DTM de communication TCP Modbus

Manuel utilisateur

02/2019

EIO0000000366.06

www.schneider-electric.com

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

	Consignes de sécurité	5
	A propos de ce manuel	7
Chapitre 1	**Configuration matérielle et logicielle requise**	9
	Configuration système requise	10
	Compatibilité	11
	Installation et suppression	12
Chapitre 2	**Types de connexion et modèles de communication**	13
	Type de connexion	14
	Modèle de communication	15
Chapitre 3	**Interface utilisateur graphique**	17
	Interface utilisateur graphique	17
Chapitre 4	**Configuration**	21
	Onglet Configuration	22
	Onglet Exécution	25
	Table d'adresses	29
	Configuration de la scrutation	31
Chapitre 5	**Cybersécurité**	35
	Présentation de la cybersécurité	36
	Recommandations de Schneider Electric	38
Glossaire		41
Index		45

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 manuel utilisateur décrit l'utilisation du DTM (Device Type Manager) de communication du Modbus.

Champ d'application

Ce document a été mis à jour suite au lancement de la bibliothèque Modbus Communication Library V2.6.9.

Information spécifique au produit

⚠ AVERTISSEMENT

PERTE DE CONTROLE

- 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.
- Des canaux de commande séparés ou redondants doivent être prévus pour les fonctions de commande critique.
- Les chemins de commande système peuvent inclure les liaisons de communication. Soyez particulièrement attentif aux implications des retards de transmission imprévus ou des pannes de liaison.
- Respectez toutes les réglementations de prévention des accidents ainsi que les consignes de sécurité locales.[1]
- Chaque implémentation de cet équipement doit être testée individuellement et entièrement pour s'assurer du fonctionnement correct avant la mise en service.

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

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

Chapitre 1
Configuration matérielle et logicielle requise

Contenu de ce chapitre

Ce chapitre contient les sujets suivants :

Sujet	Page
Configuration système requise	10
Compatibilité	11
Installation et suppression	12

Configuration système requise

Configuration matérielle requise

Configuration requise	Minimum	Recommandé
Ordinateur	Pentium 4 ou équivalent	
RAM	1 Go	2 Go
Espace disponible sur le disque dur du système	100 Mo	
Espace disponible sur le disque dur du lecteur d'installation	100 Mo	
Fichier d'échange	1024 Mo	2048 Mo
Ecran	SVGA 256 couleurs, résolution 800 x 600	XGA couleurs vraies, résolution 1024 x 768

Configuration logicielle requise

Systèmes d'exploitation

Système d'exploitation	Edition/Service Pack	Remarques
Windows 7 32 bits	SP1	Vous devez avoir des droits d'accès d'administrateur pour installer le DTM de communication Modbus TCP
Windows 7 64 bits	SP1	
Windows 8.1, 10 Professionnel	–	

Logiciels installés sur l'ordinateur

Logiciel	Edition	Remarques
Microsoft.NET Framework	V2.0 SP2	–
Application cadre FDT	FDT 1.2 ou FDT 1.2.1	Le DTM de communication Modbus TCP requiert une application cadre FDT conforme la norme FDT. Cette application cadre FDT doit prendre en charge Microsoft.NET Framework 2.0.

Compatibilité

Compatibilité avec FDT

Le Modbus Comm DTM est conforme aux normes FDT 1.2 et FDT 1.2.1. Il s'appuie sur l'annexe Modbus 1.0 de FDT.

Compatibilité avec Modbus

Le Modbus Comm DTM prend en charge les services Modbus inclus dans la spécification 1.1b du Protocole d'application Modbus.

Installation et suppression

Installation

Double-cliquez sur le fichier *setup.exe* et suivez les instructions de l'assistant d'installation.

Dépose

Pour supprimer le DTM de votre ordinateur, sélectionnez **Démarrer → Paramètres → Panneau de configuration → Ajout/Suppression de programmes**.

Chapitre 2
Types de connexion et modèles de communication

Présentation

Ce chapitre présente les différentes configurations permettant d'établir des communications Modbus.

Contenu de ce chapitre

Ce chapitre contient les sujets suivants :

Sujet	Page
Type de connexion	14
Modèle de communication	15

Type de connexion

Présentation

Le DTM de communication Modbus TCP permet d'établir une communication Modbus selon le type de connexion suivant :

Connexion TCP

Le DTM de communication Modbus TCP permet d'établir une communication Modbus sur TCP. La connexion est établie via l'adaptateur réseau Ethernet du PC.

Modèle de communication

Présentation

Ce chapitre décrit le modèle de communication pris en charge par le DTM de communication Modbus TCP.

NOTE : La technologie FDT n'est pas conçue pour transférer les données en temps réel. Selon votre système et votre modèle de communication, les données peuvent ne pas refléter l'état en temps réel de l'équipement.

