11 + (N-1)*20	Car. 15	Car. 16	Adresse IP distante
Offset + 12 + (N-1)*20	IP 1	IP 2	
Offset + 13 + (N-1)*20	IP 3	IP 4	Numéro de port distant
Offset + 14 + (N-1)*20	Octet de poids fort	Octet de poids faible	
Offset + 15 + (N-1)*20	Octet de poids fort	Octet de poids faible	Numéro de port local
Offset + 16 + (N-1)*20	Bits 15~8	Bits 7~0	Code d'erreur : Bit 0 : Sécurité de la voie non configurée Bit 1 : Erreur d'initialisation de variable non localisée Bit 2 : Erreur interne (erreur de création de tuyau, erreur d'initialisation d'IPC, etc.) Bit 3 : Authentification non effectuée Bit 4 : Réponse inattendue Bit 5 : Pas de réponse Bit 6 : Mode agressif non pris en charge Bit 7 : Algorithme MAC non pris en charge Bit 8 : Algorithme d'enveloppe de clé non pris en charge Bit 9 : Autorisation non effectuée Bit 10 : Méthode de modification de clé de mise à jour non autorisée Bit 11 : Signature non valide Bit 12 : Données de certification non valides Bit 13 : Utilisateur inconnu Bit 14 : Nombre maximum de requêtes d'état de clé de session dépassé Bit 15 : Erreur TLS
Offset + 17 + (N-1)*20	C01	C00	Code d'erreur TLS
Offset + 18 + (N-1)*20	Octet de poids fort	Octet de poids faible	Réservé 1

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset + 19 + (N-1)*20	Octet de poids fort	Octet de poids faible	Réservé 2
Offset + 20 + (N-1)*20	Octet de poids fort	Octet de poids faible	Réservé 3

Diagnostic de sécurité du serveur/serveur DNP (offset 3784)

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset			Nombre d'entrées
Offset + 1	Octet de poids fort réservé	Index de voie octet de poids faible	Index de voie
Offset + 2	C03	C02	Messages inattendus (SAv2, SAv5)
Offset + 3	C01	C00	
Offset + 4	C03	C02	Problèmes d'autorisation (SAv2, SAv5)
Offset + 5	C01	C00	
Offset + 6	C03	C02	Problèmes d'authentification (SAv2, SAv5)
Offset + 7	C01	C00	
Offset + 8	C03	C02	Timeout de réponse (SAv2, SAv5)
Offset + 9	C01	C00	
Offset + 10	C03	C02	Re-saisie en raison d'un problème d'authentification (SAv5 uniquement)
Offset + 11	C01	C00	
Offset + 12	C03	C02	Nombre total de messages envoyés (SAv5 uniquement)
Offset + 13	C01	C00	
Offset + 14	C03	C02	Nombre total de messages reçus (SAv5 uniquement)
Offset + 15	C01	C00	
Offset + 16	C03	C02	Message critique envoyé (SAv2, SAv5)
Offset + 17	C01	C00	
Offset + 18	C03	C02	Message critique reçu (SAv2, SAv5)
Offset + 19	C01	C00	
Offset + 20	C03	C02	Messages rejetés (SAv5 uniquement)
Offset + 21	C01	C00	
Offset + 22	C03	C02	Message d'erreur envoyé (SAv2, SAv5)
Offset + 23	C01	C00	
Offset + 24	C03	C02	Message d'erreur reçu (SAv2, SAv5)
Offset + 25	C01	C00	
Offset + 26	C03	C02	Authentifications réussies (SAv2, SAv5)
Offset + 27	C01	C00	
Offset + 28	C03	C02	Modifications de clé de session (SAv2, SAv5)
Offset + 29	C01	C00	
Offset + 30	C03	C02	Modifications de clé de session non effectuées (SAv2, SAv5)
Offset + 31	C01	C00	
Offset + 32	C03	C02	Modifications de clé de mise à jour (SAv5 uniquement)
Offset + 33	C01	C00	
Offset + 34	C03	C02	Modifications de clé de mise à jour non effectuées (SAv5 uniquement)
Offset + 35	C01	C00	
Offset + 36	C03	C02	Re-saisie suite à un redémarrage (SAv5 uniquement)
Offset + 37	C01	C00	
Offset + 38	C01	C00	Réservé 0
Offset + 39	C01	C00	Réservé 1
...			
Offset + (N-1)*39 + 01	Octet de poids fort réservé	Octet de poids faible Index de voie	Index de voie
Offset + (N-1)*39 + 02	C03	C02	Messages inattendus (SAv2, SAv5)
Offset + (N-1)*39 + 03	C01	C00	
Offset + (N-1)*39 + 04	C03	C02	Problèmes d'autorisation (SAv2, SAv5)
Offset + (N-1)*39 + 05	C01	C00	

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset + (N-1)*39 + 06	C03	C02	Problèmes d'authentification (SAv2, SAv5)
Offset + (N-1)*39 + 07	C01	C00	
Offset + (N-1)*39 + 08	C03	C02	Timeout de réponse (SAv2, SAv5)
Offset + (N-1)*39 + 09	C01	C00	
Offset + (N-1)*39 + 10	C03	C02	Re-saisie en raison d'un problème d'authentification (SAv5 uniquement)
Offset + (N-1)*39 + 11	C01	C00	
Offset + (N-1)*39 + 12	C03	C02	Nombre total de messages envoyés (SAv5 uniquement)
Offset + (N-1)*39 + 13	C01	C00	
Offset + (N-1)*39 + 14	C03	C02	Nombre total de messages reçus (SAv5 uniquement)
Offset + (N-1)*39 + 15	C01	C00	
Offset + (N-1)*39 + 16	C03	C02	Messages critiques envoyés (SAv2, SAv5)
Offset + (N-1)*39 + 17	C01	C00	
Offset + (N-1)*39 + 18	C03	C02	Messages critiques reçus (SAv2, SAv5)
Offset + (N-1)*39 + 19	C01	C00	
Offset + (N-1)*39 + 20	C03	C02	Messages rejetés (SAv5 uniquement)
Offset + (N-1)*39 + 21	C01	C00	
Offset + (N-1)*39 + 22	C03	C02	Messages d'erreur envoyés (SAv2, SAv5)
Offset + (N-1)*39 + 23	C01	C00	
Offset + (N-1)*39 + 24	C03	C02	Messages d'erreur reçus (SAv2, SAv5)
Offset + (N-1)*39 + 25	C01	C00	
Offset + (N-1)*39 + 26	C03	C02	Authentifications réussies (SAv2, SAv5)
Offset + (N-1)*39 + 27	C01	C00	
Offset + (N-1)*39 + 28	C03	C02	Modifications de clé de session (SAv2, SAv5)
Offset + (N-1)*39 + 29	C01	C00	
Offset + (N-1)*39 + 30	C03	C02	Modifications de clé de session non effectuées (SAv2, SAv5)
Offset + (N-1)*39 + 31	C01	C00	
Offset + (N-1)*39 + 32	C03	C02	Modifications de clé de mise à jour (SAv5 uniquement)
Offset + (N-1)*39 + 33	C01	C00	
Offset + (N-1)*39 + 34	C03	C02	Modifications de clé de mise à jour non effectuées (SAv5 uniquement)
Offset + (N-1)*39 + 35	C01	C00	
Offset + (N-1)*39 + 36	C03	C02	Re-saisie suite à un redémarrage (SAv5 uniquement)
Offset + (N-1)*39 + 37	C01	C00	
Offset + (N-1)*39 + 38	C03	C02	Réservé 0
Offset + (N-1)*39 + 39	C01	C00	Réservé 1

Diagnostic de sécurité client/client DNP (offset 3961)

