Modicon TMS

Modules d'extension

Guide de programmation

EIO0000003692.04
12/2023

www.se.com

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.

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

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.

A propos de ce manuel

Objet du document

Ce document décrit la configuration des modules d'extension TMS pour EcoStruxure Machine Expert. Pour plus d'informations, consultez les documents fournis dans l'aide en ligne de EcoStruxure Machine Expert.

Champ d'application

Ce document a été actualisé pour le lancement de EcoStruxure™ Machine Expert V2.2.

Les caractéristiques décrites dans le présent document, ainsi que celles décrites dans les documents mentionnés dans la section Documents associés ci-dessous, sont consultables en ligne. Pour accéder aux informations en ligne, allez sur la page d'accueil de Schneider Electric www.se.com/ww/fr/download/.

Les caractéristiques décrites dans le présent document doivent être identiques à celles fournies en ligne. Toutefois, en application de notre politique 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 le document et les informations fournies en ligne, utilisez ces dernières en priorité.

Document(s) à consulter

Titre du document	Numéro de référence
EcoStruxure Machine Expert - Guide de programmation	EIO0000002854 (ENG) EIO0000002855 (FRE) EIO0000002856 (GER) EIO0000002858 (SPA) EIO0000002857 (ITA) EIO0000002859 (CHS)
Modicon M262 Logic/Motion Controller - Guide de programmation	EIO0000003651 (ENG) EIO0000003652 (FRA) EIO0000003653 (GER) EIO0000003654 (SPA) EIO0000003655 (ITA) EIO0000003656 (CHS) EIO0000003657 (POR) EIO0000003658 (TUR)
Modules d'extension TMS - Guide de référence du matériel	EIO0000003699 (ENG) EIO0000003700 (FRA) EIO0000003701 (GER) EIO0000003702 (SPA) EIO0000003703 (ITA) EIO0000003704 (CHS) EIO0000003705 (POR) EIO0000003706 (TUR)

Titre du document	Numéro de référence
Modules d'extension TMSES4 - Instruction de service	PHA44907
Modules d'extension TMSCO1 - Instruction de service	PHA44909

Informations produit

⚠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, d'installation et d'exploitation de variateurs de vitesse) ou leur équivalent en vigueur dans votre pays.

⚠AVERTISSEMENT

FONCTIONNEMENT IMPRÉVU DE L'ÉQUIPEMENT

- N'utilisez que le logiciel approuvé par Schneider Electric pour faire fonctionner cet équipement.
- Mettez à jour votre programme d'application chaque fois que vous modifiez la configuration matérielle physique.

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

Terminologie utilisée dans les normes

Les termes techniques, la terminologie, les symboles et les descriptions correspondantes employés dans ce manuel ou figurant dans ou sur les produits proviennent généralement des normes internationales.

Dans les domaines des systèmes de sécurité fonctionnelle, des variateurs et de l'automatisme en général, les termes employés sont *sécurité*, *fonction de sécurité*, *état sécurisé*, *défaut*, *réinitialisation du défaut*, *dysfonctionnement*, *panne*, *erreur*, *message d'erreur*, *dangereux*, etc.

Entre autres, les normes concernées sont les suivantes :

Norme	Description
IEC 61131-2:2007	Automates programmables - Partie 2 : exigences et essais des équipements
ISO 13849-1:2015	Sécurité des machines : parties des systèmes de commande relatives à la sécurité. Principes généraux de conception
EN 61496-1:2013	Sécurité des machines : équipements de protection électro-sensibles. Partie 1 : Prescriptions générales et essais
ISO 12100:2010	Sécurité des machines - Principes généraux de conception - Appréciation du risque et réduction du risque
EN 60204-1:2006	Sécurité des machines - Équipement électrique des machines - Partie 1 : règles générales
ISO 14119:2013	Sécurité des machines - Dispositifs de verrouillage associés à des protecteurs - Principes de conception et de choix
ISO 13850:2015	Sécurité des machines - Fonction d'arrêt d'urgence - Principes de conception
IEC 62061:2015	Sécurité des machines - Sécurité fonctionnelle des systèmes de commande électrique, électronique et électronique programmable relatifs à la sécurité
IEC 61508-1:2010	Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité : prescriptions générales.
IEC 61508-2:2010	Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité : exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité.
IEC 61508-3:2010	Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité : exigences concernant les logiciels.
IEC 61784-3:2016	Réseaux de communication industriels - Profils - Partie 3 : Bus de terrain de sécurité fonctionnelle - Règles générales et définitions de profils.
2006/42/EC	Directive Machines
2014/30/EU	Directive sur la compatibilité électromagnétique
2014/35/EU	Directive sur les basses tensions

De plus, des termes peuvent être utilisés dans le présent document car ils proviennent d'autres normes telles que :

Norme	Description
Série IEC 60034	Machines électriques rotatives
Série IEC 61800	Entraînements électriques de puissance à vitesse variable
Série IEC 61158	Communications numériques pour les systèmes de mesure et de commande – Bus de terrain utilisés dans les systèmes de commande industriels

Enfin, le terme *zone de fonctionnement* utilisé dans le contexte de la description de dangers spécifiques a la même signification que les termes *zone dangereuse*

ou *zone de danger* employés dans la *directive Machines* (*2006/42/EC*) et la norme *ISO 12100:2010*.

NOTE: Les normes susmentionnées peuvent s'appliquer ou pas aux produits cités dans la présente documentation. Pour plus d'informations sur chacune des normes applicables aux produits décrits dans le présent document, consultez les tableaux de caractéristiques de ces références de produit.

Description des modules TMS

TMS - Description générale

Introduction

Les modules d'extension TMS s'installent sur le côté gauche du contrôleur et sont dédiés à Ethernet et CANopen. Vous pouvez configurer vos modules d'extension TMS dans l'arborescence EcoStruxure Machine Expert **Equipements**.

Caractéristiques des module d'extension TMS

Le tableau suivant présente les caractéristiques des modules d'extension TMS :

Référence du module	Type	Type de bornier	Compatibilité
TMSES4	Communication Ethernet	RJ45	TM262L10MESE8T TM262L20MESE8T TM262M15MESS8T TM262M25MESS8T TM262M35MESS8T
TMSCO1	Module maître CANopen	SUB-D 9 broches, mâle	TM262L• TM262M•

NOTE: Le module d'extension TMSES4 n'est pas un commutateur Ethernet autonome.

Configuration du bus de communication (COM_Bus)

Configuration du bus de communication

Pour configurer le bus de communication, procédez comme suit :

Etape	Action
1	Dans l'arborescence **Equipements**, double-cliquez sur **COM_Bus**. **Résultat :** La fenêtre de configuration **COM_Bus** s'affiche.
2	Cliquez sur l'un des onglets : • **Bus TMS** • **Mappage E/S** • **Tableau de diagnostic**

Onglet Bus TMS

Le bus de communication TMS possède une architecture réseau IP interne. L'adresse réseau est fixe pour les configurations générales. En revanche, l'adresse réseau doit être entrée manuellement pour les configurations complexes qui nécessitent plusieurs réseaux et contrôleurs M262 interconnectés.

Pour configurer l'adresse réseau, procédez comme suit :

Etape	Action
1	Cliquez sur **Adresse réseau**.
2	Saisissez la nouvelle adresse réseau. **Résultat :** Les champs **Masque de sous réseau**, **Min hôte** et **Max hôte** sont automatiquement mis à jour.

Onglet Mappage E/S

L'onglet **Mappage E/S** est fixe et ne peut pas être modifié.

Onglet Tableau de diagnostic

L'onglet **Tableau de diagnostic** fournit l'état de diagnostic de chaque module connecté.

NOTE: Ce tableau concerne uniquement les modules TMSES4.

Paramètre	Type de données	Valeur par défaut	Valeur	Description
ConfState	UNIT	0	0 : **Aucune configuration**	Etat global du bus
			1 : **Configuration non valide**	
			2 : **Réservé**	
			3 : **Configuration valide et appliquée**	
NbModules	UNIT	0	0 à 3	Nombre de modules TMS détectés
Name	STRING(15)	–	–	Nom du module TMS
MajorType	WORD	0	–	Code de type du module TMS
SubType	WORD	0	–	Code de sous-type du module TMS
Version	STRING(15)	–	–	Version du micrologiciel du module TMS(1)
ModuleState	DWORD	TMS_MODULE_POWERED	0	Détection du module TMS par le contrôleur
		TMS_MODULE_INITIALIZED	1	
		TMS_MODULE_CONFIGURED	2	
		TMS_MODULE_EXCHANGE_FAULT	3	
		MODULE_ERROR	4	
		TMS_MODULE_HEALTH_SEND_FAULT	5	
		TMS_MODULE_HEALTH_RCV_TIMEOUT	6	
		TMS_MODULE_HEALTH_RCV_MISC	7	
		TMS_MODULE_HEALTH_RESP_ERR	8	
		TMS_MODULE_DISCOVERY	9	

Paramètre	Type de données	Valeur par défaut	Valeur	Description
IpState	DWORD	TMS_IP_PING_SUCCESS	0	Communication IP entre M262 et le module TMS
		TMS_IP_CONFIG_CMD_ERROR	1	
		TMS_IP_CONFIG_RESP_WAIT	2	
		TMS_IP_CONFIG_RESP_ERROR	3	
		TMS_IP_CONFIG_RESP_NONE	4	
		TMS_IP_CONFIG_SUCCESS	5	
		TMS_IP_PING_CMD_ERROR	6	
		TMS_IP_PING_RESP_WAIT	7	
		TMS_IP_PING_RESP_ERROR	8	
		TMS_IP_PING_RESP_NONE	9	
		TMS_IP_NOT_CONFIGURED	11	
PixCmdState	Enumeration of DWORD	TMS_PIXCMD_EXCHING	0	Le module TMS traite une image de processus
		TMS_PIXCMD_CONFIG_NONE	1	
		TMS_PIXCMD_CONFIG_CMD_ERROR	2	
		TMS_PIXCMD_CONFIG_RESP_WAIT	3	
		TMS_PIXCMD_CONFIG_RESP_ERROR	4	
		TMS_PIXCMD_CONFIG_ONLY	5	
		TMS_PIXCMD_CONFIG_SUCCESS	6	
		TMS_PIXCMD_ENABLE_CMD_ERROR	7	
		TMS_PIXCMD_ENABLE_RESP_WAIT	8	
		TMS_PIXCMD_ENABLE_RESP_ERROR	9	
		TMS_PIXCMD_EXCH_ERROR	10	
		TMS_PIXCMD_DISABLING	11	
		TMS_PIXCMD_DISABLED	12	
(1) Consultez la documentation Mise à jour du micrologiciel du module d'extension TMSES4 (voir Modicon M262 - Logic/Motion Controller - Guide de programmation) pour plus d'informations sur la manière de mise à jour le micrologiciel des modules d'extension TMSES4.				

