

# Modicon TMS

## Modules d'extension

### Guide de programmation

05/2019



EIO0000003692.00

[www.schneider-electric.com](http://www.schneider-electric.com)

**Schneider**  
Electric

---

Le présent document comprend des descriptions générales et/ou des caractéristiques techniques des produits mentionnés. Il ne peut pas être utilisé pour définir ou déterminer l'adéquation ou la fiabilité de ces produits pour des applications utilisateur spécifiques. Il incombe à chaque utilisateur ou intégrateur de réaliser l'analyse de risques complète et appropriée, l'évaluation et le test des produits pour ce qui est de l'application à utiliser et de l'exécution de cette application. Ni la société Schneider Electric ni aucune de ses sociétés affiliées ou filiales ne peuvent être tenues pour responsables de la mauvaise utilisation des informations contenues dans le présent document. Si vous avez des suggestions, des améliorations ou des corrections à apporter à cette publication, veuillez nous en informer.

Vous acceptez de ne pas reproduire, excepté pour votre propre usage à titre non commercial, tout ou partie de ce document et sur quelque support que ce soit sans l'accord écrit de Schneider Electric. Vous acceptez également de ne pas créer de liens hypertextes vers ce document ou son contenu. Schneider Electric ne concède aucun droit ni licence pour l'utilisation personnelle et non commerciale du document ou de son contenu, sinon une licence non exclusive pour une consultation « en l'état », à vos propres risques. Tous les autres droits sont réservés.

Toutes les réglementations locales, régionales et nationales pertinentes doivent être respectées lors de l'installation et de l'utilisation de ce produit. Pour des raisons de sécurité et afin de garantir la conformité aux données système documentées, seul le fabricant est habilité à effectuer des réparations sur les composants.

Lorsque des équipements sont utilisés pour des applications présentant des exigences techniques de sécurité, suivez les instructions appropriées.

La non-utilisation du logiciel Schneider Electric ou d'un logiciel approuvé avec nos produits matériels peut entraîner des blessures, des dommages ou un fonctionnement incorrect.

Le non-respect de cette consigne peut entraîner des lésions corporelles ou des dommages matériels.

© 2019 Schneider Electric. Tous droits réservés.

---

# Table des matières

---



	<b>Consignes de sécurité</b> .....	<b>5</b>
	<b>A propos de ce manuel</b> .....	<b>7</b>
<b>Chapitre 1</b>	<b>Description des modules TMS</b> .....	<b>11</b>
	TMS- Description générale .....	<b>12</b>
	Configuration du bus de communication ( <b>COM_Bus</b> ) .....	<b>13</b>
	Ajout d'un module d'extension .....	<b>16</b>
<b>Chapitre 2</b>	<b>TMSES4 Ethernet Module</b> .....	<b>17</b>
2.1	Services Ethernet .....	<b>18</b>
	Présentation .....	<b>19</b>
	Configuration de l'adresse IP .....	<b>21</b>
	Modicon M262 Logic/Motion Controller en tant qu'équipement cible sur EtherNet/IP .....	<b>26</b>
	Modicon M262 Logic/Motion Controller en tant qu'équipement esclave sur Modbus TCP .....	<b>28</b>
2.2	Configuration du pare-feu .....	<b>34</b>
	Introduction .....	<b>35</b>
	Procédure de modification dynamique .....	<b>37</b>
	Comportement du pare-feu .....	<b>38</b>
	Commandes de script de pare-feu .....	<b>40</b>
<b>Chapitre 3</b>	<b>Module de communication TMSCO1 CANopen</b> .....	<b>47</b>
	Configuration de l'interface CANopen .....	<b>47</b>
<b>Glossaire</b>	.....	<b>51</b>
<b>Index</b>	.....	<b>55</b>



# Consignes de sécurité



## Informations importantes

### AVIS

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



## Présentation

### Objectif 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 V1.1.

### Document(s) à consulter

Titre de documentation	Référence
EcoStruxure Machine Expert - Guide de programmation	<a href="#">EIO0000002854 (ENG)</a> <a href="#">EIO0000002855 (FRE)</a> <a href="#">EIO0000002856 (GER)</a> <a href="#">EIO0000002858 (SPA)</a> <a href="#">EIO0000002857 (ITA)</a> <a href="#">EIO0000002859 (CHS)</a>
Modicon M262 Logic/Motion Controller - Guide de programmation	<a href="#">EIO0000003651 (ENG)</a> <a href="#">EIO0000003652 (FRA)</a> <a href="#">EIO0000003653 (GER)</a> <a href="#">EIO0000003654 (SPA)</a> <a href="#">EIO0000003655 (ITA)</a> <a href="#">EIO0000003656 (CHS)</a> <a href="#">EIO0000003657 (POR)</a> <a href="#">EIO0000003658 (TUR)</a>
Modules d'extension TMS - Guide de référence du matériel	<a href="#">EIO0000003691 (ENG)</a> <a href="#">EIO0000003692 (FRA)</a> <a href="#">EIO0000003693 (GER)</a> <a href="#">EIO0000003694 (SPA)</a> <a href="#">EIO0000003695 (ITA)</a> <a href="#">EIO0000003696 (CHS)</a> <a href="#">EIO0000003697 (POR)</a> <a href="#">EIO0000003698 (TUR)</a>

