

HANDBUCH

ICDM-RX

Installation und Konfiguration der Hardware

EtherNet/IP (EN)

Ethernet/IP zu Modbus (EN1)

Modbus (MOD)

PROFINET IO (PN)

PROFINET IO zu Modbus (ON1)





Bezüglich der Lieferung von Produkten ist die aktuelle Ausgabe des folgenden Dokuments maßgeblich: Die Allgemeinen Lieferbedingungen für Produkte und Dienstleistungen der Elektroindustrie, veröffentlicht durch den Zentralverband der Elektrotechnik und Elektroindustrie (ZVEI) e.V. einschließlich der Ergänzungsklausel: „Erweiterter Eigentumsvorbehalt“.



Inhaltsverzeichnis

Inhaltsverzeichnis	3
1. Erste Schritte	6
1.1. Konventionen in diesem Handbuch	6
1.2. Installationsübersicht	7
1.3. Nur ICDM-RX/MOD-Modelle	7
1.4. Auffinden von Software und Dokumentation	7
2. Installation der Hardware	8
2.1. ICDM-RX/xxx-DB9/RJ45-PM Installation	8
2.2. Installation des ICDM-RX/xxx-ST/RJ45-DIN	10
2.3. Installation des ICDM-RX/xxx-DB9/RJ45-DIN	12
2.4. Installation des ICDM-RX/xxx-2ST/RJ45-DIN	14
2.5. Installation des ICDM-RX/xxx-2DB9RJ45-DIN	16
2.6. Installation des ICDM-RX/xxx-4DB9/2RJ45-DIN	18
2.7. Hinzufügen einer Einheit zu einer vorhandenen Installation	19
2.8. Austauschen der Hardware	20
3. Vorbereiten des ICDM-RX für die Konfiguration	21
3.1. Übersicht über PortVision DX	21
3.2. PortVision DX-Anforderungen	21
3.3. Installation von PortVision DX	22
3.4. Konfigurieren der Netzwerkeinstellungen	25
3.5. Überprüfen der Protokoll-Firmwareversion	29
3.6. Hochladen der Firmware auf den ICDM-RX ICDM-RX	30
4. ICDM-RX Sicherheit	32
4.1. Sicherheitsmethoden und Terminologie	32
4.2. Vom ICDM-RX verwendete TCP- und UDP-Socket-Ports	37
4.3. ICDM-RX-Sicherheitsfunktionen	38
4.3.1. Secure Config Mode	38
4.3.2. Sicherheitsvergleich	38
4.3.3. SSH-Server	39
4.3.4. SSL-Übersicht	39
4.3.5. SSL-Authentifizierung	39
4.3.5.1. Server-Authentifizierung	39
4.3.5.2. Client-Authentifizierung	40
4.3.5.3. Zertifikate und Schlüssel	40
4.3.6. SSL-Leistung	41
4.3.7. SSL-Chiffrensammlungen	42
4.3.8. Vom ICDM-RX unterstützte Chiffrensammlungen	43
4.3.8.1. SSL-Ressourcen	43
4.4. Konfigurieren/Aktivieren der Sicherheitsfunktionen – Übersicht	44
4.4.1. Schlüssel- und Zertifikatsverwaltung	45
4.5. Verwendung eines Webbrowsers zum Festlegen von Sicherheitsfunktionen	47

4.5.1. Ändern der Sicherheitskonfiguration	47
4.5.2. Ändern von Schlüsseln und Zertifikaten	48
4.6. Kennwortauthentifizierung	49
4.6.1. Über die Webseite	49
4.6.2. Über Telnet oder SSH	49
4.6.2.1. Anmeldeauthentifizierung.....	49
4.6.2.2. Konfigurieren von Passwörtern.....	52
4.6.2.3. Telnet-Befehle	54
4.6.3. Webseitenkennwort-Zugriff	55
5. Anschließen von seriellen Geräten	56
5.1. DB9-Steckverbinder.....	57
5.1.1. DB9-Nullmodemkabel (RS-232).....	58
5.1.2. DB9-Nullmodemkabel (RS-422).....	58
5.1.3. Nicht gekreuzte DB9-Netzwerkkabel (RS-232/485)	58
5.1.4. DB9-Loopback-Stecker	59
5.1.5. Anschließen von seriellen DB9-Geräten.....	59
5.2. RJ45-Steckverbinder	60
5.2.1. RJ45-Nullmodemkabel (RS-232)	60
5.2.2. RJ45-Nullmodemkabel (RS-422)	61
5.2.3. Nicht gekreuzte RJ45-Netzwerkkabel (RS-232/485).....	61
5.2.4. RJ45-Loopback-Stecker	61
5.2.5. RJ45-RS-485-Testkabel.....	61
5.2.6. Anschließen von RJ45-Geräten	62
5.3. Vier Schraubklemmen (ICDM-RX/xxx-2ST/RJ45-DIN)	63
5.3.1. Serielle 4-fach-Anschlussklemme für Steckverbinder.....	63
5.3.2. Serielle 4-fach-Anschlussklemme für Nullmodemkabel (RS-232)	64
5.3.3. Serielle 4-fach-Anschlussklemme für Nullmodemkabel (RS-422)	64
5.3.4. Serielle 4-fach-Anschlussklemme für nicht gekreuzte Kabel (RS-232/485).....	65
5.3.5. Serielle 4-fach-Anschlussklemme für Loopback-Signale	65
5.3.6. Anschließen von seriellen Geräten.....	65
5.4. Neun Schraubklemmen (ICDM-RX/xxx-ST/RJ45-DIN).....	66
5.4.1. 9-fach-Schraubklemmen	66
5.4.2. 9-fach-Schraubklemme für RS-232-Nullmodemkabel	67
5.4.3. 9-fach-Schraubklemme für RS-422-Nullmodemkabel	67
5.4.4. 9-fach-Schraubklemme für nicht gekreuzte RS-232/485-Kabel.....	68
5.4.5. 9-fach-Schraubklemme für Loopback-Signale	68
5.4.6. Anschließen von seriellen Geräten.....	68
6. Verwalten des ICDM-RX.....	69
6.1. Neustarten des ICDM-RX.....	69
6.2. Hochladen der Firmware auf mehrere ICDM-RX-Einheiten	70
6.3. Konfigurieren mehrerer ICDM-RX-Netzwerkadressen	71
6.4. Neues Gerät in PortVision DX hinzufügen.....	71
6.4.1. Remote-Einheit mit IP-Adresse	71
6.4.2. Lokale Einheit mit IP-Adresse oder MAC-Adresse	72
6.5. Ändern der Bootloader-Zeitüberschreitung.....	73
6.6. Verwenden von Konfigurationsdateien	74
6.6.1. Speichern von Konfigurationsdateien.....	74
6.6.2. Laden von Konfigurationsdateien.....	75
6.7. Verwalten des Bootloaders.....	75
6.7.1. Überprüfen der Bootloader-Version	76



6.7.2. Hochladen des Bootloaders	77
6.8. Wiederherstellen der Werkseinstellungen (spezifische Modelle – Reset-Schaltfläche)	78
6.9. Wiederherstellen der Standardwerte	80
6.10. Zugreifen auf RedBoot-Befehle in Telnet-/SSH-Sitzungen (PortVision DX)	81
7. RedBoot-Verfahren	85
7.1. Zugreifen auf die RedBoot-Übersicht	85
7.2. Einrichten einer seriellen Verbindung	86
7.3. Einrichten einer Telnet-Verbindung	87
7.4. Festlegen der Netzwerkeinstellungen	88
7.5. Konfigurieren der Netzwerkeinstellungen.....	88
7.6. Ändern der Bootloader-Zeitüberschreitung.....	89
7.7. Ermitteln der Bootloader-Version	89
7.8. Zurücksetzen des ICDM-RX	90
7.9. Konfigurieren von Passwörtern.....	90
7.10. RedBoot-Befehlsübersicht.....	91
8. Spezifikationen des externen Netzteils	94
8.1. ICDM-RX/xxx-DB9/RJ45-PM Netzteil	94
8.2. ICDM-RX/xxx-DB9/RJ45-DIN oder ICDM-RX/xxx-ST/RJ45-DIN Netzteil.....	95
8.3. ICDM-RX/xxx-2ST/RJ45-DIN Netzteil.....	96
8.4. ICDM-RX/xxx-2DB9RJ45-DIN Netzteil	97
8.5. ICDM-RX/xxx-4DB9/2RJ45-DIN Netzteil	98
9. Fehlerbehandlung und technischer Support	99
9.1. Checkliste zur Fehlerbehandlung	99
9.2. Allgemeine Fehlerbehandlung.....	100
9.3. Verkettung des ICDM-RX mit zwei Ethernet-Ports.....	101
9.4. ICDM-RX LEDs	102

1. Erste Schritte

In diesem Handbuch werden die Erstinstallation des ICDM-RX Industrial Gateway und die Hardwarekonfiguration für die folgenden Plattform für industrielle Protokolle erläutert.

- EtherNET/IP (Typenschlüssel, die mit ICDM-RX/EN beginnen)
- Ethernet/IP zu Modbus (Typenschlüssel, die mit ICDM-RX/EN1 beginnen)
- Modbus-Gateways (Typenschlüssel, die mit ICDM-RX/MOD beginnen)
- PROFINET IO (Typenschlüssel, die mit ICDM-RX/PN beginnen)
- PROFINET IO zu Modbus (Typenschlüssel, die mit ICDM-RX/PN1 beginnen)

1.1. Konventionen in diesem Handbuch

In diesem Handbuch werden die Produkte als ICDM-RX/xxx bezeichnet, wobei xxx in der folgenden Tabelle definiert ist.

Physische Beschreibung	Modell	Modellname im Handbuch
1-Port, serieller DB9-Port, Hutschienenmontage	ICDM-RX/EN-DB9/RJ45-DIN ICDM-RX/EN1-DB9/RJ45-DIN ICDM-RX/MOD-DB9/RJ45-DIN ICDM-RX/PN-DB9/RJ45-DIN ICDM-RX/PN1-DB9/RJ45-DIN	ICDM-RX/xxx-DB9/RJ45-DIN
1-Port, serieller DB9-Port, Schalttafeleinbau	ICDM-RX/EN-DB9/RJ45-PM ICDM-RX/EN1-DB9/RJ45-PM ICDM-RX/MOD-DB9/RJ45-PM ICDM-RX/PN-DB9/RJ45-PM ICDM-RX/PN1-DB9/RJ45-PM	ICDM-RX/xxx-DB9/RJ45-PM
1-Port, Schraubklemme serieller Port, Hutschienenmontage	ICDM-RX/EN-ST/RJ45-DIN ICDM-RX/EN1-ST/RJ45-DIN ICDM-RX/MOD-ST/RJ45-DIN ICDM-RX/PN-ST/RJ45-DIN ICDM-RX/PN1-ST/RJ45-DIN	ICDM-RX/xxx-ST/RJ45-DIN
2-Port, serielle DB9-Ports, Hutschienenmontage	ICDM-RX/EN-2DB9/RJ45-DIN ICDM-RX/EN1-2DB9/RJ45-DIN ICDM-RX/MOD-2DB9/RJ45-DIN ICDM-RX/PN-2DB9/RJ45-DIN ICDM-RX/PN1-2DB9/RJ45-DIN	ICDM-RX/xxx-2DB9RJ45-DIN

Physische Beschreibung	Modell	Modellname im Handbuch
2-Port, Schraubklemme serielle Ports, Hutschienenmontage	ICDM-RX/EN-2ST/RJ45-DIN	ICDM-RX/ xxx -2ST/RJ45-DIN
	ICDM-RX/EN1-2ST/RJ45-DIN	
	ICDM-RX/MOD-2ST/RJ45-DIN	
	ICDM-RX/PN-2ST/RJ45-DIN	
	ICDM-RX/PN1-2ST/RJ45-DIN	
4-Port, serielle DB9-Ports, Hutschienenmontage	ICDM-RX/EN-4DB9/2RJ45-DIN	ICDM-RX/ xxx -4DB9/2RJ45-DIN
	ICDM-RX/EN1-4DB9/2RJ45-DIN	
	ICDM-RX/MOD-4DB9/2RJ45-DIN	
	ICDM-RX/PN-4DB9/2RJ45-DIN	
	ICDM-RX/PN1-4DB9/2RJ45-DIN	

1.2. Installationsübersicht

Bei der Installation und Konfiguration werden die folgenden Schritte ausgeführt.