Ajout d'un module d'extension

Ajout d'un module d'extension

Pour ajouter un module d'extension à votre contrôleur, sélectionnez le module dans le **Catalogue de matériels**, faites-le glisser jusqu'à l'arborescence **Equipements** et déposez-le sur le nœud **COM_Bus**.

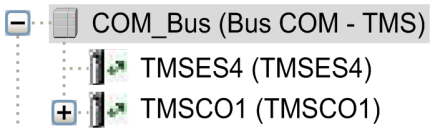
Pour plus d'informations sur l'ajout d'un équipement à votre projet, consultez :

• Utilisation de la méthode glisser-déposer (voir EcoStruxure Machine Expert, Programming Guide)

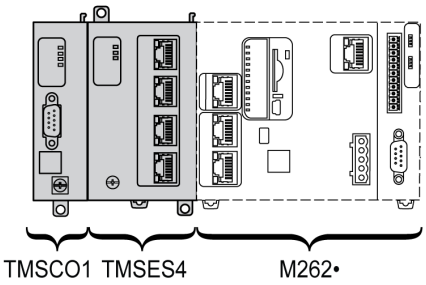
• Utilisation du Menu contextuel ou du bouton Plus (voir EcoStruxure Machine Expert, Programming Guide)

Disposition du module d'extension

Dans le logiciel, le module est disposé de haut en bas



Physiquement, les modules d'extension sont connectés de la droite vers la gauche :



Pour plus d'informations sur la compatibilité avec le M262 Logic/Motion Controller, reportez-vous à la section Caractéristiques des module d'extension TMS, page 10.

Configuration d'un module d'extension

Pour configurer votre module d'extension, double-cliquez sur le noeud qui le représente dans l'arborescence **Equipements**.

Module Ethernet TMSES4

Introduction

Ce chapitre décrit la configuration du module d'extension Ethernet TMSES4.

Services Ethernet

Introduction

Cette section explique comment configurer les services Ethernet fournis par le module d'extension TMSES4.

Présentation

Services Ethernet

Le module d'extension TMSES4 ajoute une interface Ethernet pour augmenter le nombre de ports Ethernet d'un contrôleur.

Le module prend en charge les services du contrôleur suivants :

- Serveur Modbus TCP, page 15
- Serveur Web (voir Modicon M262 - Logic/Motion Controller - Guide de programmation)
- Serveur FTP (voir Modicon M262 - Logic/Motion Controller - Guide de programmation)
- SNMP (voir Modicon M262 - Logic/Motion Controller - Guide de programmation)
- M262 Logic/Motion Controller en tant qu'équipement cible sur EtherNet/IP, page 20
- M262 Logic/Motion Controller en tant qu'équipement esclave sur Modbus TCP, page 21
- IEC VAR ACCESS, page 15

  NOTE: La communication NVL (Network Variable List) exige que le port Ethernet ait une adresse IP valide et que l'équipement soit connecté.

Protocole Ethernet

Le module Ethernet prend en charge les protocoles suivants :

- IP (Internet Protocol)
- UDP (User Datagram Protocol)
- TCP (Transmission Control Protocol)
- ARP (Address Resolution Protocol)
- ICMP (Internet Control Messaging Protocol)
- IGMP (Internet Group Management Protocol)

Connexions serveur TCP

Ce tableau indique le nombre total de connexions serveur TCP pour le contrôleur et les modules TMSES4 :

Type de connexion	Nombre maximum de connexions serveur simultanées
Serveur Modbus	8 connexions simultanées au serveur TCP maximum pour TMSES4 et contrôleur ou pour le contrôleur seul.
Equipement EtherNet/IP	16
Serveur FTP	4
Serveur Web	10

Chaque serveur TCP gère son propre pool de connexions.

Lorsqu'un client tente d'établir une connexion Serveur Modbus et que le nombre maximum de connexions est dépassé, le contrôleur ferme la connexion la plus ancienne. Dans les autres cas, la tentative d'ouverture de connexion est refusée.

Si toutes les connexions sont occupées (échange en cours) lorsqu'un client tente d'établir une nouvelle connexion, cette dernière est refusée.

Les connexions serveur restent ouvertes tant que le contrôleur est dans un état opérationnel (*RUN*, *STOP*, *HALT*).

Les connexions serveur sont fermées lors de la sortie ou de l'entrée des états opérationnels (*RUN*, *STOP*, *HALT*), sauf en cas de coupure de courant (car le contrôleur n'a pas le temps de fermer les connexions).

Pour plus d'informations sur les états opérationnels, consultez le schéma des états de contrôleur (voir Modicon M262 - Logic/Motion Controller - Guide de programmation).

Serveur Modbus TCP

Le serveur Modbus prend en charge les requêtes Modbus suivantes :

Code fonction Déc (Hex)	Sous-fonction Déc (Hex)	Fonction
1 (1h)	–	Lecture de sorties numériques (%Q)
2 (2h)	–	Lecture d'entrées numériques (%I)
3 (3h)	–	Lecture de registre de maintien (%MW)
6 (6h)	–	Ecriture d'un registre (%MW)
8 (8h)	–	Diagnostic
15 (Fh)	–	Ecriture de plusieurs sorties numériques (%Q)
16 (10h)	–	Ecriture de plusieurs registres (%MW)
23 (17h)	–	Lecture/écriture de plusieurs registres (%MW)
43 (2Bh)	14 (Eh)	Lecture de l'identification de l'équipement

Services disponibles

Avec une communication Ethernet, le service **IEC VAR ACCESS** est pris en charge par le contrôleur. Le service **IEC VAR ACCESS** permet un échange de variables entre le contrôleur et un IHM.

Le service **Variables de réseau** est également pris en charge par le contrôleur. Le service **Variables de réseau** permet un échange de données entre les contrôleurs.

NOTE: Pour plus d'informations, reportez-vous à la documentation EcoStruxure Machine Expert Guide de programmation.

Configuration de l'adresse IP

Introduction

Lorsque TMSES4 n'est pas configuré, il démarre et obtient automatiquement son adresse IP par défaut :

- 10.12.x.z pour le premier module
- 10.13.x.z pour le deuxième module
- 10.14.x.z pour le troisième module

x et z représentent le 5ème et le 6ème octets de l'adresse MAC d'interface. Par exemple, pour l'adresse MAC 00:80:F4:50:02:5D, l'adresse IP est 10.12.2.93.

Pour plus d'informations sur l'emplacement de l'adresse MAC, reportez-vous à la section Configuration Ethernet, page 18.

Le masque de sous-réseau par défaut est 255.255.0.0.

Il existe plusieurs façons d'affecter l'adresse IP à l'interface Ethernet ajoutée du contrôleur :

- Affectation d'adresse par serveur DHCP
- Affectation d'adresse par serveur BOOTP
- Adresse IP fixe
- Fichier de post-configuration (voir Modicon M262 - Logic/Motion Controller - Guide de programmation). S'il existe un fichier de post-configuration, cette méthode d'affectation a la priorité sur les autres.

L'adresse IP peut également être changée dynamiquement via :

- L'onglet Paramètres de communication (voir Modicon M262 Logic/Motion Controller, Guide de programmation) dans EcoStruxure Machine Expert
- **changeIPAddress**, bloc fonction (voir Modicon M262 - Logic/Motion Controller - Guide de programmation)

  NOTE: Si la méthode d'adressage essayée échoue, la liaison utilise une adresse IP par défaut dérivée de l'adresse MAC.

Gérez les adresses IP avec soin, car chaque équipement du réseau requiert une adresse unique. Si plusieurs équipements ont la même adresse IP, le réseau et le matériel associé risquent de se comporter de manière imprévisible.

⚠AVERTISSEMENT

FONCTIONNEMENT IMPRÉVU DE L'ÉQUIPEMENT

- Vérifiez qu'un seul contrôleur maître est configuré sur le réseau ou la liaison distante.
- Vérifiez que chaque équipement a une adresse unique.
- Obtenez votre adresse IP auprès de l'administrateur système.
- Vérifiez que l'adresse IP de l'équipement est unique avant de mettre le système en service.
- N'attribuez pas la même adresse IP aux autres équipements du réseau.
- Après avoir cloné une application comprenant des communications Ethernet, mettez à jour l'adresse IP pour qu'elle soit unique.

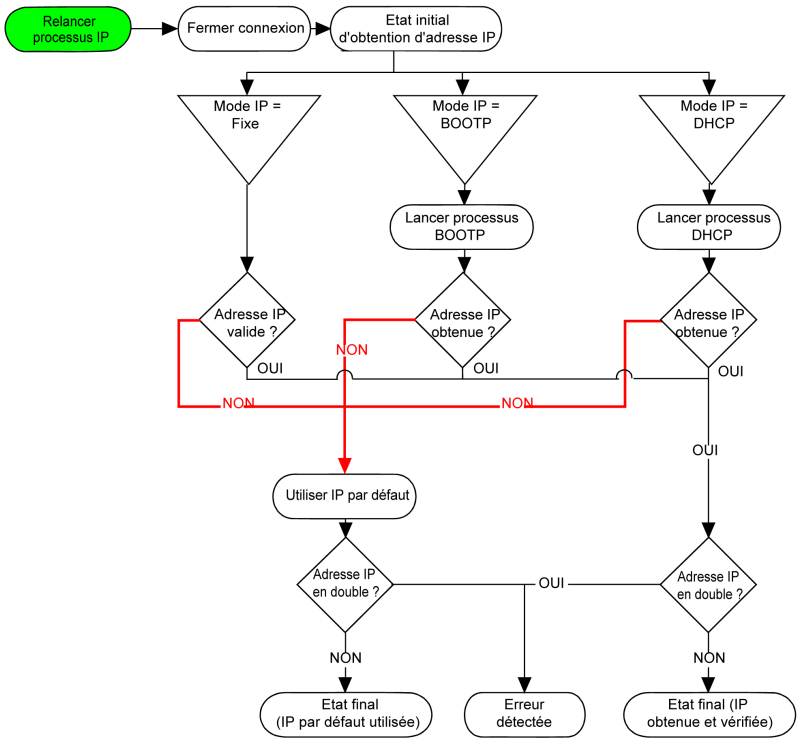
Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

NOTE: Vérifiez que votre administrateur système gère toutes les adresses IP affectées sur le réseau et le sous-réseau, et informez-le de toutes les modifications apportées à la configuration.