⚠ AVERTISSEMENT

INFORMATIONS INCORRECTES SUR L'ETAT DE L'EQUIPEMENT

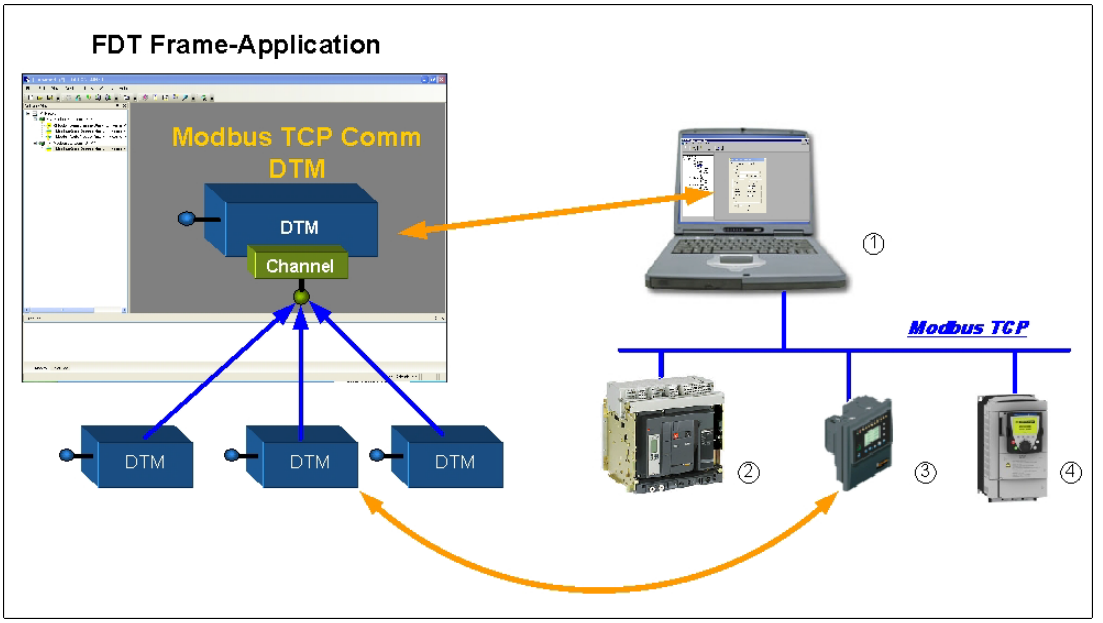
N'utilisez pas le Modbus Comm DTM pour contrôler ou surveiller des tâches stratégiques car les données transférées peuvent ne pas correspondre à l'état réel de l'équipement. La technologie FDT n'est pas conçue à cet effet.

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

Connexion réseau

Le DTM de communication Modbus TCP permet d'établir une communication Modbus entre l'ordinateur et l'équipement cible sur un réseau Ethernet.

Dans cette configuration, le DTM de communication Modbus TCP joue le rôle de client Modbus.



1 Ordinateur avec DTM de communication Modbus TCP
2 - 4 Equipements cibles

Chapitre 3
Interface utilisateur graphique

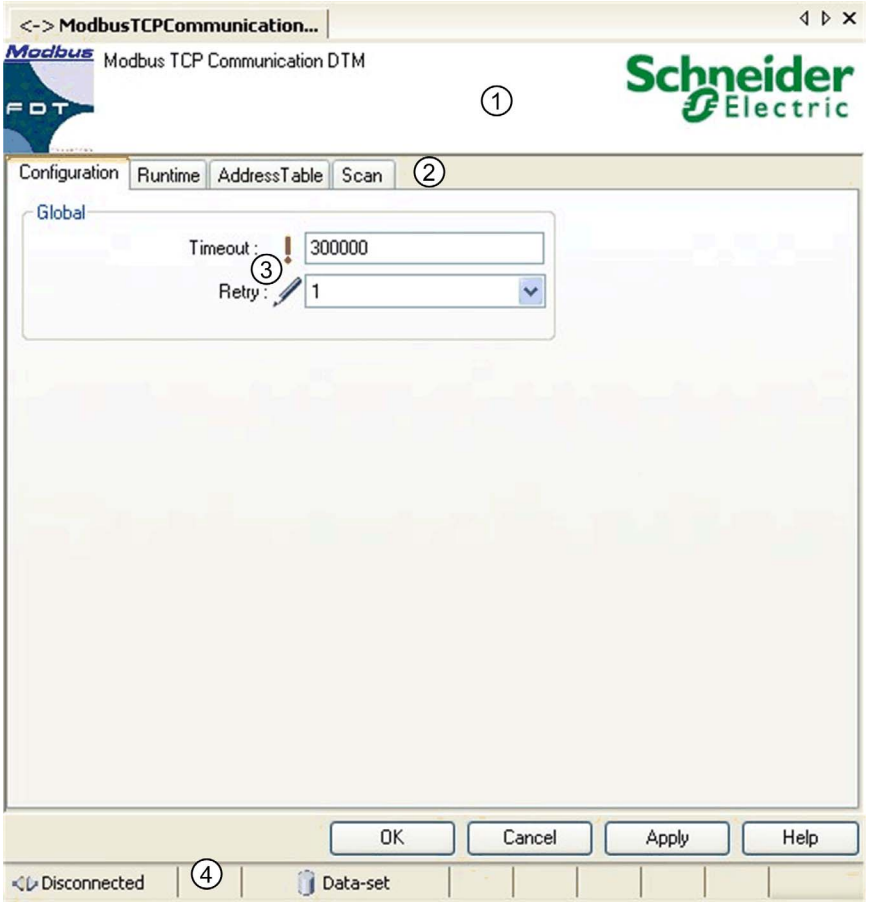
Interface utilisateur graphique

Présentation

Ce chapitre décrit l'interface utilisateur graphique du DTM de communication Modbus TCP.

