

Modicon TMS

Erweiterungsmodulare

Programmierhandbuch

EIO0000003693.04

12/2023



Rechtliche Hinweise

Die in diesem Dokument enthaltenen Informationen umfassen allgemeine Beschreibungen, technische Merkmale und Kenndaten und/oder Empfehlungen in Bezug auf Produkte/Lösungen.

Dieses Dokument ersetzt keinesfalls eine detaillierte Analyse bzw. einen betriebs- und standortspezifischen Entwicklungs- oder Schemaplan. Es darf nicht zur Ermittlung der Eignung oder Zuverlässigkeit von Produkten/Lösungen für spezifische Benutzeranwendungen verwendet werden. Es liegt im Verantwortungsbereich eines jeden Benutzers, selbst eine angemessene und umfassende Risikoanalyse, Risikobewertung und Testreihe für die Produkte/Lösungen in Übereinstimmung mit der jeweils spezifischen Anwendung bzw. Nutzung durchzuführen bzw. von entsprechendem Fachpersonal (Integrator, Spezifikateur oder ähnliche Fachkraft) durchführen zu lassen.

Die Marke Schneider Electric sowie alle anderen in diesem Dokument enthaltenen Markenzeichen von Schneider Electric SE und seinen Tochtergesellschaften sind das Eigentum von Schneider Electric SE oder seinen Tochtergesellschaften. Alle anderen Marken können Markenzeichen ihrer jeweiligen Eigentümer sein.

Dieses Dokument und seine Inhalte sind durch geltende Urheberrechtsgesetze geschützt und werden ausschließlich zu Informationszwecken bereitgestellt. Ohne die vorherige schriftliche Genehmigung von Schneider Electric darf kein Teil dieses Dokuments in irgendeiner Form oder auf irgendeine Weise (elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen oder anderweitig) zu irgendeinem Zweck vervielfältigt oder übertragen werden.

Schneider Electric gewährt keine Rechte oder Lizenzen für die kommerzielle Nutzung des Dokuments oder dessen Inhalts, mit Ausnahme einer nicht-exklusiven und persönlichen Lizenz, es „wie besehen“ zu konsultieren.

Schneider Electric behält sich das Recht vor, jederzeit ohne entsprechende schriftliche Vorankündigung Änderungen oder Aktualisierungen mit Bezug auf den Inhalt bzw. am Inhalt dieses Dokuments oder dessen Format vorzunehmen.

Soweit nach geltendem Recht zulässig, übernehmen Schneider Electric und seine Tochtergesellschaften keine Verantwortung oder Haftung für Fehler oder Auslassungen im Informationsgehalt dieses Dokuments oder für Folgen, die aus oder infolge der sachgemäßen oder missbräuchlichen Verwendung der hierin enthaltenen Informationen entstehen.

© 2023 - Schneider Electric. Alle Rechte vorbehalten.

Inhaltsverzeichnis

Sicherheitshinweise.....	5
Über das Handbuch.....	6
TMS – Beschreibung	10
TMSAllgemeine Beschreibung.....	10
Konfigurieren des Kommunikationsbusses (COM_Bus).....	10
Hinzufügen von Erweiterungsmodulen	12
TMSES4-Ethernet-Modul	14
Ethernet-Dienste	14
Beschreibung	14
Konfiguration der IP-Adresse	16
Modicon M262 Logic/Motion Controller als Zielgerät für EtherNet/ IP	20
Modicon M262 Logic/Motion Controller als Slavegerät in einem Modbus TCP-Netzwerk	21
Firewallkonfiguration.....	25
Einführung	25
Verfahren für dynamische Änderungen.....	27
Verhalten der Firewall.....	28
Skriptbefehle für die Firewall.....	29
TMSCO1 CANopen-Kommunikationsmodul	35
Konfiguration der CANopen-Schnittstelle.....	35
Glossar	39
Index	42

Sicherheitshinweise

Wichtige Informationen

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 das Handbuch

Inhalt des Dokuments

In diesem Dokument wird die Konfiguration der TMS-Erweiterungsmodule für EcoStruxure Machine Expert beschrieben. Weiterführende Informationen finden Sie in den verschiedenen Dokumenten in der Online-Hilfe von EcoStruxure Machine Expert.

Gültigkeit

Dieses Dokument wurde für die Version EcoStruxure™ Machine Expert V2.2 aktualisiert.

Die im vorliegenden Dokument sowie in den Dokumenten im Abschnitt „Weiterführende Dokumentation“ beschriebenen Merkmale sind ebenfalls online verfügbar. Um auf die Online-Informationen zuzugreifen, gehen Sie zur Homepage von Schneider Electric www.se.com/ww/en/download/.

Die im vorliegenden Dokument beschriebenen Merkmale sollten denjenigen entsprechen, die online angezeigt werden. Im Rahmen unserer Bemühungen um eine ständige Verbesserung werden Inhalte im Laufe der Zeit möglicherweise überarbeitet, um deren Verständlichkeit und Genauigkeit zu verbessern. Sollten Sie einen Unterschied zwischen den Informationen in diesem Dokument und denjenigen online feststellen, verwenden Sie die Online-Informationen als Referenz.

Weiterführende Dokumente

Titel der Dokumentation	Referenznummer
EcoStruxure Machine Expert - Programmierhandbuch	EIO0000002854 (ENG)
	EIO0000002855 (FRE)
	EIO0000002856 (GER)
	EIO0000002858 (SPA)
	EIO0000002857 (ITA)
	EIO0000002859 (CHS)
Modicon M262 Logic/Motion Controller - Programmierhandbuch	EIO0000003651 (ENG)
	EIO0000003652 (FRA)
	EIO0000003653 (GER)
	EIO0000003654 (SPA)
	EIO0000003655 (ITA)
	EIO0000003656 (CHS)
	EIO0000003657 (POR)
	EIO0000003658 (TUR)
TMS-Erweiterungsmodule - Hardwarehandbuch	EIO0000003699 (ENG)
	EIO0000003700 (FRA)
	EIO0000003701 (GER)
	EIO0000003702 (SPA)
	EIO0000003703 (ITA)
	EIO0000003704 (CHS)
	EIO0000003705 (POR)
	EIO0000003706 (TUR)

Titel der Dokumentation	Referenznummer
TMSES4-Erweiterungsmodule - Anweisungsblatt	PHA44907
TMSCO1-Erweiterungsmodule - Anweisungsblatt	PHA44909

Produktinformationen

⚠️ WARNUNG
<p>STEUERUNGS AUSFALL</p> <ul style="list-style-type: none"> • Führen Sie vor der Implementierung eine Fehlermodus- und Effektanalyse (FMEA, Failure Mode and Effects Analysis) oder eine gleichwertige Risikoanalyse Ihrer Anwendung durch und wenden Sie Vorbeugemaßnahmen und Kontrollen an. • Stellen Sie einen Fallback-Zustand für den Fall unerwünschter Steuerungsereignisse oder -sequenzen bereit. • Sorgen Sie für separate oder redundante Steuerungspfade, wann immer erforderlich. • Stellen Sie geeignete Parameter bereit, insbesondere für Grenzwerte. • Überprüfen Sie die Auswirkungen von Übertragungsverzögerungen und ergreifen Sie Maßnahmen, um diese zu mindern. • Überprüfen Sie die Auswirkungen von Unterbrechungen der Kommunikationsverbindung und ergreifen Sie Maßnahmen, um diese zu mindern. • Stellen Sie unabhängige Pfade für Steuerungsfunktionen bereit (z. B. Not-Aus, Bedingungen bei Grenzüberschreitung und Fehler), die Ihrer Risikobewertung sowie den geltenden Vorschriften entsprechen. • Wenden Sie lokale Unfallverhütungsvorschriften und -richtlinien an. ¹ • Jede Implementierung eines Systems muss auf ihre ordnungsgemäße Funktion getestet werden, bevor sie in Betrieb genommen wird. <p>Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.</p>

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.

⚠️ WARNUNG
<p>UNBEABSICHTIGTER GERÄTEBETRIEB</p> <ul style="list-style-type: none"> • Verwenden Sie mit diesem Gerät nur von Schneider Electric genehmigte Software. • Aktualisieren Sie Ihr Anwendungsprogramm jedes Mal, wenn Sie die physische Hardwarekonfiguration ändern. <p>Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.</p>

Terminologie gemäß den geltenden Standards

Die technischen Begriffe, Terminologie, Symbole und die entsprechenden Beschreibungen in diesem Handbuch, oder die in beziehungsweise auf den Produkten selbst erscheinen, sind im Allgemeinen von den Begriffen und Definitionen der internationalen Normen hergeleitet.

Im Bereich der funktionalen Sicherheitssysteme, Antriebe und allgemeinen Automatisierungssysteme betrifft das unter anderem Begriffe wie *Sicherheit*, *Sicherheitsfunktion*, *Sicherer Zustand*, *Fehler*, *Fehlerreset/Zurücksetzen bei Fehler*, *Ausfall*, *Störung*, *Warnung/Warmmeldung*, *Fehlermeldung*, *gefährlich/ gefahrbringend* usw.

Unter anderem schließen diese Normen ein:

Standard	Beschreibung
IEC 61131-2:2007	Speicherprogrammierbare Steuerungen, Teil 2: Betriebsmittelanforderungen und Prüfungen.
ISO 13849-1:2015	Sicherheit von Maschinen: Sicherheitsspezifische Teile von Steuerungen. Allgemeine Gestaltungsleitsätze.
EN 61496-1:2013	Sicherheit von Maschinen: Berührungslos wirkende Schutzeinrichtung. Teil 1: Allgemeine Anforderungen und Prüfungen.
ISO 12100:2010	Sicherheit von Maschinen - Allgemeine Gestaltungsleitsätze - Risikobeurteilung und Risikominderung
EN 60204-1:2006	Sicherheit von Maschinen - Elektrische Ausrüstung von Maschinen - Teil1: Allgemeine Anforderungen
ISO 14119:2013	Sicherheit von Maschinen - Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen - Leitsätze für Gestaltung und Auswahl
ISO 13850:2015	Sicherheit von Maschinen - Not-Halt- Gestaltungsleitsätze
IEC 62061:2015	Sicherheit von Maschinen - Funktionale Sicherheit von sicherheitsbezogenen elektrischen, elektronischen und elektronisch programmierbaren Steuerungen.
IEC 61508-1:2010	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme: Allgemeine Anforderungen.
IEC 61508-2:2010	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme: Anforderungen für sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme.
IEC 61508-3:2010	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme: Softwareanforderungen.
IEC 61784-3:2016	Industrielle Kommunikationsnetze - Profile - Teil 3: Funktional sichere Übertragung bei Feldbussen - Allgemeine Regeln und Festlegungen für Profile.
2006/42/EC	Maschinenrichtlinie
2014/30/EU	EG-Richtlinie Elektromagnetische Verträglichkeit
2014/35/EU	EG-Richtlinie Niederspannung

Zusätzlich kann die in vorliegendem Dokument verwendete Nomenklatur tangential verwendet werden, wenn sie aus anderen Normen abgeleitet ist, wie z. B.:

Standard	Beschreibung
Normenreihe IEC 60034	Drehende elektrische Maschinen
Reihe IEC 61800	Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl
Serie IEC 61158	Digitale Datenkommunikation in der Leittechnik – Feldbus für industrielle Leitsysteme

Bei einer Verwendung des Begriffs *Betriebsumgebung/Betriebsbereich* in Verbindung mit der Beschreibung bestimmter Gefahren und Risiken entspricht der Begriff der Definition von *Gefahrenbereich* oder *Gefahrenzone* in der *Maschinenrichtlinie (2006/42/EC)* der Norm *ISO 12100:2010*.