NOTE: Le module TMSES4 doit se trouver dans un sous-réseau différent de celui des ports Ethernet du contrôleur.

Gestion des adresses

Ce schéma représente les différents types de système d'adressage du contrôleur :



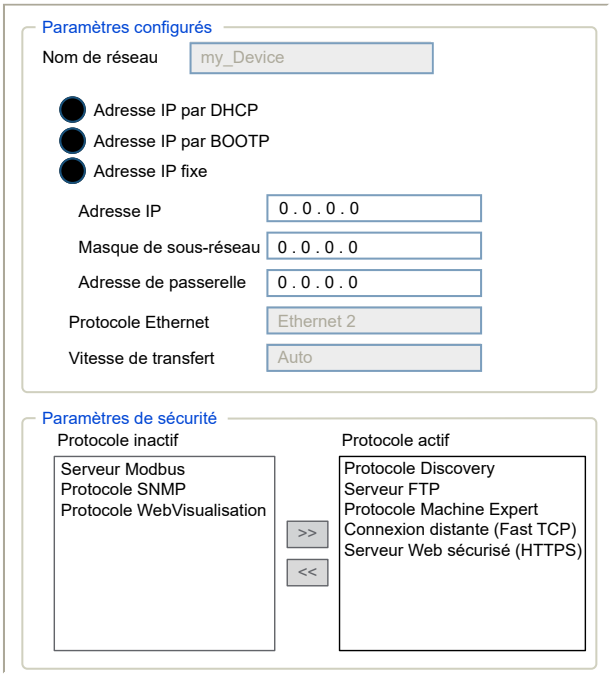
NOTE: Si un équipement programmé pour utiliser les méthodes d'adressage DHCP ou BOOTP ne parvient pas à contacter son serveur respectif, le contrôleur utilise l'adresse IP par défaut. Il répète constamment sa requête.

La procédure d'adressage IP redémarre automatiquement dans les cas suivants :

- Redémarrage du contrôleur
- Reconnexion du câble Ethernet
- Téléchargement d'application (si les paramètres IP sont modifiés)
- Détection d'un serveur DHCP ou BOOTP après l'échec d'une tentative d'adressage précédente.

Configuration Ethernet

Dans l'arborescence **Equipements**, double-cliquez sur **TMSES4** :



NOTE:

- Si vous êtes en mode hors ligne, le **Paramètres configurés** (ci-dessus) apparaît. Vous pouvez modifier les paramètres.
- Si vous êtes en mode connecté (en ligne), les fenêtres **Paramètres configurés** et **Paramètres actuels** s'affichent. Vous ne pouvez pas modifier les paramètres.

Le tableau suivant décrit les paramètres configurés :

Paramètres configurés	Description
Nom du réseau	Utilisé comme nom d'équipement pour récupérer une adresse IP via DHCP, 15 caractères maximum.
Adresse IP par DHCP	L'adresse IP est obtenue via un serveur DHCP.
Adresse IP par BOOTP	L'adresse IP est obtenue via un serveur BOOTP. L'adresse MAC est située sur le côté gauche du contrôleur.
Adresse IP fixe	L'adresse IP, le masque de sous-réseau et l'adresse de passerelle sont définis par l'utilisateur.
Protocole Ethernet	Type de protocole utilisé : Ethernet 2
Vitesse de transfert	Vitesse et duplex sont en mode autonégociation.

Adresse IP par défaut

L'adresse MAC du port Ethernet est mentionnée sur l'étiquette placée sur la face avant du contrôleur M262. L'adresse MAC du port TMSES4 est mentionnée sur l'étiquette placée sur le côté gauche du contrôleur M262.

NOTE: Une adresse MAC s'écrit en format hexadécimal et une adresse IP en format décimal. Convertissez l'adresse MAC au format décimal.

Exemple de conversion :

Port	Adresse MAC	Adresse IP
TMS_1	00.80.F4.50.03.31	10.12.3.49
TMS_2	00.80.F4.50.03.32	10.13.3.50
TMS_3	00.80.F4.50.03.33	10.14.3.51

Masque de sous-réseau

Le masque de sous-réseau est utilisé pour accéder à plusieurs réseaux physiques avec une adresse réseau unique. Le masque sert à séparer le sous-réseau et l'adresse de l'équipement hôte.

L'adresse de sous-réseau est obtenue en conservant les bits de l'adresse IP qui correspondent aux positions du masque contenant la valeur 1 et en remplaçant les autres par 0.

Inversement, l'adresse de sous-réseau de l'équipement hôte est obtenue en conservant les bits de l'adresse IP qui correspondent aux positions du masque contenant la valeur 0 et en remplaçant les autres par 1.

Exemple d'adresse de sous-réseau :

Adresse IP	192 (11000000)	1 (00000001)	17 (00010001)	11 (00001011)
Masque de sous-réseau	255 (11111111)	255 (11111111)	240 (11110000)	0 (00000000)
Adresse de sous-réseau	192 (11000000)	1 (00000001)	16 (00010000)	0 (00000000)

NOTE: L'équipement ne communique pas sur son sous-réseau en l'absence de passerelle.

Adresse de passerelle

La passerelle permet de router un message vers un équipement qui ne se trouve pas sur le réseau actuel.

En l'absence de passerelle, l'adresse de passerelle est 0.0.0.0.

L'adresse de passerelle doit être définie sur l'interface Ethernet_1. Le trafic à destination de réseaux externes transite par cette interface.

Paramètres de sécurité

Le tableau suivant décrit les différents paramètres de sécurité :

Paramètres de sécurité	Description	Paramètres par défaut
Protocole de découverte	Ce paramètre désactive le **protocole Discovery**. Lorsqu'il est désactivé, les requêtes Discovery sont ignorées.	Actif
Serveur FTP	Ce paramètre désactive le serveur FTP du contrôleur. Lorsqu'il est désactivé, les requêtes FTP sont ignorées.	Actif
Protocole Machine Expert	Ce paramètre désactive le protocole Machine Expert sur les interfaces Ethernet. Lorsqu'il est désactivé, toute requête Machine Expert provenant d'un équipement est rejetée. Par conséquent, aucune connexion Ethernet n'est possible à partir d'un PC équipé de EcoStruxure Machine Expert, d'une cible IHM qui souhaite échanger des variables avec ce contrôleur, d'un serveur OPC ou de Controller Assistant.	Actif
Serveur Modbus	Ce paramètre désactive le serveur Modbus du contrôleur. Lorsqu'il est désactivé, les requêtes Modbus adressées au contrôleur sont ignorées.	Inactif
Connexion à distance	Ce paramètre désactive la connexion à distance. Lorsqu'elle est désactivée, les requêtes Fast TCP sont ignorées.	Actif
Serveur Web sécurisé	Ce paramètre désactive le Serveur Web sécurisé du contrôleur. Lorsqu'il est désactivé, les requêtes HTTPS adressées au Serveur Web sécurisé du contrôleur sont ignorées.	Actif
Protocole SNMP	Ce paramètre désactive le serveur SNMP du contrôleur. Lorsqu'il est désactivé, les requêtes SNMP sont ignorées.	Inactif
Protocole WebVisualisation	Ce paramètre désactive les pages WebVisualisation du contrôleur. Lorsqu'il est désactivé, les requêtes HTTP adressées au protocole WebVisualisation du contrôleur sont ignorées.	Inactif

Modicon M262 Logic/Motion Controller en tant qu'équipement cible sur EtherNet/IP

Introduction

Cette section décrit la configuration du M262 Logic/Motion Controller en tant qu'équipement cible EtherNet/IP.

Pour plus d'informations sur EtherNet/IP, consultez le site Web www.odva.org.

Ajout d'un gestionnaire EtherNet/IP

Pour configurer votre M262 Logic/Motion Controller en tant qu'équipement cible sur Ethernet/IP, vous devez ajouter un gestionnaire EthernetIP à votre contrôleur.

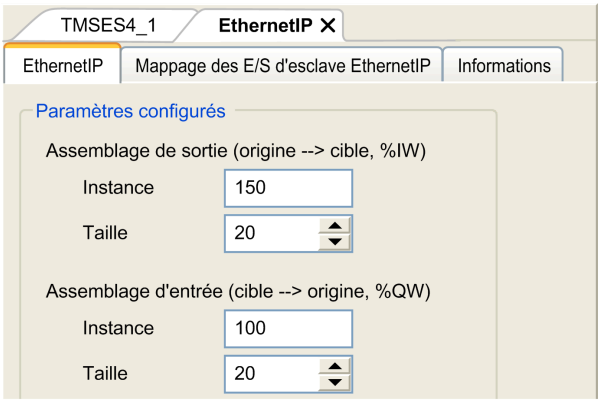
Pour ajouter un gestionnaire EthernetIP à votre M262 Logic/Motion Controller :

Etape	Action
1	Ajoutez un module d'extension TMSES4 à votre configuration.
2	Depuis le noeud **TMSES4** noeud dans l'arborescence **Equipements**, ajoutez le **Gestionnaire EthernetIP** en le sélectionnant dans le **Catalogue de matériels**, en le faisant glisser vers l'arborescence **Equipements** et en le déposant sur le nœud **TMSES4**. Pour plus d'informations sur l'ajout d'un équipement à votre projet, consultez : • Utilisation de la méthode glisser-déposer (voir EcoStruxure Machine Expert, Programming Guide) • Utilisation du Menu contextuel ou du bouton Plus (voir EcoStruxure Machine Expert, Programming Guide)

Configuration des paramètres EtherNet/IP

Pour configurer les paramètres EtherNet/IP, double-cliquez sur **COM_Bus > TMSES4 > EthernetIP** dans l'arborescence **Equipements**.