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset			Nombre d'entrées
Offset + 01	Octet de poids fort réservé	Octet de poids faible Index de voie	Index de voie
Offset + 02	C03	C02	Messages inattendus (SAv2, SAv5)
Offset + 03	C01	C00	
Offset + 04	C03	C02	Problèmes d'autorisation (SAv2, SAv5)
Offset + 05	C01	C00	
Offset + 06	C03	C02	Problèmes d'authentification (SAv2, SAv5)
Offset + 07	C01	C00	
Offset + 08	C03	C02	Timeout de réponse (SAv2, SAv5)
Offset + 09	C01	C00	
Offset + 10	C03	C02	Re-saisie en raison d'un problème d'authentification (SAv5 uniquement)
Offset + 11	C01	C00	
Offset + 12	C03	C02	Nombre total de messages envoyés (SAv5 uniquement)
Offset + 13	C01	C00	
Offset + 14	C03	C02	Nombre total de messages reçus (SAv5 uniquement)
Offset + 15	C01	C00	
Offset + 16	C03	C02	Message critique envoyé (SAv2, SAv5)
Offset + 17	C01	C00	
Offset + 18	C03	C02	Messages critiques reçus (SAv2, SAv5)
Offset + 19	C01	C00	
Offset + 20	C03	C02	Messages rejetés (SAv5 uniquement)
Offset + 21	C01	C00	
Offset + 22	C03	C02	Message d'erreur envoyé (SAv2, SAv5)
Offset + 23	C01	C00	
Offset + 24	C03	C02	Message d'erreur reçu (SAv2, SAv5)
Offset + 25	C01	C00	
Offset + 26	C03	C02	Authentifications réussies (SAv2, SAv5)
Offset + 27	C01	C00	
Offset + 28	C03	C02	Modifications de clé de session (SAv2, SAv5)
Offset + 29	C01	C00	
Offset + 30	C03	C02	Modifications de clé de session non effectuées (SAv2, SAv5)
Offset + 31	C01	C00	
Offset + 32	C03	C02	Modifications de clé de mise à jour (SAv5 uniquement)
Offset + 33	C01	C00	
Offset + 34	C03	C02	Modifications de clé de mise à jour non effectuées (SAv5 uniquement)
Offset + 35	C01	C00	
Offset + 36	C03	C02	Re-saisie suite à un redémarrage (SAv5 uniquement)
Offset + 37	C01	C00	
Offset + 38	C01	C00	Réservé 0
Offset + 39	C01	C00	Réservé 1
...			
Offset = (N-1)*39 + 01	Octet de poids fort réservé	Octet de poids faible Index de voie	Index de voie
Offset = (N-1)*39 + 02	C03	C02	Messages inattendus (SAv2, SAv5)
Offset = (N-1)*39 + 03	C01	C00	

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset = (N-1)*39 + 04	C03	C02	Problèmes d'autorisation (SAv2, SAv5)
Offset = (N-1)*39 + 05	C01	C00	
Offset = (N-1)*39 + 06	C03	C02	Problèmes d'authentification (SAv2, SAv5)
Offset = (N-1)*39 + 07	C01	C00	
Offset = (N-1)*39 + 08	C03	C02	Timeout de réponse (SAv2, SAv5)
Offset = (N-1)*39 + 09	C01	C00	
Offset = (N-1)*39 + 10	C03	C02	Re-saisie en raison d'un problème d'authentification (SAv5 uniquement)
Offset = (N-1)*39 + 11	C01	C00	
Offset = (N-1)*39 + 12	C03	C02	Nombre total de messages envoyés (SAv5 uniquement)
Offset = (N-1)*39 + 13	C01	C00	
Offset = 3(N-1)*39 + 14	C03	C02	Nombre total de messages reçus (SAv5 uniquement)
Offset = (N-1)*39 + 15	C01	C00	
Offset = (N-1)*39 + 16	C03	C02	Messages critiques envoyés (SAv2, SAv5)
Offset = (N-1)*39 + 17	C01	C00	
Offset = (N-1)*39 + 18	C03	C02	Messages critiques reçus (SAv2, SAv5)
Offset = (N-1)*39 + 19	C01	C00	
Offset = (N-1)*39 + 20	C03	C02	Messages rejetés (SAv5 uniquement)
Offset = (N-1)*39 + 21	C01	C00	
Offset = (N-1)*39 + 22	C03	C02	Messages d'erreur envoyés (SAv2, SAv5)
Offset = (N-1)*39 + 23	C01	C00	
Offset = (N-1)*39 + 24	C03	C02	Messages d'erreur reçus (SAv2, SAv5)
Offset = (N-1)*39 + 25	C01	C00	
Offset = (N-1)*39 + 26	C03	C02	Authentification réussie (SAv2, SAv5)
Offset = (N-1)*39 + 27	C01	C00	
Offset = (N-1)*39 + 28	C03	C02	Modifications de clé de session (SAv2, SAv5)
Offset = (N-1)*39 + 29	C01	C00	
Offset = (N-1)*39 + 30	C03	C02	Modifications de clé de session non effectuées (SAv2, SAv5)
Offset = (N-1)*39 + 31	C01	C00	
Offset = (N-1)*39 + 32	C03	C02	Modifications de clé de mise à jour (SAv5 uniquement)
Offset = (N-1)*39 + 33	C01	C00	
Offset = (N-1)*39 + 34	C03	C02	Modifications de clé de mise à jour non effectuées (SAv5 uniquement)
Offset = (N-1)*39 + 35	C01	C00	
Offset = (N-1)*39 + 36	C03	C02	Re-saisie suite à un redémarrage (SAv5 uniquement)
Offset = (N-1)*39 + 37	C01	C00	
Offset = (N-1)*39 + 38	C01	C00	Réservé 0
Offset = (N-1)*39 + 39	C01	C00	Réservé 1

Diagnostic d'horloge (offset 6458)

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset			Nombre d'entrées
Offset + 01	Octet de poids fort réservé	Etat de l'horloge octet de poids faible 1 : Synchronisé 0 : Non synchronisé	Etat de l'horloge
Offset + 02	C03	C02	Heure actuelle
Offset + 03	C01	C00	
Offset + 04	C01	C00	Date actuelle
Offset + 05			Réservé
Offset + 06	C03	C02	Fuseau horaire
Offset + 07	C01	C00	
Offset + 08	C03	C02	Heure de la dernière synchronisation horaire
Offset + 09	C01	C00	
Offset + 10	C01	C00	Date de la dernière synchronisation horaire
Offset + 11			Réservé
Offset + 12	Octet de poids fort réservé	Source horaire octet de poids faible 1 : SNTP 2 : DNP3 3 : contrôleur 4 : IEC60870 5 : module partenaire ...	Source de la dernière synchronisation horaire

Diagnostic SNMP (offset 6471)

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset	Octet de poids fort	Octet de poids faible	SNMP_service 0 : Le service ne fonctionne pas normalement. 1 : Le service fonctionne normalement ou est désactivé

Diagnostic du service Web (offset 6472)

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset	Octet de poids fort	Octet de poids faible	Web_service 0 : Le service ne fonctionne pas normalement. 1 : Le service fonctionne normalement ou est désactivé

Diagnostic du service LLDP (offset 6473)

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset	Octet de poids fort	Octet de poids faible	Etat du service LLDP Etat de la mise à niveau de micrologiciel 0 : Le service ne fonctionne pas normalement. 1 : Le service fonctionne normalement ou est désactivé

Diagnostic du service de mise à niveau du micrologiciel (offset 6474)

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset	Octet de poids fort	Octet de poids faible	Etat du service de mise à niveau de micrologiciel 0 : Le service ne fonctionne pas normalement. 1 : Le service fonctionne normalement ou est désactivé

Diagnostic du service Syslog (Offset 6475)

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset	Octet de poids fort	Octet de poids faible	Octet de poids fort : Etat du service Syslog : 0 : le service Syslog ne fonctionne pas normalement 1 : le service Syslog fonctionne normalement ou est désactivé Octet de poids faible : Serveur Syslog inaccessible : 1 : Aucun acquittement reçu du serveur Syslog 0 : Cas contraire

Diagnostic du service SD (offset 6476)

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset	Octet de poids fort	Octet de poids faible	Etat SD : 0 : Carte SD manquante ou inutilisable 1 : Carte SD normale

Diagnostic de l'état d'adresse IP (offset 6477)