1. Schließen Sie die Hardware an (Seite 8).
2. Installieren Sie PortVision DX (Seite 22).
3. Konfigurieren Sie die ICDM-RX-Netzwerkeinstellungen (Seite 25).
4. Aktualisieren Sie ggf. die Firmware auf dem ICDM-RX (Seite 30).
5. Suchen Sie unter <https://www.pepperl-fuchs.com> nach Ihrem Produkt, um das Protokollhandbuch für Ihre Plattform zu finden, damit Sie die folgenden Verfahren durchführen können:
 - Konfigurieren der Porteigenschaften über die entsprechende Webschnittstellenseite.
 - Programmieren der SPS.
6. Schließen Sie das serielle Gerät bzw. die seriellen Geräte an (Seite 56).

1.3. Nur ICDM-RX/MOD-Modelle

Standardmäßig werden ICDM-RX/MOD-Modelle mit Modbus-Router geladen. Wenn Sie die Modbus-Server- oder Modbus TCP-Plattform implementieren möchten, müssen Sie die entsprechende Firmware unter <https://www.pepperl-fuchs.com> herunterladen.

Informationen zum Laden der entsprechenden Firmware finden Sie im Abschnitt *Hochladen der Firmware auf den ICDM-RX ICDM-RX* auf Seite 30.

1.4. Auffinden von Software und Dokumentation

Sie können die neueste Firmware-Assembly, PortVision DX, und die ICDM-RX-Dokumentation auf folgender Website herunterladen: <https://www.pepperl-fuchs.com>.

Note: Überprüfen Sie Ihre Firmwareversion mit PortVision DX oder der Startseite der Webschnittstelle und vergleichen Sie sie dann mit der Firmwareversion auf der Website. Wenn keine Firmwareversion verfügbar ist, bedeutet dies, dass die neueste Version auf dem Gerät geladen ist.

2. Installation der Hardware

In diesem Kapitel werden folgende Themen behandelt:

- **ICDM-RX/xxx-DB9/RJ45-PM Installation**
- *Installation des ICDM-RX/xxx-ST/RJ45-DIN* auf Seite 10
- *Installation des ICDM-RX/xxx-DB9/RJ45-DIN* auf Seite 12
- *Installation des ICDM-RX/xxx-2ST/RJ45-DIN* auf Seite 14
- *Installation des ICDM-RX/xxx-2DB9RJ45-DIN* auf Seite 16
- *Installation des ICDM-RX/xxx-4DB9/2RJ45-DIN* auf Seite 18
- *Hinzufügen einer Einheit zu einer vorhandenen Installation* auf Seite 19
- *Austauschen der Hardware* auf Seite 20

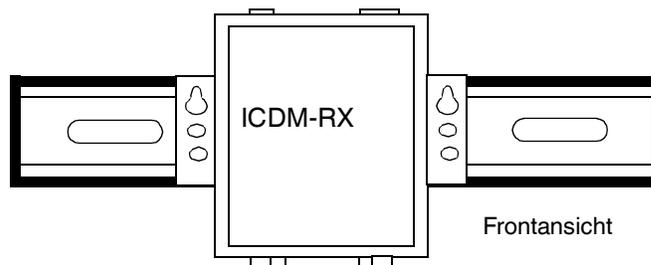
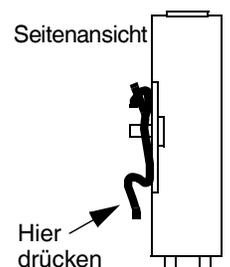
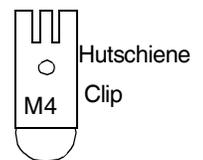
2.1. ICDM-RX/xxx-DB9/RJ45-PM Installation

Gehen Sie wie folgt vor, um den ICDM-RX/xxx-DB9/RJ45-PM zu installieren.

1. Stellen Sie den ICDM-RX/xxx-DB9/RJ45-PM auf eine stabile Oberfläche, und fahren Sie mit Schritt 2 fort, oder montieren Sie optional den ICDM-RX/xxx-DB9/RJ45-PM mit den Montageflanschen oder Hutschiennenadaptern.
 - a. Nehmen Sie den ICDM-RX/xxx-DB9/RJ45-PM so auf, dass die Vorderseite des Geräts zu Ihnen zeigt.
 - b. Nehmen Sie einen Hutschiennenclip auf. (Die drei Zinken müssen oben sein, und das **M4**-Etikett muss Ihnen entgegengerichtet sein.)
 - c. Schieben Sie den Hutschiennenclip hinter den ICDM-RX/xxx-DB9/RJ45-PM, und richten Sie ihn an einer der Schraubenöffnungen am ICDM-RX/xxx-DB9/RJ45-PM aus.
 - d. Setzen Sie die **M4**-Schraube in das Loch ein, und ziehen Sie sie mit einem Kreuzschlitzschraubendreher fest.
 - e. Wiederholen Sie die Schritte b bis d mit dem zweiten Hutschiennenclip. Stellen Sie sicher, dass die Schrauben an beiden Hutschiennenclips ausgerichtet sind.

Note: Wenn Sie den ICDM-RX/xxx-DB9/RJ45-PM von der Hutschiene entfernen müssen, drücken Sie auf die Rückseite der Laschen an der Unterseite der beiden Hutschiennenclips.

 - f. Befestigen Sie den ICDM-RX/xxx-DB9/RJ45-PM an der Hutschiene.



Note: Schließen Sie mehrere Einheiten erst an, nachdem Sie die Standard-IP-Adresse geändert haben, siehe Vorbereiten des ICDM-RX für die Konfiguration auf Seite 21.

2. Verbinden Sie den Port mit der Beschriftung **10/100 ETHERNET** am ICDM-RX/xxx-DB9/RJ45-PM über ein Standardnetzwerkkabel mit demselben Ethernet-Netzwerksegment wie den PLC.

3/26/20

3. Schließen Sie den ICDM-RX/xxx-DB9/RJ45-PM wie folgt an die Stromversorgung an.

Note: Siehe ICDM-RX/xxx-DB9/RJ45-PM Netzteil auf Seite 94, wenn Sie Ihr eigenes Netzteil verwenden möchten.

Achten Sie beim Anschließen und Trennen des ICDM-RX/xxx-DB9/RJ45-PM auf die richtigen ESD-Maßnahmen.

- Setzen Sie den Masseleiter in die Masseschraubklemme ein.
- Stecken Sie den DC-Hinleiter in die Plus-Schraubklemme und den DC-Rückleiter in die Minus-Schraubklemme.

Ausführliche Informationen zu den Anforderungen an die Stromversorgung finden Sie unter ICDM-RX/xxx-DB9/RJ45-PM Netzteil auf Seite 94.

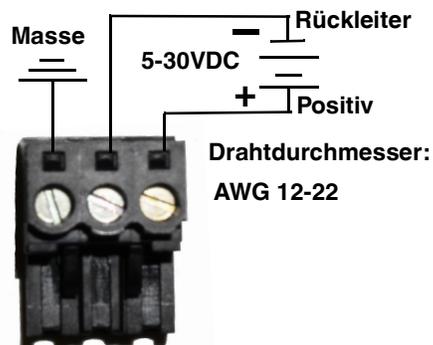
- Verwenden Sie eine kleine Schlitzschraube, um die Drähte zu fixieren.
- Überprüfen Sie, ob alle Kabel fest angezogen sind.
- Stecken Sie den Schraubklemmen-Stromanschluss in den ICDM-RX/xxx-DB9/RJ45-PM.

Note: Richten Sie den Stecker richtig aus. Die gewellte Seite des Schraubklemmen-Netzsteckers muss auf die gewellte Seite der Strombuchse am Gerät ausgerichtet sein.

- Verbinden Sie das Netzteil mit einer Stromquelle.

4. Überprüfen Sie anhand der folgenden Tabelle, ob die **Status**-LED den Startvorgang abgeschlossen hat und die Netzwerkverbindung für den ICDM-RX/xxx-DB9/RJ45-PM ordnungsgemäß funktioniert.

ICDM-RX/MOD



ICDM-RX/xxx-DB9/RJ45-PM Beschreibung der LEDs	
Zustand	Die orangefarbene Status -LED am Gerät leuchtet, wenn das Gerät eingeschaltet ist und den Startvorgang abgeschlossen hat. Die Status -LED blinkt während des Startvorgangs. Es dauert ca. 15 Sekunden, bis der Bootloader den Zyklus abgeschlossen hat. Wenn der Bootloader den Zyklus abgeschlossen hat, leuchtet die LED durchgehend und blinkt nur etwa alle 10 Sekunden. Bei PN- oder PN1-Modell: Wenn der Bootloader den Zyklus beendet, blinkt die LED mehrmals schnell, erlischt dann, und blinkt ca. alle 10 Sekunden, wenn keine SPS-Verbindung besteht.
Link/Act	Wenn die rote Link/Act -LED leuchtet, weist dies auf eine funktionierende Ethernet-Verbindung hin.
Duplex	Wenn die rote Duplex -LED leuchtet, weist dies auf Vollduplex-Aktivität hin.
100	Wenn die rote 100 -LED leuchtet, weist dies auf eine funktionierende 100-MB-Ethernet-Verbindung hin (nur 100-MB-Netzwerk). Wenn die LED nicht leuchtet, weist dies auf eine 10-MB-Ethernet-Verbindung hin.
Note: Weitere Informationen zu den LEDs finden Sie in der Status-LED-Tabelle auf Seite 99.	



Schließen Sie RS-422/485-Geräte erst an, wenn die IP-Adresse und ein geeigneter Schnittstellentyp konfiguriert wurden. Die Standardeinstellung für den Port ist RS-232.

3/26/20

- Im Abschnitt *Vorbereiten des ICDM-RX für die Konfiguration* auf Seite 21 finden Sie Informationen zur Installation des PortVision DX, zur Konfiguration der Netzwerkeinstellungen, und bei Bedarf zum Hochladen der entsprechenden Protokollfirmware auf den ICDM-RX/xxx-DB9/RJ45-PM.

2.2. Installation des ICDM-RX/xxx-ST/RJ45-DIN

Gehen Sie wie folgt vor, um den ICDM-RX/xxx-ST/RJ45-DIN zu installieren. Prüfen Sie gemäß *Installation des ICDM-RX/xxx-DB9/RJ45-DIN* auf Seite 12, ob der ICDM-RX über serielle DB9-Anschlüsse verfügt.

- Befestigen Sie den ICDM-RX/xxx-ST/RJ45-DIN 1-Port am Hutschienenadapter.
- Schließen Sie das Netzteil an, und schließen Sie den ICDM-RX/xxx-ST/RJ45-DIN mithilfe der Netzteilspezifikationen auf dem Produktetikett und den folgenden Informationen an die Stromversorgung an.



Achten Sie beim Anschließen und Trennen des ICDM-RX/xxx-ST/RJ45-DIN auf die richtigen ESD-Maßnahmen.

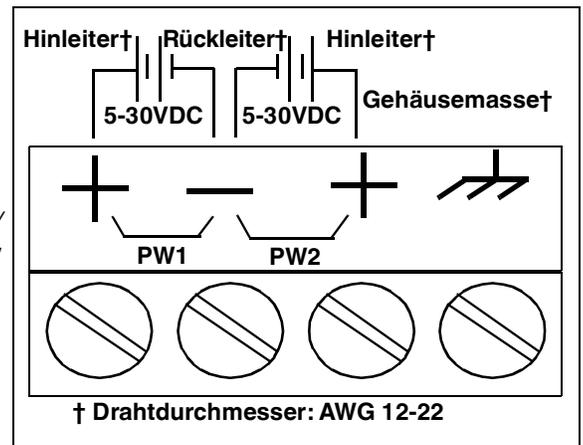
- Wenn die Hutschiene nicht mit Masse verbunden ist, führen Sie die Masseleitung in die Masseschraubklemme des Gehäuses ein.