HINWEIS: Die vorherig erwähnten Standards können auf die spezifischen Produkte in der vorliegenden Dokumentation zutreffen oder nicht. Weitere Informationen über die einzelnen anwendbaren Normen die hier beschriebenen Produkte betreffend, entnehmen Sie den entsprechenden Tabellen dieser Produktbezeichnungen.

TMS – Beschreibung

TMS Allgemeine Beschreibung

Einführung

TMS -Erweiterungsmodule werden an der linken Seite der Steuerung angebracht und sind für Ethernet und CANopen vorgesehen. Die TMS-Erweiterungsmodule können in der EcoStruxure Machine Expert **Gerätebaumstruktur** konfiguriert werden.

Merkmale der TMS-Erweiterungsmodule

In der folgenden Tabelle sind die Merkmale der TMS-Erweiterungsmodule beschrieben:

Modulreferenz	Typ	Klemmentyp	Kompatibilität
TMSES4	Ethernet-Kommunikation	RJ45	TM262L10MESE8T TM262L20MESE8T TM262M15MESS8T TM262M25MESS8T TM262M35MESS8T
TMSCO1	CANopen-Mastermodul	SUB-D 9-Pin, Stecker	TM262L• TM262M•

HINWEIS: Das TMSES4-Erweiterungsmodul ist kein eigenständiger Ethernet-Switch.

Konfigurieren des Kommunikationsbusses (COM_Bus)

Konfigurieren des Kommunikationsbusses

Gehen Sie vor wie folgt, um den Kommunikationsbus zu konfigurieren:

Schritt	Aktion
1	Doppelklicken Sie in der Gerätebaumstruktur , auf COM_Bus . Ergebnis: Das COM_Bus -Konfigurationsfenster wird angezeigt.
2	Klicken Sie auf eine der Registerkarten: <ul style="list-style-type: none"> • TMS-Bus • E/A-Abbild • Diagnosetabelle

Registerkarte TMS-Bus

Der TMS-Kommunikationsbus verfügt über eine interne IP-Netzwerkarchitektur. Die Netzwerkadresse ist für allgemeine Konfigurationseinstellungen festgelegt. Die Netzwerkadresse muss jedoch für komplexe Konfigurationen mit mehreren Netzwerken und untereinander verbundenen M262-Steuerungen manuell eingegeben werden.

Gehen Sie vor wie folgt, um die Netzwerkadresse zu konfigurieren:

Schritt	Aktion
1	Klicken Sie auf Netzwerkadresse .
2	Geben Sie die neue Netzwerkadresse ein. Ergebnis: Die Subnetzmaske , Host min und Host max werden automatisch aktualisiert.

Registerkarte E/A-Abbild

Die Registerkarte **E/A-Abbild** ist festgelegt und kann nicht geändert werden.

Registerkarte Diagnosetabelle

Die Registerkarte **Diagnosetabelle** enthält einen Diagnosestatus für jedes angeschlossene Modul.

HINWEIS: Diese Tabelle gilt nur für TMSES4-Module.

Parameter	Datentyp	Standardwert	Wert	Beschreibung
<i>ConfState</i>	UNIT	0	0: Keine Konfiguration	Globaler Busstatus
			1: Konfiguration ungültig	
			2: Reserviert	
			3: Konfiguration gültig und angewendet	
<i>NbModules</i>	UNIT	0	0 bis 3	Anzahl der erkannten TMS-Module
<i>Name</i>	STRING(15)	–	–	Name des TMS-Moduls
<i>MajorType</i>	WORD	0	–	Typcode des TMS-Moduls
<i>SubType</i>	WORD	0	–	Untertypcode des TMS-Moduls
<i>Version</i>	STRING(15)	–	–	Firmwareversion des TMS-Moduls ⁽¹⁾
<i>ModuleState</i>	DWORD	TMS_MODULE_POWERED	0	Erkennung des TMS-Moduls durch die Steuerung
		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	

Parameter	Datentyp	Standardwert	Wert	Beschreibung
<i>IpState</i>	DWORD	TMS_IP_PING_SUCCESS	0	IP-Kommunikation zwischen M262- und TMS-Modul
		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	
<i>PixCmdState</i>	Enumeration of DWORD	TMS_PIXCMD_EXCHING	0	Das TMS-Modul verarbeitet ein Prozessabbild.
		TMS_PIXCMD_CONFIG_NONE	1	
		TMS_PIXCMD_CONFIG_CMD_ERROR	2	
		TMS_PIXCMD_CONFIG_RESP_WAIT	3	
		TMS_PIXCMD_CONFIG_RESP_ERROR	4	
		TMS_PIXCMD_CONFIG_ONLY	5	
		TMS_PIXCMD_CONFIG_SUCCESS	6	
		TMS_PIXCMD_ENABLE_CMD_ERROR	7	
		TMS_PIXCMD_ENABLE_RESP_WAIT	8	
		TMS_PIXCMD_ENABLE_RESP_ERROR	9	
		TMS_PIXCMD_EXCH_ERROR	10	
		TMS_PIXCMD_DISABLING	11	
		TMS_PIXCMD_DISABLED	12	

(1) Siehe Aktualisieren der Firmware von TMS4-Erweiterungsmodulen (siehe Modicon M262 Logic/Motion Controller, Programmierhandbuch) für Informationen zur Aktualisierung der Firmware des TMS4-Erweiterungsmoduls.

Hinzufügen von Erweiterungsmodulen

Hinzufügen von Erweiterungsmodulen

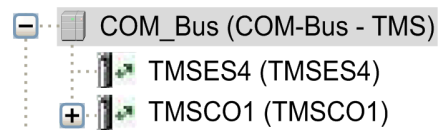
Um Ihrer Steuerung ein Erweiterungsmodul hinzuzufügen, wählen Sie das betreffende Erweiterungsmodul im **Hardwarekatalog** aus, ziehen Sie es in die **Gerätebaumstruktur** und legen Sie es auf dem **COM_Bus**-Knoten ab.

Weitere Informationen zum Hinzufügen von Geräten in einem Projekt finden Sie unter:

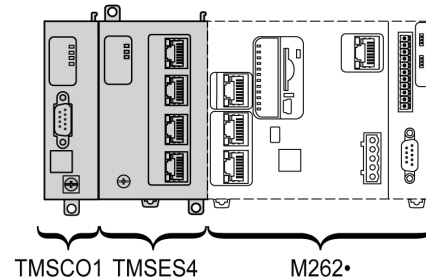
- Verwenden der Methode Drag&Dop (siehe EcoStruxure Machine Expert, Programming Guide) (Ziehen und Ablegen)
- Verwenden der Kontextmenüs oder Plus-Schaltflächen (siehe EcoStruxure Machine Expert, Programming Guide)

Layout von Erweiterungsmodulen

In der Software wird das Modullayout von oben nach unten angezeigt:



Physisch werden die Erweiterungsmodule von rechts nach links angeschlossen:



Weitere Informationen zur Kompatibilität mit dem M262 Logic/Motion Controller finden Sie unter [Merkmale der TMS-Erweiterungsmodule](#), Seite 10.

Konfigurieren von Erweiterungsmodulen

Um Ihr Erweiterungsmodul zu konfigurieren, doppelklicken Sie auf den Knoten des Erweiterungsmoduls in der **Gerätebaumstruktur**.

TMSES4-Ethernet-Modul

Einführung

In diesem Kapitel wird die Konfiguration des TMSES4-Ethernet-Erweiterungsmoduls beschrieben.

Ethernet-Dienste

Einführung

In diesem Abschnitt wird die Konfiguration der vom TMSES4-Erweiterungsmodul bereitgestellten Ethernet-Dienste beschrieben.

Beschreibung

Ethernet-Dienste

Das TMSES4-Erweiterungsmodul fügt eine Ethernet-Schnittstelle hinzu, um die Anzahl der Ethernet-Ports für eine Steuerung zu erweitern.

Das Modul unterstützt die folgenden Dienste der Steuerung:

- Modbus TCP-Server, Seite 15
- Webserver (siehe Modicon M262 Logic/Motion Controller, Programmierhandbuch)
- FTP-Server (siehe Modicon M262 Logic/Motion Controller, Programmierhandbuch)
- SNMP (siehe Modicon M262 Logic/Motion Controller, Programmierhandbuch)
- M262 Logic/Motion Controller als Zielgerät auf EtherNet/IP, Seite 20
- M262 Logic/Motion Controller als Slavegerät auf Modbus TCP, Seite 21
- IEC VAR ACCESS, Seite 15

HINWEIS: Für eine Kommunikation über die Netzwerkvariablenliste (NVL) muss der Ethernet-Port über eine gültige IP-Adresse verfügen und das Gerät muss verbunden sein.

Ethernet-Protokoll

Das Ethernet-Modul unterstützt die folgenden Protokolle:

- 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)

TCP-Serververbindungen

Diese Tabelle zeigt die Gesamtzahl von TCP-Serververbindungen für die Steuerung und die TMSES4-Module:

Verbindungstyp	Maximale Anzahl gleichzeitiger Serververbindungen
Modbus-Server	Maximal 8 gleichzeitige TCP-Serververbindungen für TMSES4-Module und die Steuerung oder für die Steuerung allein.
EtherNet/IP-Gerät	16
FTP-Server	4
Webserver	10

Jeder TCP-basierte Server verwaltet seine eigenen Verbindungen.

Wenn ein Client versucht, eine Modbus-Serververbindung zu öffnen, durch die die maximal zulässige Anzahl Verbindungen überschritten wird, schließt die Steuerung die älteste Verbindung. In den übrigen Fällen wird der Versuch, eine Verbindung zu öffnen, abgelehnt.

Wenn ein Client eine neuen Verbindung zu öffnen versucht und alle Verbindungen belegt sind (ein Datenaustausch stattfindet), wird die neue Verbindung zurückgewiesen.

Die Serververbindungen bleiben geöffnet, solange sich die Steuerung in einem Betriebszustand (*RUN*, *STOP*, *HALT*) befindet.

Die Serververbindungen werden geschlossen, wenn ein Betriebszustand verlassen oder in einen Betriebszustand gewechselt wird (*RUN*, *STOP*, *HALT*), außer bei einem Stromausfall (da der Steuerung keine Zeit bleibt, die Verbindungen zu schließen).

Weitere Informationen zu den Betriebszuständen finden Sie im Zustandsdiagramm der Steuerung (siehe Modicon M262 Logic/Motion Controller, Programmierhandbuch).

Modbus TCP-Server

Der Modbus-Server unterstützt die folgenden Modbus-Anforderungen:

Funktions-code Dez. (Hex.)	Unterfunktion Dez. (Hex.)	Funktion
1 (1h)	–	Digitalausgänge lesen (%Q)
2 (2h)	–	Digitaleingänge lesen (%I)
3 (3h)	–	Halteregister lesen (%MW)
6 (6h)	–	Einzelnes Register schreiben (%MW)
8 (8h)	–	Diagnose
15 (Fh)	–	Mehrere digitale Ausgänge schreiben (%Q)
16 (10h)	–	Mehrere Register schreiben (%MW)
23 (17h)	–	Mehrere Register lesen/schreiben (%MW)
43 (2Bh)	14 (Eh)	Geräteidentifikation lesen

Verfügbare Dienste

Bei der Ethernet-Kommunikation wird der Dienst **IEC VAR ACCESS** von der Steuerung unterstützt. Der Dienst **IEC VAR ACCESS** ermöglicht den Austausch von Variablen zwischen der Steuerung und einer HMI.