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset	Octet de poids fort	Octet de poids faible	Etat de l'adresse IP : 0 : Adresse IP en double ou absente 1 : Adresse IP normale configurée

Diagnostic HSBY (offset 6491)

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset	Octet de poids fort Etat de la fonction HSBY	Octet de poids faible Service HSBY	Fonction HSBY : 0 : Désactivé NOTE: Si l'état est Désactivé, toutes les autres données de diagnostic sont à zéro. Dans ce cas, la page Web n'affiche pas de diagnostic HSBY. 1 : Activé Service HSBY : 0 : Non exécuté 1 : En cours d'exécution
Offset + 01	Octet de poids fort Etat de synchronisation	Octet de poids faible Etat HSBY interne	Etat de synchronisation : 0 : En cours 1 : OK Etat HSBY interne : 0 : Init 1 : Liaison établie 2 : Réservé 3 : Intégrité 4 : Attente de synchronisation 5. Synchronisé (n'apparaît pas sur la page Web)
Offset + 02	Octet de poids fort Validité du partenaire	Octet de poids faible réservé	Validité du partenaire : 0 : Injoignable 1 : OK
Offset + 03	Bit 31 - Bit 24	Bit 23 - Bit 16	Code d'erreur Bit 0 : Non-correspondance de micrologiciel Bit 1 : Configuration de DTM non concordante Bit 2 : Mode de sécurité non concordant Bit 3 : Erreur de certification Bit 4 : Configuration CS non concordante (réservé) Bits 5-31 : Réservé
Offset + 04	Bit 15 - Bit 8	Bit 7 - Bit 0	
Offset + 05	C03	C02	Compteur de synchronisation
Offset + 06	C01	C00	
Offset + 07	C03	C02	Heure de la dernière synchronisation horaire
Offset + 08	C01	C00	
Offset + 09	C01	C00	Date de la dernière synchronisation horaire
Offset + 10	C01	C00	Réservé
Offset + 11	C03	C02	Paquets d'entrée HSBY
Offset + 12	C01	C00	
Offset + 13	C03	C02	Paquets d'erreur d'entrée HSBY
Offset + 14	C01	C00	
Offset + 15	C03	C02	Paquets de sortie HSBY
Offset + 16	C01	C00	
Offset + 17	C03	C02	Paquets d'erreur de sortie HSBY
Offset + 18	C01	C00	
Offset + 19	IP 1	IP 2	Adresse IP locale
Offset + 20	IP 3	IP 4	

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset + 21	C03 Réservé	C02 Version majeure	Version du micrologiciel local
Offset + 22	C01 Version mineure	C00 Révision interne	
Offset + 23	Rôle distant octet de poids fort	Octet de poids faible Réservé	Rôle local : 0 : Inconnu 1 : Primaire 2 : Redondant
Offset + 24	C1	C0	Réservé
Offset + 25	C1	C0	Réservé
Offset + 26	IP 1	IP 2	Adresse IP distante
Offset + 27	IP 3	IP 4	
Offset + 28	C03 Réservé	C02 Version majeure	Version du micrologiciel distant
Offset + 29	C01 Version mineure	C00 Révision interne	
Offset + 30	Rôle distant octet de poids fort	Octet de poids faible réservé	Rôle distant : 0 : Primaire 1 : Redondant
Offset + 31	C01	C00	Réservé
Offset + 32	C01	C00	Réservé
Offset + 33	C01	C00	Réservé
Offset + 34	C01	C00	Réservé

Diagnostic du service de journalisation des données (offset 6526)

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset + 0	Octet de poids fort	Octet de poids faible	Octet de poids fort : Nombre de tables configurées : Octet de poids faible : Etat du service.
Offset + 1	Octet de poids fort	Octet de poids faible	Validation du nombre de tables.
Offset + 2	C03	C02	Espace libre sur la carte SD (Ko)
Offset + 3	C01	C00	
Offset + 4	Octet de poids fort	Octet de poids faible	Etat de la carte SD : Bit 0 : 1/0 : Carte SD normale/manquante Bit 1 : 1/0 : Carte SD occupée/non occupée Bit 2 : 1/0 : L'alarme d'espace faible est activée/désactivée.
Offset + 5	C01	C00	Réservé
Offset + 6	C01	C00	Réservé
Offset + 7	C01	C00	Réservé
Offset + 8	C01	C00	Réservé
Offset + 9	C01	C00	Réservé
Offset + 10	Octet de poids fort	Octet de poids faible	ID de la table
Offset + 11	Octet de poids fort	Octet de poids faible	Etat de la table : 0 : désactivé 1 : activé
Offset + 12	Octet de poids fort	Octet de poids faible	Etat du journal : 0 : aucune erreur 4 : pas d'espace mémoire 5 : variable non disponible 6 : table saturée 8 : erreur système
Offset + 13	Octet de poids fort	Octet de poids faible	Etat de la sauvegarde : 0 : aucune erreur détectée 1 : aucune carte SD compatible 2 : erreur du système de fichiers 3 : espace insuffisant sur la carte SD 7 : carte SD occupée 8 : erreur système
Offset + 14	C03	C02	Heure de la dernière sauvegarde
Offset + 15	C01	C00	
Offset + 16	C01	C00	Date de la dernière sauvegarde
Offset + 17	C01	C00	Réservé
Offset + 18	Octet de poids fort	Octet de poids faible	Nombre d'enregistrements dans la RAM
Offset + 19	Octet de poids fort	Octet de poids faible	Nombre de sauvegardes sur la carte SD
Offset + 20	C01	C00	Réservé
Offset + 21	C01	C00	Réservé
Offset + 22	C01	C00	Réservé
Offset + 23	C01	C00	Réservé
Offset + 24	C01	C00	Réservé
Offset + 25	C01	C00	Réservé
Offset + 26	C01	C00	Réservé
Offset + 27	C01	C00	Réservé

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset + 28	C01	C00	Réservé
Offset + 29	C01	C00	Réservé
Offset + 30	C01	C00	Réservé
Offset + 31	C01	C00	Réservé
...			
Offset + 10 + (X-1) * 22	Octet de poids fort	Octet de poids faible	ID de la table
Offset + 11 + (X-1) * 22	Octet de poids fort	Octet de poids faible	Etat de la table : 0 : désactivé 1 : activé
Offset + 12 + (X-1) * 22	Octet de poids fort	Octet de poids faible	Etat du journal : 0 : aucune erreur détectée 4 : pas d'espace mémoire 5 : variable non disponible, 6 : table saturée 7 : erreur de transfert 8 : erreur système
Offset + 13 + (X-1) * 22	Octet de poids fort	Octet de poids faible	Etat de la sauvegarde : 0 : aucune erreur détectée 1 : pas de carte SD 2 : erreur du système de fichiers 3 : espace insuffisant sur la carte SD 8 : erreur système
Offset + 14 + (X-1) * 22	C03	C02	Heure de la dernière sauvegarde
Offset + 15 + (X-1) * 22	C01	C00	
Offset + 16 + (X-1) * 22	C01	C00	Date de la dernière sauvegarde
Offset + 17 + (X-1) * 22	C01	C00	Réservé
Offset + 18 + (X-1) * 22	Octet de poids fort	Octet de poids faible	Nombre d'enregistrements en RAM
Offset + 19 + (X-1) * 22	Octet de poids fort	Octet de poids faible	Nombre de sauvegardes sur la carte SD
Offset + 20 + (X-1) * 22	C01	C00	Réservé
Offset + 21 + (X-1) * 22	C01	C00	Réservé
Offset + 22 + (X-1) * 22	C01	C00	Réservé
Offset + 23 + (X-1) * 22	C01	C00	Réservé
Offset + 24 + (X-1) * 22	C01	C00	Réservé
Offset + 25 + (X-1) * 22	C01	C00	Réservé
Offset + 26 + (X-1) * 22	C01	C00	Réservé
Offset + 27 + (X-1) * 22	C01	C00	Réservé
Offset + 28 + (X-1) * 22	C01	C00	Réservé
Offset + 29 + (X-1) * 22	C01	C00	Réservé
Offset + 30 + (X-1) * 22	C01	C00	Réservé