Titre de documentation	Référence
Modules d'extension TMSES4 - Instruction de service	<a href="#">PHA44907</a>
Modules d'extension TMSCO1 - Instruction de service	<a href="#">PHA44909</a>

Vous pouvez télécharger ces publications et autres informations techniques depuis notre site web à l'adresse : <https://www.schneider-electric.com/en/download>

### Information spécifique au produit

 <b>AVERTISSEMENT</b>
<p><b>PERTE DE CONTROLE</b></p>
<ul style="list-style-type: none"> <li>● Le concepteur d'un système de commande doit envisager les modes de défaillance possibles des chemins de commande et, pour certaines fonctions de commande critiques, prévoir un moyen d'atteindre un état sécurisé en cas de défaillance d'un chemin, et après cette défaillance. Par exemple, l'arrêt d'urgence, l'arrêt en cas de surcourse, la coupure de courant et le redémarrage sont des fonctions de contrôle cruciales.</li> <li>● Des canaux de commande séparés ou redondants doivent être prévus pour les fonctions de commande critique.</li> <li>● Les liaisons de communication peuvent faire partie des canaux de commande du système. Soyez particulièrement attentif aux implications des retards de transmission imprévus ou des pannes de liaison.</li> <li>● Respectez toutes les réglementations de prévention des accidents ainsi que les consignes de sécurité locales.<sup>1</sup></li> <li>● Chaque implémentation de cet équipement doit être testée individuellement et entièrement pour s'assurer du fonctionnement correct avant la mise en service.</li> </ul>
<p><b>Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.</b></p>

<sup>1</sup> 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 son équivalent en vigueur dans votre pays.

## AVERTISSEMENT

### FONCTIONNEMENT IMPREVU DE L'EQUIPEMENT

- 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.

Norme	Description
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.

---

# Chapitre 1

## Description des modules TMS

---

### Contenu de ce chapitre

Ce chapitre contient les sujets suivants :

Sujet	Page
TMS- Description générale	12
Configuration du bus de communication ( <b>COM_Bus</b> )	13
Ajout d'un module d'extension	16

## TMS- Description générale

### Introduction

Les modules d'extension TMS prennent place sur le côté gauche du contrôleur et sont dédiés aux communications à haut débit 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
TMSES4	Communication Ethernet	RJ45
TMSCO1	Module maître CANopen	SUB-D 9 broches, mâle

**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 <b>Equipements</b> , double-cliquez sur <b>COM_Bus</b> : <b>Résultat</b> : la fenêtre de configuration <b>COM_Bus</b> s'affiche.
2	Cliquez sur l'un des onglets : <ul style="list-style-type: none"> <li>● <b>Bus TMS</b></li> <li>● <b>Mappage E/S</b></li> <li>● <b>Tableau de diagnostic</b></li> </ul>

### 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 <b>Adresse réseau</b> .
2	Saisissez la nouvelle adresse réseau. <b>Résultat</b> : les champs <b>Masque de sous-réseau</b> , <b>Min hôte</b> et <b>Max hôte</b> sont mis à jour automatiquement.

### 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** indique 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
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	

## Ajout d'un module d'extension

### Ajout d'un module d'extension

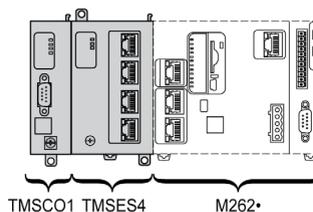
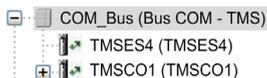
Pour ajouter un module d'extension à votre contrôleur, sélectionnez-le dans le **Catalogue de matériels**, faites-le glisser vers l'arborescence **Equipements** et déposez-le sur le nœud **COM\_Bus**.

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

- Utilisation de la méthode glisser-déposer (*voir EcoStruxure Machine Expert, Guide de programmation*)
- Utilisation du Menu contextuel ou du bouton Plus (*voir EcoStruxure Machine Expert, Guide de programmation*)

### 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 :



### Configuration d'un module d'extension

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

---

# Chapitre 2

## TMSES4 Ethernet Module

---

### Introduction

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

### Contenu de ce chapitre

Ce chapitre contient les sous-chapitres suivants :

Sous-chapitre	Sujet	Page
2.1	Services Ethernet	18
2.2	Configuration du pare-feu	34

## Sous-chapitre 2.1

### Services Ethernet

---

#### Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Présentation	19
Configuration de l'adresse IP	21
Modicon M262 Logic/Motion Controller en tant qu'équipement cible sur EtherNet/IP	26
Modicon M262 Logic/Motion Controller en tant qu'équipement esclave sur Modbus TCP	28

## 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 (*voir page 20*)
- 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 (*voir page 26*)
- M262 Logic/Motion Controller en tant qu'équipement esclave sur Modbus TCP (*voir page 28*)
- Accès IEC VAR (*voir page 20*)

### 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 présente le total de connexions serveur TCP pour le contrôleur et les modules TMSES4 :

Type de connexion	Nombre maximum de connexions serveur
Serveur Modbus	8
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 tous les autres cas, la tentative d'établissement 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.