Der Dienst **NetWork variables** wird ebenfalls von der Steuerung unterstützt. Der Dienst **NetWork variables** ermöglicht den Datenaustausch zwischen Steuerungen.

HINWEIS: Weitere Informationen, siehe das EcoStruxure Machine Expert - Programmierhandbuch.

Konfiguration der IP-Adresse

Einführung

Wenn TMSES4 nicht konfiguriert ist, wird das Modul gestartet und bezieht automatisch die Standard-IP-Adresse:

- 10.12.x.z für das erste Modul
- 10.13.x.z für das zweite Modul
- 10.14.x.z für das dritte Modul

x und z entsprechen dem 5. und 6. Byte der MAC-Schnittstellenadresse. Beispiel: Lautet die MAC-Adresse 00:80:F4:50:02:5D, dann ist die IP-Adresse 10.12.2.93.

Weitere Informationen zur Position der MAC-Adresse finden Sie unter Ethernet-Konfiguration, Seite 18.

Die Standardsubnetzmaske lautet 255.255.0.0.

Es gibt verschiedene Methoden, um die IP-Adresse der hinzugefügten Ethernet-Schnittstelle der Steuerung zuzuweisen:

- Adresszuweisung durch den DHCP-Server
- Adresszuweisung durch den BOOTP-Server
- Feste IP-Adresse
- Post-Konfigurationsdatei (siehe Modicon M262 Logic/Motion Controller, Programmierhandbuch). Wenn eine Post-Konfigurationsdatei vorhanden ist, hat diese Methode vor den anderen Methoden Vorrang.

Die IP-Adresse kann auch dynamisch geändert werden:

- Registerkarte Kommunikationseinstellungen (siehe Modicon M262 Logic/Motion Controller, Programmierhandbuch) in EcoStruxure Machine Expert
- **changelPAddress**-Funktionsbaustein (siehe Modicon M262 Logic/Motion Controller, Programmierhandbuch)

HINWEIS: Wenn die verwendete Adressierungsmethode fehlschlägt, verwendet die Verbindung eine von der MAC-Adresse abgeleitete Standard-IP-Adresse.

Sie müssen die IP-Adressen sorgfältig verwalten, da jedes Gerät im Netzwerk eine eindeutige Adresse benötigt. Wenn mehrere Geräte dieselbe IP-Adresse besitzen, kann dies ein unbeabsichtigtes Betriebsverhalten Ihres Netzwerks und der zugehörigen Geräte zur Folge haben.

⚠️ WARNUNG

UNBEABSICHTIGTER GERÄTEBETRIEB

- Vergewissern Sie sich, dass im Netzwerk oder auf der dezentralen Verbindung nur eine Master-Steuerung konfiguriert ist.
- Stellen Sie sicher, dass alle Geräte über eindeutige Adressen verfügen.
- Erfragen Sie Ihre IP-Adresse bei Ihrem Systemadministrator.
- Vergewissern Sie sich, dass die IP-Adresse des Geräts eindeutig ist, bevor Sie das System in Betrieb nehmen.
- Weisen Sie dieselbe IP-Adresse keinem anderen Gerät im Netzwerk zu.
- Aktualisieren Sie die IP-Adresse nach dem Klonen einer Anwendung, die auf eine Ethernet-Kommunikation mit eindeutigen Adressen zurückgreift.

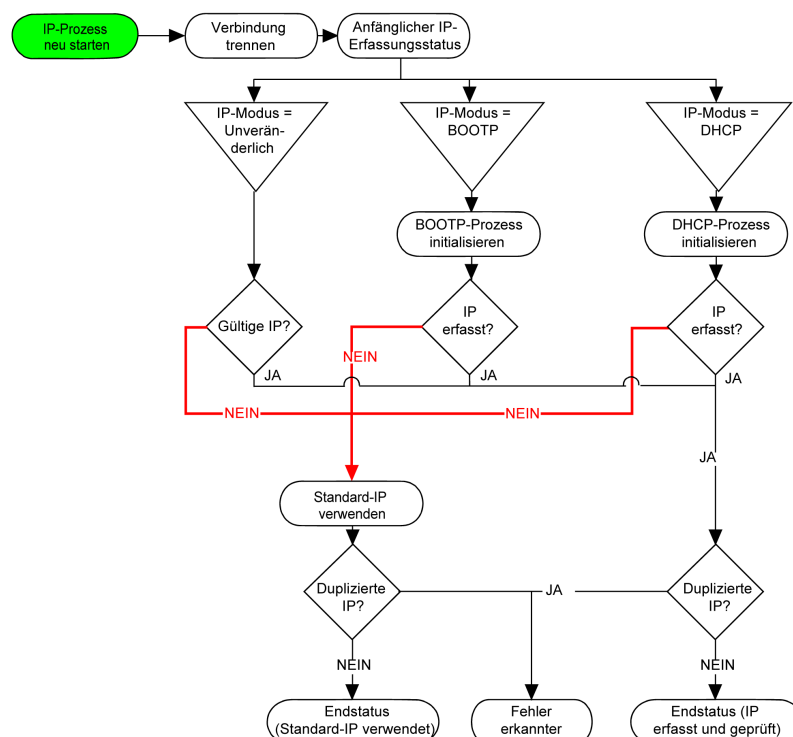
Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

HINWEIS: Stellen Sie sicher, dass der Systemadministrator über die zugewiesenen IP-Adressen im Netzwerk und im Subnetz Buch führt und dass er über alle durchgeführten Konfigurationsänderungen unterrichtet wird.

HINWEIS: Das TMSES4-Modul muss sich in einem anderen Subnetz befinden als die Ethernet-Ports der Steuerung.

Adressverwaltung

Das nachstehende Diagramm zeigt die verschiedenen Typen von Adresssystemen für die Steuerung:



HINWEIS: Wenn ein Gerät für die Verwendung der DHCP- oder BOOTP-Adressierungsmethoden programmiert wurde und keine Verbindung zum entsprechenden Server herstellen kann, verwendet die Steuerung die Standard-IP-Adresse. Der Request wird ständig wiederholt.

Der IP-Prozess wird in den folgenden Fällen neu gestartet:

- Neustart der Steuerung
- Erneuter Anschluss des Ethernet-Kabels
- Anwendungsdownload (falls sich IP-Parameter ändern)
- DHCP- oder BOOTP-Server nach einem gescheiterten Adressierungsversuch erkannt

Ethernet-Konfiguration

Doppelklicken Sie in der **Gerätebaumstruktur** auf **TMSES4**:

HINWEIS:

- Wenn Sie sich im Offline-Modus befinden, wird das Fenster **Konfigurierte Parameter** (Abbildung oben) angezeigt. Sie können die Parameter bearbeiten.
- Wenn Sie sich im Online-Modus befinden, werden die Fenster **Konfigurierte Parameter** und **Stromeinstellungen** (keine Abbildung) angezeigt. Sie können die Parameter bearbeiten.

In der folgenden Tabelle werden die konfigurierten Parameter beschrieben:

Konfigurierte Parameter	Beschreibung
Netzwerkname	Dient als Gerätename zum Abrufen der IP-Adresse über DHCP, maximal 15 Zeichen.
IP-Adresse nach DHCP	IP-Adresse wird vom DHCP-Server abgerufen.
IP-Adresse nach BOOTP	IP-Adresse wird vom BOOTP-Server abgerufen. Die MAC-Adresse ist an der linken Seite der Steuerung angegeben.
Feste IP-Adresse	IP-Adresse, Subnetzmaske und Gateway-Adresse werden vom Benutzer definiert.
Ethernet-Protokoll	Verwendeter Protokolltyp: Ethernet 2
Übertragungsrate	Geschwindigkeit und Duplex befinden sich im Autonegotiationsmodus (automatische Verhandlung).

Standard-IP-Adresse

Die MAC-Adresse des Ethernet-Ports ist auf dem Etikett an der Vorderseite des M262 Controller angegeben. Die MAC-Adresse des TMSES4-Ports ist auf dem Etikett an der linken Seite des M262 Controller angegeben.

HINWEIS: Eine MAC-Adresse wird im Hexadezimalformat und eine IP-Adresse im Dezimalformat geschrieben. Konvertieren Sie die MAC-Adresse in das Dezimalformat.

Konvertierungsbeispiel:

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

Subnetzmaske

Die Subnetzmaske wird verwendet, um mehrere physische Netzwerke mit einer einzigen Netzwerkadresse zu adressieren. Durch die Maske werden das Subnetz und die Geräteadresse in der Host-ID getrennt.

Man erhält die Subnetzadresse, indem die Bits der IP-Adresse, die den Positionen der Maske entsprechen, die 1 enthalten, beibehalten und die restlichen durch 0 ersetzt werden.

Umgekehrt erhält man die Subnetzmaske des Hostgeräts, indem die Bits der IP-Adresse, die den Positionen der Maske entsprechen, die 0 enthalten, beibehalten und die restlichen durch 1 ersetzt werden.

Beispiel für eine Subnetzadresse:

IP-Adresse	192 (11000000)	1 (00000001)	17 (00010001)	11 (00001011)
Subnetzmaske	255 (11111111)	255 (11111111)	240 (11110000)	0 (00000000)
Subnetzadresse	192 (11000000)	1 (00000001)	16 (00010000)	0 (00000000)

HINWEIS: Wenn kein Gateway vorhanden ist, kommuniziert das Gerät nicht in seinem Subnetz.

Gateway-Adresse

Das Gateway ermöglicht, dass eine Nachricht an ein Gerät geleitet wird, das sich nicht im aktuellen Netzwerk befindet.

Wenn kein Gateway vorhanden ist, lautet die Gateway-Adresse 0.0.0.0.

Die Gateway-Adresse muss an der Ethernet_1-Schnittstelle definiert sein. Der Datenverkehr an externe Netzwerke wird über diese Schnittstelle gesendet.