Note: Der Masseanschluss des Gehäuses wird nur dann hergestellt, wenn die Hutschiene NICHT mit Masse verbunden ist.

- Stecken Sie den DC-Hinleiter in die Plus-Schraubklemme und den DC-Rückleiter in die Minus-Schraubklemme.

Ausführliche Informationen zu den Anforderungen an die Stromversorgung finden Sie unter *ICDM-RX/xxx-DB9/RJ45-DIN oder ICDM-RX/xxx-ST/RJ45-DIN Netzteil* auf Seite 95.

- Verwenden Sie einen kleinen Schlitzschraubendreher, um die Drähte zu fixieren.
- Überprüfen Sie, ob alle Kabel fest angezogen sind.
- Schließen Sie ein UL-zugelassenes Netzteil und ein UL-zugelassenes Netzkabel an eine Stromquelle an, um Strom anzulegen.



Note: Schließen Sie mehrere Einheiten erst an, nachdem Sie die Standard-IP-Adresse geändert haben, siehe *Vorbereiten des ICDM-RX für die Konfiguration* auf Seite 21.

- Verbinden Sie den **10/100-Port** über ein Standardnetzkabel mit demselben Ethernet-Netzwerksegment wie den Host-PC.

4. Überprüfen Sie anhand der folgenden Tabelle, ob die **STATUS**-LED den Startvorgang abgeschlossen hat und die Netzwerkverbindung für den ICDM-RX/xxx-ST/RJ45-DIN funktioniert.

ICDM-RX/xxx-ST/RJ45-DIN Beschreibung der LEDs	
STATUS	<p>Die STATUS-LED am Gerät leuchtet, wenn das Gerät eingeschaltet ist und den Startvorgang abgeschlossen hat.</p> <p>Die Status-LED blinkt während des Startvorgangs. Es dauert ca. 15 Sekunden, bis der Bootloader den Zyklus abgeschlossen hat. Wenn der Bootloader den Zyklus abgeschlossen hat, leuchtet die LED durchgehend und blinkt nur etwa alle 10 Sekunden.</p> <p>Bei PN- oder PN1-Modell:</p> <p>Wenn der Bootloader den Zyklus beendet, blinkt die LED mehrmals schnell, erlischt dann, und blinkt ca. alle 10 Sekunden, wenn keine SPS-Verbindung besteht.</p>
LINK	Wenn die LED LINK (grün) leuchtet, weist dies auf eine funktionierende Ethernet-Verbindung hin.
ACT	Wenn die LED ACT (gelb) blinkt, weist dies auf Netzwerkaktivität hin.
Note: Weitere Informationen zu den LEDs finden Sie in der Status-LED-Tabelle auf Seite 99.	



Schließen Sie RS-422/485-Geräte erst an, wenn die IP-Adresse und ein geeigneter Schnittstellentyp konfiguriert wurden. Die Standardeinstellung für den Port ist RS-232.

5. Unter *Vorbereiten des ICDM-RX für die Konfiguration* auf Seite 21 finden Sie die Standard-Netzwerkeinstellungen und Informationen zur Konfigurierung des ICDM-RX für den Einsatz.

2.3. Installation des ICDM-RX/xxx-DB9/RJ45-DIN

Gehen Sie wie folgt vor, um den ICDM-RX/xxx-DB9/RJ45-DIN zu installieren.

1. Befestigen Sie den ICDM-RX/xxx-DB9/RJ45-DIN am Hutschienenadapter.
2. Schließen Sie das Netzteil an, und schließen Sie den ICDM-RX/xxx-DB9/RJ45-DIN mithilfe der Netzteilspezifikationen auf dem Produktetikett und den folgenden Informationen an die Stromversorgung an.

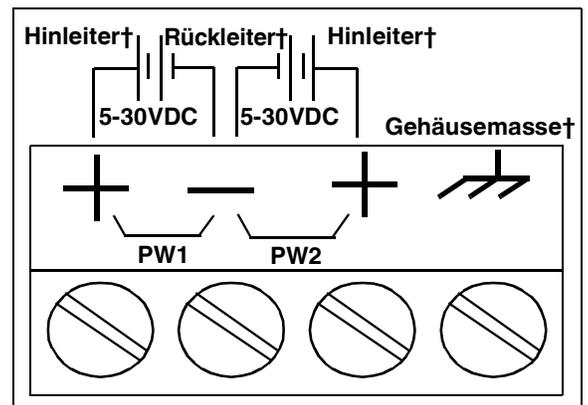


Achten Sie beim Anschließen und Trennen des ICDM-RX/xxx-DB9/RJ45-DIN auf die richtigen ESD-Maßnahmen.

- a. Wenn die Hutschiene nicht mit Masse verbunden ist, führen Sie die Masseleitung in die Masseschraubklemme des Gehäuses ein.

Note: Der Masseanschluss des Gehäuses wird nur dann hergestellt, wenn die Hutschiene NICHT mit Masse verbunden ist.

- b. Stecken Sie den DC-Hinleiter in eine der Plus-Schraubklemmen und den DC-Rückleiter in die Minus-Schraubklemme.
 - Ein zweites redundantes Netzteil kann an das Gerät angeschlossen werden, indem der DC-Hinleiter in die andere Plus-Schraubklemme und der DC-Rückleiter in die Minus-Schraubklemme eingeführt wird.
 - Der ICDM-RX/xxx-DB9/RJ45-DIN arbeitet weiter, wenn eines der beiden angeschlossenen Netzteile ausfällt.



† Drahtdurchmesser: AWG 12-22

Ausführliche Informationen zu den Anforderungen an die Stromversorgung finden Sie unter **ICDM-RX/xxx-DB9/RJ45-DIN oder ICDM-RX/xxx-ST/RJ45-DIN Netzteil** auf Seite 95.

- c. Verwenden Sie einen kleinen Schlitzschraubendreher, um die Drähte zu fixieren.
- d. Überprüfen Sie, ob alle Kabel fest angezogen sind.
- e. Schließen Sie ein UL-zugelassenes Netzteil und ein UL-zugelassenes Netzkabel an eine Stromquelle an, um Strom anzulegen.

Note: Schließen Sie mehrere Einheiten erst an, nachdem Sie die Standard-IP-Adresse geändert haben, siehe *Vorbereiten des ICDM-RX für die Konfiguration* auf Seite 21.

3. Verbinden Sie den Port **10/100** über ein Standard-Ethernet-Kabel mit demselben Ethernet-Netzwerksegment wie den Host-PC.

4. Überprüfen Sie anhand der folgenden Tabelle, ob die **STATUS**-LED den Startvorgang abgeschlossen hat und die Netzwerkverbindung für den ICDM-RX/xxx-DB9/RJ45-DIN ordnungsgemäß funktioniert.

ICDM-RX/xxx-DB9/RJ45-DIN Beschreibung der LEDs	
STATUS	<p>Die STATUS-LED leuchtet, wenn Sie das Gerät eingeschaltet haben und der Startvorgang abgeschlossen ist.</p> <p>Die STATUS-LED blinkt während des Startvorgangs. Es dauert ca. 15 Sekunden, bis der Bootloader den Zyklus abgeschlossen hat. Wenn der Bootloader den Zyklus abgeschlossen hat, leuchtet die LED durchgehend und blinkt nur etwa alle 10 Sekunden.</p> <p>Bei PN- oder PN1-Modell:</p> <p>Wenn der Bootloader den Zyklus beendet, blinkt die LED mehrmals schnell, erlischt dann, und blinkt ca. alle 10 Sekunden, wenn keine SPS-Verbindung besteht.</p>
LINK	Wenn die LED LINK (grün) leuchtet, weist dies auf eine funktionierende Ethernet-Verbindung hin.
ACT	Wenn die LED ACT (gelb) blinkt, weist dies auf Netzwerkaktivität hin.
Note: Weitere Informationen zu den LEDs finden Sie in der Status-LED-Tabelle auf Seite 99.	



Schließen Sie RS-422/485-Geräte erst an, wenn die IP-Adresse und ein geeigneter Schnittstellentyp konfiguriert wurden. Die Standardeinstellung für den Port ist RS-232.

5. Unter *Vorbereiten des ICDM-RX für die Konfiguration* auf Seite 21 finden Sie die Standard-Netzwerkeinstellungen und Informationen zur Konfigurierung des ICDM-RX für den Einsatz.

2.4. Installation des ICDM-RX/xxx-2ST/RJ45-DIN

Gehen Sie wie folgt vor, um den ICDM-RX/xxx-2ST/RJ45-DIN zu installieren. Prüfen Sie gemäß *Installation des ICDM-RX/xxx-2DB9RJ45-DIN* auf Seite 16, ob der ICDM-RX über serielle DB9-Anschlüsse verfügt.

1. Befestigen Sie den ICDM-RX/xxx-2ST/RJ45-DIN am Hutschienenadapter.
2. Schließen Sie das Netzteil an, und schließen Sie den ICDM-RX/xxx-2ST/RJ45-DIN mithilfe der Netzteilspezifikationen auf dem Produktetikett und den folgenden Informationen an die Stromversorgung an.



Achten Sie beim Anschließen und Trennen des ICDM-RX/xxx-2ST/RJ45-DIN auf die richtigen ESD-Maßnahmen.

- a. Wenn die Hutschiene nicht mit Masse verbunden ist, führen Sie die Masseleitung in die Masseschraubklemme des Gehäuses ein.

Note: Der Masseanschluss des Gehäuses wird nur dann hergestellt, wenn die Hutschiene NICHT mit Masse verbunden ist.

- b. Stecken Sie den DC-Hinleiter in die Plus-Schraubklemme und den DC-Rückleiter in die Minus-Schraubklemme.

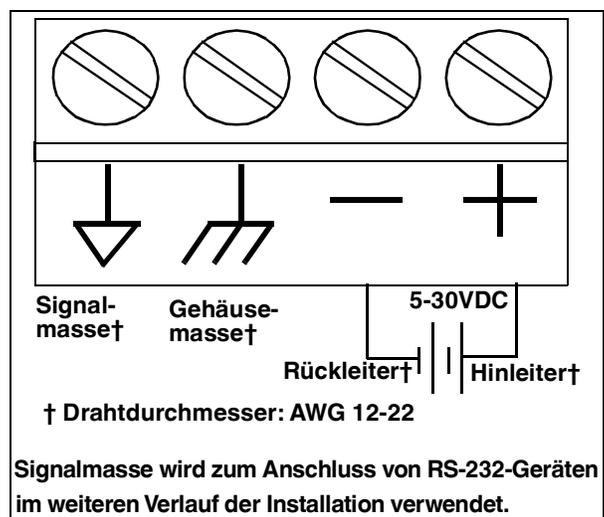
Informationen zu den Anforderungen an die Stromversorgung finden Sie unter *ICDM-RX/xxx-2ST/RJ45-DIN Netzteil* auf Seite 96.

- c. Verwenden Sie einen kleinen Schlitzschraubendreher, um die Drähte zu fixieren.
- d. Überprüfen Sie, ob alle Kabel fest angezogen sind.
- e. Schließen Sie ein UL-zugelassenes Netzteil und ein UL-zugelassenes Netzkabel an eine Stromquelle an, um Strom anzulegen.

Note: Schließen Sie mehrere Einheiten erst an, nachdem Sie die Standard-IP-Adresse geändert haben, siehe *Vorbereiten des ICDM-RX für die Konfiguration* auf Seite 21.

3. Verbinden Sie den **10/100-Port** über ein Standardnetzwerkkabel mit demselben Ethernet-Netzwerksegment wie den Host-PC.

