Modbus TCP Comm DTM (Device Type Manager)

Benutzerhandbuch

02/2019

EIO0000000367.06

www.schneider-electric.com

Die Informationen in der vorliegenden Dokumentation enthalten allgemeine Beschreibungen und/oder technische Leistungsmerkmale der hier erwähnten Produkte. Diese Dokumentation dient keinesfalls als Ersatz für die Ermittlung der Eignung oder Verlässlichkeit dieser Produkte für bestimmte Verwendungsbereiche des Benutzers und darf nicht zu diesem Zweck verwendet werden. Jeder Benutzer oder Integrator ist verpflichtet, angemessene und vollständige Risikoanalysen, Bewertungen und Tests der Produkte im Hinblick auf deren jeweils spezifischen Verwendungszweck vorzunehmen. Weder Schneider Electric noch deren Tochtergesellschaften oder verbundene Unternehmen sind für einen Missbrauch der Informationen in der vorliegenden Dokumentation verantwortlich oder können diesbezüglich haftbar gemacht werden. Verbesserungs- und Änderungsvorschlage sowie Hinweise auf angetroffene Fehler werden jederzeit gern entgegengenommen.

Sie erklären, dass Sie ohne schriftliche Genehmigung von Schneider Electric dieses Dokument weder ganz noch teilweise auf beliebigen Medien reproduzieren werden, ausgenommen zur Verwendung für persönliche nichtkommerzielle Zwecke. Darüber hinaus erklären Sie, dass Sie keine Hypertext-Links zu diesem Dokument oder seinem Inhalt einrichten werden. Schneider Electric gewährt keine Berechtigung oder Lizenz für die persönliche und nichtkommerzielle Verwendung dieses Dokument oder seines Inhalts, ausgenommen die nichtexklusive Lizenz zur Nutzung als Referenz. Das Handbuch wird hierfür „wie besehen“ bereitgestellt, die Nutzung erfolgt auf eigene Gefahr. Alle weiteren Rechte sind vorbehalten.

Bei der Montage und Verwendung dieses Produkts sind alle zutreffenden staatlichen, landesspezifischen, regionalen und lokalen Sicherheitsbestimmungen zu beachten. Aus Sicherheitsgründen und um die Übereinstimmung mit dokumentierten Systemdaten besser zu gewährleisten, sollten Reparaturen an Komponenten nur vom Hersteller vorgenommen werden.

Beim Einsatz von Geräten für Anwendungen mit technischen Sicherheitsanforderungen sind die relevanten Anweisungen zu beachten.

Die Verwendung anderer Software als der Schneider Electric-eigenen bzw. einer von Schneider Electric genehmigten Software in Verbindung mit den Hardwareprodukten von Schneider Electric kann Körperverletzung, Schäden oder einen fehlerhaften Betrieb zur Folge haben.

Die Nichtbeachtung dieser Informationen kann Verletzungen oder Materialschäden zur Folge haben!

© 2019 Schneider Electric. Alle Rechte vorbehalten.

Inhaltsverzeichnis

	Sicherheitshinweise	5
	Über dieses Buch	7
Kapitel 1	**Hardware- und Softwareanforderungen**	9
	Systemanforderungen	10
	Kompatibilität	11
	Installieren und Entfernen	12
Kapitel 2	**Verbindungstypen und Kommunikationsmodelle**	13
	Verbindungstyp	14
	Kommunikationsmodell	15
Kapitel 3	**Grafische Benutzeroberfläche**	17
	Grafische Benutzeroberfläche	17
Kapitel 4	**Konfiguration**	21
	Registerkarte „Konfiguration“	22
	Registerkarte „Laufzeit“	25
	Adresstabelle	29
	Konfiguration der Abfrage (Scan)	31
Kapitel 5	**Cyber-Sicherheit**	35
	Was ist Cyber-Sicherheit?	36
	Schneider Electric-Richtlinien	38
Glossar		41
Index		45

Sicherheitshinweise

Wichtige Informationen

HINWEISE

Lesen Sie sich diese Anweisungen sorgfältig durch und machen Sie sich vor Installation, Betrieb, Bedienung und Wartung mit dem Gerät vertraut. Die nachstehend aufgeführten Warnhinweise sind in der gesamten Dokumentation sowie auf dem Gerät selbst zu finden und weisen auf potenzielle Risiken und Gefahren oder bestimmte Informationen hin, die eine Vorgehensweise verdeutlichen oder vereinfachen.



Wird dieses Symbol zusätzlich zu einem Sicherheitshinweis des Typs „Gefahr“ oder „Warnung“ angezeigt, bedeutet das, dass die Gefahr eines elektrischen Schlags besteht und die Nichtbeachtung der Anweisungen unweigerlich Verletzung zur Folge hat.



Dies ist ein allgemeines Warnsymbol. Es macht Sie auf mögliche Verletzungsgefahren aufmerksam. Beachten Sie alle unter diesem Symbol aufgeführten Hinweise, um Verletzungen oder Unfälle mit Todesfälle zu vermeiden.

⚠ GEFAHR

GEFAHR macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, Tod oder schwere Verletzungen **zur Folge hat.**

⚠ WARNUNG

WARNUNG macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, Tod oder schwere Verletzungen **zur Folge haben kann.**

⚠ VORSICHT

VORSICHT macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, leichte Verletzungen **zur Folge haben kann.**

HINWEIS

HINWEIS gibt Auskunft über Vorgehensweisen, bei denen keine Verletzungen drohen.

BITTE BEACHTEN

Elektrische Geräte dürfen nur von Fachpersonal installiert, betrieben, bedient und gewartet werden. Schneider Electric haftet nicht für Schäden, die durch die Verwendung dieses Materials entstehen.

Als qualifiziertes Fachpersonal gelten Mitarbeiter, die über Fähigkeiten und Kenntnisse hinsichtlich der Konstruktion und des Betriebs elektrischer Geräte und deren Installation verfügen und eine Schulung zur Erkennung und Vermeidung möglicher Gefahren absolviert haben.

Über dieses Buch

Auf einen Blick

Ziel dieses Dokuments

In diesem Benutzerhandbuch wird die Verwendung des COM DTM (Device Type Manager) für Modbus beschrieben.

Gültigkeitsbereich

Dieses Dokument wurde für die Modbus Communication Library V2.6.9 aktualisiert.

Produktbezogene Informationen

⚠ WARNUNG

STEUERUNGSAUSFALL

- Bei der Konzeption von Steuerungsstrategien müssen mögliche Störungen auf den Steuerungspfaden berücksichtigt werden, und bei bestimmten kritischen Steuerungsfunktionen ist dafür zu sorgen, dass während und nach einem Pfadfehler ein sicherer Zustand erreicht wird. Beispiele kritischer Steuerfunktionen sind die Notabschaltung (Not-Aus) und der Nachlauf-Stopp, Stromausfall und Neustart.
- Für kritische Steuerfunktionen müssen separate oder redundante Steuerpfade bereitgestellt werden.
- Systemsteuerungspfade können Kommunikationsverbindungen umfassen. Dabei müssen die Auswirkungen unerwarteter Sendeverzögerungen und Verbindungsstörungen berücksichtigt werden.
- Sämtliche Unfallverhütungsvorschriften und lokale Sicherheitsrichtlinien sind zu beachten.[1]
- Jede Implementierung des Geräts muss individuell und sorgfältig auf einen einwandfreien Betrieb geprüft werden, bevor das Gerät an Ort und Stelle in Betrieb gesetzt wird.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

[1] Weitere Informationen finden Sie in den aktuellen Versionen von NEMA ICS 1.1 „Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control“ sowie von NEMA ICS 7.1, „Safety Standards for Construction and Guide for Selection, Installation, and Operation of Adjustable-Speed Drive Systems“ oder den entsprechenden, vor Ort geltenden Vorschriften.