Diagnostic du service SNMP (offset 6471)

Adresse	Octet de poids fort	Octet de poids faible	Commentaires
Offset + 0	Octet de poids fort : Code d'erreur	Octet de poids faible : Etat du service	Etat du service : 0 : Inconnu 1 : Activé 2 : Fonctionnement correct 3 : Désactivé 4 : Non configuré 5 : Au moins une connexion est incorrecte 6 : Voyant d'activation allumé 7 : Voyant d'activation éteint Code d'erreur : Bit 8 - non-correspondance snmp Version DTM
Offset + 1	Octet de poids fort	Octet de poids faible	Version SNMP : 0 : V1 / 1 : V3 / 3 : Inconnu
Offset + 2	C03	C02	Paquets entrants SNMP
Offset + 3	C01	C00	
Offset + 4	C03	C02	
Offset + 5	C01	C00	Paquets sortants SNMP
Offset + 6	C03	C02	Versions incorrectes d'entrée SNMP
Offset + 7	C01	C00	
Offset + 8	C03	C02	
Offset + 9	C01	C00	SNMP V3 uniquement : USM Stats noms d'utilisateur inconnus
Offset + 10	C03	C02	SNMP V3 uniquement : USM entrée Communauté incorrecte utilisée
Offset + 11	C01	C00	
Offset + 12	C03	C02	
Offset + 13	C01	C00	Stats USM abrégés incorrects
Offset + 14	C03	C02	SNMP V3 uniquement : USM Modèles de sécurité inconnus
Offset + 15	C01	C00	

Codes d'erreur détectée

Présentation

Cette section contient une liste de codes décrivant l'état des messages du module de communication Ethernet.

Messagerie explicite : rapports de communication et d'opération

Présentation

Les rapports de communication et d'opération font partie des paramètres de gestion.

NOTE: Il est recommandé de tester les rapports sur la fonction de communication à la fin de leur exécution et avant l'activation suivante. Lors d'un démarrage à froid, vérifiez que tous les paramètres de gestion de la fonction de communication ont été vérifiés et remis à 0.

Examinez le premier cycle après un démarrage à froid ou à chaud. Voir *Ecostruxure™ Control Expert - Bits et mots système - Manuel de référence* (Documents à consulter).

Rapport de communication

Ce rapport est commun à toutes les fonctions de messagerie explicite. Il est pertinent lorsque la valeur du bit d'activité passe de 1 à 0. Les rapports dont la valeur est comprise entre 16#01 et 16#FE concernent les erreurs détectées par le processeur qui a exécuté la fonction.

Les différentes valeurs de ce rapport sont répertoriées dans le tableau suivant :

Valeur	Rapport de communication (octet de poids faible)
16#00	Echange correct
16#01	Echange arrêté suite à un timeout
16#02	Echange arrêté à la demande de l'utilisateur (ANNULER)
16#03	Format d'adresse incorrect
16#04	Adresse cible incorrecte
16#05	Format du paramètre Management incorrect
16#06	Paramètres spécifiques incorrects
16#07	Erreur détectée lors de l'envoi vers la destination
16#08	Réservé
16#09	Taille du tampon de réception insuffisante
16#0A	Taille du tampon d'envoi insuffisante
16#0B	Aucune ressource système : le nombre d'EF de communication simultanées dépasse le nombre maximum autorisé par le processeur
16#0C	Numéro d'échange incorrect
16#0D	Pas de réception de télégramme
16#0E	Longueur incorrecte
16#0F	Service de télégramme non configuré
16#10	Module réseau manquant
16#11	Requête manquante

Valeur	Rapport de communication (octet de poids faible)
16#12	Serveur d'application déjà actif
16#13	Numéro de transaction UNI-TE V2 incorrect
16#FF	Message refusé

NOTE: la fonction peut détecter une erreur de paramètre avant d'activer l'échange. Dans ce cas, le bit d'activité reste à 0 et le compte rendu est initialisé avec les valeurs correspondant à l'erreur.

Rapport d'opération

Ce rapport est spécifique de chaque fonction. Il indique le résultat de l'opération effectuée sur l'application distante :

Valeur	Rapport d'opération (octet de poids fort)
16#05	Longueurs différentes (CIP)
16#07	Adresse IP incorrecte
16#08	Erreur d'application
16#09	Réseau arrêté
16#0A	Réinitialisation connexion par pair
16#0C	Fonction de communication non active
16#0D	- Modbus TCP : timeout de transaction - EtherNet/IP : timeout de la requête
16#0F	Pas de routage vers l'hôte distant
16#13	Connexion refusée
16#15	- Modbus TCP : aucune ressource - EtherNet/IP : aucune ressource pour traiter le message ; ou événement interne ; ou aucun tampon disponible ; ou aucune liaison disponible ; ou impossibilité d'envoi du message
16#16	Adresse distante non autorisée
16#18	- Modbus TCP : limite du nombre de connexions ou de transactions simultanées atteinte - EtherNet/IP : Session de connexion ou d'encapsulation TCP en cours
16#19	Connexion expirée
16#22	Modbus TCP : réponse incorrecte
16#23	Modbus TCP : réponse de l'ID d'équipement incorrecte
16#30	- Modbus TCP : hôte distant arrêté - EtherNet/IP : timeout de la connexion établie
16#80 à 16#87 : Erreurs détectées de réponse Forward_Open :	
16#80	Erreur interne détectée :
16#81	la longueur du message explicite ou l'intervalle de trame demandé (RPI) doit être ajusté
16#82	Événement d'équipement : l'équipement cible ne prend pas ce service en charge
16#83	Événement de ressource matérielle : aucune ressource disponible pour ouvrir la connexion
16#84	Événement de ressource système : impossible d'atteindre l'équipement
16#85	Événement de fiche de données : fichier EDS incorrect
16#86	Taille de connexion non valide
16#90 à 16#9F : Erreurs détectées de réponse de session de registre :	
16#90	L'équipement cible n'a pas assez de ressources

Valeur	Rapport d'opération (octet de poids fort)
16#98	L'équipement cible ne reconnaît pas l'en-tête d'encapsulation du message
16#9F	Erreur inconnue détectée à partir de la cible

Codes d'erreur détectée pour la communication RTU

Introduction

Les tableaux ci-après décrivent les codes correspondant aux erreurs détectées pour les normes de communication DNP3 et IEC60870.

Codes d'erreur détectée DNP3

Code d'erreur détectée	Description
0x0000	Aucune erreur détectée
0x0001	Sécurité non configurée
0x0002	Erreur détectée d'initialisation de variable non localisée
0x0004	Erreur interne détectée
0X0008	Problème d'authentification détecté
0x0010	Réponse inattendue
0x0020	Pas de réponse
0x0040	Mode agressif non pris en charge
0x0080	Algorithme MAC non pris en charge
0x0100	Algorithme d'enveloppe de clé non pris en charge
0x0200	Problème d'autorisation détecté
0x0400	Méthode de modification de clé de mise à jour non autorisée
0x0800	Signature non valide
0x1000	Données de certification non valides
0x2000	Utilisateur inconnu
0x4000	Nombre maximum de requêtes d'état de clé de session dépassé
0x8000	Erreur TLS

Codes d'erreur détectée de communication IEC60870

Code d'erreur détectée	Description
0x0000	Aucune erreur détectée
0x0001	Sécurité non configurée
0x0002	Erreur détectée d'initialisation de variable non localisée
0x0004	Erreur interne détectée
0X0008	Erreur TLS

Codes d'erreur détectée pour Open SSL/TLS

Introduction

Cette section décrit les codes d'erreur Open SSL/TLS qui peuvent être détectés dans un système M580 avec un module BMENOR2200H.