Présentation

La figure suivante présente l'interface utilisateur du DTM.



1 Zone d'identification
2 Menu de tabulation
3 Icônes d'état de paramètre
4 Barre d'état

Zone d'identification

Zone indiquant le nom et la version du DTM.

Menu à onglet

Menu permettant d'accéder aux différents fonctions du DTM.

Icônes d'état de paramètre

Icônes fournissant des informations sur l'état courant du paramètre.

Etats possibles du paramètre

Icône	Signification
	Le paramètre a été modifié et sa valeur est non valide.
	Le paramètre a été modifié et sa valeur est valide.

Barre d'état

Barre fournissant des informations sur l'état courant du DTM.

Etats possibles de la connexion

Icône	Texte	Signification	Etat du DTM
	Connecter	Connexion en cours	Mise en ligne
	Connecté	Connecté	En ligne
	Déconnecter	Déconnexion en cours	Mise hors ligne
	Interrompu	Interrompu	Interruption de communication détectée
	Déconnecté	Déconnecté	Tous les autres états

Etats possibles de la source de données

Icône	Texte	Comportement
	Jeu de données	Les valeurs affichées sont chargées à partir du jeu de données de l'instance. Les valeurs modifiées ne sont affectées qu'au jeu de données de l'instance.
	Jeu de données verrouillé	Les valeurs affichées sont chargées à partir du jeu de données de l'instance. Le jeu de données est verrouillé.

Chapitre 4
Configuration

Contenu de ce chapitre

Ce chapitre contient les sujets suivants :

Sujet	Page
Onglet Configuration	22
Onglet Exécution	25
Table d'adresses	29
Configuration de la scrutation	31

Onglet Configuration

Présentation

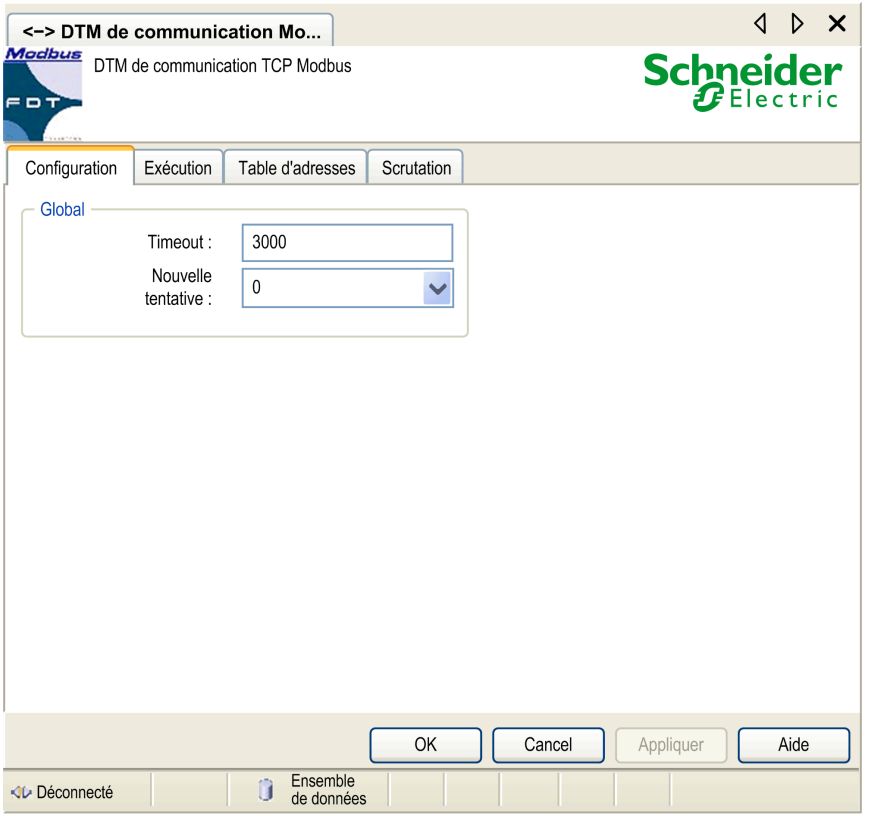
L'onglet **Configuration** du DTM de communication Modbus TCP contient les paramètres de communication.

Onglet Configuration

Pour accéder à l'onglet **Configuration** du DTM de communication Modbus TCP, plusieurs solutions s'offrent à vous :

- Dans la vue réseau de votre application cadre FDT, cliquez deux fois sur l'icône DTM de communication Modbus TCP.
- Dans la vue réseau de votre application cadre FDT, cliquez avec le bouton droit de la souris sur l'icône DTM de communication Modbus TCP, puis cliquez sur **Configuration**.

La figure suivante illustre l'onglet **Configuration** de la boîte de dialogue DTM de communication Modbus TCP :



Paramètres de communication

Ce tableau décrit les paramètres de communication de la connexion Modbus TCP.

Paramètre	Description	Valeur par défaut
Timeout global	Timeout de réponse du serveur Modbus.	3000 ms
Nombre de tentatives	Nombre de renvois de la requête Modbus par le DTM de communication Modbus TCP sur la connexion TCP, en cas de timeout de communication.	0

Commandes de configuration

Commandes de configuration disponibles dans l'onglet **Configuration**

Commande	Description
Ok	Les paramètres sont enregistrés et la fenêtre DTM de communication Modbus TCP est fermée. Les nouvelles valeurs des paramètres seront appliquées lors de la prochaine connexion.
Annuler	Les modifications apportées aux paramètres sont annulées et la fenêtre DTM de communication Modbus TCP est fermée. Les valeurs d'origine seront appliquées lors de la prochaine connexion.
Appliquer	Les paramètres sont enregistrés et la fenêtre DTM de communication Modbus TCP reste ouverte. Les nouvelles valeurs des paramètres seront appliquées lors de la prochaine connexion.