Kapitel 1
Hardware- und Softwareanforderungen

Inhalt dieses Kapitels

Dieses Kapitel enthält die folgenden Themen:

Thema	Seite
Systemanforderungen	10
Kompatibilität	11
Installieren und Entfernen	12

Systemanforderungen

Hardwareanforderungen

Anforderungen	Minimum	Empfohlen
Computer	Pentium 4 oder vergleichbar	
RAM	1 GB	2 GB
Freier Festplattenspeicherplatz auf Systemlaufwerk	100 MB	
Freier Festplattenspeicherplatz auf Installationslaufwerk	100 MB	
Auslagerungsdatei	1024 MB	2048 MB
Bildschirmanzeige	256 Farben, SVGA, Auflösung 800 x 600	True Color XGA, Auflösung 1024 x 768

Softwareanforderungen

Betriebssysteme

Betriebssystem	Edition/Service Pack	Besondere Hinweise
Windows 7 32 Bit	SP1	Sie benötigen Administratorrechte, um den Modbus TCP Comm DTM zu installieren.
Windows 7 64 Bit	SP1	
Windows 8.1, 10 Professional	–	

Auf dem PC installierte Software

Software	Edition	Besondere Hinweise
Microsoft.NET Framework	V2.0 SP2	–
FDT-Rahmenanwendung	FDT 1.2 oder FDT 1.2.1	Für den Modbus TCP Comm DTM ist eine FDT-Rahmenanwendung gemäß dem FDT-Standard erforderlich. Die FDT-Rahmenanwendung muss Microsoft.NET Framework 2.0 unterstützen.

Kompatibilität

FDT-Kompatibilität

Der Modbus Comm DTM entspricht den FDT-Standards FDT 1.2 und FDT 1.2.1 und basiert auf dem FDT Modbus-Annex 1.0.

Modbus-Kompatibilität

Der Modbus Comm DTM bietet Unterstützung für die in der Modbus-Anwendungsprotokoll-Spezifikation V1.1b definierten Modbus-Dienste.

Installieren und Entfernen

Installation

Doppelklicken Sie auf die Datei *setup.exe* und folgen Sie den Anweisungen im Installationsassistenten.

Demontage

Um den DTM aus Ihrem Computer zu entfernen, wählen Sie **Start** → **Einstellungen** → **Systemsteuerung** → **Programme hinzufügen/entfernen**.

Kapitel 2
Verbindungstypen und Kommunikationsmodelle

Einführung

Dieses Kapitel bietet einen Überblick über die verschiedenen Konfigurationen, die zur Einrichtung von Modbus-Kommunikation verwendet werden können.

Inhalt dieses Kapitels

Dieses Kapitel enthält die folgenden Themen:

Thema	Seite
Verbindungstyp	14
Kommunikationsmodell	15

Verbindungstyp

Einführung

Der Modbus TCP Comm DTM kann zum Aufbau einer Modbus-Kommunikation auf Grundlage des nachstehenden Verbindungstyps verwendet werden.

TCP-Verbindung

Der Modbus TCP Comm DTM bietet die Möglichkeit zum Aufbau einer Modbus-Kommunikation über TCP. Die Verbindung wird dabei über den Ethernet-Netzwerkadapter des PC hergestellt.

Kommunikationsmodell

Einführung

In diesem Kapitel wird das vom Modbus TCP Comm DTM unterstützte Kommunikationsmodell beschrieben.

HINWEIS: Die FDT-Technologie wurde nicht für Datenübertragungen in Echtzeit konzipiert. Je nach Ihrem System und dem von Ihnen verwendeten Kommunikationsmodell geben die Daten deshalb nicht den tatsächlichen Echtzeit-Gerätestatus wieder.

⚠ WARNUNG

UNGÜLTIGE INFORMATIONEN ZUM GERÄTESTATUS

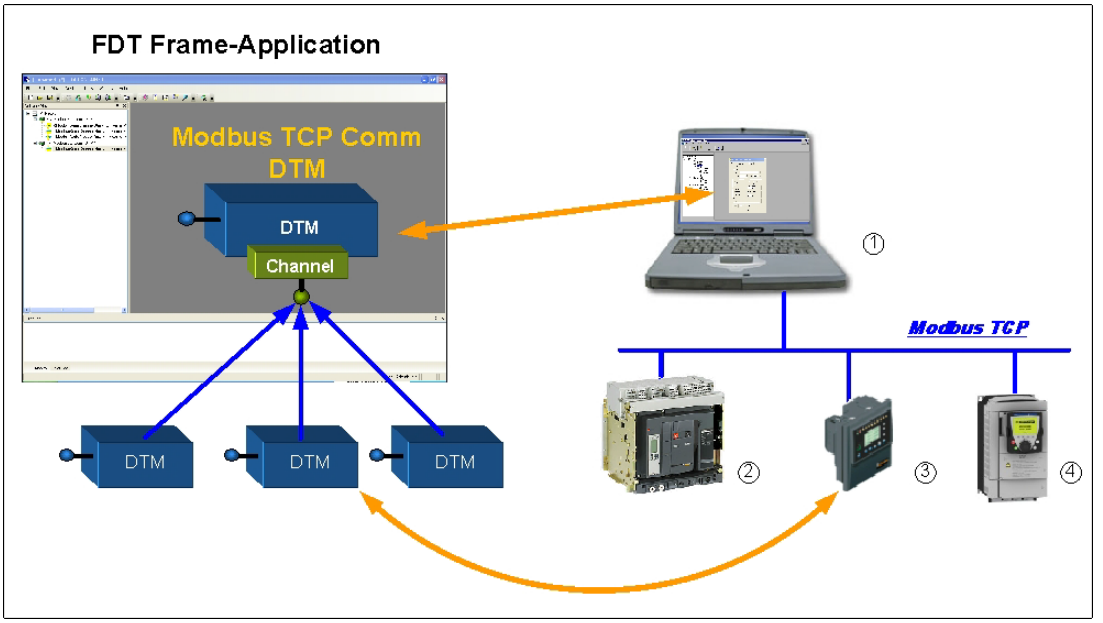
Der Modbus Comm DTM sollte nicht für zeitkritische Steuerungs- und Überwachungsaufgaben eingesetzt werden, da die übertragenen Daten unter Umständen nicht den tatsächlichen Gerätestatus widerspiegeln. Die FDT-Technologie wurde nicht zu diesem Zweck entwickelt.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Netzwerkverbindung

Der Modbus TCP Comm DTM kann zur Einrichtung einer Modbus-Kommunikation zwischen PC und Zielgerät über Ethernet verwendet werden.

In dieser Konfiguration fungiert der Modbus TCP Comm DTM als Modbus-Client.