Stromanschluss – Unterseite des Geräts



4. Überprüfen Sie anhand der folgenden Tabelle, ob die **STATUS**-LED den Startvorgang abgeschlossen hat und die Netzwerkverbindung für den ICDM-RX/xxx-2ST/RJ45-DIN ordnungsgemäß funktioniert.

ICDM-RX/xxx-2ST/RJ45-DIN Beschreibung der LEDs	
STATUS	<p>Die STATUS-LED leuchtet, wenn Sie das Gerät eingeschaltet haben und der Startvorgang abgeschlossen ist.</p> <p>Die STATUS-LED blinkt während des Startvorgangs. Es dauert ca. 15 Sekunden, bis der Bootloader den Zyklus abgeschlossen hat. Wenn der Bootloader den Zyklus abgeschlossen hat, leuchtet die LED durchgehend und blinkt nur etwa alle 10 Sekunden.</p> <p>Bei PN- oder PN1-Modell:</p> <p>Wenn der Bootloader den Zyklus beendet, blinkt die LED mehrmals schnell, erlischt dann, und blinkt ca. alle 10 Sekunden, wenn keine SPS-Verbindung besteht.</p>
LINK	Wenn die LED LINK (grün) leuchtet, weist dies auf eine funktionierende Ethernet-Verbindung hin.
ACT	Wenn die LED ACT (gelb) blinkt, weist dies auf Netzwerkaktivität hin.
Note: Weitere Informationen zu den LEDs finden Sie in der Status-LED-Tabelle auf Seite 99.	



Schließen Sie RS-422/485-Geräte erst an, wenn die IP-Adresse und ein geeigneter Schnittstellentyp konfiguriert wurden. Die Standardeinstellung für den Port ist RS-232.

5. Im Abschnitt *Vorbereiten des ICDM-RX für die Konfiguration* auf Seite 21 finden Sie Informationen zu den standardmäßigen Netzwerkeinstellungen und zur Konfigurierung des ICDM-RX/xxx-2ST/RJ45-DIN für den Einsatz.

2.5. Installation des ICDM-RX/xxx-2DB9RJ45-DIN

Gehen Sie wie folgt vor, um den ICDM-RX/xxx-2DB9RJ45-DIN zu installieren.

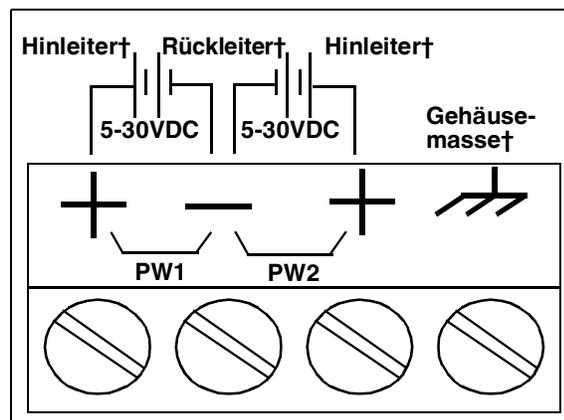
1. Befestigen Sie den ICDM-RX/xxx-2DB9RJ45-DIN am Hutschienenadapter.
2. Schließen Sie das Netzteil an, und schließen Sie den ICDM-RX/xxx-2DB9RJ45-DIN mithilfe der Netzteilspezifikationen auf dem Produktetikett und den folgenden Informationen an die Stromversorgung an.



Achten Sie beim Anschließen und Trennen des ICDM-RX/xxx-2DB9RJ45-DIN auf die richtigen ESD-Maßnahmen.

- a. Wenn die Hutschiene nicht mit Masse verbunden ist, führen Sie die Masseleitung in die Masseschraubklemme des Gehäuses ein.

Note: Der Masseanschluss des Gehäuses wird nur dann hergestellt, wenn die Hutschiene NICHT mit Masse verbunden ist.



- b. Stecken Sie den DC-Hinleiter in eine der Plus-Schraubklemmen und den DC-Rückleiter in die Minus-Schraubklemme.

Ein zweites redundantes Netzteil kann an das Gerät angeschlossen werden, indem der DC-Hinleiter in die andere Plus-Schraubklemme und der DC-Rückleiter in die Minus-Schraubklemme eingeführt wird. Der ICDM-RX/xxx-2DB9RJ45-DIN arbeitet weiter, wenn eines der beiden angeschlossenen Netzteile ausfällt.

Ausführliche Informationen zu den Anforderungen an die Stromversorgung finden Sie unter **ICDM-RX/xxx-2DB9RJ45-DIN Netzteil** auf Seite 97.

- c. Verwenden Sie einen kleinen Schlitzschraubendreher, um die Drähte zu fixieren.
- d. Überprüfen Sie, ob alle Kabel fest angezogen sind.
- e. Schließen Sie ein UL-zugelassenes Netzteil und ein UL-zugelassenes Netzkabel an eine Stromquelle an, um Strom anzulegen.

Note: Schließen Sie mehrere Einheiten erst an, nachdem Sie die Standard-IP-Adresse geändert haben, siehe *Vorbereiten des ICDM-RX für die Konfiguration* auf Seite 21.

3. Verbinden Sie den **10/100-Port** über ein Standardnetzwerkabel mit demselben Ethernet-Netzwerksegment wie den Host-PC.

4. Überprüfen Sie anhand der folgenden Tabelle, ob die **STATUS**-LED den Startvorgang abgeschlossen hat und die Netzwerkverbindung für den ICDM-RX/xxx-2DB9RJ45-DIN funktioniert.

ICDM-RX/xxx-2DB9RJ45-DIN Beschreibung der LEDs	
STATUS	<p>Die STATUS-LED leuchtet, wenn Sie das Gerät eingeschaltet haben und der Startvorgang abgeschlossen ist.</p> <p>Die STATUS-LED blinkt während des Startvorgangs. Es dauert ca. 15 Sekunden, bis der Bootloader den Zyklus abgeschlossen hat. Wenn der Bootloader den Zyklus abgeschlossen hat, leuchtet die LED durchgehend und blinkt nur etwa alle 10 Sekunden.</p> <p>Bei PN- oder PN1-Modell:</p> <p>Wenn der Bootloader den Zyklus beendet, blinkt die LED mehrmals schnell, erlischt dann, und blinkt ca. alle 10 Sekunden, wenn keine SPS-Verbindung besteht.</p>
LINK	Wenn die LED LINK (grün) leuchtet, weist dies auf eine funktionierende Ethernet-Verbindung hin.
ACT	Wenn die LED ACT (gelb) blinkt, weist dies auf Netzwerkaktivität hin.
Note: Weitere Informationen zu den LEDs finden Sie in der Status-LED-Tabelle auf Seite 99.	



Schließen Sie RS-422/485-Geräte erst an, wenn die IP-Adresse und ein geeigneter Schnittstellentyp konfiguriert wurden. Die Standardeinstellung für den Port ist RS-232.

5. Unter *Vorbereiten des ICDM-RX für die Konfiguration* auf Seite 21 finden Sie die Standard-Netzwerkeinstellungen und Informationen zur Konfigurierung des ICDM-RX für den Einsatz.

2.6. Installation des ICDM-RX/xxx-4DB9/2RJ45-DIN

Gehen Sie wie folgt vor, um den ICDM-RX/xxx-4DB9/2RJ45-DIN zu installieren.

1. Befestigen Sie den ICDM-RX/xxx-4DB9/2RJ45-DIN am Hutschienenadapter.
2. Schließen Sie das Netzteil an, und schließen Sie den ICDM-RX/xxx-4DB9/2RJ45-DIN mithilfe der Netzteilspezifikationen auf dem Produktetikett und den folgenden Informationen an die Stromversorgung an.

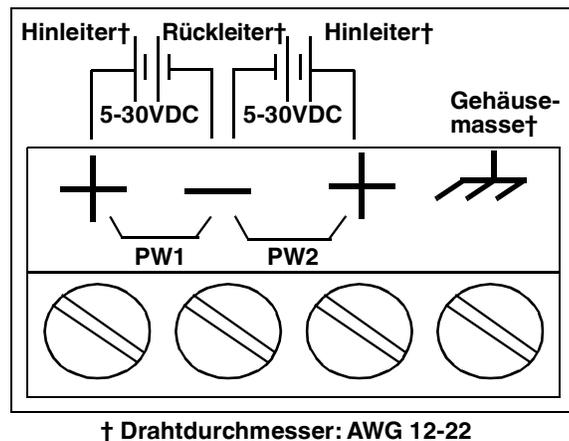


Achten Sie beim Anschließen und Trennen des ICDM-RX/xxx-4DB9/2RJ45-DIN auf die richtigen ESD-Maßnahmen.

- a. Wenn die Hutschiene nicht mit Masse verbunden ist, führen Sie die Masseleitung in die Masseschraubklemme des Gehäuses ein.

Note: Der Masseanschluss des Gehäuses wird nur dann hergestellt, wenn die Hutschiene NICHT mit Masse verbunden ist.

- b. Stecken Sie den DC-Hinleiter in eine der Plus-Schraubklemmen und den DC-Rückleiter in die Minus-Schraubklemme.
 - Ein zweites redundantes Netzteil kann an das Gerät angeschlossen werden, indem der DC-Hinleiter in die andere Plus-Schraubklemme und der DC-Rückleiter in die Minus-Schraubklemme eingeführt wird.
 - Der ICDM-RX/xxx-4DB9/2RJ45-DIN arbeitet weiter, wenn eines der beiden angeschlossenen Netzteile ausfällt.



Ausführliche Informationen zu den Anforderungen an die Stromversorgung finden Sie unter *ICDM-RX/xxx-4DB9/2RJ45-DIN Netzteil* auf Seite 98.

- c. Verwenden Sie einen kleinen Schlitzschraubendreher, um die Drähte zu fixieren.
- d. Überprüfen Sie, ob alle Kabel fest angezogen sind.
- e. Schließen Sie ein UL-zugelassenes Netzteil und ein UL-zugelassenes Netzkabel an eine Stromquelle an, um Strom anzulegen.

Note: Schließen Sie mehrere Einheiten erst an, nachdem Sie die Standard-IP-Adresse geändert haben, siehe *Vorbereiten des ICDM-RX für die Konfiguration* auf Seite 21.

3. Verbinden Sie einen der Ports **10/100** über ein Standard-Ethernet-Kabel mit demselben Ethernet-Netzwerksegment wie den Host-PC. Sie können einen anderen ICDM-RX oder ein Ethernet-Gerät über ein Standard-Ethernet-Kabel mit dem anderen Port verbinden.

Note: PN- und PN1-Modelle: diese Modelle verfügen über zwei Ethernet-Ports, E1 ist der erste und E2 der zweite Port.

- Überprüfen Sie anhand der folgenden Tabelle, ob die **STATUS**-LED den Startvorgang abgeschlossen hat und die Netzwerkverbindung für den ICDM-RX ordnungsgemäß funktioniert.

ICDM-RX/xxx-4DB9/2RJ45-DIN Beschreibung der LEDs	
STATUS	<p>Die STATUS-LED leuchtet, wenn Sie das Gerät eingeschaltet haben und der Startvorgang abgeschlossen ist.</p> <p>Die STATUS-LED blinkt während des Startvorgangs. Es dauert ca. 15 Sekunden, bis der Bootloader den Zyklus abgeschlossen hat. Wenn der Bootloader den Zyklus abgeschlossen hat, leuchtet die LED durchgehend und blinkt nur etwa alle 10 Sekunden.</p> <p>Bei PN- oder PN1-Modell:</p> <p>Wenn der Bootloader den Zyklus beendet, blinkt die LED mehrmals schnell, erlischt dann, und blinkt ca. alle 10 Sekunden, wenn keine SPS-Verbindung besteht.</p>
LINK	Wenn die LED LINK (grün) leuchtet, weist dies auf eine funktionierende Ethernet-Verbindung hin.
ACT	Wenn die LED ACT (gelb) blinkt, weist dies auf Netzwerkaktivität hin.
Note: Weitere Informationen zu den LEDs finden Sie in der Status-LED-Tabelle auf Seite 99.	