Onglet Exécution

Introduction

Le DTM de communication Modbus TCP fournit différents types d'informations d'exécution. Ce chapitre décrit les informations fournies par le DTM de communication Modbus TCP et la configuration de la fonction de journalisation.

Onglet Exécution

Le DTM de communication Modbus TCP fournit différents types d'informations d'exécution, qui permettent de surveiller les communications établies.

Les informations d'exécution sont disponibles dans l'onglet **Exécution** du DTM de communication Modbus TCP, accessible au choix comme suit :

- Dans la vue réseau de votre application cadre FDT, double-cliquez sur l'icône du DTM de communication Modbus TCP. Ensuite, sélectionnez l'onglet **Exécution**.
- Dans la vue réseau de votre application cadre FDT, cliquez avec le bouton droit de la souris sur l'icône du DTM de communication Modbus TCP, puis cliquez sur **Configuration**. Ensuite, sélectionnez l'onglet **Exécution**.

La figure suivante illustre l'onglet **Exécution** de la boîte de dialogue du DTM de communication Modbus TCP :



Commandes de configuration

Le tableau suivant propose une description des commandes de configuration disponibles dans l'onglet **Exécution** :

Commande	Description
OK	Les paramètres sont enregistrés et la fenêtre du DTM de communication Modbus TCP est fermée. Les nouvelles valeurs des paramètres seront appliquées lors de la prochaine connexion.

Commande	Description
Annuler	Les modifications apportées aux paramètres sont annulées et la fenêtre du DTM de communication Modbus TCP est fermée. Les valeurs d'origine seront appliquées lors de la prochaine connexion.
Parcourir	Ouvre un navigateur permettant de spécifier le chemin d'accès au fichier journal.
Réinitialiser	Remet tous les paramètres d'exécution à zéro.
Appliquer	Les paramètres sont enregistrés et la fenêtre du DTM de communication Modbus TCP reste ouverte. Les nouvelles valeurs des paramètres seront appliquées lors de la prochaine connexion.

Paramètres d'exécution

Le tableau suivant propose une description des paramètres d'exécution disponibles dans l'onglet **Exécution** du DTM de communication Modbus TCP :

Commande	Description
Connexions	Nombre de connexions actives au DTM de communication Modbus TCP.
Messages envoyés	Nombre de messages envoyés par le DTM de communication Modbus TCP.
Messages reçus	Nombre de messages reçus par le DTM de communication Modbus TCP.
Exceptions	Nombre de messages d'exception Modbus reçus par le DTM de communication Modbus TCP.
Timeouts	Nombre d'erreurs de timeout détectées en réception.

Fichier journal

Le DTM de communication Modbus TCP permet de créer un fichier journal. Dans le champ **Fichier journal**, spécifiez le répertoire dans lequel enregistrer le fichier journal.

Le tableau suivant décrit les informations qui seront consignées dans le fichier journal selon le **mode de journalisation** sélectionné :

Mode de journalisation	Description
Désactivé	Désactive la fonction de fichier journal.
Journalisation des erreurs	Seules les informations sur les erreurs de timeout détectées et les exceptions Modbus reçues sont consignées dans le fichier journal.
Journalisation complète	Outre les informations sur les erreurs de timeout détectées et les exceptions Modbus reçues, les informations concernant les requêtes Modbus envoyées, les réponses Modbus reçues et les requêtes reçues du DTM de l'équipement sont consignées dans le fichier journal.

Recommandation pour une meilleure cybersécurité

Le fichier journal contient des données généralement sensibles, du type :
- Adresses d'équipement
- Noms d'équipement
- Détails sur la topologie du réseau
- Détails sur la configuration du réseau

Il est stocké sur le disque dur de votre PC. Supprimez-le dès que vous n'en avez plus besoin ou stockez-le dans un endroit sécurisé contre les accès non autorisés.

Table d'adresses

Présentation

Le Modbus Comm DTM fournit une table d'adresses qui répertorie les DTM d'équipement connectés et leurs adresses cibles. Ce chapitre décrit les informations fournies dans la table d'adresses ainsi que la configuration des adresses cibles des équipements.