Toutes les connexions serveur restent ouvertes tant que le contrôleur conserve l'un des états opérationnels (RUN, STOP ou HALT).

Toutes les connexions serveur sont fermées lorsque le contrôleur passe à un état opérationnel (RUN, STOP ou HALT) ou le quitte, sauf en cas de coupure de courant (car le contrôleur n'a pas eu le temps de fermer les connexions).

Pour plus d'informations sur les états opérationnels, reportez-vous au diagramme des états du 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 des sorties numériques (%Q)
2 (2h)	–	Lecture des entrées numériques (%I)
3 (3h)	–	Lecture du 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, consultez le document EcoStruxure Machine Expert - Guide de programmation.

## Configuration de l'adresse IP

### Introduction

Lorsque TMSES4 n'est pas configuré, il démarre et son adresse IP par défaut automatiquement affectée est 10.12.x.x.

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. 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 dans EcoStruxure Machine Expert ;
- le bloc fonction **changeIPAddress**.

**NOTE** : Si la méthode d'adressage essayée échoue, le lien 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 IMPREVU DE L'EQUIPEMENT

- 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.

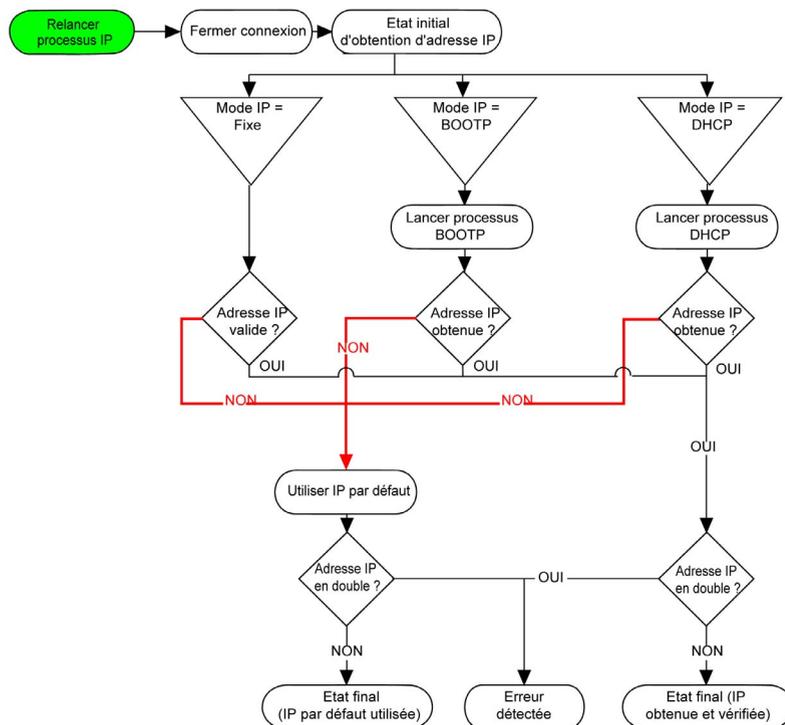
**Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.**

**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, 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 échec d'une tentative d'adressage

## Ethernet Configuration

Double-cliquez sur **TMSES4** dans l'arborescence **Equipements**.

The screenshot displays the Ethernet Configuration interface with the following details:

- Paramètres configurés (Active):**
  - Nom du réseau: my\_Device
  - Adresse IP par DHCP:
  - Adresse IP par BOOTP:
  - Adresse IP fixe:
  - Adresse IP: 192 . 168 . 0 . 50
  - Masque de sous-réseau: 255 . 255 . 255 . 0
  - Adresse de la passerelle: 0 . 0 . 0 . 0
  - Protocole Ethernet: Ethernet 2
  - Vitesse de transfert: Auto
- Paramètres de sécurité:**
  - Protocoles inactifs: (Empty list)
  - Protocoles actifs:
    - Protocole de découverte
    - Serveur FTP
    - Protocole Machine Expert
    - Serveur Modbus
    - Connexion distante (Fast TCP)
    - Serveur Web sécurisé (HTTPS)
    - Protocole SNMP
    - Serveur Web (HTTP)
    - Protocole de visualisation Web
- Etat de l'adaptateur:**
  - MAC Address: 00:80:F4:4E:00:BA
  - Etat réseau: Echanges de données

**Remarque :** En mode connecté (en ligne), deux fenêtres s'affichent. Vous ne pouvez pas les modifier. En mode déconnecté (hors ligne), la fenêtre **Paramètres configurés** est affichée. Vous pouvez la modifier.