La boîte de dialogue suivante s'affiche :



Les paramètres de configuration des E/S EtherNet/IP sont définis comme suit :

- **Instance** :

  Numéro de référencement de l'Assemblage d'entrée ou de sortie.

- **Taille** :

  Nombre de voies d'un Assemblage d'entrée ou de sortie.

  Chaque voie dispose d'une mémoire de 2 octets qui stocke la valeur d'un objet *%IWx* ou *%QWx*, où *x* correspond au numéro de la voie.

  Par exemple, si le paramètre **Taille** de l'**Assemblage de sortie** vaut 20, il y a 20 voies d'entrée (IW0 à IW19) qui s'adressent à *%IW*y à *%IW*(y+20-1), où y est la première voie disponible pour l'assemblage.

Elément		Plage autorisée par le contrôleur	Valeur par défaut dans EcoStruxure Machine Expert
Assemblage de sortie	**Instance**	150 à 189	150
	Taille	2 à 120	20
Assemblage d'entrée	**Instance**	100 à 149	100
	Taille	2 à 120	20

Reportez-vous au Guide de programmation M262 pour plus d'informations sur les sujets suivants :

- Génération d'un fichier EDS
- Configuration des E/S
- Objets pris en charge par le contrôleur

Modicon M262 Logic/Motion Controller en tant qu'équipement esclave sur Modbus TCP

Présentation

Cette section décrit la configuration du M262 Logic/Motion Controller en tant qu'**Equipement esclave Modbus TCP**.

Pour configurer votre M262 Logic/Motion Controller en tant qu'**Equipement esclave Modbus TCP**, vous devez ajouter la fonctionnalité **Equipement esclave Modbus TCP** à votre contrôleur (voir Ajout d'un équipement esclave Modbus TCP).

Cette fonctionnalité crée dans le contrôleur une zone d'E/S spécifique, accessible à l'aide du protocole Modbus TCP. Cette zone d'E/S est utilisée lorsqu'un maître externe a besoin d'accéder aux objets *%IW* et *%QW* du contrôleur. La fonctionnalité **Equipement esclave Modbus TCP** vous permet de fournir à cette zone les objets d'E/S du contrôleur qui seront ensuite accessibles via une requête Modbus de lecture/écriture de registres.

La fonctionnalité **Equipement esclave Modbus TCP** ajoute une fonction de serveur Modbus supplémentaire au contrôleur. Ce serveur est contacté par l'application cliente Modbus à l'aide d'un ID d'unité configuré (adresse Modbus) compris entre 1 et 247. Le serveur Modbus intégré du contrôleur esclave est contacté à l'aide d'un ID d'unité égal à 255 et ne nécessite aucune configuration. Consultez Configuration de Modbus TCP, page 22.

Les entrées/sorties sont visibles depuis le contrôleur esclave : elles sont respectivement écrites/lues par le maître.

La fonctionnalité **Equipement esclave Modbus TCP** peut définir une application cliente Modbus privilégiée, dont la connexion n'est pas fermée de force (les connexions Modbus intégrées peuvent être coupées si vous avez besoin de plus de huit connexions).

Grâce à la temporisation de la connexion privilégiée, vous pouvez vérifier si le contrôleur est scruté par le maître privilégié. Si aucune requête Modbus n'est reçue dans le délai imparti, les informations de diagnostic *i_byMasterIpLost* sont définies sur 1 (TRUE). Pour plus d'informations, reportez-vous à la section traitant des variables système en lecture seule des ports Ethernet (voir Modicon M262 Logic/Motion Controller - Fonctions et variables système - Guide de la bibliothèque système).

Pour plus d'informations sur Modbus TCP, consultez le site Web www.modbus.org.

Ajout d'un équipement esclave Modbus TCP

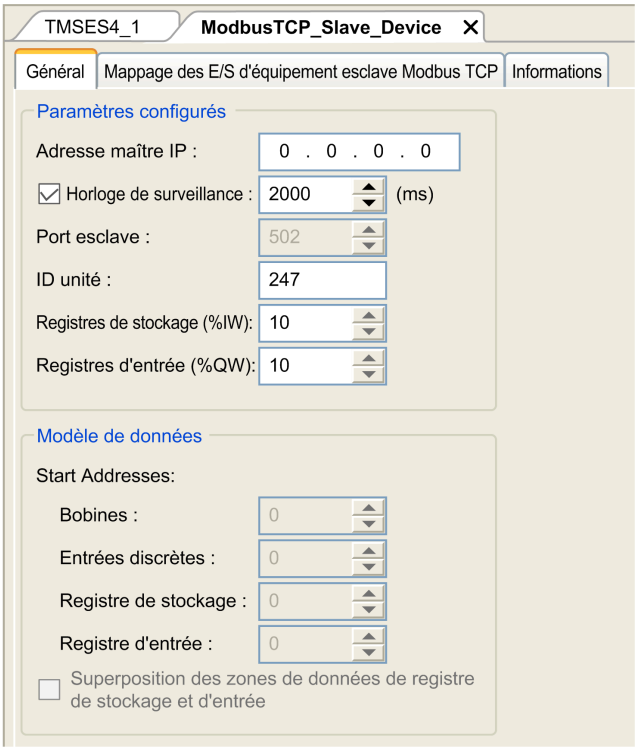
Pour ajouter la fonctionnalité Equipement esclave Modbus TCP à votre M262 Logic/Motion Controller :

Etape	Action
1	Ajoutez un module d'extension TMSES4 à votre configuration.
2	Depuis le nœud **TMSES4** de l'arborescence **Equipements**, ajoutez l'**Equipement esclave Modbus TCP** en le sélectionnant dans le **Catalogue de matériels**, en le faisant glisser vers l'arborescence **Equipements** et en le déposant sur le nœud **TMSES4**. Pour plus d'informations sur l'ajout d'un équipement à votre projet, consultez : • Utilisation de la méthode glisser-déposer (voir EcoStruxure Machine Expert, Programming Guide) • Utilisation du Menu contextuel ou du bouton Plus (voir EcoStruxure Machine Expert, Programming Guide)

Configuration d'un équipement esclave Modbus TCP

Pour configurer le Equipement esclave Modbus TCP, double-cliquez sur **COM_Bus > TMSES4 > ModbusTCP_Slave_Device** dans l'arborescence **Equipements**.

La boîte de dialogue suivante s'affiche :



Elément	Description
Adresse maître IP	Adresse IP du maître Modbus. Les connexions ne sont pas fermées sur cette adresse.
Horloge de surveillance	Temporisation, par incréments de 500 ms. **NOTE:** La temporisation s'applique à l'**Adresse IP maître**, sauf si l'adresse est 0.0.0.0.
Port esclave	Port de communication Modbus (502).
ID unité	Envoie les requêtes à l'équipement Equipement esclave Modbus TCP (1 à 247) au lieu du serveur Modbus intégré (255).
Registres de stockage (%IW)	Nombre de registres %IW à utiliser dans l'échange (2 à 120), chaque registre stockant 2 octets)
Registres d'entrée (% QW)	Nombre de registres %QW à utiliser dans l'échange (2 à 120), chaque registre stockant 2 octets)

Onglet Mappage des E/S d'équipement esclave Modbus TCP

Les E/S sont mappées aux registres Modbus du point de vue du maître, comme suit :

- Les %IW sont mappées du registre 0 au registre n-1 et sont en lecture/écriture (n = nombre de registres de stockage, chaque registre %IW représentant 2 octets).
- Les %QW sont mappées du registre n au registre n+m -1 et sont en lecture seule (m = nombre de registres d'entrée, chaque registre %QW représentant 2 octets).

Lorsqu'un **équipement esclave Modbus TCP** a été configuré, les commandes Modbus envoyées à son ID d'unité (adresse Modbus) sont traitées différemment des mêmes commandes adressées à un autre équipement Modbus du réseau. Par exemple, lorsque la commande Modbus 3 (3 hex) est envoyée à un équipement Modbus, elle lit et renvoie la valeur d'un ou de plusieurs registres. Lorsque la même commande est envoyée à l'esclave Modbus TCP (voir Modicon M262 Logic/Motion Controller - Guide de programmation), elle permet une opération de lecture par le scrutateur d'E/S externe.