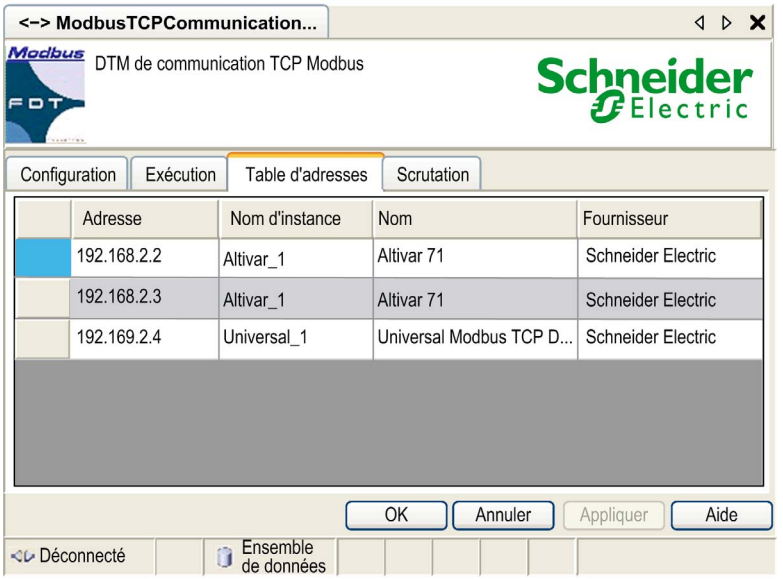
Table d'adresses

Le DTM de communication Modbus TCP fournit une table d'adresses qui répertorie les DTM d'équipement connectés et leurs adresses cibles. Dans cette table, vous pouvez spécifier les adresses cibles des DTM d'équipement connectés.

Pour accéder à l'onglet **Table d'adresses**, procédez au choix comme suit :

- Dans la vue réseau de votre application cadre FDT, cliquez deux fois sur l'icône du DTM de communication Modbus TCP. Ensuite, sélectionnez l'onglet **Table d'adresses**.
- Dans la **Vue réseau** de votre application cadre FDT, cliquez avec le bouton droit de la souris sur l'icône du DTM de communication Modbus TCP, puis cliquez sur **Configuration**. Ensuite, sélectionnez l'onglet **Table d'adresses**.

La figure suivante illustre l'onglet **Table d'adresses** de la boîte de dialogue DTM de communication Modbus TCP :



Commandes de configuration

Le tableau suivant propose une description des commandes de configuration disponibles dans l'onglet **Table d'adresses** :

Commande	Description
OK	Les modifications sont enregistrées et la fenêtre du DTM de communication Modbus TCP est fermée. Les nouvelles valeurs seront appliquées lors de la prochaine connexion.
Annuler	Les modifications sont annulées et la fenêtre du DTM de communication Modbus TCP est fermée. Les valeurs d'origine seront appliquées lors de la prochaine connexion.
Appliquer	Les modifications sont enregistrées et la fenêtre du DTM de communication Modbus TCP reste ouverte. Les nouvelles valeurs seront appliquées lors de la prochaine connexion.

Informations sur les adresses

Le tableau suivant propose une description des informations d'adresse disponibles dans l'onglet **Table d'adresses** du DTM de communication Modbus TCP :

Paramètre	Description
Adresse	Adresse cible de l'équipement physique, qui doit être configurée avec le DTM connecté
Nom de l'instance	Nom d'instance du DTM
Nom	Nom du DTM
Fournisseur	Nom du fournisseur du DTM

Affectation d'adresse

La table d'adresses du DTM de communication Modbus TCP permet de spécifier l'adresse cible de l'équipement physique, qui doit être configurée avec un DTM spécifique. Pour spécifier l'adresse cible, vous devez saisir la nouvelle adresse dans le champ **Adresse** de ce DTM et valider cette modification en cliquant sur le bouton **Appliquer** ou **OK**.

Configuration de la scrutation

Présentation

Le Modbus Comm DTM permet de spécifier la plage d'adresses pour la scrutation du FDT. Ce chapitre décrit la configuration des paramètres de scrutation du FDT.

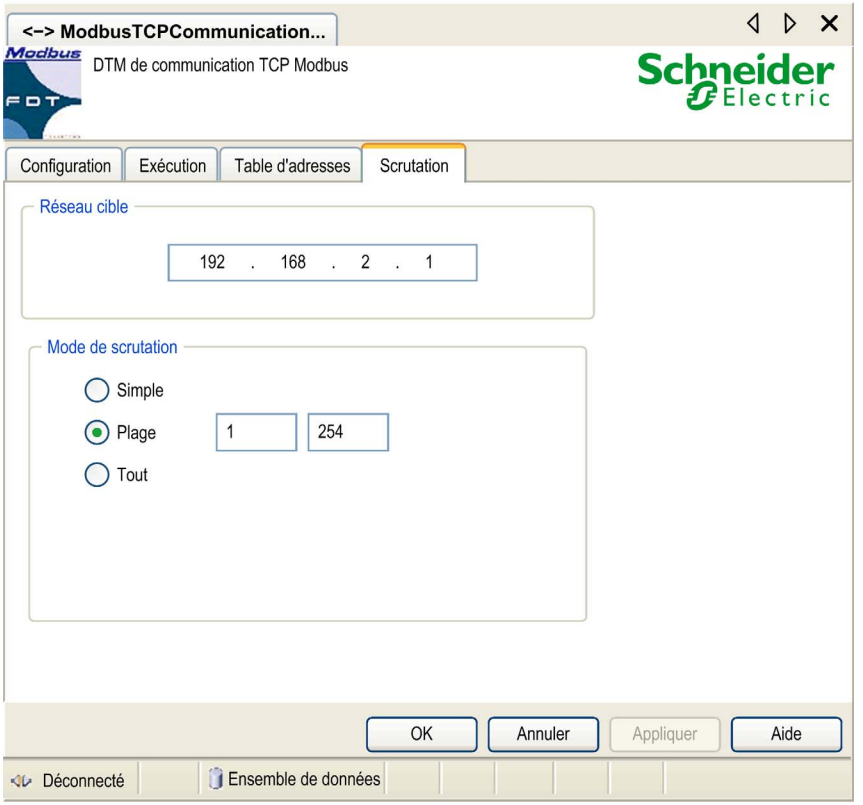
Onglet Scrutation

Le DTM de communication Modbus TCP prend en charge la fonction de scrutation telle qu'elle est définie dans la spécification V1.2.1 du FDT. La scrutation génère automatiquement la topologie du réseau de communication sous-jacent. Le DTM de communication Modbus TCP permet de spécifier la plage des adresses scrutées.