Codes d'erreur détectée pour Open SSL/TLS

Codes d'erreur détectée

Erreur détectée	Code
SSL_R_APP_DATA_IN_HANDSHAKE	100
SSL_R_ATTEMPT_TO_REUSE_SESSION_IN_DIFFERENT_CONTEXT	272
SSL_R_BAD_ALERT_RECORD	101
SSL_R_BAD_AUTHENTICATION_TYPE	102
SSL_R_BAD_CHANGE_CIPHER_SPEC	103
SSL_R_BAD_CHECKSUM	104
SSL_R_BAD_DATA	390
SSL_R_BAD_DATA_RETURNED_BY_CALLBACK	106
SSL_R_BAD_DECOMPRESSION	107
SSL_R_BAD_DH_G_LENGTH	108
SSL_R_BAD_DH_G_VALUE	375
SSL_R_BAD_DH_PUB_KEY_LENGTH	109
SSL_R_BAD_DH_PUB_KEY_VALUE	393
SSL_R_BAD_DH_P_LENGTH	110
SSL_R_BAD_DH_P_VALUE	395
SSL_R_BAD_DIGEST_LENGTH	111
SSL_R_BAD_DSA_SIGNATURE	112
SSL_R_BAD_ECC_CERT	304
SSL_R_BAD_ECDSA_SIGNATURE	305
SSL_R_BAD_ECPOINT	306
SSL_R_BAD_HANDSHAKE_LENGTH	332
SSL_R_BAD_HELLO_REQUEST	105
SSL_R_BAD_LENGTH	271
SSL_R_BAD_MAC_DECODE	113
SSL_R_BAD_MAC_LENGTH	333
SSL_R_BAD_MESSAGE_TYPE	114
SSL_R_BAD_PACKET_LENGTH	115
SSL_R_BAD_PROTOCOL_VERSION_NUMBER	116
SSL_R_BAD_PSK_IDENTITY_HINT_LENGTH	316
SSL_R_BAD_RESPONSE_ARGUMENT	117
SSL_R_BAD_RSA_DECRYPT	118
SSL_R_BAD_RSA_ENCRYPT	119

Erreur détectée	Code
SSL_R_BAD_RSA_E_LENGTH	120
SSL_R_BAD_RSA_MODULUS_LENGTH	121
SSL_R_BAD_RSA_SIGNATURE	122
SSL_R_BAD_SIGNATURE	123
SSL_R_BAD_SRP_A_LENGTH	347
SSL_R_BAD_SRP_B_LENGTH	348
SSL_R_BAD_SRP_G_LENGTH	349
SSL_R_BAD_SRP_N_LENGTH	350
SSL_R_BAD_SRP_PARAMETERS	371
SSL_R_BAD_SRP_S_LENGTH	351
SSL_R_BAD_SRTP_MKI_VALUE	352
SSL_R_BAD_SRTP_PROTECTION_PROFILE_LIST	353
SSL_R_BAD_SSL_FILETYPE	124
SSL_R_BAD_SSL_SESSION_ID_LENGTH	125
SSL_R_BAD_STATE	126
SSL_R_BAD_VALUE	384
SSL_R_BAD_WRITE_RETRY	127
SSL_R_BIO_NOT_SET	128
SSL_R_BLOCK_CIPHER_PAD_IS_WRONG	129
SSL_R_BN_LIB	130
SSL_R_CA_DN_TOO_LONG	132
SSL_R_CCS_RECEIVED_EARLY	133
SSL_R_CERTIFICATE_VERIFY_FAILED	134
SSL_R_CERT_LENGTH_MISMATCH	135
SSL_R_CHALLENGE_IS_DIFFERENT	136
SSL_R_CIPHER_CODE_WRONG_LENGTH	137
SSL_R_CIPHER_OR_HASH_UNAVAILABLE	138
SSL_R_CIPHER_TABLE_SRC_ERROR	139
SSL_R_CLIENTHELLO_TLSEXT	226
SSL_R_COMPRESSED_LENGTH_TOO_LONG	140
SSL_R_COMPRESSION_DISABLED	343
SSL_R_COMPRESSION_FAILURE	141
SSL_R_COMPRESSION_ID_NOT_WITHIN_PRIVATE_RANGE	307
SSL_R_COMPRESSION_LIBRARY_ERROR	142
SSL_R_CONNECTION_ID_IS_DIFFERENT	143
SSL_R_CONNECTION_TYPE_NOT_SET	144
SSL_R_COOKIE_MISMATCH	308
SSL_R_DATA_BETWEEN_CCS_AND_FINISHED	145
SSL_R_DATA_LENGTH_TOO_LONG	146
SSL_R_DECRYPTION_FAILED	147
SSL_R_DECRYPTION_FAILED_OR_BAD_RECORD_MAC	281
SSL_R_DH_KEY_TOO_SMALL	372

Erreur détectée	Code
SSL_R_DH_PUBLIC_VALUE_LENGTH_IS_WRONG	148
SSL_R_DIGEST_CHECK_FAILED	149
SSL_R_DTLS_MESSAGE_TOO_BIG	334
SSL_R_DUPLICATE_COMPRESSION_ID	309
SSL_R_ECC_CERT_NOT_FOR_KEY_AGREEMENT	317
SSL_R_ECC_CERT_NOT_FOR_SIGNING	318
SSL_R_ECC_CERT_SHOULD_HAVE_RSA_SIGNATURE	322
SSL_R_ECC_CERT_SHOULD_HAVE_SHA1_SIGNATURE	323
SSL_R_ECDH_REQUIRED_FOR_SUITEB_MODE	374
SSL_R_ECGROUP_TOO_LARGE_FOR_CIPHER	310
SSL_R_EMPTY_SRTP_PROTECTION_PROFILE_LIST	354
SSL_R_ENCRYPTED_LENGTH_TOO_LONG	150
SSL_R_ERROR_GENERATING_TMP_RSA_KEY	282
SSL_R_ERROR_IN_RECEIVED_CIPHER_LIST	151
SSL_R_EXCESSIVE_MESSAGE_SIZE	152
SSL_R_EXTRA_DATA_IN_MESSAGE	153
SSL_R_GOT_A_FIN_BEFORE_A_CCS	154
SSL_R_GOT_NEXT_PROTO_BEFORE_A_CCS	355
SSL_R_GOT_NEXT_PROTO_WITHOUT_EXTENSION	356
SSL_R_HTTPS_PROXY_REQUEST	155
SSL_R_HTTPS_REQUEST	156
SSL_R_ILLEGAL_PADDING	283
SSL_R_ILLEGAL_SUITEB_DIGEST	380
SSL_R_INAPPROPRIATE_FALLBACK	373
SSL_R_INCONSISTENT_COMPRESSION	340
SSL_R_INVALID_CHALLENGE_LENGTH	158
SSL_R_INVALID_COMMAND	280
SSL_R_INVALID_COMPRESSION_ALGORITHM	341
SSL_R_INVALID_NULL_CMD_NAME	385
SSL_R_INVALID_PURPOSE	278
SSL_R_INVALID_SERVERINFO_DATA	388
SSL_R_INVALID_SRP_USERNAME	357
SSL_R_INVALID_STATUS_RESPONSE	328
SSL_R_INVALID_TICKET_KEYS_LENGTH	325
SSL_R_INVALID_TRUST	279
SSL_R_KEY_ARG_TOO_LONG	284
SSL_R_KRB5	285
SSL_R_KRB5_C_CC_PRINC	286
SSL_R_KRB5_C_GET_CRED	287
SSL_R_KRB5_C_INIT	288
SSL_R_KRB5_C_MK_REQ	289
SSL_R_KRB5_S_BAD_TICKET	290