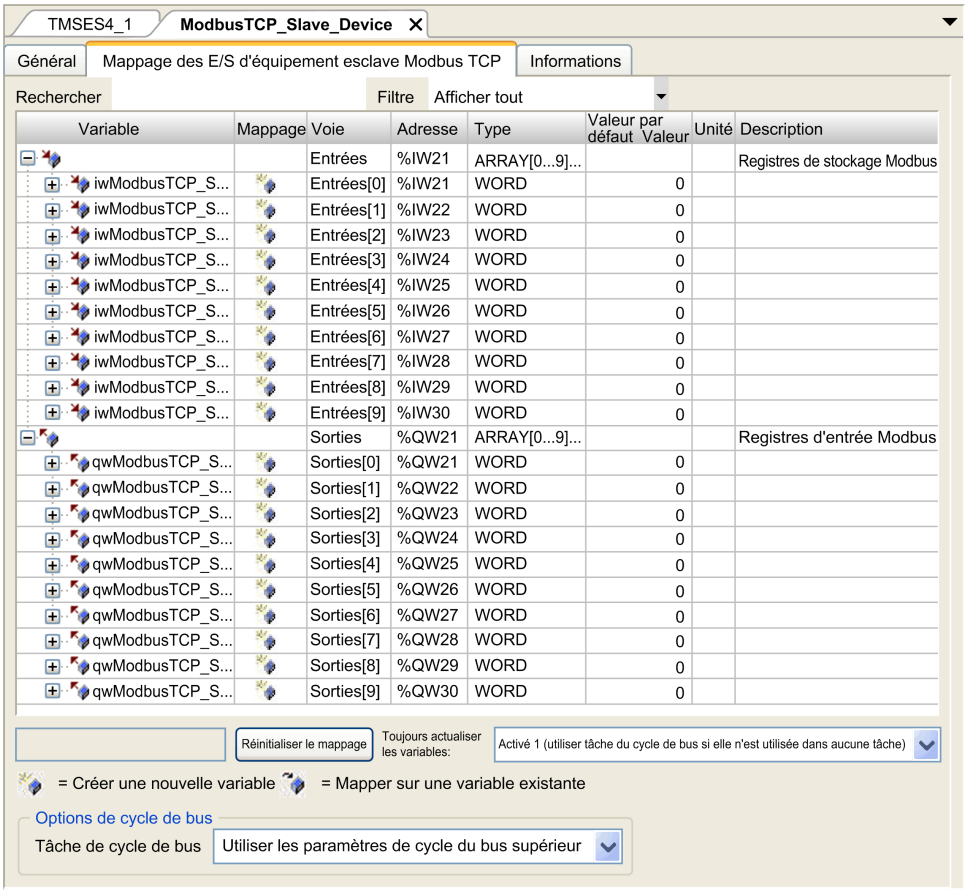
Lorsqu'un **équipement esclave Modbus TCP** a été configuré, les commandes Modbus envoyées à son ID d'unité (adresse Modbus) accèdent aux objets *%IW* et *%QW* du contrôleur lié à l'équipement Modbus TCP et non aux mots Modbus standard (accessibles avec l'ID d'unité 255). Cela facilite les opérations de lecture/écriture par une application de scrutateur d'E/S Modbus TCP.

L'**équipement esclave Modbus TCP** répond à un sous-ensemble des commandes Modbus dans le but d'échanger des données avec le scrutateur d'E/S externe. Les commandes Modbus suivantes sont prises en charge par l'**équipement esclave Modbus TCP** :

Code fonction décimal (hexadéci-mal)	Fonction	Commentaire
3 (3)	Lecture d'un registre de stockage	Permet au maître de lire les objets *%IW* et *%QW* de l'équipement
6 (6)	Ecriture d'un registre	Permet au maître d'écrire les objets *%IW* de l'équipement
16 (10)	Ecriture de plusieurs registres	Permet au maître d'écrire les objets *%IW* de l'équipement
23 (17)	Lecture/écriture de plusieurs registres	Permet au maître de lire les objets *%IW* et *%QW* de l'équipement et d'écrire les objets *%IW* objets de l'équipement
Autre	Non pris en charge	–

NOTE: Les requêtes Modbus qui tentent d'accéder aux registres supérieurs à n+m-1 reçoivent en retour le code d'exception 02 - ADRESSE DE DONNEES INCORRECTE.

Pour lier des objets d'E/S à des variables, sélectionnez l'onglet **Mappage E/S Equipement esclave Modbus TCP** :



Voie		Type	Description
Entrée	IW0	WORD	Registre de stockage 0
	...	...	...
	IWx	WORD	Registre de stockage x
Sortie	QW0	WORD	Registre d'entrée 0
	...	...	...
	QWy	WORD	Registre d'entrée y

Le nombre de mots dépend des paramètres **Registres de stockage (%IW)** et **Registres d'entrée (%QW)** de l'onglet **Modbus TCP**.

NOTE: Sortie signifie SORTIE du contrôleur client/maître (%IW pour le contrôleur serveur/esclave). Entrée signifie ENTREE depuis le contrôleur client/maître (%QW pour le contrôleur serveur/esclave).

Options de cycle de bus

Sélectionnez la **Tâche de cycle de bus** à utiliser :

- **Utiliser les paramètres de cycle du bus supérieur** (option par défaut),
- **MAST**

Il existe un paramètre **Tâche de cycle de bus** correspondant dans l'éditeur de mappage d'E/S du contrôleur qui contient le Equipement esclave Modbus TCP. Ce paramètre définit la tâche responsable de l'actualisation des registres *%IW* et *%QW*.

Configuration du pare-feu

Introduction

Cette section explique comment configurer le pare-feu du Modicon M262 Logic/ Motion Controller.

Introduction

Présentation du pare-feu

De manière générale, les pare-feu permettent de protéger les périmètres des zones de sécurité des réseaux en bloquant les accès non autorisés et en laissant passer les accès autorisés. Un pare-feu est un équipement ou un groupe d'équipements qui est configuré pour autoriser, refuser, crypter, décrypter ou filtrer le trafic entre différentes zones de sécurité en s'appuyant sur un ensemble de règles et d'autres critères.

Les équipements de contrôle de processus et les machines de fabrication à grande vitesse nécessitent un débit de données rapide et ne peuvent souvent pas tolérer les délais de latence introduits par une stratégie de sécurité drastique au sein du réseau de contrôle. Par conséquent, les pare-feu jouent un rôle important dans une stratégie de sécurité en offrant des niveaux de protection aux périmètres du réseau. Les pare-feu représentent une part importante d'une stratégie globale au niveau du système.

NOTE: Schneider Electric respecte les bonnes pratiques de l'industrie, en vigueur dans le développement et la mise en œuvre des systèmes de contrôle. Cette approche, dite de « défense en profondeur », permet de sécuriser les systèmes de contrôle industriels. Elle place les contrôleurs derrière des pare-feu pour restreindre leur accès aux seuls personnels et protocoles autorisés.

⚠AVERTISSEMENT

ACCÈS NON AUTHENTIFIÉ ET UTILISATION NON AUTORISÉE DE LA MACHINE

- Estimer si votre environnement ou vos machines sont connecté(e)s à votre infrastructure vitale et, le cas échéant, prendre les mesures nécessaires de prévention, basées sur le principe de défense en profondeur, avant de connecter le système d'automatisme à un réseau quelconque.
- Limiter au strict nécessaire le nombre d'équipements connectés à un réseau.
- Isoler votre réseau industriel des autres réseaux au sein de votre société.
- Protéger chaque réseau contre les accès non autorisés à l'aide d'un pare-feu, d'un VPN ou d'autres mesures de sécurité éprouvées.
- Surveiller les activités au sein de votre système.
- Empêcher tout accès direct ou liaison directe aux équipements sensibles par des utilisateurs non autorisés ou des actions non authentifiées.
- Préparer un plan de récupération intégrant la sauvegarde des informations de votre système et de votre processus.

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

Configuration du pare-feu

Trois méthodes permettent de gérer la configuration du pare-feu du contrôleur :

- Configuration statique
- Modifications dynamiques
- Paramètres d'application

La configuration statique et les modifications dynamiques reposent sur des fichiers de script.

Configuration statique

La configuration statique est chargée au démarrage du contrôleur.

Vous pouvez configurer le pare-feu du contrôleur de manière statique à l'aide d'un fichier de script par défaut enregistré sur ce dernier (dans le répertoire */usr/Cfg/FirewallDefault.cmd*).

NOTE: Le nom de fichier est sensible à la casse.

Modifications dynamiques

Une fois le contrôleur démarré, vous pouvez modifier la configuration du pare-feu à l'aide de fichiers de script.

Voici les deux moyens permettant de charger ces modifications dynamiques :

- Une carte SD, page 26 physique.
- Un bloc fonction, page 27 dans l'application.

Paramètres d'application

Consultez Configuration Ethernet, page 18

Procédure de modification dynamique

Utilisation d'une carte SD

Le tableau suivant décrit la procédure d'exécution d'un fichier de script à partir d'une carte SD :

Etape	Action
1	Créez un fichier de script, page 29 valide. Par exemple, nommez le fichier de script *FirewallMaintenance.cmd*.
2	Chargez le fichier de script sur la carte SD. Par exemple, chargez le fichier de script dans le dossier *usr/Cfg* .

3	Dans le fichier *Sys/Cmd/Script.cmd*, ajoutez une ligne de code avec la commande
	`Firewall_install "/pathname/FileName"`
	Par exemple, la ligne de code est
	`Firewall_install "/sd0/usr/Cfg/FirewallMaintenance.cmd"`
	NOTE: Le nom de fichier fait la distinction entre les majuscules et les minuscules.

4	Insérez la carte SD dans le contrôleur.

Utilisation d'un bloc fonction dans l'application

Le tableau suivant décrit la procédure d'exécution d'un fichier de script à partir d'une application :

Etape	Action
1	Créez un fichier de script, page 29 valide. Par exemple, nommez le fichier de script *FirewallMaintenance.cmd*.
2	Chargez le fichier de script dans la mémoire du contrôleur. Par exemple, chargez le fichier de script dans le dossier *usr/Syslog* avec FTP.
3	Utilisez un bloc fonction `ExecuteScript`. Pour plus d'informations, reportez-vous au document M262 - Guide de la bibliothèque System (voir Modicon M262 Logic/Motion Controller - Fonctions et variables système - Guide de la bibliothèque System). Par exemple, l'entrée **[SCmd]** est `'Firewall_install "/usr/Syslog/FirewallMaintenance.cmd"'` **NOTE:** Le nom de fichier fait la distinction entre les majuscules et les minuscules.

Comportement du pare-feu

Introduction

La configuration du pare-feu dépend des opérations réalisées sur le contrôleur et de l'état de configuration initial. Il existe cinq états initiaux possibles :

- Le contrôleur ne contient aucun fichier de script par défaut.
- Le contrôleur contient un fichier de script valide.
- Le contrôleur contient un fichier de script incorrect.
- Le contrôleur ne contient aucun fichier de script par défaut et le pare-feu a été configuré par l'application.
- Une configuration de fichier de script dynamique a déjà été exécutée.

  NOTE: Pour déterminer si le pare-feu est configuré et activé, consultez le journaliseur de messages.