Le tableau suivant décrit les paramètres configurés :

Paramètres configurés	Description
<b>Nom du réseau</b>	Utilisé comme nom d'équipement pour récupérer l'adresse IP via le protocole DHCP (15 caractères maximum).
<b>Adresse IP par DHCP</b>	L'adresse IP est obtenue par le serveur DHCP.
<b>Adresse IP par BOOTP</b>	L'adresse IP est obtenue par le serveur BOOTP. L'adresse MAC est située sur le côté gauche du contrôleur.
<b>Adresse IP fixe</b>	L'adresse IP, le masque de sous-réseau et l'adresse de passerelle sont définis par l'utilisateur.
<b>Protocole Ethernet</b>	Type de protocole utilisé : Ethernet2
<b>Vitesse de transfert</b>	Vitesse et duplex sont en mode autonégociation.

### 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 la 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 inconnus transite par cette interface.

## Paramètres de sécurité

Le tableau suivant décrit les différents paramètres de sécurité :

Paramètres de sécurité	Description
<b>Protocole de découverte</b>	Ce paramètre désactive le protocole Discovery. Lorsqu'il est désactivé, les requêtes Discovery sont ignorées.
<b>Serveur FTP</b>	Ce paramètre désactive le serveur FTP du contrôleur. Lorsqu'il est désactivé, les requêtes FTP sont ignorées.
<b>Protocole Machine Expert</b>	Ce paramètre désactive le protocole Machine Expert sur les interfaces Ethernet. Lorsqu'il est désactivé, chaque requête Machine Expert provenant de chaque équipement est rejetée . 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.
<b>Serveur Modbus</b>	Ce paramètre désactive le serveur Modbus du contrôleur. Lorsqu'il est désactivé, chaque requête Modbus adressée au contrôleur est ignorée.
<b>Connexion à distance</b>	Ce paramètre désactive la connexion à distance. Lorsqu'elle est désactivée, les requêtes Fast TCP sont ignorées.
<b>Serveur Web sécurisé</b>	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.
<b>Protocole SNMP</b>	Ce paramètre désactive le serveur SNMP du contrôleur. Lorsqu'il est désactivé, les requêtes SNMP sont ignorées.
<b>Serveur Web</b>	Ce paramètre désactive le serveur Web du contrôleur. Lorsqu'il est désactivé, les requêtes HTTP adressées au serveur Web du contrôleur sont ignorées.
<b>Protocole WebVisualisation</b>	Ce paramètre désactive les pages de visualisation Web du contrôleur. Lorsqu'elles sont désactivées, les requêtes HTTP adressées au protocole WebVisualisation du contrôleur logique sont ignorées.

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

### Introduction

Cette section explique comment configurer votre 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](http://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.

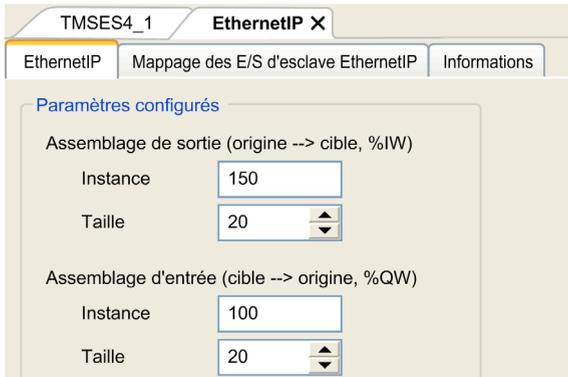
Pour ajouter un gestionnaire EthernetIP à votre M262 Logic/Motion Controller :

Etape	Action
1	Ajoutez un module d'extension TMSES4 à votre configuration.
2	<p>A partir du nœud <b>TMSES4</b> de l'arborescence <b>Equipements</b>, ajoutez le <b>gestionnaire EthernetIP</b> en le sélectionnant dans le <b>catalogue de matériels</b>. Faites-le glisser vers l'arborescence <b>Equipements</b>, puis déposez-le sur le nœud <b>TMSES4</b>.</p> <p>Pour plus d'informations sur l'ajout d'un équipement à votre projet, consultez :</p> <ul style="list-style-type: none"><li>• Utilisation de la méthode glisser-déposer (<i>voir EcoStruxure Machine Expert, Guide de programmation</i>)</li><li>• Utilisation du Menu contextuel ou du bouton Plus (<i>voir EcoStruxure Machine Expert, Guide de programmation</i>)</li></ul>

## Configuration des paramètres EtherNet/IP

Pour configurer les paramètres EtherNet/IP, double-cliquez sur **COM\_Bus** → **TM4** → **EthernetIP** dans l'arborescence Equipements.