Sicherheitsparameter

In der folgenden Tabelle werden die verschiedenen Sicherheitsparameter beschrieben:

Sicherheitsparameter	Beschreibung	Standardeinstellungen
Discovery-Protokoll	Dieser Parameter deaktiviert das Discovery-Protokoll . Bei Deaktivierung werden Discovery-Requests ignoriert.	Aktiv
FTP-Server	Dieser Parameter deaktiviert den FTP-Server der Steuerung. Bei Deaktivierung werden FTP-Requests ignoriert.	Aktiv
Machine Expert-Protokoll	Dieser Parameter deaktiviert das Machine Expert-Protokoll an den Ethernet-Schnittstellen. Wenn dieser Parameter deaktiviert ist, wird jeder Machine Expert-Request von jedem Gerät zurückgewiesen. Aus diesem Grund ist keine Verbindung über Ethernet von einem PC mit EcoStruxure Machine Expert, von einem HMI-Ziel, das Variablen mit dieser Steuerung austauschen möchte, von einem OPC-Server oder von Controller Assistant möglich.	Aktiv
Modbus-Server	Dieser Parameter deaktiviert den Modbus-Server der Steuerung. Bei Deaktivierung werden Modbus-Requests an die Steuerung ignoriert.	Inaktiv
Remote-Verbindung	Dieser Parameter deaktiviert die Remote-Verbindung. Wenn der Parameter deaktiviert ist, werden Fast TCP-Requests ignoriert.	Aktiv
Sicherer Webserver	Dieser Parameter deaktiviert den sicheren Webserver der Steuerung. Wenn dieser Parameter deaktiviert ist, werden HTTPS-Requests an die den sicheren Webserver der Steuerung ignoriert.	Aktiv
SNMP-Protokoll	Dieser Parameter deaktiviert den SNMP-Server der Steuerung. Bei Deaktivierung werden SNMP-Requests ignoriert.	Inaktiv
WebVisualisation-Protokoll	Dieser Parameter deaktiviert die WebVisualisation-Seiten der Steuerung. Bei Deaktivierung werden HTTP-Requests an das WebVisualisation-Protokoll des Logic Controller ignoriert.	Inaktiv

Modicon M262 Logic/Motion Controller als Zielgerät für EtherNet/IP

Einführung

In diesem Abschnitt wird die Konfiguration des M262 Logic/Motion Controller als EtherNet/IP-Zielgerät beschrieben.

Für weitere Informationen über EtherNet/IP siehe die Website www.odva.org.

Hinzufügen eines EtherNet/IP-Managers

Um den M262 Logic/Motion Controller als Zielgerät für Ethernet/IP zu konfigurieren, müssen Sie der Steuerung einen EthernetIP-Manager hinzufügen.

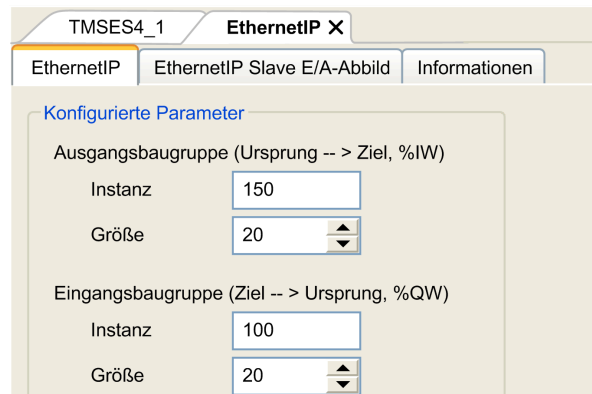
So fügen Sie dem M262 Logic/Motion Controller einen EthernetIP-Manager hinzu:

Schritt	Aktion
1	Fügen Sie ein TMSES4-Erweiterungsmodul in Ihrer Konfiguration hinzu.
2	<p>Fügen Sie ausgehend vom TMSES4-Knoten in der Gerätebaumstruktur den EthernetIP-Manager hinzu, indem Sie ihn im Hardwarekatalog auswählen, in die Gerätebaumstruktur ziehen und auf dem TMSES4-Knoten ablegen.</p> <p>Weitere Informationen zum Hinzufügen von Geräten in einem Projekt finden Sie unter:</p> <ul style="list-style-type: none"> • Verwenden der Methode Drag&Dop (siehe EcoStruxure Machine Expert, Programming Guide) (Ziehen und Ablegen) • Verwenden der Kontextmenüs oder Plus-Schaltflächen (siehe EcoStruxure Machine Expert, Programming Guide)

EtherNet/IP-Parameterkonfiguration

Um den EtherNet/IP-Parameter zu konfigurieren, doppelklicken Sie auf **COM_Bus > TMSES4 > EthernetIP** in der **Gerätebaumstruktur**.

Daraufhin erscheint ein Dialogfeld:



Die EtherNet/IP-E/A-Konfigurationsparameter sind wie folgt definiert:

- **Instanz:**
Nummer der Eingangs- oder Ausgangs-Assembly.
- **Größe:**
Anzahl der Kanäle einer Eingangs- oder Ausgangs-Assembly.
Jeder Kanal verfügt über einen 2-Byte-Speicher, in dem der Wert eines $\%IWx$ - oder $\%QWx$ -Objekts abgelegt wird, wobei x die Kanalnummer ist.
Beispiel: Wenn die **Größe** der **Ausgangs-Assembly** 20 ist, gibt es 20 Eingangskanäle ($IW0...IW19$), die $\%IWy...%IW(y+20-1)$ adressieren, wobei y der erste verfügbare Kanal für die Assembly ist.

Element		Zulässiger Steuerungsbereich	EcoStruxure Machine Expert Standardwert
Ausgangs-Assembly	Instanz	150...189	150
	Größe	2...120	20
Eingangs-Assembly	Instanz	100...149	100
	Größe	2...120	20

Weitere Informationen zu den folgenden Themen finden Sie im M262 – Programmierhandbuch:

- Generieren einer EDS-Datei
- Konfigurieren von E/A
- Von der Steuerung unterstützte Objekte

Modicon M262 Logic/Motion Controller als Slavegerät in einem Modbus TCP-Netzwerk

Überblick

In diesem Abschnitt wird die Konfiguration des M262 Logic/Motion Controller als **Modbus TCP-Slavegerät** beschrieben.

Um M262 Logic/Motion Controller als **Modbus TCP-Slavegerät** zu konfigurieren, müssen Sie die Funktion **Modbus TCP-Slavegerät** Ihrer Steuerung hinzufügen (siehe Hinzufügen eines Modbus TCP-Slavegeräts).

Diese Funktion richtet einen spezifischen E/A-Bereich in der Steuerung ein, auf den über das Modbus TCP-Protokoll zugegriffen werden kann. Dieser E/A-Bereich wird immer dann verwendet, wenn ein externer Master auf die %IW- und %QW-Objekte der Steuerung zugreifen muss. Dieses **Modbus TCP-Slavegerät** ermöglicht Ihnen die Bereitstellung der E/A-Objekte der Steuerung für diesen Bereich, auf die dann über einen einzigen Modbus-Lese-/Schreibregister-Request zugegriffen werden kann.

Das **Modbus TCP-Slavegerät** fügt eine weitere Modbus-Serverfunktion zur Steuerung hinzu. Dieser Server wird von der Modbus-Clientanwendung durch Angabe einer konfigurierten Geräte-ID (Modbus-Adresse) im Bereich 1 bis 247 adressiert. Der integrierte Modbus-Server der Slave-Steuerung erfordert keine Konfiguration; er wird über die Geräte-ID = 255 adressiert. Weitere Informationen finden Sie unter [Modbus TCP-Konfiguration](#), Seite 22.

Die Eingänge/Ausgänge aus Sicht der Slave-Steuerung: Die Eingänge werden vom Master geschrieben, die Ausgänge vom Master gelesen.

Das **Modbus TCP-Slavegerät** kann eine privilegierte Modbus-Clientanwendung definieren, deren Verbindung nicht unterbrochen wird (die integrierten Modbus-Verbindungen werden unter Umständen beendet, wenn mehr als acht Verbindungen benötigt werden).

Über die Timeout-Dauer der privilegierten Verbindung können Sie prüfen, ob der privilegierte Master die Steuerung per Polling abfragt. Wenn innerhalb der Timeout-Dauer kein Modbus-Request empfangen wird, werden die Diagnoseinformationen *i_byMasterIpLost* auf 1 (TRUE) gesetzt. Weitere Informationen finden Sie unter [Schreibgeschützte Ethernet-Port-Systemvariablen](#) (siehe [Modicon M262 Logic Controller, Systemfunktionen und Variablen](#), Systembibliothekshandbuch).

Weitere Informationen zu Modbus TCP finden Sie auf der Website www.modbus.org.

Hinzufügen eines Modbus TCP -Slavegeräts

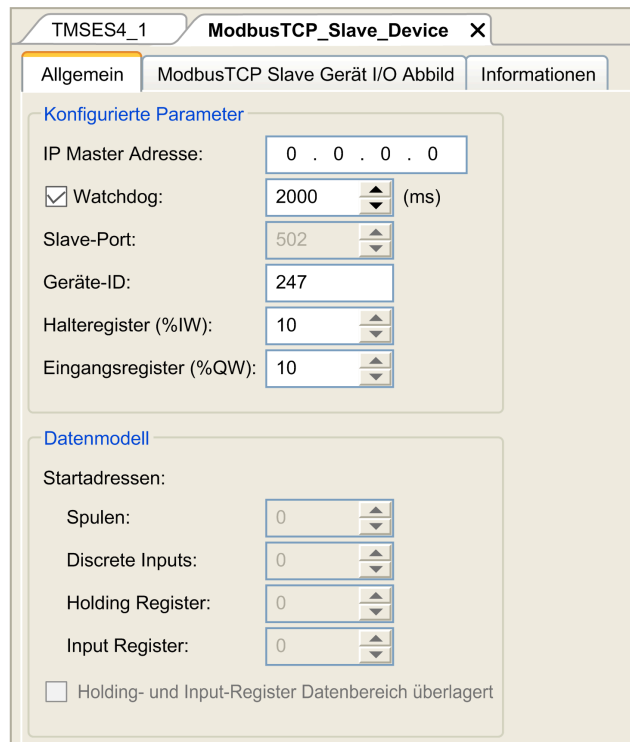
So fügen Sie Ihrem M262 Logic/Motion Controller die Modbus TCP-Slave-Gerät-Funktion hinzu:

Schritt	Aktion
1	Fügen Sie ein TMSES4-Erweiterungsmodul in Ihrer Konfiguration hinzu.
2	<p>Fügen Sie ausgehend vom TMSES4-Knoten in der Gerätebaumstruktur das Modbus TCP-Slavegerät hinzu, indem Sie es im Hardwarekatalog auswählen, in die Gerätebaumstruktur ziehen und auf dem TMSES4-Knoten ablegen.</p> <p>Weitere Informationen zum Hinzufügen von Geräten in einem Projekt finden Sie unter:</p> <ul style="list-style-type: none"> • Verwenden der Methode Drag&Dop (siehe EcoStruxure Machine Expert, Programming Guide) (Ziehen und Ablegen) • Verwenden der Kontextmenüs oder Plus-Schaltflächen (siehe EcoStruxure Machine Expert, Programming Guide)

Konfigurieren eines Modbus TCP Slavegeräts

Um das Modbus TCP-Slave-Gerät zu konfigurieren, doppelklicken Sie auf **COM_Bus > TMSES4 > ModbusTCP_Slave_Device** in der **Gerätebaumstruktur**.

Das folgende Dialogfeld wird angezeigt:



Element	Beschreibung
Master-IP-Adresse	IP-Adresse des Modbus-Masters. Die Verbindungen an dieser Adresse werden nicht geschlossen.
Watchdog	Timeout in 500-ms-Inkrementen. HINWEIS: Das Timeout gilt für die Master-IP-Adresse , sofern sie nicht 0.0.0.0 lautet.
Slave-Port	Modbus-Kommunikationsport (502).
Geräte-ID	Sendet die Requests an das Modbus TCP-Slavegerät (Modbus TCP-Slave-Gerät) (1 bis 247) anstatt an den integrierten Modbus-Server (255).
Haltereister (%IW)	Anzahl der %IW-Register, die beim Austausch verwendet werden sollen (2 bis 120) (jedes Register umfasst 2 Byte).
Eingangsregister (%QW)	Anzahl der %QW-Register, die beim Austausch verwendet werden sollen (2 bis 120) (jedes Register umfasst 2 Byte).