1 PC mit dem Modbus TCP Comm DTM
2 - 4 Zielgeräte

Kapitel 3
Grafische Benutzeroberfläche

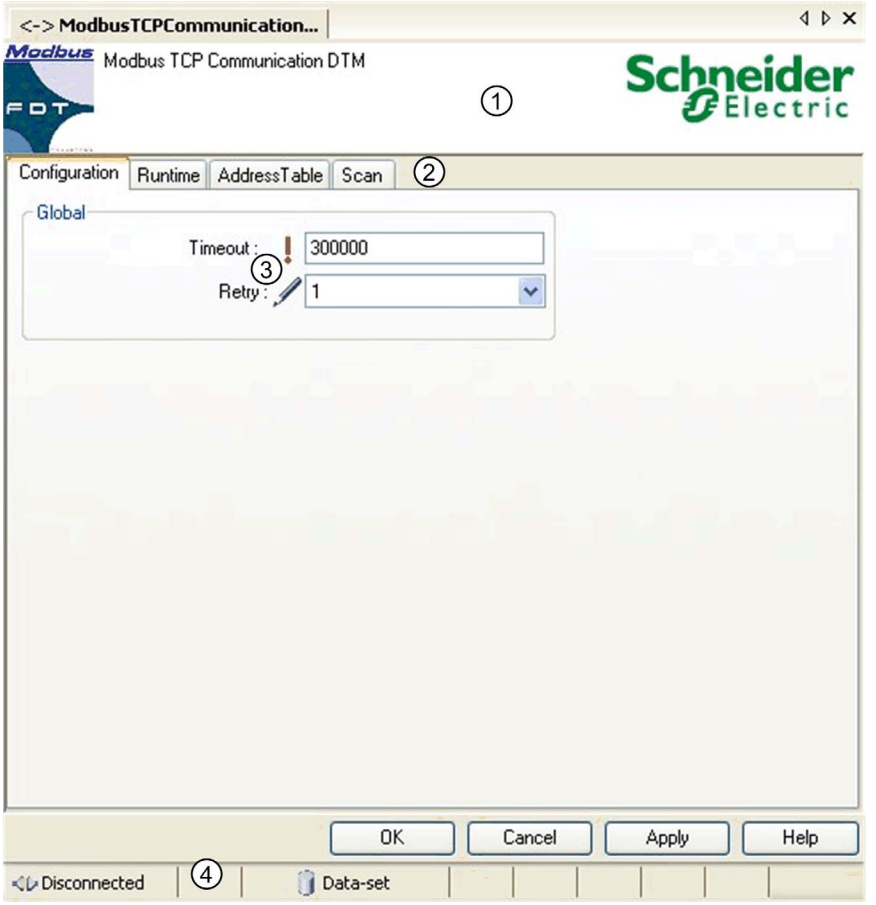
Grafische Benutzeroberfläche

Übersicht

In diesem Kapitel wird die grafische Benutzeroberfläche (GUI) des Modbus TCP Comm DTM beschrieben.

Einführung

Die nachstehende Abbildung zeigt die GUI (grafische Benutzeroberfläche) des DTM.



1 Identifikationsbereich
2 Registerkarten-Menü
3 Parameterstatus-Symbole
4 Statusleiste

Identifikationsbereich

Der Identifikationsbereich gibt Aufschluss über den Namen und die Version des DTM.

Registerkarten-Menü

Die Registerkarten des Menüs ermöglichen den Zugriff auf die verschiedenen vom DTM bereitgestellten Funktionen.

Parameterstatus-Symbole

Die Parameterstatus-Symbole verweisen auf den aktuellen Status des Parameters.

Mögliche Parameterstatus

Symbol	Bedeutung
	Der Parameter wurde geändert und weist einen ungültigen Wert auf.
	Der Parameter wurde geändert und weist einen gültigen Wert auf.

Statusleiste

Die Statusleiste enthält Informationen zum aktuellen Status des DTM.

Mögliche Verbindungsstatus

Symbol	Text	Bedeutung	DTM-Status
	Verbindung wird hergestellt	Die Verbindung wird hergestellt.	Verbindung herstellen
	Verbunden	Die Verbindung wurde hergestellt.	Online
	Verbindung wird getrennt	Die Verbindung wird getrennt.	Verbindung trennen
	Unterbrochen	Die Verbindung wurde unterbrochen.	Unterbrechung der Kommunikation erkannt
	Nicht verbunden	Die Verbindung wurde getrennt.	Alle anderen Status

Mögliche Status der Datenquelle

Symbol	Text	Verhalten
	Datensatz	Die angezeigten Daten werden aus dem Instanz-Datensatz geladen. Die Änderung von Werten wirkt sich lediglich auf den Instanz-Datensatz aus.
	Datensatz gesperrt	Die angezeigten Daten werden aus dem Instanz-Datensatz geladen. Der Datensatz ist gesperrt.

Kapitel 4
Konfiguration

Inhalt dieses Kapitels

Dieses Kapitel enthält die folgenden Themen:

Thema	Seite
Registerkarte „Konfiguration“	22
Registerkarte „Laufzeit“	25
Adresstabelle	29
Konfiguration der Abfrage (Scan)	31

Registerkarte „Konfiguration“

Einführung

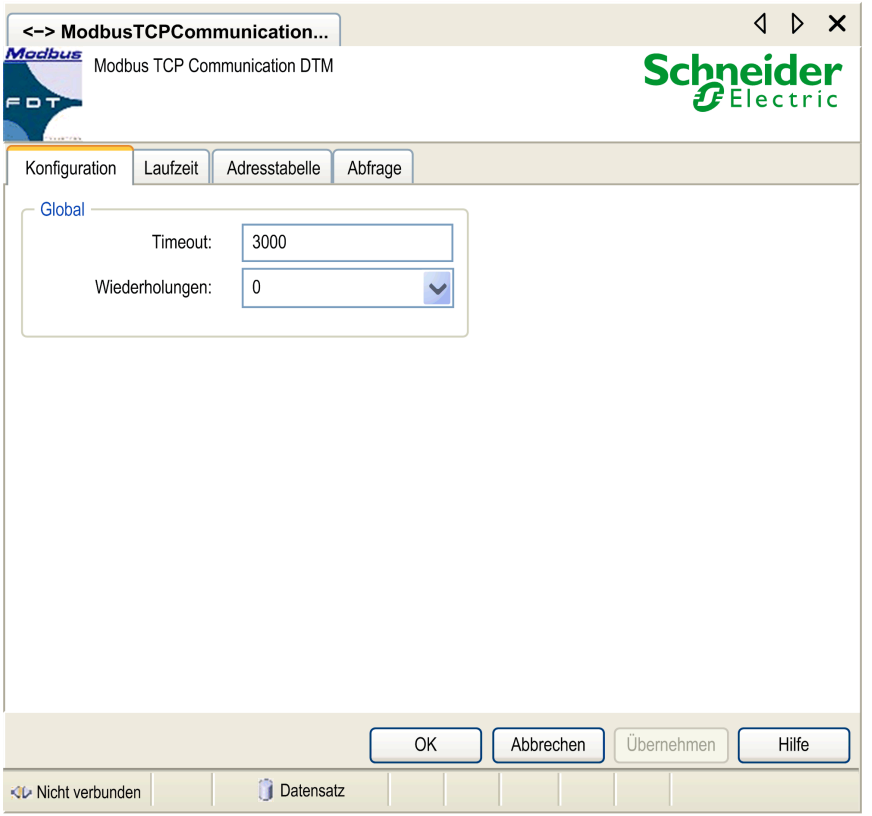
Die Registerkarte **Konfiguration** des Modbus TCP Comm DTM enthält die Kommunikationsparameter.