La boîte de dialogue suivante s'affiche :



Les paramètres de configuration d'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 la **taille** de l'**assemblage de sortie** est égale à 20, il existe 20 voies d'entrée (IW0 à IW19) qui adressent  $\%IWy... \%IW(y+20-1)$ ,  $y$  étant la première voie disponible pour l'assemblage.

Élément		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

Consultez le 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 explique comment configurer votre M262 Logic/Motion Controller en tant qu'**équipement esclave Modbus TCP**.

Pour configurer votre M262 Logic/Motion Controller en tant qu'**équipement esclave Modbus TCP**, vous devez ajouter la fonctionnalité **Equipement esclave Modbus TCP** à votre contrôleur (consultez 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 doit accéder aux objets %IW et %QW du contrôleur. Cette fonctionnalité **Equipement esclave Modbus TCP** vous permet de fournir les objets d'E/S du contrôleur à cette zone, qui est ensuite accessible à l'aide d'une requête Modbus de lecture/écriture de registres.

La fonctionnalité **Equipement esclave Modbus TCP** ajoute une fonction de serveur Modbus supplémentaire au contrôleur. L'application cliente Modbus identifie ce serveur en spécifiant un ID d'unité configuré (adresse Modbus) entre 1 et 247. Le serveur Modbus intégré du contrôleur esclave ne requiert aucune configuration et est identifié par un ID d'unité égal à 255. Consultez la section Configuration de Modbus TCP (*voir page 29*).

Les entrées/sorties sont visibles depuis le contrôleur : elles sont respectivement écrites et 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. En l'absence de requête Modbus dans le délai d'expiration, les informations de diagnostic `i_byMasterIpLost` sont définies sur 1 (TRUE). Pour plus d'informations, consultez la section relative aux Variables système en lecture seule du port 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](http://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	Ajouter un module d'extension TMSES4 à votre configuration.
2	<p>A partir du nœud <b>TMSES4</b> de l'arborescence <b>Equipements</b>, ajoutez l'<b>équipement esclave Modbus TCP</b> en le sélectionnant dans le <b>catalogue de matériels</b>. Faites-le glisser vers l'arborescence <b>Equipements</b>, puis déposez-le sur le nœud <b>TMSES4</b>.</p> <p>Pour plus d'informations sur l'ajout d'un équipement à votre projet, consultez :</p> <ul style="list-style-type: none"> <li>• Utilisation de la méthode glisser-déposer (<i>voir EcoStruxure Machine Expert, Guide de programmation</i>)</li> <li>• Utilisation du Menu contextuel ou du bouton Plus (<i>voir EcoStruxure Machine Expert, Guide de programmation</i>)</li> </ul>

## Configuration d'un équipement esclave Modbus TCP

Pour configurer Equipement esclave Modbus TCP, double-cliquez sur → **TMSES4** → **ModbusTCP\_Slave\_Device** dans l'arborescence **Equipements**.

La boîte de dialogue suivante s'affiche :

TMSES4\_1 ModbusTCP\_Slave\_Device X

Général Mappage des E/S d'équipement esclave Modbus TCP Informations

Paramètres configurés

Adresse maître IP : 0 . 0 . 0 . 0

Horloge de surveillance : 2000 (ms)

Port esclave : 502

ID unité : 247

Registres de stockage (%IW): 10

Registres d'entrée (%QW): 10

Modèle de données

Start Addresses:

Bobines : 0

Entrées discrètes : 0

Registre de stockage : 0

Registre d'entrée : 0

Superposition des zones de données de registre de stockage et d'entrée

Élément	Description
<b>Adresse maître IP</b>	Adresse IP du maître Modbus. Les connexions ne sont pas fermées à cette adresse.
<b>Chien de garde</b>	Timeout par incréments de 500 ms. <b>NOTE</b> : Le timeout s'applique à l' <b>Adresse IP maître</b> , sauf si l'adresse est 0.0.0.0.
<b>Port esclave</b>	Port de communication Modbus (502).
<b>ID unité</b>	Envoie les requêtes à l'Équipement esclave Modbus TCP (1 à 247), au lieu du serveur Modbus intégré (255).
<b>Registres de stockage (%IW)</b>	Nombre de registres %IW à utiliser dans l'échange (2 à 120) (chaque registre stocke 2 octets)
<b>Registres d'entrée (%QW)</b>	Nombre de registres %QW à utiliser dans l'échange (2 à 120) (chaque registre stocke 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 entrées %IW sont en lecture/écriture et mappées du registre 0 au registre n-1 (n = nombre de registres de stockage %IW, faisant chacun 2 octets).
- Les sorties %QW sont en lecture seule et mappées du registre n au registre n+m -1 (m = nombre de registres d'entrée %QW, chacun faisant 2 octets).