Registerkarte ModbusTCP Slave Gerät E/A-Abbild

Die E/A werden aus der Sicht des Masters wie folgt den Modbus-Registern zugeordnet:

- %IWs werden von Register 0 bis n-1 zugeordnet und sind R/W (n = Anzahl Haltereister, ein %IW-Register umfasst jeweils 2 Byte).
- %QWs werden von Register n bis n+m -1 zugeordnet und sind schreibgeschützt (m = Anzahl Eingangsregister, ein %QW-Register umfasst jeweils 2 Byte).

Wenn ein **Modbus TCP-Slavegerät** konfiguriert wurde, werden Modbus-Befehle, die an die Geräte-ID (Modbus-Adresse) gesendet werden, anders gehandhabt als der gleiche Befehl, wenn er an ein anderes Modbus-Gerät im Netzwerk adressiert wird. Wird beispielsweise der Modbus-Befehl 3 (3 hex) an das Modbus-Standardgerät gesendet, liest das Gerät den Wert eines oder mehrerer Register und gibt diesen Wert zurück. Wenn derselbe Befehl an den Modbus TCP-Slave (siehe Modicon M262 Logic/Motion Controller, Programmierhandbuch) gesendet wird, ermöglicht er einen Lesevorgang durch den externen E/A-Scanner.

Wenn ein **Modbus TCP-Slavegerät** konfiguriert wurde, greifen Modbus-Befehle, die an die Geräte-ID (Modbus-Adresse) gesendet werden, auf die %IW- und %QW-Objekte der Steuerung zu, die mit dem Modbus TCP-Gerät verbunden sind, anstelle der regulären Modbus-Wörter (auf die zugegriffen wird, wenn die Geräte-ID 255 ist). Dies ermöglicht Lese-/Schreibvorgänge durch eine Modbus TCP-IOScanner-Anwendung.

Das **Modbus TCP-Slavegerät** antwortet auf eine Teilmenge der Modbus-Befehle zum Austausch von Daten mit dem externen E/A-Scanner. Die folgenden Modbus-Befehle werden vom **Modbus TCP-Slavegerät** unterstützt:

Funktions-code dez. (hex.)	Funktion	Kommentar
3 (3)	Halteregister lesen	Ermöglicht dem Master das Lesen der %IW- und %QW-Geräteobjekte.
6 (6)	Einzelnes Register schreiben	Ermöglicht dem Master das Schreiben der %IW-Geräteobjekte.
16 (10)	Mehrere Register schreiben	Ermöglicht dem Master das Schreiben der %IW-Geräteobjekte.
23 (17)	Mehrere Register lesen/schreiben	Ermöglicht dem Master das Lesen der %IW- und %QW- und das Schreiben der %IW-Geräteobjekte.
Sonstige	Nicht unterstützt.	–

HINWEIS: Bei Modbus-Requests, die auf Register oberhalb von n+m-1 zugreifen, wird der Ausnahmecode 02 – ILLEGAL DATA ADDRESS zurückgegeben.

Um E/A-Objekte mit Variablen zu verknüpfen, wählen Sie die Registerkarte **Modbus TCP Slave Gerät I/O Abbild** aus:

The screenshot shows the configuration interface for a Modbus TCP Slave Device. The active tab is 'ModbusTCP Slave Gerät I/O Abbild'. The main area contains a table with the following columns: Variable, Zuordnung, Kanal, Adresse, Typ, Standardwert, Einheit, and Beschreibung. The table is divided into two sections: 'Eingänge' (Inputs) and 'Ausgänge' (Outputs). Each section lists 10 variables (iwModbusTCP_S... and qwModbusTCP_S...) corresponding to addresses %IW21-%IW30 and %QW21-%QW30. The 'Typ' column shows 'ARRAY[0...9]...' for the first row of each section and 'WORD' for the others. The 'Standardwert' column is set to 0 for all. Below the table, there are buttons for 'Mapping zurücksetzen' and 'Buszyklus-Optionen'. The 'Buszyklus-Optionen' section has a dropdown menu set to 'Zykluseinstellungen des übergeordneten Busses verwenden'.

Kanal		Typ	Beschreibung
Eingang	IW0	WORD	Halteregister 0

	IWx	WORD	Halteregister x
Ausgang	QW0	WORD	Eingangsregister 0

	QWy	WORD	Eingangsregister y

Die Anzahl der Wörter ist abhängig von den Parametern **Halteregister (%IW)** und **Eingangsregister (%QW)** der Registerkarte **Modbus TCP**.

HINWEIS: Ausgang bedeutet AUSGANG der Client/Master-Steuerung (%IW für die Server/Slave-Steuerung). Eingang bedeutet EINGANG der Client/Master-Steuerung (%QW für die Server/Slave-Steuerung).

Buszyklus-Optionen

Wählen Sie die zu verwendende **Buszyklus-Task** aus:

- **Zykluseinstellungen des übergeordneten Busses verwenden** (Standard)
- **MAST**

Im E/A-Abbild-Editor des Geräts, das das Modbus TCP-Slavegerät (Modbus TCP-Slave-Gerät) enthält, ist der entsprechende Parameter **Buszyklus-Task** vorhanden. Dieser Parameter definiert die Task, die für die Aktualisierung der %IW- und %QW-Register zuständig ist.

Firewallkonfiguration

Einführung

In diesem Abschnitt wird die Konfiguration der Firewall des Modicon M262 Logic/Motion Controller beschrieben.

Einführung

Firewall – Beschreibung

Im Allgemeinen dienen Firewalls dem Schutz der Netzwerksicherheitszone, indem Sie jeden unbefugten Zugriff verhindern und ausschließlich autorisierten Zugriff gewähren. Bei einer Firewall handelt es sich um ein Gerät bzw. um eine Gruppe von Geräten, die für die Genehmigung, Verweigerung, Verschlüsselung, Entschlüsselung oder Umleitung über Proxy des Datenverkehrs zwischen verschiedenen Sicherheitszonen auf der Grundlage einer Reihe von Regeln und anderen Kriterien konfiguriert wurden.

Geräte zur Prozesssteuerung und Maschinen zur Hochgeschwindigkeitsproduktion benötigen einen hohen Datendurchsatz und tolerieren in vielen Fällen die Latenz nicht, die bei einer aggressiven Sicherheitsstrategie innerhalb des Steuerungsnetzwerks gegeben ist. Aus diesem Grund spielen Firewalls eine bedeutende Rolle in jeder Sicherheitsstrategie, da sie bestimmte Schutzniveaus am Netzwerkperimeter bereitstellen. Firewalls sind ein wichtiger Bestandteil einer globalen Strategie auf Systemebene.

HINWEIS: Schneider Electric operiert unter den Industriestandards bei der Entwicklung und Implementierung von Steuerungssystemen. Dies beinhaltet ein „Defense-in-Depth-Konzept“ zum Schutz industrieller Steuerungssysteme. Bei diesem Verfahren werden die Steuerungen hinter einer oder mehreren Firewalls platziert, um den Zugriff auf autorisierte Personen und Protokolle zu beschränken.

▲ WARNUNG

UNBERECHTIGTER ZUGRIFF MIT UNBERECHTIGTEM MASCHINENBETRIEB

- Beurteilen Sie, ob Ihre Betriebsumgebung bzw. Ihre Maschinen mit Ihrer kritischen Infrastruktur verbunden sind. Ist das der Fall, dann ergreifen Sie angemessene Präventivmaßnahmen auf der Basis des Defense-in-Depth-Konzepts, bevor Sie das Automatisierungssystem mit einem Netzwerk verbinden.
- Begrenzen Sie die Anzahl der mit einem Netzwerk verbundenen Geräte auf das strikte Minimum.
- Isolieren Sie Ihr Industrienetzwerk von anderen Netzwerken in Ihrer Firma.
- Schützen Sie alle Netzwerke vor unberechtigtem Zugriff mithilfe von Firewalls, VPNs oder anderen bewährten Schutzmaßnahmen.
- Überwachen Sie die Aktivität in Ihren Systemen.
- Verhindern Sie jeden direkten Zugriff bzw. jede direkte Verbindung von Fachgeräten durch unberechtigte Personen oder nicht autorisierte Vorgänge.
- Stellen Sie einen Wiederherstellungsplan für den Notfall auf. Dazu gehört ebenfalls der Backup Ihrer System- und Prozessdaten.

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

Firewallkonfiguration

Es gibt zwei Möglichkeiten, um die Konfiguration der Steuerungsfirewall zu verwalten:

- Statische Konfiguration
- Dynamische Änderungen
- Anwendungseinstellungen

Für die statische Konfiguration und dynamische Änderungen werden Skriptdateien verwendet.

Statische Konfiguration

Die statische Konfiguration wird geladen, wenn die Steuerung gestartet wird.

Die Firewall der Steuerung kann statisch konfiguriert werden, indem eine auf der Steuerung befindliche Standardskriptdatei verwaltet wird. Speicherort dieser Datei: `/usr/Cfg/FirewallDefault.cmd`

HINWEIS: Der Dateiname unterliegt der Groß-/Kleinschreibung.

Dynamische Änderungen

Nachdem die Steuerung gestartet wurde, kann die Konfiguration der Steuerungsfirewall mittels Skriptdateien geändert werden.

Es stehen zwei Methoden zum Laden dieser dynamischen Änderungen zur Auswahl:

- Eine SD-Karte, Seite 27.

- Ein Funktionsbaustein, Seite 27 in der Anwendung.

Anwendungseinstellungen

Siehe Ethernet-Konfiguration, Seite 18.

Verfahren für dynamische Änderungen

Über eine SD-Karte

In dieser Tabelle wird das Verfahren zum Ausführen einer Skriptdatei über eine SD-Karte beschrieben:

Schritt	Aktion
1	Erstellen Sie eine gültige Skriptdatei, Seite 29. Geben Sie der Skriptdatei beispielsweise folgenden Namen: <i>FirewallMaintenance.cmd</i> .
2	Laden Sie die Skriptdatei auf die SD-Karte. Laden Sie die Skriptdatei beispielsweise in den Ordner <i>usr/Cfg</i> .
3	Fügen Sie in der Datei <i>Sys/Cmd/Script.cm</i> eine Codezeile mit folgendem Befehl hinzu: <code>Firewall_install "/pathname/FileName"</code> Beispiel: Die Codezeile lautet folgendermaßen: <code>Firewall_install "/sd0/usr/Cfg/FirewallMaintenance.cmd"</code> HINWEIS: Der Dateiname unterliegt der Groß-/Kleinschreibung.
4	Setzen Sie die SD-Karte in die Steuerung ein.

Über einen Funktionsbaustein in der Anwendung

In dieser Tabelle wird das Verfahren zum Ausführen einer Skriptdatei von einer Anwendung aus beschrieben:

Schritt	Aktion
1	Erstellen Sie eine gültige Skriptdatei, Seite 29. Geben Sie der Skriptdatei beispielsweise folgenden Namen: <i>FirewallMaintenance.cmd</i> .
2	Laden Sie die Skriptdatei in den Speicher der Steuerung. Laden Sie die Skriptdatei beispielsweise in den Ordner <i>usr/Syslog</i> per FTP.
3	Verwenden Sie einen <code>ExecuteScript</code> -Funktionsbaustein. Für weitere Informationen siehe das M262 System-Bibliothekshandbuch (siehe Modicon M262 Logic/Motion Controller, Systemfunktionen und Variablen, System-Bibliothekshandbuch). Beispiel: Der Eingang [SCmd] ist <code>'Firewall_install "/usr/Syslog/FirewallMaintenance.cmd"'</code> . HINWEIS: Der Dateiname unterliegt der Groß-/Kleinschreibung.