Registerkarte „Konfiguration“

Für den Zugriff auf die Registerkarte **Konfiguration** des Modbus TCP Comm DTM sind verschiedene Möglichkeiten gegeben:

- Doppelklicken Sie in der Netzwerkansicht Ihrer FDT-Rahmenanwendung auf das Symbol des Modbus TCP Comm DTM.
- Klicken Sie in der Netzwerkansicht Ihrer FDT-Rahmenanwendung mit der rechten Maustaste auf das Symbol des Modbus TCP Comm DTM und klicken Sie dann auf **Konfiguration**.

Die nachstehende Abbildung zeigt die Registerkarte **Konfiguration** im Dialogfeld desModbus TCP Comm DTM:



Kommunikationsparameter

Die Tabelle enthält eine Beschreibung der Kommunikationsparameter für eine Modbus TCP-Verbindung.

Parameter	Beschreibung	Standardwert
Timeout	Antwort-Timeout des Modbus-Servers	3000 ms
Wiederholungen	Anzahl der erneuten Sendeversuche eines Modbus-Requests über die TCP-Verbindung durch den Modbus TCP Comm DTM, wenn ein Kommunikations-Timeout auftritt.	0

Konfigurationsbefehle

Auf der Registerkarte **Konfiguration** verfügbare Konfigurationsbefehle

Befehl	Beschreibung
OK	Die Parameter werden gespeichert und das Fenster des Modbus TCP Comm DTM wird geschlossen. Die neuen Parameterwerte werden beim nächsten Verbindungsaufbau angewendet.
Abbrechen	Die Parameteränderungen werden abgebrochen und das Fenster des Modbus TCP Comm DTM wird geschlossen. Beim nächsten Verbindungsaufbau werden die ursprünglichen Werte angewendet.
Übernehmen	Die Parameter werden gespeichert, das Modbus TCP Comm DTM-Fenster bleibt jedoch geöffnet. Die neuen Parameterwerte werden beim nächsten Verbindungsaufbau angewendet.

Registerkarte „Laufzeit“

Einführung

Der Modbus TCP Comm DTM stellt verschiedene Typen von Laufzeit-Informationen bereit. In diesem Kapitel werden die vom Modbus TCP Comm DTM bereitgestellten Informationen sowie die Konfiguration der Protokollfunktion beschrieben.

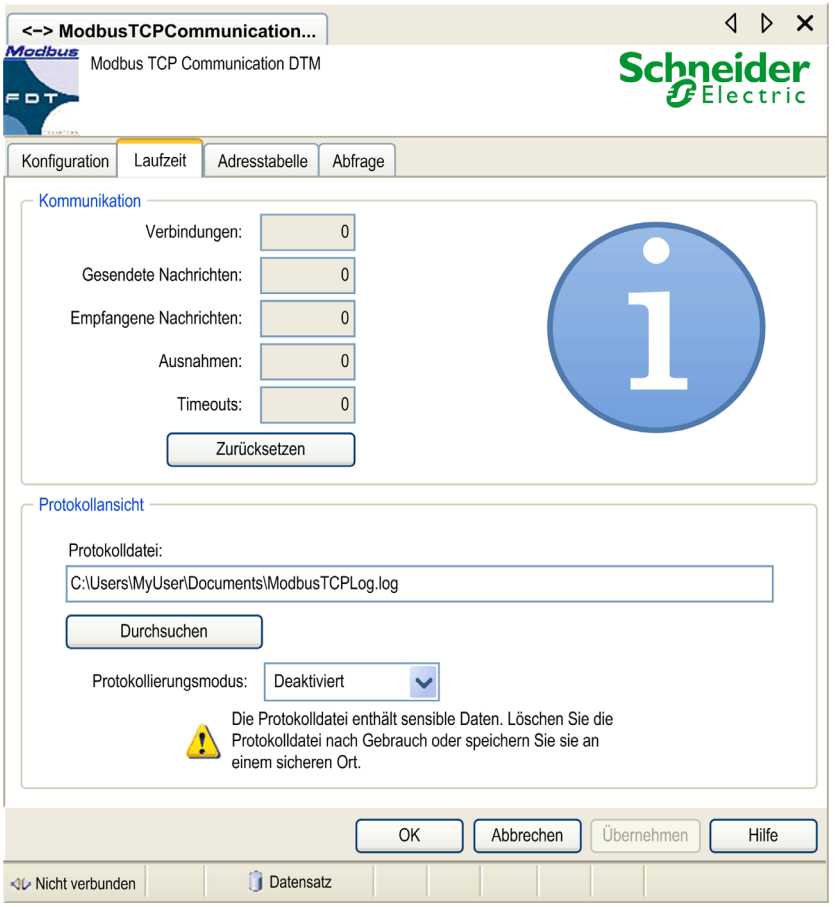
Registerkarte „Laufzeit“

Der Modbus TCPComm DTM stellt verschiedene Typen von Laufzeit-Informationen bereit, die zur Überwachung der aktiven Kommunikation herangezogen werden können.

Die laufzeitspezifischen Informationen sind auf der Registerkarte **Laufzeit** des Modbus TCP Comm DTM verfügbar. Auf die Registerkarte kann folgendermaßen zugegriffen werden:

- Doppelklicken Sie in der Netzwerkansicht Ihrer FDT-Rahmenanwendung auf das Symbol des Modbus TCP Comm DTM. Wählen Sie die Registerkarte **Laufzeit** aus.
- Klicken Sie in der Netzwerkansicht Ihrer FDT-Rahmenanwendung mit der rechten Maustaste auf das Symbol des Modbus TCP Comm DTM und klicken Sie dann auf **Konfiguration**. Wählen Sie die Registerkarte **Laufzeit** aus.

Die nachstehende Abbildung zeigt die Registerkarte **Laufzeit** im Dialogfeld desModbus TCP Comm DTM:



Konfigurationsbefehle

Die folgende Tabelle enthält eine Beschreibung der auf der Registerkarte **Laufzeit** verfügbaren Konfigurationsbefehle.

Befehl	Beschreibung
OK	Die Parameter werden gespeichert und das Fenster des Modbus TCP Comm DTM wird geschlossen. Die neuen Parameterwerte werden beim nächsten Verbindungsaufbau angewendet.

Befehl	Beschreibung
Abbrechen	Die Parameteränderungen werden abgebrochen und das Fenster des Modbus TCP Comm DTM wird geschlossen. Beim nächsten Verbindungsaufbau werden die ursprünglichen Werte angewendet.
Durchsuchen	Ein Fenster zur Dateisuche wird geöffnet, in dem Sie den Pfad der Protokolldatei angeben können.
Zurücksetzen	Alle Laufzeit-Parameter werden auf Null zurückgesetzt.
Übernehmen	Die Parameter werden gespeichert, das Fenster des Modbus TCP Comm DTM bleibt jedoch geöffnet. Die neuen Parameterwerte werden beim nächsten Verbindungsaufbau angewendet.