Dès lors qu'un **équipement esclave Modbus TCP** est configuré, les commandes Modbus envoyées à son ID d'unité (adresse Modbus) sont traitées différemment que si elles étaient adressées à un autre équipement Modbus du réseau. Ainsi, lorsque la commande Modbus 3 (3 hex) est envoyée sur un équipement Modbus standard, elle lit et renvoie la valeur d'un ou de plusieurs registres. Quand cette même commande est envoyée à l'esclave Modbus TCP, elle permet une opération de lecture par le scrutateur d'E/S externe.

Dès lors qu'un **équipement esclave Modbus TCP** est configuré, les commandes Modbus envoyées à son ID d'unité (adresse Modbus) accèdent aux objets %IW et %QW du contrôleur, liés à l'équipement Modbus TCP, et non aux mots Modbus standard (accessibles avec l'ID d'unité 255). Une application de scrutateur d'E/S Modbus TCP peut alors effectuer des opérations de lecture/écriture.

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. L'équipement esclave Modbus TCP prend en charge les commandes Modbus suivantes :

Code fonction (en hexadécimal)	Fonction	Commentaire
3 (3)	Lecture du registre de maintien	Permet au maître de lire les objets %IW et %QW de l'équipement.
6 (6)	Ecriture dans un registre	Permet au maître d'écrire les objets %IW de l'équipement.
16 (10)	Ecriture dans 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 de l'équipement.
Autre	Non pris en charge	-

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

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

TMSSES4\_1
ModbusTCP\_Slave\_Device X

Général
Mappage des E/S d'équipement esclave Modbus TCP
Informations

Rechercher
Filtre
Afficher tout

Variable	Mappage	Voie	Adresse	Type	Valeur par défaut	Valeur	Unité	Description
		Entrées	%IW21	ARRAY[0...9]...				Registres de stockage Modbus
		Entrées[0]	%IW21	WORD		0		
		Entrées[1]	%IW22	WORD		0		
		Entrées[2]	%IW23	WORD		0		
		Entrées[3]	%IW24	WORD		0		
		Entrées[4]	%IW25	WORD		0		
		Entrées[5]	%IW26	WORD		0		
		Entrées[6]	%IW27	WORD		0		
		Entrées[7]	%IW28	WORD		0		
		Entrées[8]	%IW29	WORD		0		
		Entrées[9]	%IW30	WORD		0		
		Sorties	%QW21	ARRAY[0...9]...				Registres d'entrée Modbus
		Sorties[0]	%QW21	WORD		0		
		Sorties[1]	%QW22	WORD		0		
		Sorties[2]	%QW23	WORD		0		
		Sorties[3]	%QW24	WORD		0		
		Sorties[4]	%QW25	WORD		0		
		Sorties[5]	%QW26	WORD		0		
		Sorties[6]	%QW27	WORD		0		
		Sorties[7]	%QW28	WORD		0		
		Sorties[8]	%QW29	WORD		0		
		Sorties[9]	%QW30	WORD		0		

Réinitialiser le mappage

Toujours actualiser les variables:

Activé 1 (utiliser tâche du cycle de bus si elle n'est utilisée dans aucune tâche)

= Créer une nouvelle variable
 = Mapper sur une variable existante

Options de cycle de bus  
 Tâche de cycle de bus Utiliser les paramètres de cycle du bus supérieur

Voie		Type	Description
<b>Entrée</b>	IW0	WORD	Registre de stockage 0
	...	à	à
	IWx	WORD	Registre de stockage x
<b>Sortie</b>	QW0	WORD	Registre d'entrée 0
	...	à	à
	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 du 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 chargée d'actualiser les registres %IW et %QW.

## Sous-chapitre 2.2

### Configuration du pare-feu

---

#### Introduction

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

#### Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Introduction	35
Procédure de modification dynamique	37
Comportement du pare-feu	38
Commandes de script de pare-feu	40

## 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 (*voir page 37*) physique.
- Un bloc fonction (*voir page 37*) dans l'application.

## Paramètres d'application

Consultez Configuration Ethernet (*voir page 23*)

## Procédure de modification dynamique

### À l'aide d'une carte SD

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

Étape	Action
1	Créez un fichier de script ( <i>voir page 40</i> ) valide. Par exemple, nommez le fichier de script <i>FirewallMaintenance.cmd</i> .
2	Chargez le fichier de script sur la carte SD. Par exemple, chargez le fichier de script dans le dossier <i>usr/Cfg</i> .
3	Dans le fichier <i>Sys/Cmd/Script.cmd</i> , ajoutez une ligne de code contenant la commande <code>Firewall_install "/pathname/FileName"</code> Par exemple, la ligne de code est <code>Firewall_install "/sd0/usr/Cfg/FirewallMaintenance.cmd"</code> <b>NOTE</b> : Le nom de fichier fait la distinction entre les majuscules et les minuscules.
4	Branchez la carte SD au contrôleur.