Erreur détectée	Code
SSL_R_KRB5_S_INIT	291
SSL_R_KRB5_S_RD_REQ	292
SSL_R_KRB5_S_TKT_EXPIRED	293
SSL_R_KRB5_S_TKT_NYV	294
SSL_R_KRB5_S_TKT_SKEW	295
SSL_R_LENGTH_MISMATCH	159
SSL_R_LENGTH_TOO_LONG	404
SSL_R_LENGTH_TOO_SHORT	160
SSL_R_LIBRARY_BUG	274
SSL_R_LIBRARY_HAS_NO_CIPHERS	161
SSL_R_MESSAGE_TOO_LONG	296
SSL_R_MISSING_DH_DSA_CERT	162
SSL_R_MISSING_DH_KEY	163
SSL_R_MISSING_DH_RSA_CERT	164
SSL_R_MISSING_DSA_SIGNING_CERT	165
SSL_R_MISSING_ECDH_CERT	382
SSL_R_MISSING_ECDSA_SIGNING_CERT	382
SSL_R_MISSING_EXPORT_TMP_DH_KEY	166
SSL_R_MISSING_EXPORT_TMP_RSA_KEY	167
SSL_R_MISSING_RSA_CERTIFICATE	168
SSL_R_MISSING_RSA_ENCRYPTIG_CERT	169
SSL_R_MISSING_RSA_SIGNING_CERT	170
SSL_R_MISSING_SRP_PARAM	358
SSL_R_MISSING_TMP_DH_KEY	171
SSL_R_MISSING_TMP_ECDH_KEY	311
SSL_R_MISSING_TMP_RSA_KEY	172
SSL_R_MISSING_TMP_RSA_PKEY	173
SSL_R_MISSING_VERIFY_MESSAGE	174
SSL_R_MULTIPLE_SGC_RESTARTS	346
SSL_R_NON_SSLV2_INITIAL_PACKET	175
SSL_R_NO_CERTIFICATES_RETURNED	176
SSL_R_NO_CERTIFICATE_ASSIGNED	177
SSL_R_NO_CERTIFICATE_RETURNED	178
SSL_R_NO_CERTIFICATE_SET	179
SSL_R_NO_CERTIFICATE_SPECIFIED	180
SSL_R_NO_CIPHERS_AVAILABLE	181
SSL_R_NO_CIPHERS_PASSED	182
SSL_R_NO_CIPHERS_SPECIFIED	183
SSL_R_NO_CIPHER_LIST	184
SSL_R_NO_CIPHER_MATCH	185
SSL_R_NO_CLIENT_CERT_METHOD	331
SSL_R_NO_CLIENT_CERT_RECEIVED	186

Erreur détectée	Code
SSL_R_NO_COMPRESSION_SPECIFIED	187
SSL_R_NO_GOST_CERTIFICATE_SENT_BY_PEER	330
SSL_R_NO_METHOD_SPECIFIED	188
SSL_R_NO_PEM_EXTENSIONS	389
SSL_R_NO_PRIVATEKEY	189
SSL_R_NO_PRIVATE_KEY_ASSIGNED	190
SSL_R_NO_PROTOCOLS_AVAILABLE	191
SSL_R_NO_PUBLICKEY	192
SSL_R_NO_RENEGOTIATION	339
SSL_R_NO_REQUIRED_DIGEST	324
SSL_R_NO_SHARED_CIPHER	193
SSL_R_NO_SHARED_SIGNATURE_ALGORITHMS	376
SSL_R_NO_SRTP_PROFILES	359
SSL_R_NO_VERIFY_CALLBACK	194
SSL_R_NULL_SSL_CTX	195
SSL_R_NULL_SSL_METHOD_PASSED	196
SSL_R_OLD_SESSION_CIPHER_NOT_RETURNED	197
SSL_R_OLD_SESSION_COMPRESSION_ALGORITHM_NOT_RETURNED	344
SSL_R_ONLY_DTLS_1_2_ALLOWED_IN_SUITEB_MODE	387
SSL_R_ONLY_TLS_1_2_ALLOWED_IN_FIPS_MODE	297
SSL_R_OPAQUE_PRF_INPUT_TOO_LONG	327
SSL_R_PACKET_LENGTH_TOO_LONG	198
SSL_R_PARSE_TLSEXT	227
SSL_R_PATH_TOO_LONG	270
SSL_R_PEER_DID_NOT_RETURN_A_CERTIFICATE	199
SSL_R_PEER_ERROR	200
SSL_R_PEER_ERROR_CERTIFICATE	201
SSL_R_PEER_ERROR_NO_CERTIFICATE	202
SSL_R_PEER_ERROR_NO_CIPHER	203
SSL_R_PEER_ERROR_UNSUPPORTED_CERTIFICATE_TYPE	204
SSL_R_PEM_NAME_BAD_PREFIX	391
SSL_R_PEM_NAME_TOO_SHORT	392
SSL_R_PRE_MAC_LENGTH_TOO_LONG	205
SSL_R_PROBLEMS_MAPPING_CIPHER_FUNCTIONS	206
SSL_R_PROTOCOL_IS_SHUTDOWN	207
SSL_R_PSK_IDENTITY_NOT_FOUND	223
SSL_R_PSK_NO_CLIENT_CB	224
SSL_R_PSK_NO_SERVER_CB	225
SSL_R_PUBLIC_KEY_ENCRYPT_ERROR	208
SSL_R_PUBLIC_KEY_IS_NOT_RSA	209
SSL_R_PUBLIC_KEY_NOT_RSA	210
SSL_R_READ_BIO_NOT_SET	211

Erreur détectée	Code
SSL_R_READ_TIMEOUT_EXPIRED	312
SSL_R_READ_WRONG_PACKET_TYPE	212
SSL_R_RECORD_LENGTH_MISMATCH	213
SSL_R_RECORD_TOO_LARGE	214
SSL_R_RECORD_TOO_SMALL	298
SSL_R_RENEGOTIATE_EXT_TOO_LONG	335
SSL_R_RENEGOTIATION_ENCODING_ERR	336
SSL_R_RENEGOTIATION_MISMATCH	337
SSL_R_REQUIRED_CIPHER_MISSING	215
SSL_R_REQUIRED_COMPRESSION_ALGORITHM_MISSING	342
SSL_R_REUSE_CERT_LENGTH_NOT_ZERO	216
SSL_R_REUSE_CERT_TYPE_NOT_ZERO	217
SSL_R_REUSE_CIPHER_LIST_NOT_ZERO	218
SSL_R_SCSV_RECEIVED_WHEN_RENEGOTIATING	345
SSL_R_SERVERHELLO_TLSEXT	275
SSL_R_SESSION_ID_CONTEXT_UNINITIALIZED	277
SSL_R_SHORT_READ	219
SSL_R_SHUTDOWN_WHILE_IN_INIT	407
SSL_R_SIGNATURE_ALGORITHMS_ERROR	360
SSL_R_SIGNATURE_FOR_NON_SIGNING_CERTIFICATE	220
SSL_R_SRP_A_CALC	361
SSL_R_SRTCP_COULD_NOT_ALLOCATE_PROFILES	362
SSL_R_SRTCP_PROTECTION_PROFILE_LIST_TOO_LONG	363
SSL_R_SRTCP_UNKNOWN_PROTECTION_PROFILE	364
SSL_R_DOING_SESSION_ID_REUSE	221
SSL_R_CONNECTION_ID_TOO_LONG	299
SSL_R_SSL3_EXT_INVALID_ECPOINTFORMAT	321
SSL_R_SSL3_EXT_INVALID_SERVERNAME	319
SSL_R_SSL3_EXT_INVALID_SERVERNAME_TYPE	320
SSL_R_SSL3_SESSION_ID_TOO_LONG	300
SSL_R_SSL3_SESSION_ID_TOO_SHORT	222
SSL_R_SSLV3_ALERT_BAD_CERTIFICATE	1042
SSL_R_SSLV3_ALERT_BAD_RECORD_MAC	1020
SSL_R_SSLV3_ALERT_CERTIFICATE_EXPIRED	1045
SSL_R_SSLV3_ALERT_CERTIFICATE_REVOKED	1044
SSL_R_SSLV3_ALERT_CERTIFICATE_UNKNOWN	1046
SSL_R_SSLV3_ALERT_DECOMPRESSION_FAILURE	1030
SSL_R_SSLV3_ALERT_HANDSHAKE_FAILURE	1040
SSL_R_SSLV3_ALERT_ILLEGAL_PARAMETER	1047
SSL_R_SSLV3_ALERT_NO_CERTIFICATE	1041
SSL_R_SSLV3_ALERT_UNEXPECTED_MESSAGE	1010
SSL_R_SSLV3_ALERT_UNSUPPORTED_CERTIFICATE	1043