Laufzeit-Parameter

Die nachstehende Tabelle enthält eine Beschreibung der auf der Registerkarte **Laufzeit** des Modbus TCP Comm DTM verfügbaren Laufzeit-Parameter:

Befehl	Beschreibung
Verbindungen	Anzahl der aktiven Verbindungen des Modbus TCP Comm DTM
Gesendete Nachrichten	Anzahl der vom Modbus TCP Comm DTM gesendeten Nachrichten
Empfangene Nachrichten	Anzahl der vom Modbus TCP Comm DTM empfangenen Nachrichten
Ausnahmen	Anzahl der vom Modbus TCP Comm DTM empfangenen Modbus-Ausnahmenachrichten
Timeouts	Anzahl der Timeout-Fehler beim Empfang

Protokolldatei

Der Modbus TCP Comm DTM ermöglicht die Erstellung einer Protokolldatei. Im Feld **Protokolldatei** müssen Sie den Pfad angeben, in dem die Protokolldatei gespeichert werden soll.

In der nachstehenden Tabelle werden die Informationen beschrieben, die je nach **Protokollmodus** in die Protokolldatei geschrieben werden:

Protokollmodus	Beschreibung
Deaktiviert	Die Protokolldatei-Funktion wird deaktiviert.
Fehlerprotokollierung	Es werden nur Informationen zu Timeout-Fehlern und empfangenen Modbus-Ausnahmen in die Protokolldatei geschrieben.
Komplette Protokollierung	Zusätzlich zu den Informationen zu Timeout-Fehlern und empfangenen Modbus-Ausnahmen werden auch Informationen zu gesendeten Modbus-Requests und empfangenen Modbus-Antworten sowie zu den vom Geräte-DTM empfangenen Requests in die Protokolldatei geschrieben.

Empfehlung für verbesserte Cybersicherheit

Die Protokolldatei enthält normalerweise sensible Daten wie
- Geräteadressen
- Gerätenamen
- Details der Netzwerktopologie
- Details der Netzwerkkonfiguration

Sie wird auf der Festplatte Ihres PCs gespeichert. Löschen Sie die Protokolldatei, sobald sie nicht mehr benötigt wird, oder speichern Sie sie an einem sicheren Ort, an dem kein unbefugter Zugriff möglich ist.

Adresstabelle

Einführung

Der Modbus Comm DTM stellt eine Adresstabelle bereit, in der die verbundenen Geräte-DTMs mit zugehörigen Zieladressen aufgeführt werden. In diesem Kapitel werden die in der Adresstabelle enthaltenen Informationen sowie die Konfiguration der Zieladressen der Geräte beschrieben.

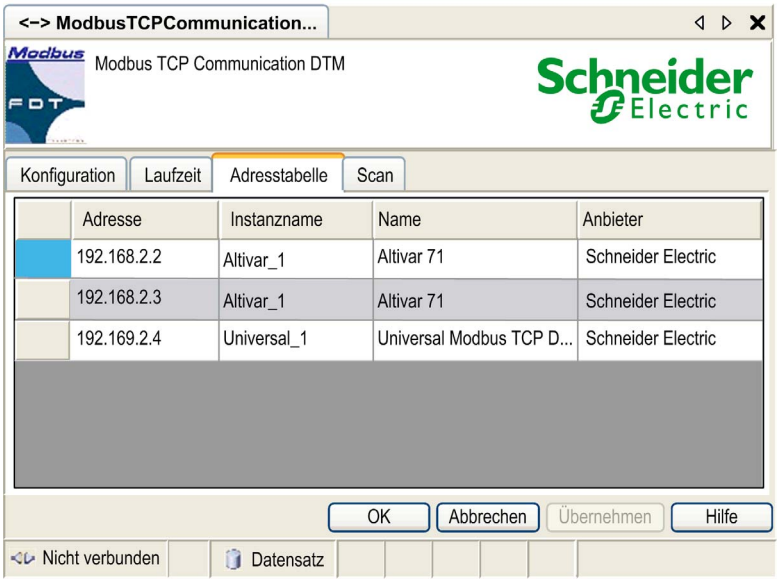
Adresstabelle

Der Modbus TCP Comm DTM stellt eine Adresstabelle bereit, in der die verbundenen Geräte-DTMs mit zugehörigen Zieladressen aufgeführt werden. In dieser Adresstabelle können Sie die Zieladressen der verbundenen Geräte-DTMs angeben.

Die Registerkarte **Adresstabelle** wird folgendermaßen aufgerufen:

- Doppelklicken Sie in der Netzwerkansicht Ihrer FDT-Rahmenanwendung auf das Symbol des Modbus TCP Comm DTM. Wählen Sie die Registerkarte **Adresstabelle** aus.
- Klicken Sie in der **Netzwerkansicht** Ihrer FDT-Rahmenanwendung mit der rechten Maustaste auf das Symbol des Modbus TCP Comm DTM und klicken Sie dann auf **Konfiguration**. Wählen Sie die Registerkarte **Adresstabelle** aus.

Die nachstehende Abbildung zeigt die Registerkarte **Adresstabelle** im Dialogfeld desModbus TCP Comm DTM:



Konfigurationsbefehle

Die Tabelle enthält eine Beschreibung der auf der Registerkarte **Adresstabelle** verfügbaren Konfigurationsbefehle.

Befehl	Beschreibung
OK	Die Änderungen werden gespeichert und das Fenster des Modbus TCP Comm DTM wird geschlossen. Die neuen Werte werden beim nächsten Verbindungsaufbau angewendet.
Abbrechen	Die Änderungen werden abgebrochen und das Fenster des Modbus TCP Comm DTM wird geschlossen. Beim nächsten Verbindungsaufbau werden die ursprünglichen Werte angewendet.
Übernehmen	Die Änderungen werden gespeichert, das Fenster des Modbus TCP Comm DTM bleibt jedoch geöffnet. Die neuen Werte werden beim nächsten Verbindungsaufbau angewendet.

Adressinformationen

Die Tabelle enthält eine Beschreibung der auf der Registerkarte **Adresstabelle** des Modbus TCP Comm DTM verfügbaren Adressinformationen:

Parameter	Beschreibung
Adresse	Zieladresse des Hardware-Geräts, das mit dem verbundenen DTM konfiguriert werden soll.
Name der Instanz	Name der DTM-Instanz
Name	DTM-spezifischer Name
Anbieter	Name des DTM-Anbieters

Adresszuweisung

Die Adresstabelle des Modbus TCP Comm DTM kann zur Angabe der Zieladresse des Hardware-Geräts verwendet werden, das mit einem bestimmten DTM konfiguriert werden soll. Für die Angabe der Zieladresse müssen Sie die neue Adresse im Feld **Adresse** des betreffenden DTM eingeben und die Änderung durch Klicken auf die Schaltfläche **Übernehmen** bzw. **OK** bestätigen.

Konfiguration der Abfrage (Scan)

Einführung

Der Modbus Comm DTM ermöglicht die Angabe des Bereichs der abzufragenden Adressen für die FDT-Abfrage. In diesem Kapitel wird die Konfiguration der Abfrageparameter für die FDT-Abfrage beschrieben.