### À l'aide d'un bloc fonction dans une application

Ce tableau décrit la procédure d'exécution d'un fichier de script à partir d'une application.

Étape	Action
1	Créez un fichier de script ( <i>voir page 40</i> ) valide. Par exemple, nommez le fichier de script <i>FirewallMaintenance.cmd</i> .
2	Chargez le fichier de script dans la mémoire du contrôleur. Par exemple, chargez le fichier de script dans le dossier <i>usr/Syslog</i> avec FTP.
3	Utilisez un bloc fonction <code>ExecuteScript</code> . Pour plus d'informations, consultez le document Guide de la bibliothèque du système M262 ( <i>voir Modicon M262 Logic/Motion Controller, Fonctions et variables système, Guide de la bibliothèque système</i> ). Par exemple, l'entrée <b>[SCmd]</b> est <code>'Firewall_install "/usr/Syslog/FirewallMaintenance.cmd"'</code> <b>NOTE</b> : 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. Les états initiaux possibles sont au nombre de cinq :

- 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 de l'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.
Téléchargement de l'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.
Téléchargement de l'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.
Téléchargement de l'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.
Téléchargement de l'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 la section 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, toute communication sur les interfaces Ethernet est impossible. <b>NOTE :</b> Par défaut, lorsque le pare-feu est activé, les trames sont rejetées.
Firewall Disable	Les adresses IP peuvent accéder au contrôleur sur les interfaces Ethernet.
Firewall Ethx Default Allow <sup>(1)</sup>	Le contrôleur accepte les trames.
Firewall Ethx Default Reject <sup>(1)</sup>	Le contrôleur rejette les trames. <b>NOTE :</b> Cela correspond par défaut à la commande Firewall Eth1 Default Reject, en l'absence de ligne.
<b>(1) Où Ethx =</b> <ul style="list-style-type: none"> <li>● Eth1 : Ethernet_1</li> <li>● Eth2 : Ethernet_2</li> <li>● Eth3 : TMSES4</li> </ul>	

## 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, quel que soit leur type.
Firewall Eth1 Allow port_type port Y	Y = (numéro du port de destination <i>(voir page 45)</i> )	Les trames avec le numéro de port de destination spécifié sont autorisées.
Firewall Eth1 Reject port_type port Y	Y = (numéro du port de destination <i>(voir page 45)</i> )	Les trames avec le numéro de port de destination spécifié sont rejetées.
Firewall Eth1 Allow port_type ports Y1 to Y2	Y = (numéro du port de destination <i>(voir page 45)</i> )	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 = (numéro du port de destination <i>(voir page 45)</i> )	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...255 Y = (numéro du port de destination <i>(voir page 45)</i> )	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...255 Y = (numéro du port de destination <i>(voir page 45)</i> )	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...255 Y = (numéro du port de destination <i>(voir page 45)</i> )	Les trames provenant de l'adresse IP spécifiée et avec un numéro de port de destination appartenant à la plage indiquée sont autorisées.
<b>(1) Si :</b> <ul style="list-style-type: none"> <li>● x=0, port USB.</li> <li>● x=1, port Ethernet 1.</li> <li>● x=2, port Ethernet 2.</li> <li>● x=3, port Ethernet de TMSES4.</li> </ul>		

Commande	Plage	Description
Firewall Eth1 Reject IP *.*.*.* on port_type ports Y1 to Y2	• = 0...255 Y = (numéro du port de destination <i>(voir page 45)</i> )	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...255 Y = (numéro du port de destination <i>(voir page 45)</i> )	Les trames provenant d'une adresse IP de 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...255 Y = (numéro du port de destination <i>(voir page 45)</i> )	Les trames provenant d'une adresse IP de 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...255 Y = (numéro du port de destination <i>(voir page 45)</i> )	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...255 Y = (numéro du port de destination <i>(voir page 45)</i> )	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.  <b>NOTE</b> : 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.
Firewall Ethx <sup>(1)</sup> Established to port_type port Y	Y = 0 à 65535	Les trames établies du contrôleur avec les protocoles TCP/UDP vers le numéro de port de destination spécifié sont autorisées.
<b>(1) Si :</b> <ul style="list-style-type: none"> <li>● x=0, port USB.</li> <li>● x=1, port Ethernet 1.</li> <li>● x=2, port Ethernet 2.</li> <li>● x=3, port Ethernet de TMSES4.</li> </ul>		

**Exemple de script**

```

; Enable FireWall. All frames are rejected;
FireWall Enable;
; Allow frames on Eth1
FireWall Eth1 Default Allow;
; Block all Modbus Requests on all IP address
Firewall Eth1 Reject tcp port 502;
; Reject frames on Eth2
FireWall Eth2 Default Reject;
; Allow FTP active connection for IP address 85.16.0.17
FireWall Eth2 Allow IP 85.16.0.17 on tcp ports 20 to 21;