Erreur détectée	Code
SSL_R_SSL_CTX_HAS_NO_DEFAULT_SSL_VERSION	228
SSL_R_SSL_HANDSHAKE_FAILURE	229
SSL_R_SSL_LIBRARY_HAS_NO_CIPHERS	230
SSL_R_SSL_SESSION_ID_CALLBACK_FAILED	301
SSL_R_SSL_SESSION_ID_CONFLICT	302
SSL_R_SSL_SESSION_ID_CONTEXT_TOO_LONG	273
SSL_R_SSL_SESSION_ID_HAS_BAD_LENGTH	303
SSL_R_SSL_SESSION_ID_IS_DIFFERENT	231
SSL_R_TLSV1_ALERT_ACCESS_DENIED	1049
SSL_R_TLSV1_ALERT_DECODE_ERROR	1050
SSL_R_TLSV1_ALERT_DECRYPTION_FAILED	1021
SSL_R_TLSV1_ALERT_DECRYPT_ERROR	1051
SSL_R_TLSV1_ALERT_EXPORT_RESTRICTION	1060
SSL_R_TLSV1_ALERT_INAPPROPRIATE_FALLBACK	1086
SSL_R_TLSV1_ALERT_INSUFFICIENT_SECURITY	1071
SSL_R_TLSV1_ALERT_INTERNAL_ERROR	1080
SSL_R_TLSV1_ALERT_NO_RENEGOTIATION	1100
SSL_R_TLSV1_ALERT_PROTOCOL_VERSION	1070
SSL_R_TLSV1_ALERT_RECORD_OVERFLOW	1022
SSL_R_TLSV1_ALERT_UNKNOWN_CA	1048
SSL_R_TLSV1_ALERT_USER_CANCELED	1090
SSL_R_TLSV1_BAD_CERTIFICATE_HASH_VALUE	1114
SSL_R_TLSV1_BAD_CERTIFICATE_STATUS_RESPONSE	1113
SSL_R_TLSV1_CERTIFICATE_UNOBTAINABLE	1111
SSL_R_TLSV1_UNRECOGNIZED_NAME	1112
SSL_R_TLSV1_UNSUPPORTED_EXTENSION	1110
SSL_R_TLS_CLIENT_CERT_REQ_WITH_ANON_CIPHER	232
SSL_R_TLS_HEARTBEAT_PEER_DOESNT_ACCEPT	365
SSL_R_TLS_HEARTBEAT_PENDING	366
SSL_R_TLS_ILLEGAL_EXPORTER_LABEL	367
SSL_R_TLS_INVALID_ECPOINTFORMAT_LIST	157
SSL_R_TLS_PEER_DID_NOT_RESPOND_WITH_CERTIFICATE_LIST	233
SSL_R_TLS_RSA_ENCRYPTED_VALUE_LENGTH_IS_WRONG	234
SSL_R_TOO_MANY_WARN_ALERTS	409
SSL_R_TRIED_TO_USE_UNSUPPORTED_CIPHER	235
SSL_R_UNABLE_TO_DECODE_DH_CERTS	236
SSL_R_UNABLE_TO_DECODE_ECDH_CERTS	313
SSL_R_UNABLE_TO_EXTRACT_PUBLIC_KEY	237
SSL_R_UNABLE_TO_FIND_DH_PARAMETERS	238
SSL_R_UNABLE_TO_FIND_ECDH_PARAMETERS	314
SSL_R_UNABLE_TO_FIND_PUBLIC_KEY_PARAMETERS	239
SSL_R_UNABLE_TO_FIND_SSL_METHOD	240

Erreur détectée	Code
SSL_R_UNABLE_TO_LOAD_SSL2_MD5_ROUTINES	241
SSL_R_UNABLE_TO_LOAD_SSL3_MD5_ROUTINES	242
SSL_R_UNABLE_TO_LOAD_SSL3_SHA1_ROUTINES	243
SSL_R_UNEXPECTED_MESSAGE	244
SSL_R_UNEXPECTED_RECORD	245
SSL_R_UNINITIALIZED	276
SSL_R_UNKNOWN_ALERT_TYPE	246
SSL_R_UNKNOWN_CERTIFICATE_TYPE	247
SSL_R_UNKNOWN_CIPHER_RETURNED	248
SSL_R_UNKNOWN_CIPHER_TYPE	249
SSL_R_UNKNOWN_CMD_NAME	386
SSL_R_UNKNOWN_DIGEST	368
SSL_R_UNKNOWN_KEY_EXCHANGE_TYPE	250
SSL_R_UNKNOWN_PKEY_TYPE	251
SSL_R_UNKNOWN_PROTOCOL	252
SSL_R_UNKNOWN_REMOTE_ERROR_TYPE	253
SSL_R_UNKNOWN_SSL_VERSION	254
SSL_R_UNKNOWN_STATE	255
SSL_R_UNSAFE_LEGACY_RENEGOTIATION_DISABLED	338
SSL_R_UNSUPPORTED_CIPHER	256
SSL_R_UNSUPPORTED_COMPRESSION_ALGORITHM	257
SSL_R_UNSUPPORTED_DIGEST_TYPE	326
SSL_R_UNSUPPORTED_ELLIPTIC_CURVE	315
SSL_R_UNSUPPORTED_PROTOCOL	258
SSL_R_UNSUPPORTED_SSL_VERSION	259
SSL_R_UNSUPPORTED_STATUS_TYPE	329
SSL_R_USE_SRTP_NOT_NEGOTIATED	369
SSL_R_WRITE_BIO_NOT_SET	260
SSL_R_WRONG_CERTIFICATE_TYPE	383
SSL_R_WRONG_CIPHER_RETURNED	261
SSL_R_WRONG_CURVE	378
SSL_R_WRONG_MESSAGE_TYPE	262
SSL_R_WRONG_NUMBER_OF_KEY_BITS	263
SSL_R_WRONG_SIGNATURE_LENGTH	264
SSL_R_WRONG_SIGNATURE_SIZE	265
SSL_R_WRONG_SIGNATURE_TYPE	370
SSL_R_WRONG_SSL_VERSION	266
SSL_R_WRONG_VERSION_NUMBER	267
SSL_R_X509_LIB	268
SSL_R_X509_VERIFICATION_SETUP_PROBLEMS	269

Compatibilité des versions de micrologiciel

Introduction

Cette section décrit l'historique des versions de micrologiciel du module BMENOR2200H et leur compatibilité avec Control Expert.

Compatibilité des versions de micrologiciel

Compatibilité amont

Le module BMENOR2200H prend en charge la compatibilité vers l'amont. Autrement dit, les nouvelles versions du micrologiciel peuvent exécuter d'anciennes applications, mais les nouvelles applications ne peuvent pas télécharger les anciennes versions de micrologiciel sur le module :

Version du logiciel	Control Expert 14.0	Control Expert 15.0	Control Expert 15.1	Control Expert 15.3
1.0	OK	Héritage	Héritage	Héritage
2.01	OK	OK	Héritage	Héritage
3.01	OK	OK	OK	Héritage
4.01	OK	OK	OK	OK

Légende :

- **OK** : Toutes les versions de micrologiciel sont compatibles avec le numéro de version de logiciel correspondant.
- **Héritage** : Les fonctionnalités héritées sont compatibles avec le numéro de version de logiciel correspondant. (Le téléchargement de nouvelles fonctions vers cette version de logiciel sur le module provoque des erreurs d'application.)

Mise à jour d'application depuis BMENOR2200.2

Pour le module BMENOR2200H, il est possible d'appliquer un nouveau matériel et un nouveau logiciel à une configuration existante. Lorsqu'il est nécessaire d'activer le port de contrôle à partir d'une ancienne configuration, un module BMENOR2200H.3 doit être configuré pour remplacer le module BMENOR2200H.2.