Verhalten der Firewall

Einführung

Die Firewallkonfiguration richtet sich nach der Aktion, die an der Steuerung durchgeführt wird, und nach dem Anfangszustand der Konfiguration. Es gibt fünf mögliche Anfangszustände:

- In der Steuerung ist keine Standardskriptdatei vorhanden.
- Eine gültige Datei ist vorhanden.
- Eine ungültige Skriptdatei ist vorhanden.
- Es ist keine Standardskriptdatei vorhanden, und die Anwendung hat die Firewall konfiguriert.
- Es wurde bereits eine dynamische Skriptdateikonfiguration durchgeführt.

HINWEIS: Um zu ermitteln, ob die Firewall konfiguriert und aktiviert ist, rufen Sie den Meldungslogger auf.

Keine Standardskriptdatei

Wenn...	Dann...
Steuerung wird gestartet.	Firewall wird nicht konfiguriert. Es ist kein Schutz aktiviert.
Dynamische Skriptdatei wird ausgeführt.	Firewall wird entsprechend der dynamischen Skriptdatei konfiguriert.
Inkorrekte dynamische Skriptdatei wird ausgeführt.	Firewall wird nicht konfiguriert. Es ist kein Schutz aktiviert.
Anwendung wird heruntergeladen.	Firewall wird entsprechend den Anwendungseinstellungen konfiguriert.

Standardskriptdatei vorhanden.

Wenn...	Dann...
Steuerung wird gestartet.	Firewall wird entsprechend der Standardskriptdatei konfiguriert.
Dynamische Skriptdatei wird ausgeführt.	Die gesamte Konfiguration der Standardskriptdatei wird gelöscht. Firewall wird entsprechend der dynamischen Skriptdatei konfiguriert.
Inkorrekte dynamische Skriptdatei wird ausgeführt.	Firewall wird entsprechend der Standardskriptdatei konfiguriert. Die dynamische Skriptdatei wird nicht berücksichtigt.
Anwendung wird heruntergeladen.	Die gesamte Konfiguration der Anwendung wird ignoriert. Firewall wird entsprechend der Standardskriptdatei konfiguriert.

Inkorrekte Standardskriptdatei vorhanden.

Wenn...	Dann...
Steuerung wird gestartet.	Firewall wird nicht konfiguriert. Es ist kein Schutz aktiviert.
Dynamische Skriptdatei wird ausgeführt.	Firewall wird entsprechend der dynamischen Skriptdatei konfiguriert.
Anwendung wird heruntergeladen.	Firewall wird entsprechend den Anwendungseinstellungen konfiguriert.

Anwendungseinstellungen ohne Standardskriptdatei.

Wenn...	Dann...
Steuerung wird gestartet.	Firewall wird entsprechend den Anwendungseinstellungen konfiguriert.
Dynamische Skriptdatei wird ausgeführt.	Die gesamte Konfiguration der Anwendungseinstellungen wird gelöscht. Firewall wird entsprechend der dynamischen Skriptdatei konfiguriert.
Inkorrekte dynamische Skriptdatei wird ausgeführt.	Firewall wird entsprechend den Anwendungseinstellungen konfiguriert. Die dynamische Skriptdatei wird nicht berücksichtigt.
Anwendung wird heruntergeladen.	Die gesamte Konfiguration der vorherigen Anwendung wird gelöscht. Firewall wird entsprechend den neuen Anwendungseinstellungen konfiguriert.

Dynamische Skriptdatei zum wiederholten Mal ausgeführt.

Wenn...	Dann...
Steuerung wird gestartet.	Firewall wird entsprechend der Konfiguration der dynamischen Skriptdatei konfiguriert (siehe Hinweis).
Dynamische Skriptdatei wird ausgeführt.	Die gesamte Konfiguration der vorherigen dynamischen Skriptdatei wird gelöscht. Firewall wird entsprechend der neuen dynamischen Skriptdatei konfiguriert.
Inkorrekte dynamische Skriptdatei wird ausgeführt.	Firewall wird entsprechend der Konfiguration der vorherigen dynamischen Skriptdatei konfiguriert. Die inkorrekte dynamische Skriptdatei wird nicht berücksichtigt.
Anwendung wird heruntergeladen.	Die gesamte Konfiguration der Anwendung wird ignoriert. Firewall wird entsprechend der dynamischen Skriptdatei konfiguriert.

Skriptbefehle für die Firewall

Überblick

In diesem Abschnitt wird beschrieben, wie Skriptdateien (Standardskriptdateien oder dynamische Skriptdateien) geschrieben werden müssen, damit sie beim Start der Steuerung bzw. bei einem bestimmten ausgelösten Befehl korrekt ausgeführt werden können.

HINWEIS: Die Regeln der MAC-Schicht werden separat verwaltet und haben höhere Priorität als die übrigen Paketfilterregeln.

Syntax einer Skriptdatei

Die Syntax von Skriptdateien wird unter Erstellen eines Skripts (siehe Modicon M262 Logic/Motion Controller, Programmierhandbuch) beschrieben.

Allgemeine Firewallbefehle

Für die Verwaltung der Ethernet-Firewall des M262 Logic/Motion Controller sind folgende Befehle verfügbar:

Befehl	Beschreibung
Firewall Enable	Blockiert die Frames von den Ethernet-Schnittstellen. Wenn keine spezifische IP-Adresse autorisiert ist, ist keine Kommunikation über die Ethernet-Schnittstellen möglich. HINWEIS: Standardmäßig werden die Frames bei aktivierter Firewall abgewiesen.
Firewall Disable	Firewall-Regeln werden nicht angewendet. Frames werden nicht blockiert.
Firewall Ethx Default Allow ⁽¹⁾	Frames werden von der Steuerung angenommen.
Firewall Ethx Default Reject ⁽¹⁾	Frames werden von der Steuerung abgewiesen. HINWEIS: Wenn diese Zeile nicht vorhanden ist, entspricht sie standardmäßig dem Befehl <code>Firewall Eth1 Default Reject</code> .
<p>(1) Hierbei gilt: Ethx =</p> <ul style="list-style-type: none"> • Eth1: Ethernet_1 • Eth2: Ethernet_2 • Eth3: TMSES4 (erstes Ethernet-Modul von links) • Eth4: TMSES4 (zweites Ethernet-Modul von links) • Eth5: TMSES4 (drittes Ethernet-Modul von links) 	

Spezifische Firewallbefehle

Für die Konfiguration der Firewallregeln für bestimmte Ports und Adressen sind folgende Befehle verfügbar:

Befehl	Bereich	Beschreibung
Firewall Eth1 Allow IP <code>•••••</code>	• = 0 bis 255	Die Frames von den genannten IP-Adressen sind für alle Portnummern und Porttypen zugelassen.
Firewall Eth1 Reject IP <code>•••••</code>	• = 0 bis 255	Die Frames von den genannten IP-Adressen werden für alle Portnummern und Porttypen abgewiesen.
Firewall Eth1 Allow IPs <code>••••• to •••••</code>	• = 0 bis 255	Die Frames von den IP-Adressen im genannten Bereich sind für alle Portnummern und Porttypen zugelassen.
Firewall Eth1 Reject IPs <code>••••• to •••••</code>	• = 0 bis 255	Die Frames von den IP-Adressen im genannten Bereich werden für alle Portnummern und Porttypen abgewiesen.
Firewall Eth1 Allow <code>port_type port Y</code>	Y = (Zielportnummern, Seite 34)	Die Frames mit der genannten Zielportnummer sind zugelassen.
Firewall Eth1 Reject <code>port_type port Y</code>	Y = (Zielportnummern, Seite 34)	Die Frames mit der genannten Zielportnummer werden zurückgewiesen.
Firewall Eth1 Allow <code>port_type ports Y1 to Y2</code>	Y = (Zielportnummern, Seite 34)	Die Frames mit einer Zielportnummer im genannten Bereich sind zugelassen.
Firewall Eth1 Reject <code>port_type ports Y1 to Y2</code>	Y = (Zielportnummern, Seite 34)	Die Frames mit einer Zielportnummer im genannten Bereich werden abgewiesen.
Firewall Eth1 Allow IP <code>••••• on port_type port Y</code>	• = 0 bis 255 Y = (Zielportnummern, Seite 34)	Die Frames von der genannten IP-Adresse und mit der genannten Zielportnummer sind zugelassen.
Firewall Eth1 Reject IP <code>••••• on port_type port Y</code>	• = 0 bis 255 Y = (Zielportnummern, Seite 34)	Die Frames von der genannten IP-Adresse und mit der genannten Zielportnummer werden abgewiesen.
Firewall Eth1 Allow IP <code>••••• on port_type ports Y1 to Y2</code>	• = 0 bis 255 Y = (Zielportnummern, Seite 34)	Die Frames von der genannten IP-Adresse und mit einer Zielportnummer im genannten Bereich sind zugelassen.
Firewall Eth1 Reject IP <code>••••• on port_type ports Y1 to Y2</code>	• = 0 bis 255 Y = (Zielportnummern, Seite 34)	Die Frames von der genannten IP-Adresse und mit einer Zielportnummer im genannten Bereich werden abgewiesen.
Firewall Eth1 Allow IPs <code>•1.1.1.1 to •2.2.2.2 on port_type port Y</code>	• = 0 bis 255 Y = (Zielportnummern, Seite 34)	Die Frames von einer IP-Adresse im genannten Bereich und mit der genannten Zielportnummer werden zugelassen.
Firewall Eth1 Reject IPs <code>•1.1.1.1 to •2.2.2.2 on port_type port Y</code>	• = 0 bis 255 Y = (Zielportnummern, Seite 34)	Die Frames von einer IP-Adresse im genannten Bereich und mit der genannten Zielportnummer werden abgewiesen.
Firewall Eth1 Allow IPs <code>•1.1.1.1 to •2.2.2.2 on port_type ports Y1 to Y2</code>	• = 0 bis 255 Y = (Zielportnummern, Seite 34)	Die Frames von einer IP-Adresse im genannten Bereich und mit einer Zielportnummer im genannten Bereich sind zugelassen.
Firewall Eth1 Reject IPs <code>•1.1.1.1 to •2.2.2.2 on port_type ports Y1 to Y2</code>	• = 0 bis 255 Y = (Zielportnummern, Seite 34)	Die Frames von einer IP-Adresse im genannten Bereich und mit einer Zielportnummer im genannten Bereich werden abgewiesen.
Firewall Eth1 Allow MAC <code>••:••:••:••:••:••</code>	• = 0...F	Die Frames von der genannten MAC-Adresse <code>••:••:~••:~••:~••:~••</code> sind zugelassen. HINWEIS: Wenn Zulassungsregeln für MAC-Adressen angewendet werden, können nur die aufgelisteten MAC-Adressen mit der Steuerung kommunizieren, auch wenn andere Regeln zulässig sind.
Firewall Eth1 Reject MAC <code>••:~••:~••:~••:~••:~••</code>	• = 0 bis F	Die Frames mit der genannten MAC-Adresse <code>••:~••:~••:~••:~••:~••</code> werden abgewiesen.