```

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.
<b>Configuration Eth1</b>	
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 port 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.
Firewall Eth2 Allow IP 192.168.1.1 to IP 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'IMH.
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 Eth3TMSES4

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 http (par exemple pour se connecter à Machine Advisor) 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**

<b>Protocole</b>	<b>Numéros de ports de destination</b>
Machine Expert	UDP 1740, 1741, 1742, 1743 TCP 11740
FTP	TCP 21, 20
HTTP	TCP 80
HTTPS	TCP 443
Modbus	TCP 502
Découverte Machine Expert	UDP 27126, 27127
Découverte dynamique des services Web	UDP 3702 TCP 5357
SNMP	UDP 161, 162
NVL	UDP Valeur par défaut : 1202
EtherNet/IP	UDP 2222 TCP 44818
Webvisualization	HTTP 8080 HTTPS 8089



---

# Chapitre 3

## Module de communication TMSCO1 CANopen

---

### Configuration de l'interface CANopen

#### Introduction

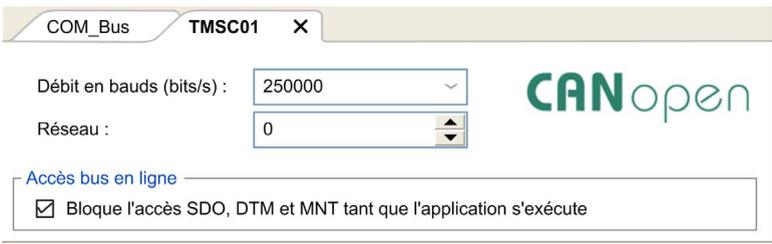
CANopen est un protocole de communication standard ouvert et une spécification de protocole d'équipement (EN 50325-4) qui repose sur le protocole CAN (Controller Area Network). Le protocole CAN de « couche 7 » a été développé pour les applications réseau intégrées et définit les fonctions de communication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

Etape	Action
1	Ajoutez un module <b>TMSCO1</b> .
2	Dans l'arborescence <b>Equipements</b> , double-cliquez sur <b>TMSCO1</b> .
3	<p>Configurez la vitesse en bauds (250 000 bits/s, par défaut) :</p>  <p><b>NOTE</b> : L'option <b>Accès bus en ligne</b> permet de bloquer l'envoi SDO, DTM et NMT via l'écran d'état.</p>

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 IMPREVU DE L'EQUIPEMENT

Placez votre machine ou processus dans un état tel que les communications DTM n'affecteront 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 la fonctionnalité **Performance CANopen**, double-cliquez sur **COM\_Bus** → **TMSCO1** → **Performance CANopen** dans l'arborescence **Equipements**.

La boîte de dialogue suivante s'affiche :

**CANopen\_Performance** X

General | CANopen I/O Mapping | Information

General

Node ID: 127

Autostart CANopenManager  Polling of Optional Slaves  
 Start Slaves NMT Error Behaviour:   
 NMT Start All (if possible)

▲ Guarding

Enable Heartbeat Producing

New ID: 127  
 Producer Time (ms): 200

▲ Sync ▲ TIME

Enable Sync Producing  Enable TIME Producing

COB-ID (Hex): 16# 80 COB-ID (Hex): 16# 100  
 Cycle Period (µs): 50000 Producer Time (ms): 1000  
 Window Length (µs): 0

Enable Sync Consuming

La boîte de dialogue de configuration **CANopen\_Performance** se divise en quatre zones :

- **Général** : informations générales contenant l'ID de nœud et les options de configuration activées.
- **Protection** : si **Activer Heartbeat Producing** est sélectionné, la surveillance est activée et le maître NMT peut vérifier individuellement l'état actuel de chaque nœud. 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 Producing est défini sur 200 ms.
- **Sync** : si **Activer la création Sync** est sélectionné, 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 l'option **Activer la création Sync** dans l'onglet **Général** de la boîte de dialogue **Performance CANopen**, la tâche **TMSCO1\_Sync** est automatiquement supprimée de l'arborescence **Applications** de votre programme.  
**NOTE** : Ne supprimez pas et ne modifiez pas les attributs **Type** et **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 IMPREVU DE L'EQUIPEMENT

- 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.



## 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.)

## 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

### Ethernet

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

### 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.

## 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.

**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.

**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).



## C

commandes de script  
pare-feu, *40*

## E

Ethernet  
  équipement esclave Modbus TCP, *28*  
EtherNet  
  Équipement EtherNet/IP, *26*  
Ethernet  
  Services, *19*

## M

modules d'extension  
  ajout, *16*  
  configuration, *16*

## P

pare-feu  
  commandes de script, *40*  
  configuration, *38*  
  fichier de script par défaut, *38*  
Protocoles, *19*  
  IP, *21*