Schließen Sie RS-422/485-Geräte erst an, wenn die IP-Adresse und ein geeigneter Schnittstellentyp konfiguriert wurden. Die Standardeinstellung für den Port ist RS-232.

- Im Abschnitt *Vorbereiten des ICDM-RX für die Konfiguration* auf Seite 21 finden Sie Informationen zu den standardmäßigen Netzwerkeinstellungen und zur Konfigurierung des ICDM-RX/xxx-4DB9/2RJ45-DIN für den Einsatz.

2.7. Hinzufügen einer Einheit zu einer vorhandenen Installation

Gehen Sie wie folgt vor, um einer vorhandenen Konfiguration einen weiteren ICDM-RX hinzuzufügen.

- Installieren Sie den ICDM-RX gemäß dem entsprechenden Unterabschnitt in diesem Kapitel auf einem Ethernet-Hub oder einer Server-NIC.

Note: Der technische Support empfiehlt, jeweils nur ein Gerät zu installieren und dieses Gerät zu testen, wenn mehrere Geräte installiert werden. Für den Fall, dass eine Fehlerbehandlung durchgeführt werden muss, ist ein Problem an einer einzelnen Einheit einfacher zu lösen als bei mehreren Einheiten gleichzeitig.
- Schalten Sie den neuen ICDM-RX ein, und stellen Sie sicher, dass die **PWR**- oder **STATUS**-LED leuchtet.
- Programmieren Sie eine IP-Adresse im neuen ICDM-RX mit PortVision DX.
- Laden Sie bei Bedarf die neueste Firmware hoch.
- Konfigurieren Sie die seriellen Schnittstellen, um die seriellen Geräte zu unterstützen, oder laden Sie Konfigurationsdateien aus PortVision DX hoch.
- Schließen Sie die seriellen Geräte an.

2.8. Austauschen der Hardware

Gehen Sie wie folgt vor, um die Hardware auszutauschen.

1. Entfernen Sie die alte Einheit, und bringen Sie eine neue oder eine ICDM-RX-Ersatzeinheit an.
2. Schließen Sie den neuen ICDM-RX an den Netzwerk-Hub oder die Server-NIC an.
3. Schalten Sie den neuen ICDM-RX ein, und stellen Sie sicher, dass der Selbsttest beim Einschalten erfolgreich verläuft.
4. Programmieren Sie die IP-Adresse des neuen ICDM-RX.
5. Laden Sie bei Bedarf die neueste Protokoll-Firmware hoch.
6. Konfigurieren Sie ggf. die Ports, die mit dem vorherigen Gerät übereinstimmen, oder laden Sie Konfigurationsdateien von PortVision DX hoch.
7. Verlegen Sie *alle* Kabel vom alten ICDM-RX zum neuen ICDM-RX.
8. *Es ist nicht nötig*, den Host-PC herunterzufahren und neu zu starten.

3. Vorbereiten des ICDM-RX für die Konfiguration

Die ICDM-RX-Plattform enthält PortVision DX, die Verwaltungs- und Konfigurationsanwendung für Windows, die Sie zur Verwaltung des ICDM-RX verwenden können.

Dieser Abschnitt enthält folgende Themen:

- *Übersicht über PortVision DX*
- *PortVision DX-Anforderungen* auf Seite 21
- *Installation von PortVision DX* auf Seite 22
- *Konfigurieren der Netzwerkeinstellungen* auf Seite 25
- *Überprüfen der Protokoll-Firmwareversion* auf Seite 29
- *Hochladen der Firmware auf den ICDM-RX* auf Seite 30

Note: Wenn PortVision DX bereits installiert ist, gehen Sie direkt zu Konfigurieren der Netzwerkeinstellungen auf Seite 25, um die IP-Adresse auf dem ICDM-RX zu ändern.

3.1. Übersicht über PortVision DX

PortVision DX erkennt automatisch Pepperl+Fuchs Control Ethernet-angeschlossenes Produkte, die physisch mit dem lokalen Netzwerksegment verbunden sind, sodass Sie die Netzwerkadresse konfigurieren, Firmware hochladen und die folgenden Produkte verwalten können:

- ICDM-RX-Familie
- IO-Link-Master (ICE2- und ICE3-Modelle)
- RocketLinx-verwaltete Switches

Neben der Identifizierung von Pepperl+Fuchs Control Ethernet-angeschlossenes Produkten können Sie PortVision DX mit beliebigen Drittanbieter-Switches und -Hardware anzeigen, die direkt mit diesen Geräten verbunden sein können. Alle Nicht-Pepperl + Fuchs-Produkte und nicht verwalteten RocketLinx-Switches werden als nicht intelligente Geräte behandelt und verfügen nur über begrenzte Funktionsunterstützung. So können Sie beispielsweise die Firmware eines Drittanbieter-Schalters nicht konfigurieren oder aktualisieren.

3.2. PortVision DX-Anforderungen

Verwenden Sie PortVision DX, um den ICDM-RX auf Windows-Betriebssystemen zu identifizieren, zu konfigurieren, zu aktualisieren und zu verwalten.

PortVision DX erfordert, dass Sie das Pepperl+Fuchs Control Ethernet-angeschlossenes Produkt mit demselben Netzwerksegment verbinden wie das Windows-Hostsystem, wenn Sie es beim Konfigurationsprozess automatisch scannen und lokalisieren möchten.

Beachten Sie Folgendes vor der Installation von PortVision DX:

- Verwenden Sie PortVision DX, um Firmware hochzuladen und Änderungen auf einem ICDM-RX umzusetzen, der sich im selben lokalen Netzwerksegment befindet wie das System, auf dem PortVision DX installiert ist. Änderungen über PortVision DX können nicht für einen ICDM-RX übernommen werden, der sich nicht im selben lokalen Netzwerksegment befindet.

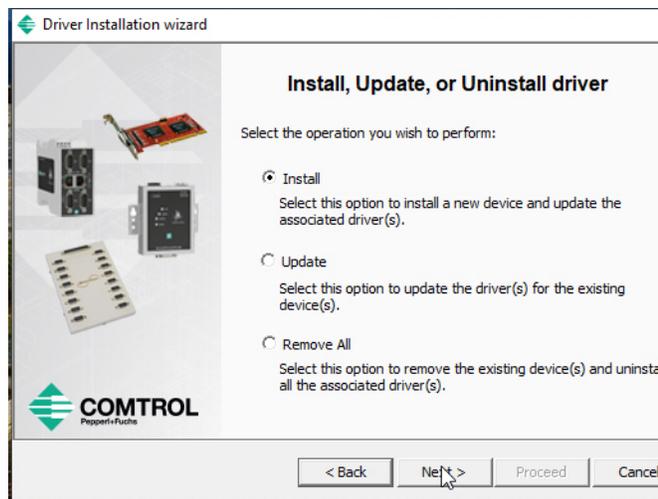
- Verwenden Sie PortVision DX zur Überwachung aller ICDM-RX-Einheiten im Netzwerk. Für Überwachungszwecke muss sich der ICDM-RX nicht im selben lokalen Netzwerksegment befinden wie PortVision DX.

3.3. Installation von PortVision DX

Während der Erstkonfiguration erkennt und identifiziert PortVision DX automatisch die ICDM-RX-Einheiten, sofern sie sich im selben Netzwerksegment befinden.

Sie können die neueste Version von PortVision DX herunterladen.

1. Laden Sie PortVision DX auf <https://www.pepperl-fuchs.com> herunter.
2. Führen Sie die Datei **PortVision_DX[version].msi** aus.
3. Klicken Sie auf dem Bildschirm *Welcome* auf **Next**.



4. Klicken Sie auf **I accept the terms in the License Agreement** und dann auf **Next**.



5. Klicken Sie auf **Next**, oder navigieren Sie optional zu einem anderen Speicherort, und klicken Sie dann auf **Next**.



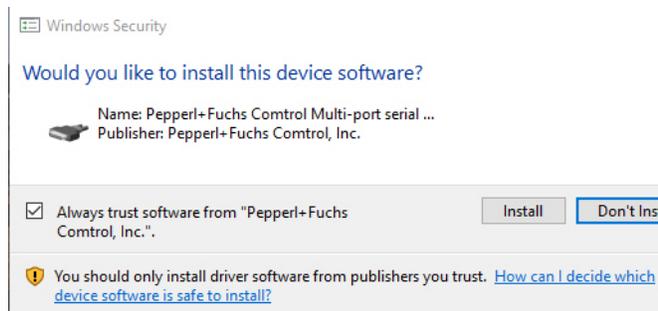
6. Klicken Sie auf **Next**, um die Verknüpfungen zu konfigurieren.



7. Klicken Sie auf **Install**.



8. Je nach Betriebssystem müssen Sie möglicherweise auf **Yes** klicken, um die Frage *Do you want to allow the following program to install software on this computer?* zu beantworten.
9. Klicken Sie auf dem letzten Installationsbildschirm auf **Launch PortVision DX** und auf **Finish**.



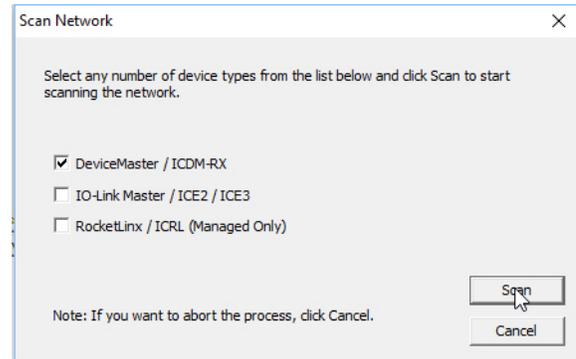
10. Je nach Betriebssystem müssen Sie möglicherweise auf **Yes** klicken, um die Frage *Do you want to allow the following program to make changes to this computer?* zu beantworten.

11. Wählen Sie die Pepperl+Fuchs Control Ethernet-angeschlossenes Produkte aus, die Sie suchen möchten, und klicken Sie dann auf **Scannen**.

Note: Wenn sich das Pepperl+Fuchs Control Ethernet-angeschlossenes Produkt nicht im lokalen Segment befindet und mit einer IP-Adresse programmiert wurde, muss das Pepperl+Fuchs Control Ethernet-angeschlossenes Produkt manuell zu PortVision DX hinzugefügt werden.

12. Gehen Sie zu Schritt 5 im nächsten Abschnitt (Konfigurieren der Netzwerkeinstellungen), um die ICDM-RX-Netzwerkeinstellungen zu programmieren.

Sie können Zeit sparen, wenn Sie nur nach ICDM-RX-Einheiten suchen.



Weitere Informationen zu PortVision DX finden Sie im **Help**-System.

3.4. Konfigurieren der Netzwerkeinstellungen

Gehen Sie wie folgt vor, um die Standard-Netzwerkeinstellungen auf dem ICDM-RX für Ihr Netzwerk zu ändern. Standardnetzwerkeinstellungen:

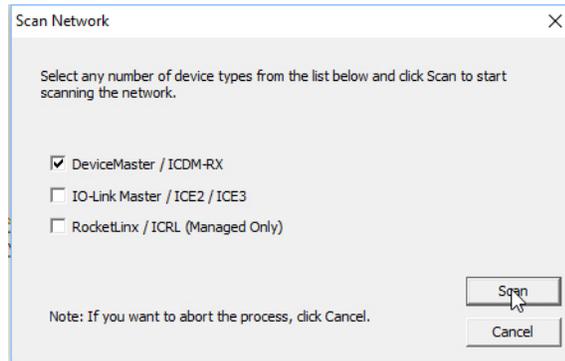
- IP-Adresse: 192.168.250.250
- Subnetzmaske: 255.255.0.0
- Gateway-Adresse: 192.168.250.1

Note: Der technische Support empfiehlt, immer nur eine neue ICDM-RX-Einheit zur Zeit zu konfigurieren, um Probleme mit der Konfiguration des Gerätetreibers zu vermeiden. Informationen zum Konfigurieren mehrerer ICDM-RX-Einheiten mithilfe der Option **Assign IP to Multiple Devices** finden Sie unter Konfigurieren mehrerer ICDM-RX-Netzwerkadressen auf Seite 71.