Fichier de script par défaut absent

Si…	Alors…
Démarrage du contrôleur	Le pare-feu n'est pas configuré. Aucune protection n'est activée.
Exécution d'un fichier de script dynamique	Le pare-feu est configuré sur la base du fichier de script dynamique.
Exécution d'un fichier de script dynamique incorrect	Le pare-feu n'est pas configuré. Aucune protection n'est activée.
Téléchargement d'application	Le pare-feu est configuré sur la base des paramètres de l'application.

Fichier de script par défaut présent

Si…	Alors…
Démarrage du contrôleur	Le pare-feu est configuré sur la base du fichier de script par défaut.
Exécution d'un fichier de script dynamique	La configuration du fichier de script par défaut est entièrement supprimée. Le pare-feu est configuré sur la base du fichier de script dynamique.
Exécution d'un fichier de script dynamique incorrect	Le pare-feu est configuré sur la base du fichier de script par défaut. Le fichier de script dynamique n'est pas pris en compte.
Télécharger une application	La configuration de l'application est entièrement ignorée. Le pare-feu est configuré sur la base du fichier de script par défaut.

Fichier de script par défaut incorrect présent

Si…	Alors…
Démarrage du contrôleur	Le pare-feu n'est pas configuré. Aucune protection n'est activée.
Exécution d'un fichier de script dynamique	Le pare-feu est configuré sur la base du fichier de script dynamique.
Télécharger une application	Le pare-feu est configuré sur la base des paramètres de l'application.

Paramètres d'application sans fichier de script par défaut

Si…	Alors…
Démarrage du contrôleur	Le pare-feu est configuré sur la base des paramètres de l'application.
Exécution d'un fichier de script dynamique	La configuration des paramètres d'application est entièrement supprimée. Le pare-feu est configuré sur la base du fichier de script dynamique.
Exécution d'un fichier de script dynamique incorrect	Le pare-feu est configuré sur la base des paramètres de l'application. Le fichier de script dynamique n'est pas pris en compte.
Télécharger une application	La configuration de l'application précédente est entièrement supprimée. Le pare-feu est configuré sur la base des nouveaux paramètres d'application.

Exécution d'un fichier de script dynamique déjà exécuté

Si…	Alors…
Démarrage du contrôleur	Le pare-feu est configuré sur la base de la configuration de fichier de script dynamique (voir remarque).
Exécution d'un fichier de script dynamique	La configuration du fichier de script dynamique précédent est entièrement supprimée. Le pare-feu est configuré sur la base du nouveau fichier de script dynamique.
Exécution d'un fichier de script dynamique incorrect	Le pare-feu est configuré sur la base de la configuration de fichier de script dynamique précédente. Le fichier de script dynamique incorrect n'est pas pris en compte.
Télécharger une application	La configuration de l'application est entièrement ignorée. Le pare-feu est configuré sur la base du fichier de script dynamique.

Commandes de script de pare-feu

Présentation

Cette section décrit la syntaxe des fichiers de script (par défaut ou dynamiques) à respecter pour qu'ils s'exécutent correctement au démarrage du contrôleur ou lors du déclenchement d'une commande particulière.

NOTE: Les règles de la couche MAC sont gérées séparément et sont prioritaires par rapport aux autres règles de filtrage de paquets.

Syntaxe des fichiers de script

La syntaxe des fichiers de script est décrite dans Création d'un script (voir Modicon M262 - Logic/Motion Controller - Guide de programmation).

Commandes de pare-feu générales

Les commandes suivantes permettent de gérer le pare-feu Ethernet du M262 Logic/Motion Controller :

Commande	Description
`Firewall Enable`	Bloque les trames provenant des interfaces Ethernet. Si aucune adresse IP spécifique n'est autorisée, il est impossible de communiquer sur les interfaces Ethernet. **NOTE:** Par défaut, lorsque le pare-feu est activé, les trames sont rejetées.
`Firewall Disable`	Les règles de pare-feu ne s'appliquent pas. Les trames ne sont pas bloquées.
`Firewall Ethx Default Allow` (1)	Le contrôleur accepte toutes les trames.
`Firewall Ethx Default Reject`(1)	Le contrôleur rejette toutes les trames. **NOTE:** Par défaut, si cette ligne est absente, l'option par défaut est `Firewall Eth1 Default Reject`.

(1) Où Ethx =

- Eth1 : Ethernet_1
- Eth2 : Ethernet_2
- Eth3 : TMSES4 (premier module Ethernet à partir de la gauche)
- Eth4 : TMSES4 (deuxième module Ethernet à partir de la gauche)
- Eth5 : TMSES4 (troisième module Ethernet à partir de la gauche)

Commandes de pare-feu spécifiques

Les commandes suivantes permettent de configurer les règles de pare-feu pour certains ports et certaines adresses :

Commande	Plage	Description
`Firewall Eth1 Allow IP •.•.•.•`	• = 0 à 255	Les trames provenant de l'adresse IP indiquée sont autorisées sur l'ensemble des ports, quel que soit leur type.
`Firewall Eth1 Reject IP •.•.•.•`	• = 0 à 255	Les trames provenant de l'adresse IP indiquée sont rejetées sur l'ensemble des ports, quel que soit leur type.
`Firewall Eth1 Allow IPs •.•.•.• to •.•.•.•`	• = 0 à 255	Les trames provenant des adresses IP de la plage indiquée sont autorisées sur l'ensemble des ports, quel que soit leur type.
`Firewall Eth1 Reject IPs •.•.•.• to •.•.•.•`	• = 0 à 255	Les trames provenant des adresses IP de la plage indiquée sont rejetées sur l'ensemble des ports, quels que soient leur numéro et leur type.
`Firewall Eth1 Allow port_type port Y`	Y = (numéros de port de destination, page 33)	Les trames avec le numéro de port de destination spécifié sont autorisées.
`Firewall Eth1 Reject port_type port Y`	Y = (numéros de port de destination, page 33)	Les trames avec le numéro de port de destination spécifié sont rejetées.
`Firewall Eth1 Allow port_type ports Y1 to Y2`	Y = (numéros de port de destination, page 33)	Les trames avec un numéro de port de destination appartenant à la plage indiquée sont autorisées.
`Firewall Eth1 Reject port_type ports Y1 to Y2`	Y = (numéros de port de destination, page 33)	Les trames avec un numéro de port de destination appartenant à la plage indiquée sont rejetées.
`Firewall Eth1 Allow IP •.•.•.• on port_type port Y`	• = 0 à 255 Y = (numéros de port de destination, page 33)	Les trames provenant de l'adresse IP spécifiée et avec le numéro de port de destination indiqué sont autorisées.
`Firewall Eth1 Reject IP •.•.•.• on port_type port Y`	• = 0 à 255 Y = (numéros de port de destination, page 33)	Les trames provenant de l'adresse IP spécifiée et avec le numéro de port de destination indiqué sont rejetées.
`Firewall Eth1 Allow IP •.•.•.• on port_type ports Y1 to Y2`	• = 0 à 255 Y = (numéros de port de destination, page 33)	Les trames provenant de l'adresse IP spécifiée et avec un numéro de port de destination appartenant à la plage indiquée sont autorisées.
`Firewall Eth1 Reject IP •.•.•.• on port_type ports Y1 to Y2`	• = 0 à 255 Y = (numéros de port de destination, page 33)	Les trames provenant de l'adresse IP spécifiée et avec un numéro de port de destination appartenant à la plage indiquée sont rejetées.
`Firewall Eth1 Allow IPs •1.•1.•1.•1 to •2.•2.•2.•2 on port_type port Y`	• = 0 à 255 Y = (numéros de port de destination, page 33)	Les trames en provenance d'une adresse IP figurant dans la plage spécifiée et avec le numéro de port de destination indiqué sont autorisées.
`Firewall Eth1 Reject IPs •1.•1.•1.•1 to •2.•2.•2.•2 on port_type port Y`	• = 0 à 255 Y = (numéros de port de destination, page 33)	Les trames provenant d'une adresse IP figurant dans la plage spécifiée et avec le numéro de port de destination indiqué sont rejetées.
`Firewall Eth1 Allow IPs •1.•1.•1.•1 to •2.•2.•2.•2 on port_type ports Y1 to Y2`	• = 0 à 255 Y = (numéros de port de destination, page 33)	Les trames provenant d'une adresse IP de la plage spécifiée et avec un numéro de port de destination appartenant à la plage indiquée sont autorisées.
`Firewall Eth1 Reject IPs •1.•1.•1.•1 to •2.•2.•2.•2 on port_type ports Y1 to Y2`	• = 0 à 255 Y = (numéros de port de destination, page 33)	Les trames provenant d'une adresse IP de la plage spécifiée et avec un numéro de port de destination appartenant à la plage indiquée sont rejetées.
`Firewall Eth1 Allow MAC ••:••:••:••:••:••`	• = 0 à F	Les trames provenant de l'adresse MAC spécifiée ••:••:••:••:••:•• sont autorisées. **NOTE:** Lorsque les règles autorisant l'adresse MAC sont appliquées, seules les adresses MAC répertoriées peuvent communiquer avec le contrôleur, même si d'autres règles sont autorisées.
`Firewall Eth1 Reject MAC ••:••:••:••:••:••`	• = 0 à F	Les trames provenant de l'adresse MAC indiquée ••:••:••:••:••:•• sont rejetées.

Commande	Plage	Description
`Firewall Ethx` (1) `Established to port_type port Y`	Y = 0 à 65535	Les trames établies à partir du contrôleur avec les protocoles TCP/UDP vers le numéro de port de destination spécifié sont autorisées.

(1) Si :

- x=0, port USB.
- x=1, port Ethernet 1.
- x=2, port Ethernet 2.
- x=3, port Ethernet du TMSES4 (premier module Ethernet à partir de la gauche).
- x=4, port Ethernet du TMSES4 (deuxième module Ethernet à partir de la gauche).
- x=5, port Ethernet du TMSES4 (troisième module Ethernet à partir de la gauche).

Exemple de script

L'exemple suivant porte sur un pare-feu en mode liste blanche. Toutes les communications sont bloquées par défaut et seuls les services nécessaires sont autorisés.

NOTE: Cet exemple vise à vous présenter la plupart des commandes disponibles avec le pare-feu. Vous avez tout intérêt à l'adapter à votre configuration et à le tester avant sa mise en œuvre.