Les paramètres de scrutation sont disponibles dans l'onglet **Scrutation** du DTM de communication Modbus TCP, accessible au choix comme suit :

- Dans la **Vue réseau** de votre application cadre FDT, cliquez deux fois sur l'icône du DTM de communication Modbus TCP. Ensuite, sélectionnez l'onglet **Scrutation**.
- Dans la **Vue réseau** de votre application cadre FDT, cliquez avec le bouton droit de la souris sur l'icône du DTM de communication Modbus TCP, puis cliquez sur **Configuration**. Ensuite, sélectionnez l'onglet **Scrutation**.

La figure suivante montre l'onglet **Scrutation** de la boîte de dialogue DTM de communication Modbus TCP :



Commandes de configuration

Le tableau suivant propose une description des commandes de configuration disponibles dans l'onglet **Scrutation** :

Commande	Description
Ok	Les modifications sont enregistrées et la fenêtre Modbus Comm DTM est fermée. Les nouvelles valeurs seront appliquées lors de la prochaine scrutation.
Annuler	Les modifications sont annulées et la fenêtre Modbus Comm DTM est fermée. Les valeurs d'origine seront appliquées lors de la prochaine scrutation.

Commande	Description
Appliquer	Les modifications sont enregistrées et la fenêtre Modbus Comm DTM reste ouverte. Les nouvelles valeurs seront appliquées lors de la prochaine scrutation.

Paramètres de scrutation pour TCP Modbus

Le tableau suivant propose une description des paramètres de scrutation disponibles dans l'onglet **Scrutation** du DTM de communication Modbus TCP :

Commande	Description	
Réseau cible	Spécifie la plage réseau à scruter.	
Mode de scrutation	**Simple**	Ne scrute qu'une adresse d'un équipement cible dans la plage comprise entre 0 et 255 de la plage réseau spécifiée.
	Plage	Scrute une plage d'adresses spécifiée entre 0 et 255 dans la plage réseau définie.
	Tout	Scrute toute la plage d'adresses de la plage réseau (toutes les adresses entre 0 et 255).

Chapitre 5
Cybersécurité

Introduction

La cybersécurité est une branche de l'administration de réseau, qui s'occupe des attaques ciblant les systèmes informatiques ou émanant d'ordinateurs via des réseaux informatiques, qui peuvent entraîner des perturbations accidentelles ou intentionnelles. Son objectif est de mieux protéger les informations et les actifs physiques contre le vol, les dommages, une utilisation abusive ou des accidents, tout en les maintenant accessibles à leurs utilisateurs.

Aucune approche, à elle seule, ne peut garantir la cybersécurité. Schneider Electric recommande une approche de défense en profondeur. Conçue par la National Security Agency (NSA) américaine, celle-ci jalonne le réseau avec des fonctionnalités, des appliances et des processus de sécurité. Ses composants de base sont les suivants :

- évaluation des risques ;
- plan de sécurité élaboré en fonction des résultats de l'évaluation des risques ;
- campagne de formation en plusieurs phases ;
- séparation physique des réseaux industriels des réseaux d'entreprise avec une zone dite démilitarisée (DMZ) et utilisation de parefeu et du routage pour créer d'autres zones de sécurité ;
- contrôle des accès au système ;
- renforcement des équipements ;
- surveillance et maintenance du réseau.

Ce chapitre définit les éléments qui vous aident à configurer un système moins vulnérable aux cyberattaques. Pour plus d'informations sur l'approche de défense en profondeur, consultez le document *TVDA : How Can I Reduce Vulnerability to Cyber Attacks in the Control Room* sur le *Schneider Electric website*.

Contenu de ce chapitre

Ce chapitre contient les sujets suivants :

Sujet	Page
Présentation de la cybersécurité	36
Recommandations de Schneider Electric	38

Présentation de la cybersécurité

Introduction

Les cybermenaces désignent des actions volontaires ou non, susceptibles de perturber le fonctionnement normal des systèmes et réseaux informatiques. Ces actions peuvent être déclenchées dans les locaux ou à l'extérieur de l'entreprise. Les défis de l'environnement de contrôle en matière de sécurité sont les suivants :

- diversité des limites physiques et logiques ;
- multiplicité des sites et ampleur des zones géographiques ;
- effets négatifs de la sécurité sur la disponibilité des processus ;
- vulnérabilité accrue aux vers et virus qui contaminent les systèmes de contrôle à partir des systèmes commerciaux, à mesure que les communications entre ces systèmes s'ouvrent ;
- vulnérabilité accrue aux logiciels malveillants provenant de périphériques USB, des ordinateurs portables de fournisseurs et de techniciens de maintenance, et du réseau de l'entreprise ;
- impact direct des systèmes de contrôle sur les systèmes physiques et mécaniques.