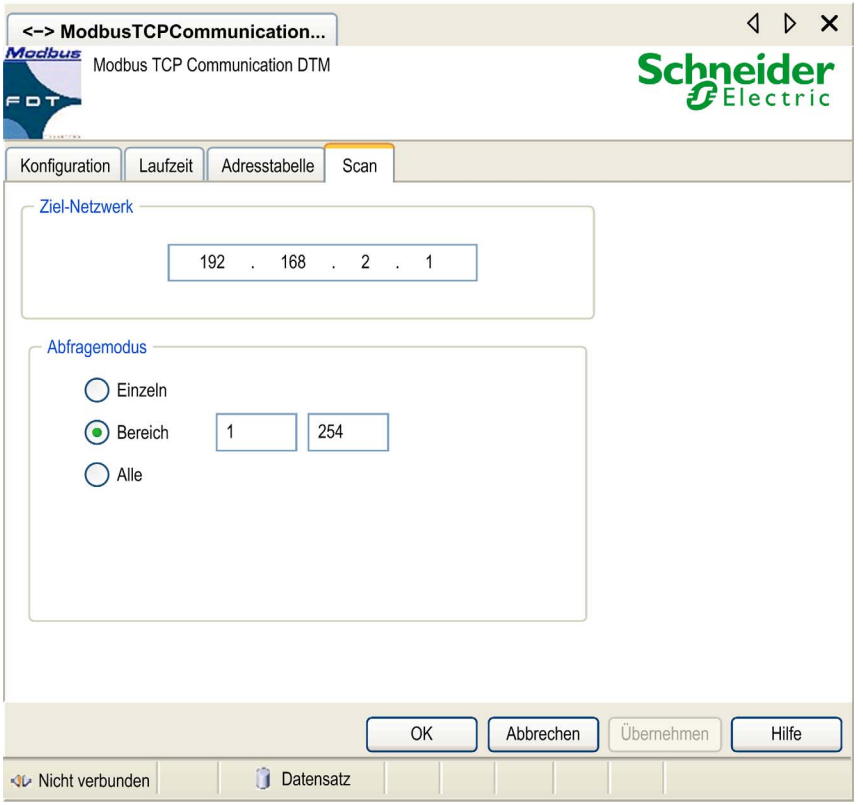
Registerkarte „Abfrage“

Der Modbus TCP Comm DTM unterstützt die Abfragefunktion, da diese für die FDT-Spezifikation V1.2.1 definiert wurde. Die Abfrage kann zur automatischen Einrichtung der Netzwerktopologie des zugrunde liegenden Kommunikationsnetzwerks verwendet werden. Der Modbus TCP Comm DTM ermöglicht die Angabe des Bereichs der abzufragenden Adressen.

Die Abfrageparameter sind auf der Registerkarte **Abfrage** des Modbus TCP Comm DTM verfügbar. Auf die Registerkarte kann folgendermaßen zugegriffen werden:

- Doppelklicken Sie in der **Netzwerkansicht** Ihrer FDT-Rahmenanwendung auf das Symbol des Modbus TCP Comm DTM. Wählen Sie die Registerkarte **Abfrage** aus.
- Klicken Sie in der **Netzwerkansicht** Ihrer FDT-Rahmenanwendung mit der rechten Maustaste auf das Symbol des Modbus TCP Comm DTM und klicken Sie dann auf **Konfiguration**. Wählen Sie die Registerkarte **Abfrage** aus.

Die Abbildung zeigt die Registerkarte **Abfrage** im Dialogfeld desModbus TCP Comm DTM:



Konfigurationsbefehle

Die Tabelle enthält eine Beschreibung der auf der Registerkarte **Abfrage** verfügbaren Konfigurationsbefehle.

Befehl	Beschreibung
OK	Die Änderungen werden gespeichert und das Fenster des Modbus Comm DTM wird geschlossen. Die neuen Werte werden bei der nächsten Abfrage angewendet.
Abbrechen	Die Änderungen werden abgebrochen und das Fenster des Modbus Comm DTM wird geschlossen. Bei der nächsten Abfrage werden die ursprünglichen Werte angewendet.

Befehl	Beschreibung
Übernehmen	Die Änderungen werden gespeichert, das Fenster des Modbus Comm DTM bleibt jedoch geöffnet. Die neuen Werte werden bei der nächsten Abfrage angewendet.

Abfrageparameter für Modbus TCP

Die Tabelle enthält eine Beschreibung der auf der Registerkarte **Abfrage** des Modbus TCP Comm DTM Comm DTM verfügbaren Abfrageparameter:

Parameter	Beschreibung	
Ziel-Netzwerk	Verweist auf den abzufragenden Netzwerkbereich.	
Abfragemodus	**Einzeln**	Es wird nur eine einzige Adresse eines Zielgeräts zwischen 0 und 255 im angegebenen Netzwerkbereich abgefragt.
	Bereich	Es wird ein bestimmter Adressenbereich zwischen 0 und 255 innerhalb des definierten Netzwerkbereichs abgefragt.
	Alle	Es wird der gesamte Adressenbereich des Netzwerkbereichs abgefragt (alle Adressen von 0 bis 255).

Kapitel 5
Cyber-Sicherheit

Einführung

Cyber-Sicherheit ist ein Teilgebiet der Netzwerkadministration, bei dem es darum geht, Angriffe auf Computersysteme bzw. von Computersystemen sowie über Computernetzwerke zu verhindern, die zu unabsichtlichen oder vorsätzlichen Schäden und Ausfällen führen können. Ziel der Cyber-Sicherheit ist es, einen höheren Schutzgrad für Daten- und physischen Ressourcen bereitzustellen, um diese vor Diebstahl, Beschädigung, Missbrauch oder Unfällen zu schützen, und dabei gleichzeitig den Zugriff für die vorgesehenen Benutzer aufrechtzuerhalten.

Einzelne Maßnahmen für die Cyber-Sicherheit sind nicht ausreichend, daher empfiehlt Schneider Electric einen Ansatz für tiefgreifende Sicherheit. Bei diesem von der amerikanischen National Security Agency (NSA) entwickelten Ansatz werden mehrere Schichten von Sicherheitsfunktionen, Appliances und Prozessen im Netzwerk implementiert. Die grundlegenden Komponenten dieses Ansatzes sind:

- Risikobewertung
- ein auf den Ergebnissen der Risikobewertung aufbauender Sicherheitsplan
- eine mehrphasige Schulungskampagne
- physische Trennung der industriellen Netzwerke von den Unternehmensnetzwerken mittels einer "Demilitarized Zone" (DMZ, entmilitarisierte Zone) sowie der Verwendung von Firewalls und Routing zur Schaffung weiterer Sicherheitszonen
- Systemzugriffssteuerung
- Geräte-Hardening
- Netzwerküberwachung und -wartung

In diesem Kapitel werden Elemente definiert, mit deren Hilfe Sie ein System so konfigurieren können, dass es weniger anfällig für Cyber-Angriffe ist. Ausführliche Informationen über den Ansatz für tiefgreifende Sicherheit finden Sie im *TVDA: How Can I Reduce Vulnerability to Cyber Attacks in the Control Room* (Wie kann ich die Anfälligkeit für Cyber-Angriffe im Leitstand senken) auf der *Schneider Electric website*.