Befehl	Bereich	Beschreibung
Firewall Ethx ⁽¹⁾ Established to port_type port Y	Y = 0 bis 65535	Frames, die von der Steuerung mit den Protokollen TCP/UDP an die angegebene Zielporntnummer gesendet werden, sind zulässig.
<p>(1) Wenn:</p> <ul style="list-style-type: none"> x=0, USB-Port. x=1, Ethernet 1-Port. x=2, Ethernet 2-Port. x=3, Ethernet-Port des TMSES4 (erstes Ethernet-Modul von links). x=4: Ethernet-Port des TMSES4 (zweites Ethernet-Modul von links). x=5: Ethernet-Port des TMSES4 (drittes Ethernet-Modul von links). 		

Beispiel für ein Skript

Nachfolgend ist ein Beispiel für eine Firewall im Whitelist-Modus aufgeführt. In dem Beispiel ist standardmäßig die gesamte Kommunikation gesperrt, und nur die notwendigen Dienste sind zugelassen.

HINWEIS: In dem Beispiel werden die meisten mit der Firewall verfügbaren Befehle gezeigt. Es sollte an Ihre Konfiguration angepasst und vor der Implementierung getestet werden.

Befehle	Kommentare
Firewall Enable	Aktiviert die Firewall.
Eth1-Konfiguration	
Firewall Eth1 Default Reject	Weist alle Frames über die Schnittstelle ETH1 zurück. In diesem Beispiel ist ETH1 mit dem Industrial Ethernet-Gerätenetzwerk verbunden und kann daher als relativ vertrauenswürdig betrachtet werden.
Firewall Eth1 Allow TCP port 502	Lässt den Modbus TCP-Server über die Schnittstelle ETH1 zu. Es erfolgt keine Modbus-Authentifizierung, daher sollte dies nur in vertrauenswürdigen Netzwerken gestattet werden.
Firewall Eth1 Established to TCP port 502	Gestattet Antworten auf die von der Steuerung hergestellte Kommunikation mit dem TCP-Port 502. Dies ist erforderlich, wenn die PlcCommunication-Bibliothek für die Kommunikation mit dem Modbus TCP-Protokoll verwendet wird.
Firewall Eth1 Allow UDP port 2222	Der ETHIP-Scanner kann implizit Antworten an den UDP-Port 2222 (ETHIP) über die Schnittstelle ETH1 austauschen.
Firewall Eth1 Established to TCP port 44818	Gestattet Antworten auf die von der Steuerung hergestellte Kommunikation mit dem TCP-Port 44818 (ETHIP) über die Schnittstelle ETH1. Die letzten 2 Befehle gestatten dem EtheNetIP-Scanner die Kommunikation mit den Industrial Ethernet-Geräten.
Eth2-Konfiguration	
Firewall Eth2 Default Reject	Weist alle Frames über die Schnittstelle ETH2 zurück. Diese Schnittstelle ist mit einem Netzwerk verbunden, das in erster Linie für die Inbetriebnahme genutzt wird.
Firewall Eth2 Allow TCP port 4840	Lässt den OPC UA-Server über die Schnittstelle ETH2 zu.
Firewall Eth2 Allow TCP port 443	Lässt den Webserver (HTTPS) über die Schnittstelle ETH2 zu.
Firewall Eth2 Allow TCP port 8089	Lässt die Webvisualisierung (HTTPS) über die Schnittstelle ETH2 zu.
Firewall Eth2 Allow TCP ports 20 to 21	Lässt FTP im aktiven Modus über die Schnittstelle ETH2 zu.
Firewall Eth2 Allow IP 192.168.1.1 on UDP ports 27126 to 27127	Ermöglicht es der IP des Inbetriebnahme-PC, die IP-Adresse der Steuerung zu ermitteln und zu konfigurieren. Dies sollte nur in einem vertrauenswürdigen Netzwerk gestattet sein, da die IP geändert werden kann, auch wenn die Benutzerrechte konfiguriert sind.

Befehle	Kommentare
Firewall Eth2 Allow IPs 192.168.1.1 to 192.168.1.2 on UDP port 1740	Ermöglicht es der IP des Inbetriebnahme-PC und einer HMI, mit der Steuerung über das Machine Expert-Protokoll zu kommunizieren.
Firewall Eth2 Allow TCP port 11740	Lässt Fast TCP über die Schnittstelle ETH2 zu. Dies ermöglicht es, eine Verbindung mit der Steuerung über TCP herzustellen.
Firewall Eth2 Allow TCP port 2222	Gestattet die implizite Kommunikation mit dem UDP-Port 2222 (ETHIP) über die Schnittstelle ETH2.
Firewall Eth2 Allow TCP port 44818	Gestattet die explizite Kommunikation mit dem TCP-Port 44818 (ETHIP) über die Schnittstelle ETH2. Die letzten beiden Befehle ermöglichen es, die Steuerung als EtherNetIP-Adapter zu verwenden.
Firewall Eth2 Allow MAC 4C:CC:6A:A1:09:C8	Lässt die MAC-Adresse der HMI zu.
Firewall Eth2 Allow MAC 00:0C:29:92:43:A8	Lässt die MAC-Adresse des Inbetriebnahme-PC zu. Nur zulässige MAC-Adressen können mit der Steuerung kommunizieren.
Eth3-Konfiguration TMSES4	
Firewall Eth3 Default Reject	Weist Frames über TMSES4 zurück. Diese Schnittstelle ist mit dem Werknetzwerk verbunden und kann auf das Internet zugreifen. Sie sollte als nicht vertrauenswürdig betrachtet werden.
Firewall Eth3 Established to TCP port 443	Lässt den https-Client (zum Beispiel zum Einrichten einer Verbindung zu Machine Advisor) über die Schnittstelle TMSES4 zu.
Firewall Eth3 Allow TCP port 11740	Lässt Fast TCP über die Schnittstelle TMSES4 zu. Dies ermöglicht es, eine Remoteverbindung mit der Steuerung herzustellen. Dies darf nicht zulässig sein, es sei denn, die Benutzerrechte sind auf der Steuerung aktiviert.

HINWEIS: Es sind maximal 200 Zeichen pro Zeile gestattet, einschließlich Kommentare.

Verwendete Ports

Protokoll	Zielpportnummern
Machine Expert	UDP 1740, 1741, 1742, 1743 TCP 11740
FTP	TCP 21, 20
HTTP ⁽¹⁾	TCP 80 ⁽¹⁾
HTTPS	TCP 443
Modbus	TCP 502
Machine Expert Discovery	UDP 27126, 27127
Web Services Dynamic Discovery	UDP 3702 TCP 5357
SNMP	UDP 161, 162
NVL	UDP-Standardwert: 1202
EtherNet/IP	UDP 2222 TCP 44818
Webvisualization	HTTP 8080 HTTPS 8089
TFTP	UDP 69 (nur für FDR-Server verwendet)
SafeLogger	UDP 35021, 45000
Maschine Assistant	UDP 45001 bis 45004
OPC UA	TCP 4840
DHCP	UDP 68
NTP	UDP 123
Discovery Service	UDP 5353
(1) HTTP-Requests an TCP-Port 80 werden zur Verwendung von HTTPS an Port 443 umgeleitet.	

TMSCO1 CANopen-Kommunikationsmodul

Einführung

In diesem Kapitel wird die Konfiguration des TMSCO1 CANopen-Kommunikationsmoduls beschrieben.

Konfiguration der CANopen-Schnittstelle

Einführung

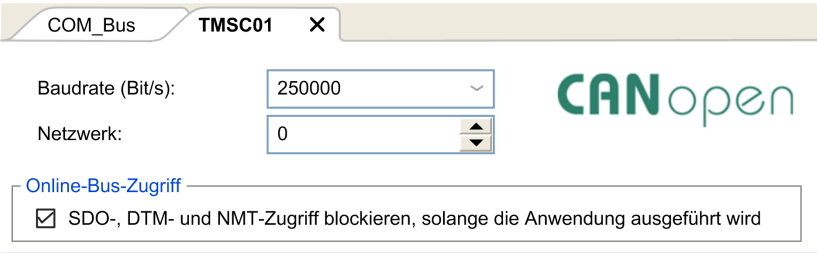
CANopen ist ein offenes Kommunikationsprotokoll nach Industriestandard und eine Geräteprofilspezifikation (EN 50325-4), die auf dem CAN-Protokoll (Controller Area Network) basiert. Das CAN-Protokoll (Schicht 7) wurde für integrierte Netzwerkanwendungen entwickelt und definiert Kommunikations- und Gerätefunktionen für CAN-basierte Systeme.

CANopen unterstützt sowohl die zyklische als auch die ereignisgesteuerte Kommunikation, was es Ihnen ermöglicht, die Buslast bei weiterhin kurzen Reaktionszeiten auf ein Minimum zu begrenzen.

Sie können die CANopen-Verbindungen über ein TMSCO1-Modul einrichten. Dieses Modul wird an den Kommunikationsbus (**COM_Bus**) auf der linken Seite der Steuerung über die linke Busanschlussschnittstelle angeschlossen. Sie können ein TMSCO1-Modul anschließen. Es muss sich um das letzte Modul auf der linken Seite der Steuerung handeln.

Konfigurieren des CAN-Busses

So konfigurieren Sie den **CAN**-Bus Ihrer Steuerung:

Schritt	Aktion
1	Fügen Sie ein TMSCO1 -Modul hinzu.
2	Doppelklicken Sie in der Gerätebaumstruktur , auf TMSCO1 .
3	Konfigurieren Sie die Baudrate (Standardwert: 250.000 bps): 

Wenn ein DTM über das Netzwerk mit einem Gerät verbunden wird, kommuniziert der DTM parallel zur laufenden Anwendung. Das beeinträchtigt die Gesamtleistung des Systems und kann zu einer Überlastung des Netzwerks führen, was wiederum eine Inkohärenz der Daten zwischen den gesteuerten Geräten zur Folge haben kann.

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEBETRIEB

Setzen Sie Ihre Maschine bzw. Ihren Prozess in einen Zustand, in dem die DTM-Kommunikation die Leistung nicht beeinträchtigt.

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

Hinzufügen eines CANopen-Leistungsmanagers

Durch das Hinzufügen eines **TMSCO1**-Moduls wird automatisch auch die **CANopen-Leistungsmanager**-Funktion zu der Steuerung hinzugefügt.

Konfigurieren eines CANopen-Leistungsmanagers

Zur Konfiguration von **CANopen Performance** doppelklicken Sie auf **COM_Bus > TMSCO1 > CANopen Performance** in der **Gerätebaumstruktur**.