Sources des cyberattaques

Mettez en œuvre un plan de cybersécurité qui tient compte des multiples sources potentielles de cyberattaques et d'accidents :

Source	Description
Interne	• Comportement inapproprié d'un employé ou d'un sous-traitant • Employé ou sous-traitant mécontent
Opportuniste externe (non ciblée)	• Script kiddies* • Pirates occasionnels • Créateurs de virus
Volontaires externes (ciblées)	• Groupes criminels • Activistes • Terroristes • Services d'états étrangers
Accidentelles	
* Terme désignant les pirates qui utilisent des scripts malveillants créés par des tiers, sans connaître nécessairement le fonctionnement de ces scripts ou leur impact potentiel sur un système.	

Une cyberattaque peut cibler délibérément un système de contrôle pour atteindre plusieurs objectifs, notamment :

- perturber le processus de production en bloquant ou en retardant le flux d'informations ;
- endommager, désactiver ou arrêter des équipements pour perturber la production ou l'environnement ;
- modifier ou désactiver les systèmes de sécurité pour causes des dommages volontairement.

Techniques utilisées par les pirates pour accéder aux systèmes

Un pirate contourne les défenses périmétriques pour accéder au réseau du système de contrôle. Les points d'accès courants sont les suivants :

- accès commuté à des équipements terminaux distants (RTU) ;
- points d'accès des fournisseurs (comme les points d'accès du support technique) ;
- solutions réseau contrôlées par informatique ;
- réseau privé virtuel d'entreprise (VPN) ;
- liens à des bases de données ;
- parefeu mal configurés ;
- services homologues ;

Certifications de cybersécurité

Les consignes de cybersécurité développées par Schneider Electric se fondent sur les recommandations suivantes :

- Achilles
- ISA Secure

Questions

Pour poser une question sur la cybersécurité, signaler des problèmes de sécurité ou recevoir les dernières informations concernant Schneider Electric, visitez notre *website*.

Recommandations de Schneider Electric

Introduction

Votre système PC peut exécuter une grande variété d'applications destinées à améliorer la sécurité dans votre environnement de contrôle. Les paramètres par défaut du système doivent être reconfigurés en fonction des recommandations de Schneider Electric concernant le renforcement de la protection des équipements.

Les instructions suivantes décrivent les procédures relatives à Windows 7. Elles sont fournies à titre d'exemple. Les exigences ou procédures de votre système d'exploitation et de votre application peuvent être différentes.

Désactivation des cartes d'interface réseau non utilisées

Vérifiez que les cartes d'interface réseau non requises par l'application sont désactivées. Par exemple, si votre système compte deux cartes et que l'application n'en utilise qu'une, vérifiez que l'autre (Connexion au réseau local 2) est désactivée.

Pour désactiver une carte réseau sous Windows 7, procédez comme suit :

Etape	Action
1	Ouvrez **Panneau de configuration → Réseau et Internet → Centre Réseau et partage → Modifier les paramètres de la carte**.
2	Cliquez avec le bouton droit de la souris sur la connexion non utilisée. Sélectionnez **Désactiver**.

Configuration de la connexion au réseau local

Différents paramètres réseau de Windows permettent de renforcer la sécurité pour la mettre au niveau de la protection renforcée recommandée par Schneider Electric.

Sur un système Windows 7, vous pouvez accéder à ces paramètres en ouvrant **Panneau de configuration → Réseau et Internet → Centre Réseau et partage → Modifier les paramètres de la carte → Connexion au réseau local (x).**

Cette liste est un exemple des modifications de configuration que vous pouvez apporter à votre système sur l'écran **Propriétés de la connexion au réseau local** :

- Désactivez toutes les piles IPv6 sur leurs cartes réseau respectives. (Cet exemple de système ne requiert pas la plage d'adresses IPv6, et la désactivation des piles IPv6 limite la vulnérabilité aux risques potentiels liés à la sécurité IPv6.
- Désactivez **Partage de fichiers et d'imprimantes Réseaux Microsoft**.

L'approche de protection renforcée de Schneider Electric inclut également les recommandations suivantes :

- Ne définissez que des adresses, masques de sous-réseau et passerelles IPv4 statiques.
- N'utilisez pas DHCP ou DNS dans la salle de contrôle.

Gestion du pare-feu Windows

L'approche de protection renforcée de Schneider Electric inclut également l'activation du pare-feu hôte Windows sur chacun des ordinateurs du système. Activez les pare-feu de chaque profil public ou privé répertorié.

Il est recommandé aux utilisateurs de définir des règles de pare-feu qui refusent les connexions provenant ou à destination d'hôtes externes inconnus ou non approuvés.

Désactivation du protocole RDP (bureau à distance)

Les recommandations de Schneider Electric relatives au renforcement de la protection incluent la désactivation du protocole de connexion de bureau à distance (RDP) sauf si votre application requiert le protocole RDP. La procédure ci-dessous décrit comment désactiver ce protocole :

Etape	Action
1	Dans Windows 2008R2 ou Windows 7, désactivez le protocole RDP via **Ordinateur → Propriétés système → Paramètres système avancés**.
2	Sur l'onglet **Utilisation à distance**, désélectionnez l'option **Autoriser les connexions d'assistance à distance vers cet ordinateur**.
3	Sélectionnez l'option **Ne pas autoriser les connexions à cet ordinateur**.