Das folgende Verfahren zeigt, wie Sie ein einzelnes ICDM-RX-Netzwerk konfigurieren, das mit demselben Netzwerksegment wie das Windows-System verbunden ist. Wenn sich der ICDM-RX nicht in demselben physischen Segment befindet, können Sie ihn manuell gemäß *Neues Gerät in PortVision DX hinzufügen* auf Seite 71 hinzufügen.

1. Gegebenenfalls müssen Sie PortVision DX installieren (*Installation von PortVision DX* auf Seite 22).
2. Starten Sie PortVision DX mit der **PortVision DX**-Verknüpfung auf dem Desktop, oder klicken Sie unter der Schaltfläche **Start** auf **Pepperl+Fuchs Control > PortVision DX**.
3. Je nach Betriebssystem müssen Sie möglicherweise die Frage *Do you want to allow the following program to make changes to this computer?* mit **Yes** beantworten.

4. Klicken Sie auf **Scan**, um die Pepperl+Fuchs Control Ethernet-angeschlossenes Produkte einschließlich des ICDM-RX im Netzwerk zu suchen.



Note: Wenn Sie über keine RocketLink-verwalteten Schalter oder IO-Link-Master (ICE2- und ICE3-Modelle) verfügen, spart dies Zeit beim Scannen, wenn Sie nicht nach ihnen suchen.

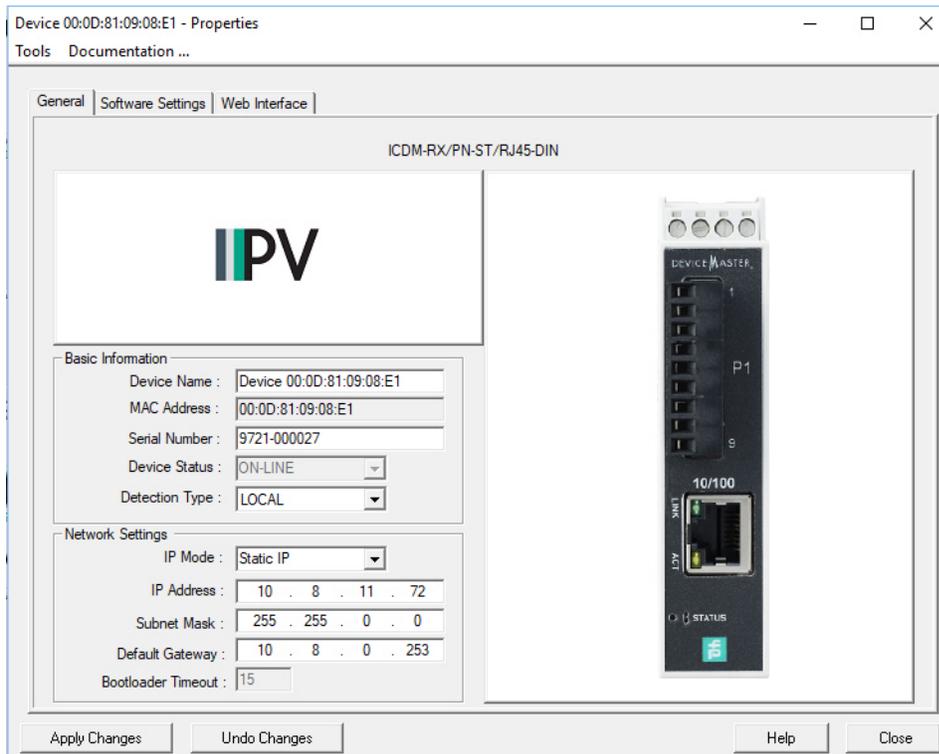
5. Markieren Sie den ICDM-RX, für den Sie die Netzwerkinformationen programmieren möchten, und öffnen Sie den Bildschirm **Properties** mit einer der folgenden Methoden.
 - Doppelklicken Sie im Teilfenster *Device Tree* oder *Device List* auf den ICDM-RX.
 - Klicken Sie mit der rechten Maustaste auf den ICDM-RX im Teilfenster *Device Tree* oder *Device List*, und klicken Sie im Kontextmenü auf **Properties**.
 - Markieren Sie den ICDM-RX im Teilfenster *Device Tree* oder *Device List*, und klicken Sie auf Schaltfläche **Properties**.

- Markieren Sie den ICDM-RX. Klicken Sie auf das Menü **Manage** und dann auf **Properties**.

Device Name	Model	IP Address	MAC Address	Software Version	Status
Device 9708-000061	ICE2-8IOL-G65L-V1D	10.8.11.179	00:0D:81:08:C1:29	EtherNet/IP 1.5.37	ON-LINE
Device 9706-000036	ICE3-8IOL-K45S-RJ45	10.8.11.180	00:0D:81:08:CD:08	PROFINET IO 1.5.37	ON-LINE
Device 00:0D:81:09:0E:C3	EN-DB9/RJ45-DIN	10.8.11.70	00:0D:81:09:0E:C3	EtherNet/IP 7.12	ON-LINE
Device 00:0D:81:09:0B:9E	MOD-DB9/RJ45-DIN	10.8.11.71	00:0D:81:09:0B:9E	Modbus Router 7.04	ON-LINE
Device 00:0D:81:09:08:E1	PN-ST/RJ45-DIN	10.8.11.72	00:0D:81:09:08:E1	PROFINET IO V 3.4.2	ON-LINE
Device 00:0D:81:09:09:FE	TCP-DB9/RJ45-PM	10.8.11.73	00:0D:81:09:09:FE	NS-Link 11.37	ON-LINE

1. Der Inhalt dieses Ordners wird im Teilfenster **Device List** unten angezeigt. Sie können die Struktur erweitern und die Geräte auch im Teilfenster **Device Tree** anzeigen.
2. Teilfenster **Device Tree**
3. Teilfenster **Device List**

4. *Optional* können Sie den ICDM-RX im Feld **Device Name** umbenennen.



Note: Die Felder „MAC address“ und „Device Status“ werden automatisch ausgefüllt, und Sie können diese Werte nicht ändern.

5. Geben Sie optional die Seriennummer ein, die auf einem Schild am ICDM-RX steht.
6. Bei Bedarf können Sie den **Detection Type** ändern.
 - **REMOTE** bedeutet, dass der ICDM-RX nicht mit diesem Netzwerksegment verbunden ist und IP-Kommunikation verwendet.
 - **LOCAL** bedeutet, dass sich der ICDM-RX in diesem lokalen Netzwerksegment befindet und UDP-Kommunikation verwendet.
7. Ändern Sie die ICDM-RX-Netzwerkeigenschaften nach Bedarf für Ihren Standort.

DHCP IP†	Klicken Sie auf diese Option, wenn Sie den ICDM-RX mit DHCP verwenden möchten. Stellen Sie sicher, dass Sie die MAC-Adresse des ICDM-RX dem Netzwerkadministrator mitteilen.
Static IP†	Klicken Sie auf diese Option, um eine statische IP-Adresse zu programmieren. Geben Sie die entsprechende IP-Adresse, Subnetzmaske und das Standard-Gateway für Ihren Standort in die dafür vorgesehenen Felder ein.
† PROFINET IO: Die hier eingegebene Netzwerkadresse muss mit der im TIA Portal-Projekt eingegebenen IP-Adresskonfiguration kompatibel sein. Informationen zur Adresszuweisung finden Sie unter .	

Note: Weitere Informationen finden Sie im PortVision DX-Hilfesystem.

8. Klicken Sie auf **Apply Changes**, um die Netzwerkinformationen auf dem ICDM-RX zu aktualisieren.
9. Klicken Sie auf **Close**, um das Fenster *Properties* zu schließen.
10. Überprüfen Sie gegebenenfalls gemäß des nächsten Unterabschnitts *Überprüfen der Protokoll-Firmwareversion*, ob es sich bei Ihrer Firmware um die neueste Version handelt.

- Bei Bedarf müssen Sie die Firmware für Ihren ICDM-RX gemäß *Hochladen der Firmware auf den ICDM-RX* ICDM-RX auf Seite 30 aktualisieren oder laden.

3.5. Überprüfen der Protokoll-Firmwareversion

Verwenden Sie PortVision DX, um die Firmwareversion zu überprüfen, bevor Sie die Ports konfigurieren. Je nach Modell ist die Protokoll-Firmware auf dem ICDM-RX möglicherweise nicht installiert.

Note: Modelle, auf denen ein Protokoll im ICDM-RX geladen ist, sind in PortVision DX gekennzeichnet, und der ICDM-RX ist entsprechend beschriftet.

Das folgende Verfahren zeigt, wie Sie mit PortVision DX die Firmwareversion auf dem ICDM-RX überprüfen und nach den neuesten Dateien suchen.

Note: Gegebenenfalls müssen Sie PortVision DX installieren (Installation von PortVision DX auf Seite 22).

- Starten Sie PortVision DX, indem Sie auf das PortVision DX-Desktop-Symbol doppelklicken oder auf **Pepperl+Fuchs Control > PortVision DX** klicken.
- Überprüfen Sie im Teilfenster *List View*, ob und welche Version der Firmware auf dem ICDM-RX geladen ist.

The screenshot shows the PortVision DX application window. The main area displays a tree view of systems. A green arrow points to the 'ICDM-RX_Devices' folder. Below the tree view is a table with the following data:

Device Name	Model	IP Address	MAC Address	Software Version	Status
Device 9708-000061	ICE2-8IOL-G65L-V1D	10.8.11.179	00:0D:81:08:C1:29	EtherNet/IP 1.5.37	ON-LINE
Device 9706-000036	ICE3-8IOL-K455-RJ45	10.8.11.180	00:0D:81:08:CD:08	PROFINet IO 1.5.37	ON-LINE
Device 00:0D:81:09:0E:C3	EN-DB9/RJ45-DIN	10.8.11.70	00:0D:81:09:0E:C3	EtherNet/IP 7.12	ON-LINE
Device 00:0D:81:09:08:9E	MOD-DB9/RJ45-DIN	10.8.11.71	00:0D:81:09:08:9E	Modbus Router 7.04	ON-LINE
Device 00:0D:81:09:08:E1	PN-ST/RJ45-DIN	10.8.11.72	00:0D:81:09:08:E1	PROFINET IO V 3.4.2	ON-LINE
Device 00:0D:81:09:09:FE	TCP-DB9/RJ45-PM	10.8.11.73	00:0D:81:09:09:FE	NS-Link 11.37	ON-LINE

- Überprüfen Sie auf <https://www.pepperl-fuchs.com>, ob eine neuere Version verfügbar ist.

Nur ICDM-RX/MOD-Modelle: Standardmäßig werden ICDM-RX/MOD-Modelle mit Modbus-Router geladen. Wenn Sie die Modbus-Server- oder Modbus TCP-Plattform implementieren möchten, müssen Sie unter <https://www.pepperl-fuchs.com> die entsprechende Firmware herunterladen und auf Ihren ICDM-RX/MOD hochladen.

- Laden Sie gegebenenfalls die neueste Version herunter, und gehen Sie zu Schritt 3 in *Hochladen der Firmware auf den ICDM-RX ICDM-RX* auf Seite 30.

3.6. Hochladen der Firmware auf den ICDM-RX ICDM-RX

Sie können unter <https://www.pepperl-fuchs.com> überprüfen, ob Sie über die neueste Firmware verfügen.