Inhalt dieses Kapitels

Dieses Kapitel enthält die folgenden Themen:

Thema	Seite
Was ist Cyber-Sicherheit?	36
Schneider Electric-Richtlinien	38

Was ist Cyber-Sicherheit?

Einführung

Cyber-Bedrohungen sind vorsätzliche oder unbeabsichtigte Handlungen, durch die der normale Betrieb von Computersystemen und Netzwerken gestört werden kann. Diese Handlungen können von der Einrichtung selbst oder von einem externen Standort ausgehen. In Steuerungsumgebungen bestehen u. a. folgende Herausforderungen im Hinblick auf die Sicherheit:

- Diverse physische und logische Grenzen
- Mehrere Standorte und große geografische Entfernungen
- Negative Auswirkungen der Sicherheitsimplementierung auf Prozessverfügbarkeit
- Erhöhtes Risiko, dass Würmer und Viren von Geschäftssystemen auf Steuerungssysteme übertragen werden, da die Kommunikation zwischen diesen Systemen offener geworden ist
- Erhöhtes Risiko einer Übertragung von Malware über USB-Geräte, Laptops von Anbietern und Wartungstechnikern und das Unternehmensnetzwerk
- Direkte Auswirkungen der Steuerungssysteme auf physische und mechanische Systeme

Quellen von Cyber-Angriffen

Implementieren Sie einen Plan für die Cyber-Sicherheit, bei dem die verschiedenen potenziellen Quellen von Cyber-Angriffen und unbeabsichtigten Vorfällen berücksichtigt werden:

Quelle	Beschreibung
intern	● unangemessenes Verhalten von Mitarbeitern oder Vertragsnehmern ● verärgerte Mitarbeiter oder Vertragsnehmer
extern opportunistisch (nicht gezielt)	● Scriptkiddies* ● Freizeit-Hacker ● Virenprogrammierer
extern vorsätzlich (gezielt)	● kriminelle Gruppen ● Aktivisten ● Terroristen ● Behörden ausländischer Staaten
versehentlich	
* Slang-Begriff für Hacker, die von anderen programmierte, bösartige Skripts verwenden, ohne dabei unbedingt wirklich zu verstehen, wie das Skript funktioniert oder welche Auswirkungen es auf ein System haben kann	

Ein vorsätzlicher Cyber-Angriff auf ein Steuerungssystem kann verschiedene böswillige Ziele verfolgen. Zum Beispiel:

- Beeinträchtigung des Produktionsprozesses durch Blockierung oder Verzögerung des Informationsflusses
- Beschädigen, Deaktivieren oder Herunterfahren von Geräten zu Beeinträchtigung der Produktion oder Umgebung
- Modifizieren oder Deaktivieren von Sicherheitssystemen, um absichtlich Schaden zuzufügen

Wie Angreifer Zugang erhalten

Ein Cyber-Angreifer umgeht die Schutzmaßnahmen am Netzwerkperimeter, um Zugriff auf das Steuerungssystem-Netzwerk zu erhalten. Gängige Zugangspunkte sind u. a. Folgende:

- Wählzugriff auf RTU-Geräte (Remote Terminal Unit)
- Zulieferer-Zugangspunkte (z. B. Zugangspunkte für technischen Support)
- IT-gesteuerte Netzwerkprodukte
- Unternehmens-VPN (virtuelles privates Netzwerk)
- Datenbank-Links
- schlecht konfigurierte Firewalls
- Peer-Dienstprogramme

Zertifizierungen für Cyber-Sicherheit

Die von Schneider Electric entwickelten Richtlinien für Cyber-Sicherheit basieren auf den folgenden Empfehlungen:

- Achilles
- ISA Secure

Sie haben Fragen?

Besuchen Sie unsere *website*, um eine Frage zur Cyber-Sicherheit zu senden, Sicherheitsprobleme zu melden oder aktuelle Neuigkeiten von Schneider Electric zu erfahren.

Schneider Electric-Richtlinien

Einführung

Auf Ihrem PC-System können verschiedene Anwendungen ausgeführt werden, um die Sicherheit in Ihrer Steuerungsumgebung zu erhöhen. Das System verfügt über werkseitige Standardeinstellungen, die umkonfiguriert werden müssen, um den Empfehlungen von Schneider Electric für das Geräte-Hardening im Rahmen eines Ansatzes für tiefgreifende Sicherheit zu entsprechen.

Die folgenden Richtlinien beschreiben die Vorgehensweisen bei einem Windows 7-Betriebssystem und dienen lediglich als Beispiel. Für Ihr Betriebssystem und Ihre Anwendungen können unterschiedliche Voraussetzungen oder Verfahren erforderlich sein.

Deaktivieren ungenutzter Netzwerkkarten

Stellen Sie sicher, dass nicht für die Anwendung erforderliche Netzwerkkarten deaktiviert werden. Wenn Ihr System beispielsweise über zwei Karten verfügt, die Anwendung jedoch nur eine davon verwendet, vergewissern Sie sich, dass die zweite Netzwerkkarte (LAN-Verbindung 2) deaktiviert ist.

So deaktivieren Sie eine Netzwerkkarte in Windows 7:

Schritt	Aktion
1	Öffnen Sie **Systemsteuerung → Netzwerk und Internet → Netzwerk- und Freigabecenter → Adaptereinstellungen ändern**.
2	Klicken Sie mit der rechten Maustaste auf die nicht genutzte Verbindung. Wählen Sie **Deaktivieren** aus.

Konfigurieren der LAN-Verbindung

Verschiedene Windows-Netzwerkeinstellungen bieten erhöhte Sicherheit in Einklang mit dem von Schneider Electric empfohlenen Ansatz für tiefgreifende Sicherheit.

In Windows 7 erfolgt der Zugriff auf diese Einstellungen unter **Systemsteuerung → Netzwerk und Internet → Netzwerk- und Freigabecenter → Adaptereinstellungen ändern → LAN-Verbindung (x).**

In Folgenden werden Beispiele für Konfigurationsänderungen angeführt, die Sie im Fenster **Eigenschaften von LAN-Verbindung** an Ihrem System vornehmen können:

- Deaktivieren Sie alle IPv6-Stapel auf den entsprechenden Netzwerkkarten. (Für dieses Systembeispiel ist der IPv6-Adressbereich nicht erforderlich, und durch Deaktivierung der IPv6-Stapel wird die Anfälligkeit für potenzielle IPv6-Sicherheitsrisiken begrenzt.)
- Deativieren Sie **Datei- und Druckerfreigabe für Microsoft Network**.

Zu von Schneider Electric empfohlenen tiefgreifenden Sicherheitsmaßnahmen zählen zudem die Folgenden:

- Definieren Sie ausschließlich statische IPv4-Adressen, Subnetzmasken und Gateways.
- Verwenden Sie im Leitstand weder DHCP noch DNS.

Verwalten der Windows-Firewall

Zu von Schneider Electric empfohlenen tiefgreifenden Sicherheitsmaßnahmen gehört die Aktivierung der Windows-Hostfirewall auf allen System-PCs. Aktivieren Sie die Firewall für alle aufgeführten privaten oder öffentlichen Profile.

Es wird Benutzern grundsätzlich empfohlen, Firewallregeln zu definieren, die jegliche Verbindung an oder von einem unbekannten/nicht vertrauenswürdigen externen Host verweigern.