Mise à jour des stratégies de sécurité

Mettez à jour les stratégies de sécurité sur les ordinateurs de votre système en utilisant `gpupdate` dans une fenêtre de commande. Pour plus d'informations, consultez la documentation Microsoft relative à `gpupdate`.

Désactivation de LANMAN et NTLM

Le protocole Microsoft LAN Manager (LANMAN ou LM) et son successeur NT LAN Manager (NTLM) présentent des vulnérabilités. Leur utilisation est donc déconseillée dans les applications de contrôle.

La procédure ci-dessous indique comment désactiver LM et NTLM sur un système Windows 7 ou Windows 2008R2 :

Etape	Action
1	Dans une fenêtre de commande, exécutez `secpol.msc` pour ouvrir la fenêtre **Stratégie de sécurité locale**.
2	Ouvrez **Paramètres de sécurité → Stratégies locales → Options de sécurité**.
3	Sélectionnez **Envoyer uniquement les réponses NTLMv2. Refuser LM et NTLM** dans le champ **Sécurité réseau : niveau d'authentification LAN Manager**.
4	Sélectionnez l'option **Sécurité réseau : ne pas stocker de valeurs de hachage de niveau Lan Manager sur la prochaine modification de mot de passe**.

Etape	Action
5	Dans une fenêtre de commande, entrez `gpupdate` pour valider la stratégie de sécurité modifiée.

Gestion des mises à jour

Avant le déploiement, mettez à jour les systèmes d'exploitation de tous les ordinateurs à l'aide des utilitaires disponibles dans la page Web **Windows Update** de Microsoft. Pour accéder à cet outil sous Windows 2008R2, Windows 7 ou Windows XP, sélectionnez **Démarrer → Tous les programmes → Windows Update**

Glossaire

C

code de fonction

Jeu d'instructions donnant à un ou plusieurs équipements esclaves situés à une ou plusieurs adresses spécifiées, l'ordre d'effectuer un type d'action, par exemple de lire un ensemble de registres de données et d'en renvoyer le contenu.

configuration

Agencement et interconnexions des composants matériels au sein d'un système, ainsi que le matériel et les logiciels qui déterminent les caractéristiques de fonctionnement du système.

CRC

contrôle de redondance cyclique (cyclic redundancy check)

Les messages mettant en œuvre ce mécanisme de contrôle des erreurs ont un champ CRC qui est calculé par l'émetteur en fonction du contenu du message. Les nœuds récepteurs recalculent le champ CRC. Toute disparité entre les deux codes révèle une différence entre le message transmis et celui qui est reçu.

D

DTM

Abréviation de Device Type Manager (gestionnaire de type d'équipement). Pilote d'équipement mis à disposition par le fabricant de l'équipement. Le DTM contient les informations propres à l'équipement et fournit une interface utilisateur graphique. Il permet d'effectuer des opérations de surveillance et de configuration sur l'équipement concerné. Un DTM n'est pas une application autonome. Il requiert une application cadre FDT pour s'exécuter.

E

Ethernet

Spécification de câblage et de signalisation LAN (Local Area Network, Réseau local) utilisée pour connecter des équipements situés dans une zone définie (un immeuble, par exemple). Ethernet utilise un bus ou une topologie en étoile pour connecter différents nœuds sur un réseau.

F

FDT

Abréviation de Field Device Tool. Technologie normalisant l'interface de communication entre les équipements et les systèmes (*www.fdtgroup.org*).

I

interface

Connexion physique au réseau, par exemple un adaptateur réseau ou un convertisseur USB-RS 232.

IP

IP (Internet Protocol).

Branche de la famille de protocoles TCP/IP, qui gère les adresses Internet des nœuds, achemine les messages sortants et reconnaît les messages entrants.

L

LAN

Acronyme de "Local Area Network", signifiant réseau local.

Réseau de communication de données à courte distance.

M

MB

Abréviation de Modbus.

Modbus

Protocole de messagerie au niveau de la couche application. Modbus offre de nombreux services spécifiés par des codes de fonction.

modèle maître/esclave

Le contrôle, dans un réseau mettant en œuvre le modèle maître/esclave, s'effectue de l'équipement maître vers les équipements esclaves.

P

passerelle

Programme ou composant matériel chargé de transmettre des données entre les réseaux.

S

SL

Abréviation de Serial Line, signifiant ligne série.

T

TCP

Protocole de contrôle de transmission, de l'anglais "Transmission Control Protocol".

Protocole de couche transport orienté connexion qui assure une transmission de données fiable en mode duplex intégral. TCP fait partie de la suite de protocoles TCP/IP.

télégramme

Paquet de données utilisé dans les communications série.

Index

C

Compatibilité, *11*
Configuration de la scrutation, *31*
configuration requise
    logicielle, *10*
    matérielle, *10*
configuration, onglet, *22*
connexion
    réseau, *15*
    TCP, *14*
    type, *14*
cyber sécurité
    bureau distant, *39*
    cartes d'interface réseau, *38*
    connexion au réseau local, *38*
    LANMAN / NTLM, *39*
    pare-feu, *39*
    recommandations, *38*
cybersécurité, *35*
    certifications, *36*
    introduction, *36*

E

Exécution, onglet, *25*

I

installation, *12*
interface utilisateur, *17*
interface utilisateur graphique, *17*

M

Mode de scrutation, *31*
modèle de communication, *15*

N

nombre de tentatives, *23*

T

Table d'adresses, *29*