Commandes	Commentaires
`Firewall Enable`	Active le pare-feu.
Configuration Eth1	
`Firewall Eth1 Default Reject`	Rejette toutes les trames sur l'interface ETH1. Dans cet exemple, l'interface ETH1 est connectée au réseau d'équipements Ethernet industriel et peut donc être considérée comme relativement fiable.
`Firewall Eth1 Allow TCP port 502`	Autorise le serveur Modbus TCP sur l'interface ETH1. Compte tenu de l'absence d'authentification sur Modbus, cela doit être autorisé uniquement sur les réseaux fiables.
`Firewall Eth1 Established to TCP port 502`	Autorise les réponses aux communications établies par le contrôleur sur le port TCP 502. Cela est nécessaire lorsque la bibliothèque PlcCommunication est utilisée pour communiquer à l'aide du protocole Modbus TCP.
`Firewall Eth1 Allow UDP port 2222`	Autorise les réponses d'échanges implicites du scrutateur ETHIP sur le port UDP 2222 (ETHIP) de l'interface ETH1.
`Firewall Eth1 Established to TCP port 44818`	Autorise les réponses aux communications établies par le contrôleur sur le port TCP 44818 (ETHIP) de l'interface ETH1. Les 2 dernières commandes autorisent le scrutateur EtheNetIP à communiquer avec les équipements de type Ethernet industriel.
Configuration Eth2	
`Firewall Eth2 Default Reject`	Rejette toutes les trames sur l'interface ETH2. Cette interface est connectée à un réseau utilisée principalement pour la mise en service.
`Firewall Eth2 Allow TCP port 4840`	Autorise le serveur OPC-UA sur l'interface ETH2.
`Firewall Eth2 Allow TCP port 443`	Autorise le serveur Web (https) sur l'interface ETH2.
`Firewall Eth2 Allow TCP port 8089`	Autorise web visu (https) sur l'interface ETH2.
`Firewall Eth2 Allow TCP ports 20 to 21`	Autorise ftp en mode actif sur l'interface ETH2.
`Firewall Eth2 Allow IP 192.168.1.1 on UDP ports 27126 to 27127`	Autorise l'adresse IP du PC de mise en service à découvrir et à configurer l'adresse IP du contrôleur. Cela doit être autorisé uniquement sur un réseau fiable, car l'adresse IP peut être changée même si les droits utilisateur sont configurés.

Commandes	Commentaires
`Firewall Eth2 Allow IPs 192.168.1.1 to 192.168.1.2 on UDP port 1740`	Autorise l'adresse IP du PC de mise en service et un HMI à communiquer avec le contrôleur à l'aide du protocole Machine Expert.
`Firewall Eth2 Allow TCP port 11740`	Autorise le protocole Fast TCP sur l'interface ETH2. Cela permet de se connecter au contrôleur à l'aide de TCP.
`Firewall Eth2 Allow TCP port 2222`	Autorise la communication implicite avec le port UDP 2222 (ETHIP) de l'interface ETH2.
`Firewall Eth2 Allow TCP port 44818`	Autorise la communication explicite sur le port TCP 44818 (ETHIP) de l'interface ETH2. Les 2 dernières commandes permettent d'utiliser le contrôleur comme adaptateur EtherNetIP.
`Firewall Eth2 Allow MAC 4C:CC:6A:A1:09:C8`	Autorise l'adresse MAC de l'IHM.
`Firewall Eth2 Allow MAC 00:0C:29:92:43:A8`	Autorise l'adresse MAC du PC de mise en service. Seule l'adresse MAC autorisée peut communiquer avec le contrôleur.
Configuration Eth3 TMSES4	
`Firewall Eth3 Default Reject`	Rejette les trames sur TMSES4. Cette interface est connectée au réseau de l'usine et peut accéder au Web. Elle doit être considérée comme non fiable.
`Firewall Eth3 Established to TCP port 443`	Autorise le client https (à se connecter à Machine Advisor, par exemple) sur l'interface TMSES4.
`Firewall Eth3 Allow TCP port 11740`	Autorise le protocole Fast TCP sur l'interface TMSES4. Cela permet de se connecter au contrôleur à distance. Il ne doit être autorisé que si les droits utilisateurs sont activés sur le contrôleur.

NOTE: Les caractères sont limités à 200 par ligne, commentaires inclus.

Ports utilisés

Protocole	Numéros de ports de destination
Machine Expert	UDP 1740, 1741, 1742, 1743 TCP 11740
FTP	TCP 21, 20
HTTP (1)	TCP 80 (1)
HTTPS	TCP 443
Modbus	TCP 502
Machine Expert Discovery	UDP 27126, 27127
Découverte dynamique des services Web	UDP 3702 TCP 5357
SNMP	UDP 161, 162
NVL	Valeur par défaut UDP : 1202
EtherNet/IP	UDP 2222 TCP 44818
Webvisualization	HTTP 8080 HTTPS 8089
TFTP	UDP 69 (utilisé pour le serveur FDR uniquement)
SafeLogger	UDP 35021, 45000
Machine Assistant	UDP 45001 à 45004
OPC UA	TCP 4840
DHCP	UDP 68
NTP	UDP 123
Service de découverte	UDP 5353
(1) Les requêtes HTTP vers le port TCP 80 seront redirigées pour utiliser HTTPS sur le port 443.	

Module de communication TMSCO1 CANopen

Introduction

Ce chapitre explique comment configurer le module de communication TMSCO1. CANopen.

Configuration de l'interface CANopen

Introduction

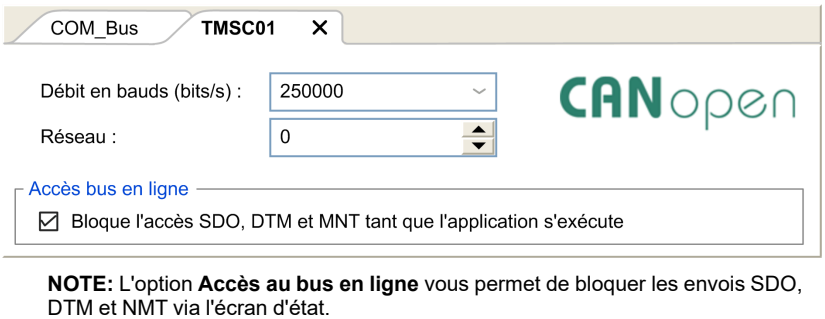
CANopen est un protocole de communication standard ouvert et une spécification de protocole d'équipement (EN 50325-4) qui repose sur le protocole CAN (Controller Area Network). Le protocole CAN de « couche 7 » a été développé pour les applications réseau intégrées et définit les fonctions de communication et d'équipement pour les systèmes CAN.

CANopen prend en charge les communications cycliques et pilotées par événement, ce qui vous permet de réduire la charge du bus au minimum tout en continuant de bénéficier de brefs temps de réaction.

Vous pouvez configurer vos communications CANopen à l'aide d'un module TMSCO1. Ce module se connecte au bus de communication (**COM_Bus**) situé sur le côté gauche du contrôleur, à l'aide de l'interface de connecteur de bus gauche. Vous pouvez connecter un seul module TMSCO1. Ce module doit être le dernier sur le côté gauche du contrôleur.

Configuration du bus CAN

Pour configurer le bus **CAN** de votre contrôleur, procédez comme suit :

Etape	Action
1	Ajoutez un module **TMSCO1**.
2	Dans l'arborescence **Equipements**, double-cliquez sur **TMSCO1**.
3	Configurez le débit de transmission (250 000 bits/s par défaut) :  **NOTE:** L'option **Accès au bus en ligne** vous permet de bloquer les envois SDO, DTM et NMT via l'écran d'état.

Lors de la connexion d'un DTM à un équipement à l'aide du réseau, le DTM communique en parallèle avec l'application en cours d'exécution. Les performances globales du système en sont affectées. Il peut en résulter une surcharge du réseau qui aurait des conséquences sur la cohérence des données sur les équipements sous contrôle.

⚠AVERTISSEMENT

FONCTIONNEMENT D'EQUIPEMENT NON INTENTIONNEL

Placez votre machine ou processus dans un état tel que les communications DTM n'affectent pas ses performances.

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

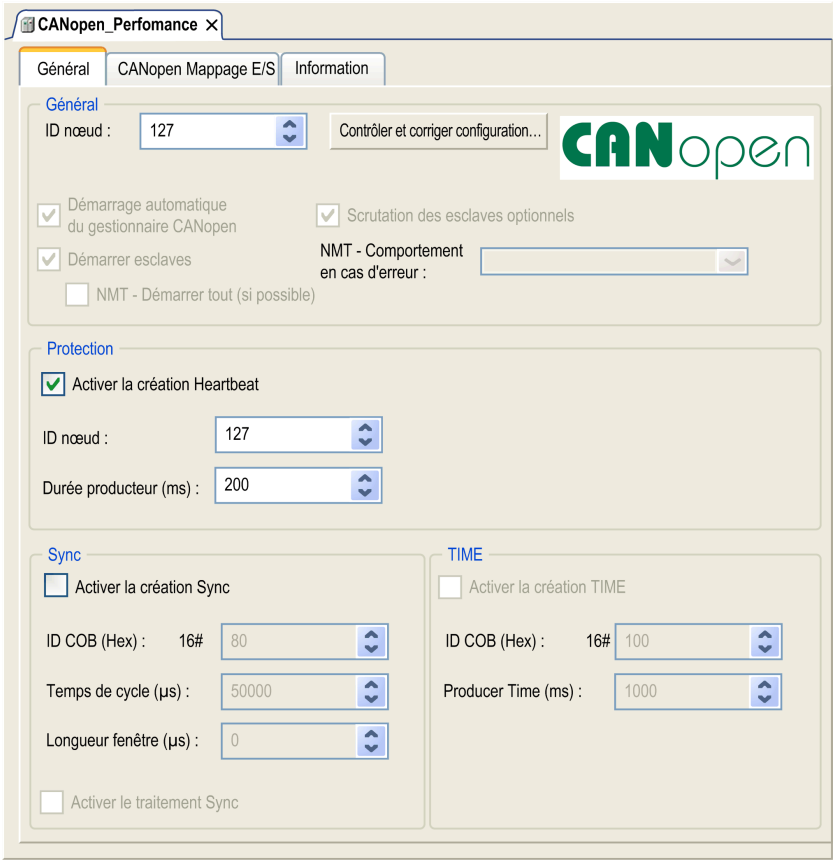
Ajout d'un gestionnaire Performance CANopen

L'ajout d'un module **TMSCO1** a pour effet d'ajouter automatiquement la fonctionnalité de gestionnaire **Performance CANopen** à votre contrôleur.