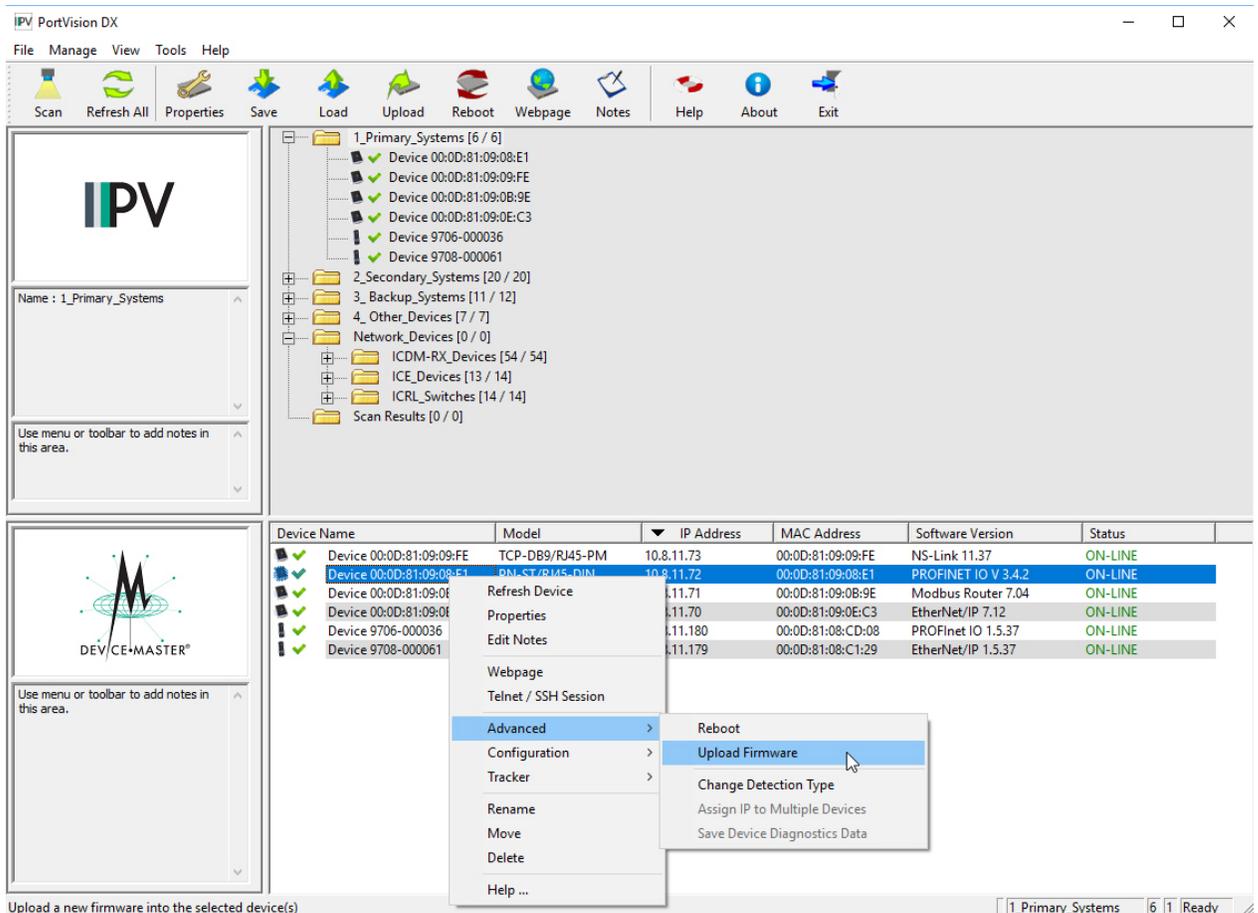
Note: Nur ICDM-RX/MOD-Modelle:

Standardmäßig werden ICDM-RX/MOD-Modelle mit Modbus-Router geladen. Wenn Sie die Modbus-Server- oder Modbus TCP-Plattform implementieren möchten, müssen Sie unter <https://www.pepperl-fuchs.com> die entsprechende Firmware herunterladen und auf Ihren ICDM-RX/MOD hochladen.

Gehen Sie wie folgt vor, um die Firmware auf Ihrem ICDM-RX für das entsprechende Protokoll zu aktualisieren.

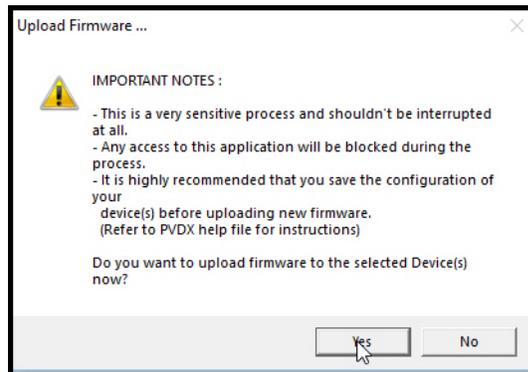
Note: Wenn Sie dies nicht getan haben, installieren Sie PortVision DX (Installation von PortVision DX auf Seite 22), und installieren Sie die Datei „firmware.msi“.

- Führen Sie die .msi-Datei aus, die Sie für die Firmware heruntergeladen haben.
- Starten Sie PortVision DX, indem Sie auf das PortVision DX-Desktop-Symbol doppelklicken oder auf **Pepperl+Fuchs Control > PortVision DX** klicken.
- Klicken Sie mit der rechten Maustaste auf das Gerät oder die Geräte, für die Sie Firmware hochladen möchten, und klicken Sie dann auf **Advanced > Upload Firmware**.



Note: Optional können Sie ein Gerät markieren und die Schaltfläche **Load** verwenden.

4. Navigieren Sie zur Protokoll-Firmware (**.cmtl**-Datei), markieren Sie diese, und klicken Sie auf **Open**.
5. Klicken Sie auf **Yes**, um die Firmware hochzuladen.



6. Klicken Sie in der Meldung, die besagt, dass Sie warten müssen, bis der ICDM-RX online ist, auf **OK**. In der nächsten Minute sollte der ICDM-RX im Feld **Status** je nach Abfragerate die Meldung **ON-LINE** anzeigen. Klicken Sie bei Bedarf auf **Refresh**.
7. Für Informationen zur Konfiguration des/der seriellen Ports über die Webseite und zur Programmierung Ihrer SPS laden Sie das entsprechende *Benutzerhandbuch* für Ihr Protokoll herunter.
8. Wenn Sie planen, mehrere ICDM-RX-Einheiten zu installieren, können Sie die Funktion *Save/Load Configuration File* in PortVision DX verwenden.

Eine Konfigurationsdatei kann Netzwerkeinstellungen und Protokolleinstellungen enthalten. Weitere Informationen finden Sie im PortVision DX-Hilfesystem oder unter *Verwenden von Konfigurationsdateien* auf Seite 74.

9. Nachdem Sie die Eigenschaften des/der seriellen Ports konfiguriert und Ihre SPS-Programme vorbereitet haben, können Sie im nächsten Abschnitt dieses Handbuchs die seriellen Geräte anschließen.

4. ICDM-RX Sicherheit

Dieser Unterabschnitt vermittelt ein grundlegendes Verständnis der ICDM-RX-Sicherheitsoptionen und der Auswirkungen, die diese Optionen haben. Informationen zum Zurücksetzen der *Wiederherstellen der Standardwerte* auf Seite 80-Einstellungen auf die voreingestellten Werte finden Sie im Abschnitt ICDM-RX.

4.1. Sicherheitsmethoden und Terminologie

Die folgende Tabelle enthält Hintergrundinformationen und Definitionen.

Erläuterung zu Begriff oder Problem	
CA (Client-Authentifizierungszertifikat) †	<p>Wenn der ICDM-RX mit einem CA-Zertifikat konfiguriert ist, müssen alle SSL/TLS-Clients ein RSA-Identitätszertifikat vorlegen, das vom konfigurierten CA-Zertifikat signiert wurde. Der ICDM-RX ist bei Auslieferung nicht mit einem CA-Zertifikat konfiguriert, und alle SSL/TLS-Clients sind zulässig.</p> <p>Dieses hochgeladene CA-Zertifikat, das zur Validierung der Identität eines Clients dient, wird manchmal als <i>Trusted Root Certificate</i>, <i>Trusted Authority Certificate</i> oder <i>Trusted CA Certificate</i> bezeichnet. Dieses CA-Zertifikat kann ein vertrauenswürdigen kommerzielles Zertifikat oder ein privat generiertes Zertifikat sein, das ein Unternehmen intern erstellt, um einen Mechanismus zur Steuerung des Zugriffs auf Ressourcen bereitzustellen, die durch die SSL/TLS-Protokolle geschützt sind.</p> <p>Weitere Informationen finden Sie unter <i>Schlüssel- und Zertifikatsverwaltung</i> auf Seite 45. Dieser Abschnitt befasst sich nicht mit der Erstellung von CA-Zertifikaten.</p>
Client-Authentifizierung	<p>Dies ist ein Prozess, bei dem gekoppelte Schlüssel und Identitätszertifikate verwendet werden, um unbefugten Zugriff auf den ICDM-RX zu verhindern. Die Client-Authentifizierung wird in <i>Client-Authentifizierung</i> auf Seite 40 und in <i>Ändern von Schlüsseln und Zertifikaten</i> auf Seite 48 erläutert.</p>
Von SSL-Servern verwendetes DH-Schlüsselpaar †	<p>Hierbei handelt es sich um ein privates/öffentliches Schlüsselpaar, das von einigen Verschlüsselungssammlungen verwendet wird, um die SSL/TLS-Handshake-Nachrichten zu verschlüsseln. Der Besitz des privaten Teils des Schlüsselpaars ermöglicht es einem Lauscher, den Datenverkehr auf SSL/TLS-Verbindungen zu entschlüsseln, die beim Handshake die DH-Verschlüsselung verwenden.</p> <p>Der DH-Schlüsselaustausch (Diffie-Hellman), auch als exponentieller Schlüsselaustausch bezeichnet, ist eine Methode der digitalen Verschlüsselung, bei der anhand von Zahlen, die auf bestimmten Befugnissen gesammelt werden, Entschlüsselungsschlüssel auf der Grundlage von Komponenten erzeugt werden, die nie direkt gesendet werden. Dadurch wird die Arbeit eines Codeknackers mathematisch extrem erschwert.</p> <p>Die schwerwiegendste Einschränkung des DH-Schlüssels in seiner grundlegenden oder <i>reinen</i> Form ist die fehlende Authentifizierung. Die Kommunikation mit dem DH-Schlüssel allein ist anfällig für Man-in-the-Middle-Angriffe. Idealerweise sollte der DH-Schlüssel zusammen mit einer anerkannten Authentifizierungsmethode (z. B. digitale Signaturen) verwendet werden, um die Identität der Benutzer über das öffentliche Kommunikationsmedium zu überprüfen.</p> <p>Weitere Informationen finden Sie unter <i>Zertifikate und Schlüssel</i> auf Seite 40 und <i>Schlüssel- und Zertifikatsverwaltung</i> auf Seite 45.</p>