Deaktivieren des Remote Desktop-Protokolls

Zu den von Schneider Electric empfohlenen tiefgreifenden Sicherheitsmaßnahmen gehört auch das Deaktivieren des Remote Desktop-Protokolls (RDP), es sei denn, Ihre Anwendung erfordert das RDP. Nachfolgend wird beschrieben, wie Sie das Protokoll deaktivieren:

Schritt	Aktion
1	In Windows 2008R2 oder Windows 7 deaktivieren Sie RDP über **Computer → Systemeigenschaften → Erweiterte Systemeinstellungen**.
2	Deaktivieren Sie auf der Registerkarte **Remote** das Kontrollkästchen **Remoteunterstützungsverbindungen mit diesem Computer zulassen**.
3	Aktivieren Sie das Kontrollkästchen **Keine Verbindung mit diesem Computer zulassen**.

Aktualisieren von Sicherheitsrichtlinien

Aktualisieren Sie die Sicherheitsrichtlinien auf den PCs in Ihrem System, indem Sie `gpupdate` in einem Befehlsfenster ausführen. Weitere Informationen finden Sie in der Microsoft-Dokumentation zu `gpupdate`.

Deaktivieren von LANMAN und NTLM

Das Microsoft LAN Manager-Protokoll (LANMAN oder LM) und sein Nachfolger NT LAN Manager (NTLM) weisen Schwachstellen auf, aufgrund derer ihre Verwendung in Steuerungsanwendungen nicht ratsam ist.

Gehen Sie wie folgt vor, um LM und NTLM in einem Windows 7- oder Windows 2008R2-System zu deaktivieren:

Schritt	Aktion
1	Führen Sie in einem Befehlsfenster den Befehl `secpol.msc` aus, um das Fenster **Lokale Sicherheitsrichtlinie** zu öffnen.
2	Öffnen Sie **Sicherheitseinstellungen → Lokale Richtlinien → Sicherheitsoptionen**.
3	Wählen Sie **Nur NTLMv2-Antworten senden.Verweigern Sie LM & NTLM** im Feld **Netzwerksicherheit: LAN Manager-Authentifizierungsebene**.
4	Aktivieren Sie das Kontrollkästchen **Netzwerksicherheit: Keine LAN Manager-Hashwerte für nächste Kennwortänderung speichern**.

Schritt	Aktion
5	Führen Sie in einem Befehlsfenster den Befehl `gpupdate` aus, um die geänderte Sicherheitsrichtlinie festzuschreiben.

Verwalten von Updates

Aktualisieren Sie vor der Bereitstellung alle PC-Betriebssysteme mithilfe der Dienstprogramme auf der **Windows Update**-Webseite von Microsoft. Zum Zugriff auf diese Funktion unter Windows 2008R2, Windows 7 oder Windows XP wählen Sie **Start → Alle Programme → Windows Update**.

Glossar

C

CRC

Cyclic Redundancy Check (zyklische Redundanzprüfung).

Nachrichten, die mit diesem Mechanismus zur Fehlerüberprüfung ausgestattet sind, weisen ein CRC-Feld auf, das vom Sender je nach Inhalt der Nachricht berechnet wird. Die empfangenden Netzknoten berechnen erneut das CRC-Feld. Eine Nichtübereinstimmung zwischen den beiden Codes weist auf einen Unterschied zwischen der übertragenen und der empfangenen Nachricht hin.

D

DTM

Ein DTM (Device Type Manager) ist eine Art Gerätetreiber, der vom Hersteller des Feldgeräts bereitgestellt wird. Der DTM enthält gerätespezifische Informationen und ist mit einer grafischen Benutzeroberfläche ausgestattet. Er kann zur Durchführung von Überwachungs- und Konfigurationstasks für ein bestimmtes Gerät verwendet werden. Ein DTM ist keine eigenständige Anwendung, sondern benötigt eine FDT-Rahmenanwendung, um ausgeführt werden zu können.

E

Ethernet

Eine LAN-Verdrahtungs- und Signalisierungsspezifikation, die zur Vernetzung von Geräten innerhalb eines definierten Bereichs, wie zum Beispiel eines Gebäudes, verwendet wird. Ethernet nutzt eine Bus- oder Sterntopologie zur Vernetzung verschiedener Knoten in einem Netzwerk.

F

FDT

Die FDT-Technologie (Field Device Tool) standardisiert die Kommunikationsschnittstelle zwischen Feldgeräten und Systemen (*www.fdtgroup.org*).

Funktionscode

Ein Funktionscode ist ein Befehlssatz, der ein oder mehrere Slave-Geräte an einer oder mehreren vorgegebenen Adressen anweist, einen bestimmten Aktionstyp auszuführen, z. B. eine Reihe von Datenregistern zu lesen und deren Inhalte zurückzumelden.

G

Gateway

Ein Programm oder eine Hardware, die Daten zwischen Netzwerken überträgt.

I

Interface

Das Interface (Deutsch: „Schnittstelle“) stellt die physische Verbindung zum Netwerk dar, wie zum Beispiel eine Netzwerkkarte oder ein USB/RS 232-Konverter.

IP

Internet Protocol.

Der Teil der TCP/IP-Protokollfamilie, der die Internetadressen der Knoten verfolgt, das Routing abgehender Nachrichten übernimmt und eingehende Nachrichten erkennt.

K

Konfiguration

Die Anordnung und Vernetzung von Hardwarekomponenten innerhalb eines Systems und die Hardware- und Softwareauswahl, die die Betriebsmerkmale des Systems bestimmen.

L

LAN

Local Area Network.

Ein Netzwerk für die Kommunikation von Daten über kurze Entfernungen.

M

Master/Slave-Modell

Die Steuerungsrichtung in einem Netzwerk mit implementiertem Master/Slave-Modell verläuft immer vom Master zu den Slave-Geräten.

MB

Abkürzung von Modbus.

Modbus

Modbus ist ein Nachrichtenaustauschprotokoll für die Anwendungsschicht. Modbus stellt zahlreiche über Funktionscodes spezifizierte Dienste bereit.

S

SL

Abkürzung von Serial Line (Serielle Leitung).

T

TCP

Transmission Control Protocol.

Ein verbindungsorientiertes Transportschichtprotokoll, das eine zuverlässige Vollduplex-Datenübertragung bietet. TCP ist Teil der TCP/IP-Protokollreihe.

Telegramm

Ein in der seriellen Kommunikation verwendetes Datenpaket.

Index

A

Abfragemodus, *31*
Abragekonfiguration, *31*
Adresstabelle, *29*
Anforderungen
    Hardware, *10*
    Software, *10*

B

Benutzeroberfläche, *17*

C

Cyber-Sicherheit, *35*
    Einführung, *36*
    Firewall, *39*
    LAN-Verbindung, *38*
    LANMAN / NTLM, *39*
    Netzwerkkarten, *38*
    Remote Desktop, *39*
    Richtlinien, *38*
    Zertifizierungen, *36*

G

Grafische Benutzeroberfläche, *17*

I

Installation, *12*

K

Kommunikationsmodell, *15*
Kompatibilität, *11*
Konfiguration (Registerkarte), *22*

L

Laufzeit (Registerkarte), *25*

V

Verbindung
    Netzwerk, *15*
    TCP, *14*
    Typ, *14*

W

Wiederholungsanzahl, *23*