Configuration d'un gestionnaire Performance CANopen

Pour configurer les **Performances CANopen**, double-cliquez sur **COM_Bus > TMSCO1 > Performances CANopen** dans l'arborescence **Equipements**.

La boîte de dialogue suivante s'affiche :



L'onglet **Général** de la boôte de dialogue de configuration **CANopen_ Performance** se divise en quatre sections :

- **Général** : Informations générales comprenant l'ID de nœud et les options de configuration activées.
- **Guarding** : Si l'option **Activer la génération Heartbeat** est sélectionnée, la protection Guarding est activée et le maître NMT peut vérifier l'état de chaque noeud. Le mécanisme Heartbeat permet au maître du réseau de détecter une perte de communication des esclaves du réseau et à ces derniers de répondre à une perte de communication du maître. Par défaut, le mécanisme heartbeat est configuré pour produire à 200 ms.
- **Sync** : Si l'option **Activer la création Sync** est sélectionnée, un objet d'événement spécifique est ajouté. La tâche **TMSCO1_Sync** est ajoutée au nœud **Application > Configuration de tâche** dans l'arborescence **Applications**.

  Si vous désélectionnez la case **Activer la création Sync** dans cette boîte de dialogue, la tâche **TMSCO1_Sync** est automatiquement supprimée de l'arborescence **Applications** dans votre programme.

  NOTE: Ne supprimez pas et ne modifiez pas les attributs **Type** ou **Événement externe** des tâches **TMSCO1_Sync**. Sinon, EcoStruxure Machine Expert détectera une erreur au moment de générer l'application et vous ne pourrez pas télécharger cette dernière sur le contrôleur.
- **TIME** : Non modifiable.

Limites de fonctionnement de CANopen

Le maître CANopen présente les limites de fonctionnement suivantes :

Nombre maximum d'équipements esclaves	63
Nombre maximum de PDO reçus (RPDO)	252
Nombre maximum de PDO transmis (TPDO)	252

⚠AVERTISSEMENT

FONCTIONNEMENT IMPRÉVU DE L'ÉQUIPEMENT

- Ne connectez pas plus de 63 équipements esclaves CANopen au contrôleur
- Programmez votre application de sorte qu'elle utilise au maximum 252 PDO de transmission (TPDO).
- Programmez votre application de sorte qu'elle utilise au maximum 252 PDO de réception (RPDO).

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

Format de bus CAN

Le format du bus CAN est CAN2.0A pour CANopen.

Glossaire

A

adresse MAC:

(*media access control*) Nombre unique sur 48 bits associé à un élément matériel spécifique. L'adresse MAC est programmée dans chaque carte réseau ou équipement lors de la fabrication.

ARP:

(*address resolution protocol*). Protocole de couche réseau IP pour Ethernet qui affecte une adresse IP à une adresse (matérielle) MAC.

B

BOOTP:

(*bootstrap protocol*). Protocole réseau UDP qu'un client réseau peut utiliser pour obtenir automatiquement une adresse IP (et éventuellement d'autres données) à partir d'un serveur. Le client s'identifie auprès du serveur à l'aide de son adresse MAC. Le serveur, qui gère un tableau préconfiguré des adresses MAC des équipements client et des adresses IP associées, envoie au client son adresse IP préconfigurée. A l'origine, le protocole BOOTP était utilisé pour amorcer à distance les hôtes sans lecteur de disque à partir d'un réseau. Le processus BOOTP affecte une adresse IP de durée illimitée. Le service BOOTP utilise les ports UDP 67 et 68.

C

CANopen:

Protocole de communication standard ouvert et spécification de profil d'équipement (EN 50325-4).

D

DHCP:

Acronyme de *dynamic host configuration protocol*. Extension avancée du protocole BOOTP. Bien que DHCP soit plus avancé, DHCP et BOOTP sont tous les deux courants. (DHCP peut gérer les requêtes de clients BOOTP.)

DNS:

Acronyme de *Domain Name System*, système de nom de domaine. Système d'attribution de nom pour les ordinateurs et les équipements connectés à un réseau local (LAN) ou à Internet.

DTM:

(*device type manager*) réparti en deux catégories :

- DTMs d'équipement connectés aux composants de la configuration d'équipements de terrain.
- CommDTMs connectés aux composants de communication du logiciel.

Le DTM fournit une structure unifiée pour accéder aux paramètres d'équipements et pour configurer, commander et diagnostiquer les équipements. Les DTMs peuvent être une simple interface utilisateur graphique pour définir des paramètres d'équipement ou au contraire une application très élaborée permettant d'effectuer des calculs complexes en temps réel pour le diagnostic et la maintenance.

E

EDS:

Acronyme de *electronic data sheet*, fiche de données électronique. Fichier de description des équipements de bus de terrain qui contient notamment les propriétés d'un équipement telles que paramètres et réglages.

EtherNet/IP:

Acronyme de *Ethernet Industrial Protocol*, protocole industriel Ethernet. Protocole de communication ouvert pour les solutions d'automatisation de la production dans les systèmes industriels. EtherNet/IP est une famille de réseaux mettant en œuvre le protocole CIP au niveau des couches supérieures. L'organisation ODVA spécifie qu'EtherNet/IP permet une adaptabilité générale et une indépendance des supports.

Ethernet:

Technologie de couche physique et de liaison de données pour les réseaux locaux (LANs) également appelée IEEE 802.3.

I

ICMP:

Acronyme de *Internet Control Message Protocol*. Le protocole ICMP signale les erreurs et fournit des informations sur le traitement des datagrammes.

IGMP:

Acronyme de *Internet Group Management Protocol*). Protocole de communications utilisé par les hôtes et les routeurs adjacents sur les réseaux IPv4 pour définir l'appartenance au groupe de multidiffusion.

IP:

Acronyme de *Internet Protocol*, protocole Internet. Le protocole IP fait partie de la famille de protocoles TCP/IP, qui assure le suivi des adresses Internet des équipements, achemine les messages sortants et reconnaît les messages entrants.

M

MSB:

Acronyme de *most significant bit/byte*, bit/octet de poids fort. Partie d'un nombre, d'une adresse ou d'un champ qui est écrite le plus à gauche dans une valeur en notation hexadécimale ou binaire classique.

N

NMT:

Abréviation de *network management*, gestion réseau. Protocoles CANopen qui assurent des services tels que l'initialisation du réseau, le contrôle des erreurs détectées et le contrôle de l'état des équipements.

P

PDO:

Acronyme de *process data object*, objet de données de processus. Message de diffusion non confirmé ou envoyé par un équipement producteur à un équipement consommateur dans un réseau CAN. L'objet PDO de transmission provenant de l'équipement producteur dispose d'un identificateur spécifique correspondant à l'objet PDO de réception de l'équipement consommateur.

protocole:

Convention ou définition standard qui contrôle ou permet la connexion, la communication et le transfert de données entre 2 systèmes informatiques et leurs équipements.

R

réseau de commande:

Réseau incluant des contrôleurs logiques, des systèmes SCADA, des PC, des IHM, des commutateurs, etc.

Deux types de topologies sont pris en charge :

- à plat : tous les modules et équipements du réseau appartiennent au même sous-réseau.
- à 2 niveaux : le réseau est divisé en un réseau d'exploitation et un réseau intercontrôleurs.

Ces deux réseaux peuvent être indépendants physiquement, mais ils sont généralement liés par un équipement de routage.

RPI:

Acronyme de « *(Requested Packet Interval)* » (intervalle entre paquets demandés). Période entre deux échanges de données cycliques demandés par le scrutateur. Les équipements EtherNet/IP publient des données selon l'intervalle spécifié par le RPI que le scrutateur leur a affecté et reçoivent des requêtes de message du scrutateur à chaque RPI.

RSTP:

Acronyme de (*Rapid Spanning Tree Protocol*). Protocole de réseau haut débit qui crée une topologie logique sans boucle pour les réseaux Ethernet.

S

SDO:

Acronyme de *service data object*, objet de données de service. Message utilisé par le maître de bus de terrain pour accéder (lecture/écriture) aux répertoires d'objets des noeuds réseau dans les réseaux CAN. Les types de SDO sont les SDOs de service (SSDOs) et les SDOs client (CSDOs).

T

TCP:

Acronyme de *transmission control protocol*, protocole de contrôle de transmission. Protocole de couche de transport basé sur la connexion qui assure la transmission de données simultanée dans les deux sens. Le protocole TCP fait partie de la suite de protocoles TCP/IP.

TPDO:

Acronyme de *transmit process data object*, objet de données de processus de transmission. Message de diffusion non confirmé ou envoyé par un équipement producteur à un équipement consommateur dans un réseau CAN. L'objet PDO de transmission provenant de l'équipement producteur dispose d'un identificateur spécifique correspondant à l'objet PDO de réception de l'équipement consommateur.

U

UDP:

Acronyme de *User Datagram Protocol*, protocole de datagramme utilisateur. Protocole de mode sans fil (défini par la norme IETF RFC 768) dans lequel les messages sont livrés dans un datagramme vers un ordinateur cible sur un réseau IP. Le protocole UDP est généralement fourni en même temps que le protocole Internet. Les messages UDP/IP n'attendent pas de réponse et, de ce fait, ils sont particulièrement adaptés aux applications dans lesquelles aucune retransmission des paquets envoyés n'est nécessaire (comme dans la vidéo en continu ou les réseaux exigeant des performances en temps réel).

Index

C

E

M

P

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.

EIO0000003692.04