Es wird das folgende Dialogfeld aufgerufen:

CANopen_Performance X

Allgemein | CANopen E/A Abbild | Informationen

Allgemein

Knoten-ID: 127 Konfiguration prüfen und korrigieren... **CANopen**

Autostart CANopenManager Abfragen optionaler Slaves

Slaves starten NMT Fehlerverhalten: [Dropdown]

NMT Start All (wenn möglich)

Nodeguarding

Heartbeat-Erzeugung aktivieren

Knoten-ID: 127

Producer Time (ms): 200

Synchronisieren

Sync-Erzeugung aktivieren

COB-ID (Hex): 16# 80

Cycle Period (µs): 50000

Fensterlänge (µs): 0

Sync-Verarbeitung aktivieren

TIME

TIME-Producing aktivieren

COB-ID (Hex): 16# 100

Producer Time (ms): 1000

Die Registerkarte **Allgemein** des **CANopen_Performance-** Konfigurationsfensters ist in vier Bereiche unterteilt:

- **Allgemein:** Allgemeine Informationen wie Knoten-ID und aktivierte Konfigurationsoptionen.
- **Guarding:** Wenn **Heartbeat-Erzeugung aktivieren** ausgewählt ist, ist Guarding aktiviert und der NMT-Master kann den Status einzelner Knoten überprüfen. Der Heartbeat-Mechanismus ermöglicht es dem Netzwerk-Master, einen Verbindungsverlust der Netzwerk-Slaves zu erkennen. Den Netzwerk-Slaves ermöglicht er, auf eine Trennung der Verbindung zum Master zu reagieren. Die Standardeinstellung ist eine Heartbeat-Erzeugung mit 200 ms.
- **Sync:** Wenn **Sync-Erzeugung aktivieren** ausgewählt ist, wird ein spezifisches Ereignisobjekt hinzugefügt. Die **TMSCO1_Sync**-Task wird dem Knoten **Anwendung > Taskkonfiguration** in der **Anwendungsbaumstruktur** hinzugefügt.

Wenn Sie die Auswahl der Option **Sync-Erzeugung aktivieren** in diesem Dialogfeld aufheben, wird die **TMSCO1_Sync**-Task automatisch in der **Anwendungsbaumstruktur** Ihres Programms gelöscht.

HINWEIS: Löschen oder ändern Sie keinesfalls die Attribute **Typ** und **Externes Ereignis** von **TMSCO1_Sync**-Tasks. Andernfalls erkennt EcoStruxure Machine Expert einen Fehler beim Generieren der Anwendung, und Sie können die Anwendung nicht in die Steuerung herunterladen.

- **TIME** Nicht bearbeitbar

CANopen-Betriebseinschränkungen

Für den CANopen-Master gelten folgende Betriebseinschränkungen:

Maximale Anzahl von Slavegeräten	63
Maximale Anzahl von Empfangs-PDO (RPDO)	252
Maximale Anzahl von Sende-PDO (TPDO)	252

⚠️ WARNUNG
<p>UNBEABSICHTIGTER GERÄTEBETRIEB</p> <ul style="list-style-type: none"> • Schließen Sie nicht mehr als 63 CANopen-Slavegeräte an die Steuerung an • Programmieren Sie Ihre Anwendung für eine Verwendung von maximal 252 Sende-PDO (TPDO). • Programmieren Sie Ihre Anwendung für eine Verwendung von maximal 252 Empfangs-PDO (RPDO). <p>Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.</p>

CAN-Busformat

Das CAN-Busformat ist CAN2.0A für CANopen.

Glossar

A

ARP:

(*Address Resolution Protocol: Adressauflösungsprotokoll*) IP-Protokoll der Netzwerkschicht für Ethernet, das eine IP-Adresse einer MAC-Adresse (Hardwareadresse) zuordnet.

B

BOOTP:

(*Bootstrap-Protokoll*) UDP-Netzwerkprotokoll, das von einem Netzwerk-Client verwendet werden kann, um automatisch eine IP-Adresse (und möglicherweise weitere Daten) von einem Server zu erhalten. Der Client identifiziert sich beim Server anhand der MAC-Adresse des Clients. Der Server, der eine vorkonfigurierte Tabelle der MAC-Adressen der Client-Geräte und der zugeordneten IP-Adressen speichert, sendet dem Client seine vorkonfigurierte IP-Adresse. BOOTP wurde ursprünglich zum dezentralen Booten von Hosts über ein Netzwerk verwendet, die über keinen eigenen Plattenspeicher verfügen. Der BOOTP-Prozess weist eine IP-Adresse mit unbegrenzter Laufzeit zu. Der BOOTP-Dienst nutzt die UDP-Ports 67 und 68.

C

CANopen:

Offenes Kommunikationsprotokoll nach Industriestandard und Geräteprofil-Spezifikation (EN 50325-4).

D

DHCP:

(*Dynamic Host Configuration Protocol*) Hochentwickelte Erweiterung von BOOTP. Das DHCP-Protokoll ist ausgereifter, doch sowohl DHCP als auch BOOTP sind gängig. (DHCP kann BOOTP-Client-Requests verarbeiten.)

DNS:

(*Domain Name System*) Namensgebungssystem für Computer und Geräte, die mit einem LAN oder mit dem Internet verbunden sind.

DTM:

(*device type manager*) In 2 Kategorien untergliedert:

- Geräte-DTMs (Device DTMs) werden mit den Komponenten in einer Feldgerätekongfiguration verbunden.
- Kommunikations-DTMs (CommDTMs) werden mit den Softwarekomponenten der Kommunikation verbunden.

Ein DTM stellt eine einheitliche Struktur für den Zugriff auf die Geräteparameter und die Konfiguration, den Betrieb und die Diagnose der Geräte bereit. Bei DTMs kann es sich um einfache grafische Benutzeroberflächen zur Einstellung der Geräteparameter bis hin zu hoch entwickelten Anwendungen handeln, die komplexe Echtzeitberechnungen zu Diagnose- und Wartungszwecken durchführen können.

E

EDS:

(*Electronic Data Sheet: Elektronisches Datenblatt*) Datei für die Beschreibung eines Feldbusgeräts, das beispielsweise die Eigenschaften des Geräts wie Parameter und Einstellungen enthält.

EtherNet/IP:

(Ethernet Industrial Protocol) Offenes Kommunikationsprotokoll für Fertigungsautomatisierungslösungen in industriellen Systemen. EtherNet/IP gehört zu einer Familie von Netzwerken, die CIP (Common Industrial Protocol) in den oberen Schichten implementieren. Die unterstützende Organisation (ODVA) gibt EtherNet/IP für globale Anpassungsfähigkeit und Medienunabhängigkeit vor.

Ethernet:

Technologie der physikalischen und der Datenverbindungsschicht für LANs, auch als IEEE 802.3 bekannt.

I**ICMP:**

(Internet Control Message Protocol) Signalisiert Fehler und stellt Informationen zur Datagramm-Verarbeitung bereit.

IGMP:

(Internet Group Management Protocol) Kommunikationsprotokoll, das von Hosts und benachbarten Routern in IPv4-Netzwerken zur Organisation von Mitgliedschaften in Multicast-Gruppen verwendet wird.

IP:

(Internet Protocol: Internetprotokoll) Teil der TCP/IP-Protokollfamilie, der die Internetadresse von Geräten verfolgt, das Routing für abgehende Nachrichten übernimmt und eingehende Nachrichten erkennt.

M**MAC-Adresse:**

(Media Access Control) Eindeutige 48-Bit-Zahl, die einer bestimmten Hardwarekomponente zugeordnet ist. Die MAC-Adresse wird bei der Fertigung in jede Netzwerkkarte bzw. jedes Gerät programmiert.

MSB:

(Most Significant Bit/Byte: Höherwertiges Byte) Teil einer Zahl, einer Adresse oder eines Felds, das als Einzelwert ganz links im herkömmlichen Hexadezimal- oder Binärformat geschrieben wird.

N**NMT:**

(Network Management: Netzwerkmanagement) CANopen-Protokolle, die Dienste für die Netzwerkinitialisierung, die Fehlerüberwachung sowie die Überwachung des Gerätestatus bereitstellen.

P**PDO:**

(Process Data Object: Prozessdatenobjekt) Wird in CAN-basierenden Netzwerken als nicht bestätigte Broadcast-Meldung übertragen oder von einem Erzeugergerät (Producer) an ein Verbrauchergerät (Consumer) gesendet. Das Sende-PDO vom Producer-Gerät hat eine spezifische Kennung, die dem Empfangs-PDO der Consumer-Geräte entspricht.

Protokoll:

Konvention oder Standarddefinition, die die Verbindung, Kommunikation und Datenübertragung zwischen 2 Rechensystemen und Geräten steuert und ermöglicht.

R

RPI:

(*Requested Packet Interval*) Der Zeitraum zwischen den vom Scanner angeforderten zyklischen Datenaustauschvorgängen. EtherNet/IP-Geräte veröffentlichen Daten mit der Rate, die durch das RPI vorgegeben wird, das ihnen vom Scanner zugewiesen wurde, und sie empfangen Nachrichtenrequests vom Scanner bei jedem RPI.

RSTP:

(*Rapid Spanning Tree Protocol*) Hochgeschwindigkeitsnetzwerkprotokoll, das eine schleifenfreie logische Topologie für Ethernet-Netzwerke einrichtet.

S

SDO:

(*Service Data Object: Dienstdatenobjekt*) Meldung, die vom Feldbus-Master verwendet wird, um (lesend/schreibend) auf die Objektverzeichnisse von Netzwerkknoten in CAN-basierten Netzwerken zuzugreifen. Zu SDO-Typen gehören Service SDOs (SSDOs) und Client SDOs (CSDOs).

Steuerungsnetzwerk:

Ein Netzwerk mit Logic Controllern, SCADA-Systemen, PCs, HMI, Switches usw.

Es werden zwei Arten von Topologien unterstützt:

- Flach: Alle Module und Geräte in diesem Netzwerk gehören demselben Teilnetz an.
- 2-stufig: Das Netzwerk ist in ein Betriebsnetzwerk und ein Steuerungsnetzwerk unterteilt.

Diese beiden Netzwerke sind zwar physisch voneinander unabhängig, in der Regel jedoch über ein Routing-Gerät miteinander verbunden.

T

TCP:

(*Transmission Control Protocol*) Verbindungsbasiertes Protokoll der Transportschicht, das die zuverlässige, simultane und bidirektionale Übertragung von Daten unterstützt. TCP ist Teil der TCP/IP-Protokollreihe.

TPDO:

(*Transmit Process Data Object: Sende-Prozessdatenobjekt*) Wird in CAN-basierenden Netzwerken als nicht bestätigte Broadcast-Meldung übertragen oder von einem Erzeugergerät (Producer) an ein Verbrauchergerät (Consumer) gesendet. Das Sende-PDO vom Producer-Gerät hat eine spezifische Kennung, die dem Empfangs-PDO der Consumer-Geräte entspricht.

U

UDP:

(*User Datagram Protocol*) Protokoll für den verbindungslosen Modus (nach IETF RFC 768), bei dem Nachrichten in einem Datagramm (Datentelegramm) an einen Zielcomputer in einem IP-Netzwerk gesendet werden. Das UDP-Protokoll ist normalerweise mit dem Internet Protocol (IP) gebündelt. UDP/IP-Nachrichten erwarten keine Antwort und sind deshalb ideal für Anwendungen, in denen verlorene Pakete keine Neuübertragung erfordern (z.B. Streaming-Video und Netzwerke, die Echtzeitverhalten verlangen).

Index

E

Erweiterungsmodule	
Hinzufügen	12
Konfiguration	13
Ethernet	
Dienste	14
Modbus TCP-Slavegerät	21
EtherNet	
EtherNet/IP-Gerät	20

F

Firewall	
Konfiguration	28
Skriptbefehle	29
Standardskriptdatei	28

P

Protokolle	14
IP	16

S

Skriptbefehle	
Firewall	29

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

Da Normen, Spezifikationen und Bauweisen sich von Zeit zu Zeit ändern, ist es unerlässlich, dass Sie die in dieser Veröffentlichung gegebenen Informationen von uns bestätigen.

© 2023 Schneider Electric. Alle Rechte vorbehalten.

EIO0000003693.04