L'outil de mise à jour d'application M580 fournit une méthode qui facilite la mise à niveau d'une application groupée pour des modules BMENOR2200H.2 (sans port de contrôle) vers des modules BMENOR2200H.3 (avec port de contrôle)

NOTE:

1. Le nouveau module avec port de contrôle peut remplacer directement l'ancien module sans port de contrôle dans un système en cours d'exécution. Le nouveau matériel peut fonctionner sur l'ancienne configuration, mais le port de contrôle est automatiquement désactivé. Dans les cas de redondance d'UC (HSBY), le micrologiciel des deux modules BMENOR doit être mis à niveau vers la même version, même si le matériel est de type différent.
2. Le logiciel minimal pour le module avec port de contrôle est la version 4.01.
3. Une configuration comportant des fonctionnalités nouvelles ne peut pas être téléchargée vers un micrologiciel plus ancien. Les nouvelles fonctionnalités ne fonctionneraient pas (défaillance d'application). Sélectionnez la version de micrologiciel correcte dans le DTM avant de procéder à la configuration.

Glossaire

B

bridge:

A bridge device connects two or more physical networks that use the same protocol. Bridges read frames and decide whether to transmit or block them based on their destination address.

D

DFB:

(*derived function block*) DFB types are function blocks that can be defined by the user in ST, IL, LD or FBD language.

Using these DFB types in an application makes it possible to:

- simplify the design and entry of the program
- make the program easier to read
- make it easier to debug
- reduce the amount of code generated

DTM:

Acronyme de *device type manager* DTM (gestionnaire de type d'équipement). Pilote d'équipement exécuté sur le PC hôte. Il offre une structure unifiée pour accéder aux paramètres de l'équipement, le configurer et l'utiliser, et pour remédier aux problèmes. Les DTM peuvent présenter différents visages, d'une simple interface graphique permettant de configurer les paramètres de l'équipement jusqu'à une application très perfectionnée susceptible d'effectuer des calculs complexes en temps réel à des fins de diagnostic et de maintenance. Dans le contexte d'un DTM, un équipement peut être un module de communication ou un équipement distant sur le réseau.

Voir FDT.

E

EFB:

Acronyme de *elementary function block* (bloc fonction élémentaire). Bloc utilisé dans un programme pour réaliser une fonction logique prédéfinie.

Les EFB possèdent des états et des paramètres internes. Même si les entrées sont identiques, les valeurs des sorties peuvent différer. Par exemple, un compteur possède une sortie qui indique que la valeur de présélection est atteinte. Cette sortie est définie sur 1 lorsque la dernière valeur implémentée est égale à la valeur de présélection.

environnement difficile:

Résistance aux hydrocarbures, aux huiles industrielles, aux détergents et aux copeaux de brasure. Humidité relative jusqu'à 100 %, atmosphère saline, fortes variations de température, température de fonctionnement comprise entre -10 °C et +70 °C ou installations mobiles. Pour les équipements renforcés (H), l'humidité relative peut atteindre 95 % et la température de fonctionnement est comprise entre -25 °C et +70 °C.

EtherNet/IP:

Protocole de communication réseau pour les applications d'automatisation industrielle, qui combine les protocoles de transmission Internet standard TCP/IP et UDP et le protocole CIP de couche applicative pour prendre en charge l'échange de données à haut débit et la commande industrielle. EtherNet/IP utilise des fiches de données électroniques (EDS) pour classer chaque équipement réseau et ses fonctionnalités.

Ethernet:

Spécification de câblage et de signalisation pour réseau local (LAN) utilisée pour connecter des équipements dans une zone définie, par exemple un bâtiment. Ethernet utilise un bus ou une topologie en étoile pour connecter différents nœuds sur un réseau.

F**FDR:**

(*fast device replacement*) A service that uses configuration software to replace an inoperable product.

I**IP address:**

The 32-bit identifier, consisting of both a network address and a host address assigned to a device connected to a TCP/IP network.

M**MAC address:**

media access control address. A 48-bit number, unique on a network, that is programmed into each network card or device when it is manufactured.

masque de sous-réseau:

Le masque de sous-réseau est un masque de 32 bits qui identifie ou détermine quels bits d'une adresse IP correspondent à l'adresse réseau et quels bits correspondent aux parties de sous-réseau de l'adresse. Le masque de sous-réseau comprend l'adresse de réseau plus les bits réservés pour l'identification du sous-réseau.

MB/TCP:

(*Modbus over TCP protocol*) This is a Modbus variant used for communications over TCP/IP networks.

P**passerelle:**

Équipement reliant des réseaux dont l'architecture est différente et qui fonctionne sur la couche application du modèle OSI. Ce terme peut désigner un routeur.

Une passerelle interconnecte deux réseaux, parfois à l'aide de différents protocoles réseau. Lorsqu'elle connecte des réseaux utilisant différents protocoles, la passerelle convertit un datagramme d'une pile de protocole dans l'autre. Lorsqu'elle connecte deux réseaux IP, la passerelle (également appelée routeur) dispose de deux adresses IP distinctes (une sur chaque réseau).

PLC:

programmable logic controller. The PLC is the brain of an industrial manufacturing process. It automates a process as opposed to relay control systems. PLCs are computers suited to survive the harsh conditions of the industrial environment.

port 502:

TCP/IP reserves specific server ports for specific applications through IANA (Internet Assigned Numbers Authority). Modbus requests are sent to registered software port 502.

R

rack local:

Rack M580 contenant le contrôleur et une alimentation. Un rack local se compose d'un ou de deux racks : le rack principal et le rack étendu qui appartient à la même famille que le rack principal. Le rack étendu est facultatif.

Redondance d'UC (Hot Standby):

Un système de redondance d'UC comprend un PAC primaire (automate) et un PAC redondant. Les configurations matérielle et logicielle sont identiques pour les deux racks PAC. Le PAC redondant surveille l'état du système du PAC primaire. Lorsque le PAC primaire n'est plus opérationnel, un contrôle de haute disponibilité est assuré tandis que le PAC redondant prend la main sur le système.

Réseau RIO:

Réseau Ethernet contenant trois types d'équipements d'E/S distantes (RIO) : un rack local, une station d'E/S distantes RIO et un commutateur double anneau ConneXium étendu (DRS). Un équipement distribué peut également faire partie d'un réseau RIO via une connexion à des DRSs ou des modules de sélection d'options de réseau BMENOS0300.

router:

A router device connects two or more sections of a network and allows information to flow between them. A router examines every packet it receives and decides whether to block the packet from the rest of the network or transmit it. The router attempts to send the packet through the network on an efficient path.

S

Serveur HTTPS:

Le serveur HTTPS installé transmet des pages Web entre un serveur et un navigateur, ce qui permet aux modules de communication Ethernet d'accéder facilement à des équipements situés partout dans le monde à partir de navigateurs standard comme Internet Explorer ou Netscape Navigator.

SNMP agent:

The SNMP application that runs on a network device.

SNMP:

(simple network management protocol) Protocol used in network management systems to monitor network-attached devices. The protocol is part of the internet protocol suite (IP) as defined by the internet engineering task force (IETF), which consists of network management guidelines, including an application layer protocol, a database schema, and a set of data objects.

SNTP:

(simple network time protocol) See NTP.

SOE:

(sequence of events) SOE software helps users understand a chain of occurrences that can lead to unsafe process conditions and possible shutdowns. SOEs can be critical to resolving or preventing such conditions.

subnet:

The subnet is that portion of the network that shares a network address with the other parts of the network. A subnet may be physically or logically independent from the rest of the network. A part of an Internet address called a subnet number, which is ignored in IP routing, distinguishes the subnet.

switch:

A network switch connects two or more separate network segments and allows traffic to be passed between them. A switch determines whether a frame should be blocked or transmitted based on its destination address.

T

Trap (déroutement):

Un déroutement est un événement dirigé par un agent SNMP qui indique l'un des événements suivants :

- L'état d'un agent a changé.
- Un équipement gestionnaire SNMP non autorisé a tenté d'obtenir (ou de modifier) des données d'un agent SMTP.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

Les normes, spécifications et conceptions pouvant changer de temps à autre, veuillez demander la confirmation des informations figurant dans cette publication.

© 2023 Schneider Electric. Tous droits réservés.

EIO0000004870.01