Erläuterung zu Begriff oder Problem (Fortsetzung)	
<p>† Alle ICDM-RX-Einheiten werden ab Werk mit identischer Konfiguration ausgeliefert. Alle haben identische, selbstsignierte Server-RSA-Zertifikate, Server-RSA-Schlüssel, Server-DH-Schlüssel von Pepperl + Fuchs und keine Client-Authentifizierungszertifikate. Für maximale Daten- und Zugriffssicherheit sollten Sie alle ICDM-RX-Einheiten mit benutzerdefinierten Zertifikaten und Schlüsseln konfigurieren.</p>	
Digitales Zertifikat	<p>Ein digitales Zertifikat ist eine elektronische <i>Kreditkarte</i>, mit der Sie Ihre Anmeldedaten für geschäftliche oder andere Transaktionen im Internet festlegen können. Es wird von einer Zertifizierungsstelle (CA) ausgestellt. Sie enthält Ihren Namen, eine Seriennummer, das Ablaufdatum, eine Kopie des öffentlichen Schlüssels des Zertifikatsinhabers (zum Verschlüsseln von Nachrichten und digitalen Signaturen) sowie die digitale Signatur der Zertifizierungsstelle, die das Zertifikat ausgestellt hat, damit der Empfänger überprüfen kann, ob das Zertifikat echt ist. Einige digitale Zertifikate entsprechen der Norm X.509. Digitale Zertifikate können in Registries gespeichert werden, sodass authentifizierende Benutzer nach öffentlichen Schlüsseln anderer Benutzer suchen können.</p> <p>Weitere Informationen finden Sie unter <i>Schlüssel- und Zertifikatsverwaltung</i> auf Seite 45.</p>
PKI (Public-Key-Infrastruktur)	<p>Eine Public-Key-Infrastruktur (PKI) ermöglicht den Benutzern eines eigentlich unsicheren öffentlichen Netzwerks (z. B. Internet) den sicheren und privaten Austausch von Daten und Geld durch die Verwendung eines öffentlichen und eines privaten Kryptografieschlüsselpaars, das über eine vertrauenswürdige Stelle abgerufen und freigegeben wird. Die Public-Key-Infrastruktur stellt ein digitales Zertifikat bereit, mit dem eine Person oder ein Unternehmen identifiziert werden kann, sowie Verzeichnisdienste, die die Zertifikate speichern und bei Bedarf widerrufen können. Obwohl die Komponenten einer PKI allgemein bekannt sind, gibt es immer mehr unterschiedliche Ansätze und Dienste. In der Zwischenzeit wird ein Internetstandard für PKI erarbeitet.</p> <p>Bei PKI wird von der Kryptografie mit einem öffentlichen Schlüssel ausgegangen, die die gängigste Methode im Internet zur Authentifizierung eines Nachrichtensenders oder zur Verschlüsselung einer Nachricht ist. Bei der herkömmlichen Kryptografie wurde in der Regel ein geheimer Schlüssel für die Ver- und Entschlüsselung von Nachrichten erstellt und freigegeben. Dieses System mit geheimen oder privaten Schlüsseln weist den erheblichen Nachteil auf, dass Nachrichten leicht entschlüsselt werden können, wenn der Schlüssel von einer anderen Person entdeckt oder abgefangen wird. Aus diesem Grund sind die Kryptografie mit öffentlichem Schlüssel und die Public-Key-Infrastruktur der bevorzugte Ansatz im Internet. (Das System mit privatem Schlüssel wird manchmal auch als symmetrische Verschlüsselung und das System mit öffentlichem Schlüssel als asymmetrische Kryptografie bezeichnet.)</p> <p>Eine Public-Key-Infrastruktur besteht aus:</p> <ul style="list-style-type: none"> • Einer Zertifizierungsstelle, die das digitale Zertifikat ausgibt und verifiziert. Das Zertifikat enthält den öffentlichen Schlüssel oder Informationen zum öffentlichen Schlüssel. • Einer Registrierungsstelle (RA, Registration Authority), die als Überprüfungsprogramm für die Zertifizierungsstelle fungiert, bevor ein digitales Zertifikat an einen Anforderer ausgegeben wird • Mindestens einem Verzeichnis, in dem die Zertifikate (mit ihren öffentlichen Schlüsseln) aufbewahrt werden • Einem Zertifikatsverwaltungssystem <p>Weitere Informationen finden Sie unter <i>SSL-Authentifizierung</i> auf Seite 39, <i>SSL-Leistung</i> auf Seite 41, <i>SSL-Chiffrensammlungen</i> auf Seite 42 und <i>Vom ICDM-RX unterstützte Chiffrensammlungen</i> auf Seite 43.</p>

Erläuterung zu Begriff oder Problem (Fortsetzung)	
RSA-Schlüsselpaar†	<p>Dies ist ein Algorithmus für die Kryptografie mit öffentlichem Schlüssel. Es ist der erste Algorithmus, der als für sowohl Signierung als auch Verschlüsselung geeignet bekannt ist. RSA wird häufig in E-Commerce-Protokollen verwendet und gilt dank ausreichend langer Schlüssel und aktueller Implementierungen als ausreichend sicher. Das System enthält einen Kommunikationskanal, der an mindestens ein Terminal mit Codierungsgerät und mindestens ein Terminal mit Decodierungsgerät gekoppelt ist.</p> <ul style="list-style-type: none"> • Der öffentliche Schlüssel ist ein Wert, der von einer bestimmten Behörde als Verschlüsselungsschlüssel bereitgestellt wird und in Kombination mit einem privaten Schlüssel, der vom öffentlichen Schlüssel abgeleitet ist, zur effektiven Verschlüsselung von Nachrichten und digitalen Signaturen verwendet werden kann. • Privater Schlüssel <ul style="list-style-type: none"> - Eine Hälfte des <i>Schlüsselpaars</i>, das in Verbindung mit einem öffentlichen Schlüssel verwendet wird - Sowohl der öffentliche als auch der private Schlüssel werden für die Ver-/Entschlüsselung benötigt, aber nur der Besitzer eines privaten Schlüssels muss ihn kennen. Beim RSA-System muss der private Schlüssel nie über das Internet gesendet werden. - Der private Schlüssel wird zum Entschlüsseln von Text verwendet, der mit dem öffentlichen Schlüssel verschlüsselt wurde. <p>Wenn <i>Benutzer A</i> also eine Nachricht an <i>Benutzer B</i> sendet, kann <i>Benutzer A</i> den öffentlichen Schlüssel von <i>Benutzer B</i> (jedoch nicht den privaten Schlüssel von <i>Benutzer B</i>) von einem zentralen Administrator ermitteln und mit dem öffentlichen Schlüssel von <i>Benutzer B</i> eine Nachricht an <i>Benutzer B</i> verschlüsseln. Wenn <i>Benutzer B</i> diese empfängt, entschlüsselt <i>Benutzer B</i> sie mit dem privaten Schlüssel von <i>Benutzer B</i>. <i>Benutzer B</i> kann nicht nur Nachrichten verschlüsseln (wodurch der Datenschutz gewährleistet wird), sondern auch <i>Benutzer B</i> für <i>Benutzer A</i> authentifizieren (damit <i>Benutzer A</i> weiß, dass es sich tatsächlich um <i>Benutzer B</i> handelt, der die Nachricht gesendet hat), indem er ein digitales Zertifikat mit dem privaten Schlüssel von <i>Benutzer B</i> verschlüsselt.</p> <p>Weitere Informationen finden Sie unter <i>Schlüssel- und Zertifikatsverwaltung</i> auf Seite 45.</p>
SSH (Secure Shell)	<p>Secure Shell (SSH) ermöglicht den Datenaustausch über einen sicheren Kanal zwischen zwei vernetzten Geräten. Es ersetzt Telnet, das keine Sicherheit hat. SSH erfordert eine Passwortauthentifizierung, auch wenn das Passwort leer ist.</p> <p>Weitere Informationen finden Sie unter <i>SSH-Server</i> auf Seite 39.</p>
SSL (Secure Sockets Layer)	<p>SSL (Secure Sockets Layer) ist der Vorgänger von TLS (Transport Layer Security).</p> <p>SSL ist ein häufig verwendetes Protokoll zur Verwaltung der Sicherheit von Nachrichtenübertragungen im Internet. SSL wurde kürzlich von Transport Layer Security (TLS) abgelöst, das auf SSL basiert. SSL verwendet eine Programmebene, die sich zwischen der HTTP-Ebene (Hypertext Transfer Protocol) des Internets und der TCP-Ebene (Transport Control Protocol) befindet.</p> <p>SSL ist im Microsoft- und im Netscape-Browser sowie in den meisten Webserver-Produkten enthalten. SSL wurde von Netscape entwickelt und von Microsoft sowie anderen Entwicklern von Internet-Clients/-Servern unterstützt. Es wurde zum De-Facto-Standard, bis es sich in Transport Layer Security entwickelte.</p> <p>SSL verwendet das Verschlüsselungssystem für öffentliche und private Schlüssel von RSA, das auch die Verwendung eines digitalen Zertifikats umfasst.</p> <p>Ausführliche Informationen zu SSL finden Sie auf Pages 39 bis 43.</p> <p>Hinweis: <i>Zwei leicht unterschiedliche SSL-Protokolle werden vom ICDM-RX unterstützt: SSLv3 und TLSv1.</i></p>

Erläuterung zu Begriff oder Problem (Fortsetzung)	
TLS (Transport Layer Security)	<p>TLS (Transport Layer Security) ist ein Protokoll, das den Datenschutz bei der Kommunikation zwischen Anwendungen und Benutzern im Internet gewährleistet. Wenn Server und Client kommunizieren, stellt TLS sicher, dass kein Dritter Nachrichten abhören oder manipulieren kann. TLS ist der Nachfolger von SSL (Secure Sockets Layer).</p> <p>TLS und SSL sind nicht interoperabel. Das TLS-Protokoll enthält einen Mechanismus, mit dem die TLS-Implementierung auf SSL 3.0 zurückgeht.</p>
Secure Config Mode	<p>Der unverschlüsselte Zugriff auf Verwaltungs- und Diagnosefunktionen ist deaktiviert. Weitere Informationen finden Sie unter <i>Secure Config Mode</i> auf Seite 38 und <i>Konfigurieren/Aktivieren der Sicherheitsfunktionen – Übersicht</i> auf Seite 44.</p>
Man-in-the-Middle-Angriff	<p>Bei einem Man-in-the-Middle-Angriff fängt der Angreifer Nachrichten in einem öffentlichen Schlüsselaustausch ab und sendet sie dann erneut, indem er den angeforderten Schlüssel durch seinen eigenen öffentlichen Schlüssel ersetzt, sodass die beiden ursprünglichen Parteien weiterhin miteinander kommunizieren.</p> <p>Der Name wurde von dem Ballspiel „Esel in der Mitte“ übernommen, bei dem zwei Personen einander einen Ball zuwerfen, während die Person in der Mitte versucht, den Ball zu fangen. Bei einem Man-in-the-Middle-Angriff verwendet der Eindringling ein Programm, das für den Client als Server auftritt und für den Server als Client. Der Angriff kann genutzt werden, um Zugriff auf die Nachricht zu erhalten oder es dem Angreifer zu ermöglichen, die Nachricht vor der erneuten Übertragung zu ändern.</p>
Kryptografie für öffentliche und private Schlüssel	<p>Bei der Kryptografie mit öffentlichen Schlüsseln werden ein öffentlicher und ein privater Schlüssel gleichzeitig mit demselben Algorithmus erstellt (ein gängiger ist als RSA bekannt), der von einer Zertifizierungsstelle (CA) erstellt wird.</p> <p>Der private Schlüssel wird nur der anfordernden Partei übergeben, und der öffentliche Schlüssel wird (als Teil eines digitalen Zertifikats) in einem für alle Parteien zugänglichen Verzeichnis öffentlich verfügbar gemacht.</p> <p>Der private Schlüssel wird niemals an andere Personen weitergegeben oder über das Internet gesendet. Sie verwenden den privaten Schlüssel, um Text zu entschlüsseln, der von einer anderen Person (die einem öffentlichen Verzeichnis entnehmen kann, was Ihr öffentlicher Schlüssel ist) mit Ihrem öffentlichen Schlüssel verschlüsselt wurde.</p> <p>Wenn <i>Benutzer A</i> also eine Nachricht an <i>Benutzer B</i> sendet, kann <i>Benutzer A</i> den öffentlichen Schlüssel von <i>Benutzer B</i> (jedoch nicht den privaten Schlüssel von <i>Benutzer B</i>) von einem zentralen Administrator ermitteln und mit dem öffentlichen Schlüssel von <i>Benutzer B</i> eine Nachricht an <i>Benutzer B</i> verschlüsseln. Wenn <i>Benutzer B</i> diese empfängt, entschlüsselt <i>Benutzer B</i> sie mit dem privaten Schlüssel von <i>Benutzer B</i>. <i>Benutzer B</i> kann nicht nur Nachrichten verschlüsseln (wodurch der Datenschutz gewährleistet wird), sondern auch <i>Benutzer B</i> für <i>Benutzer A</i> authentifizieren (damit <i>Benutzer A</i> weiß, dass es sich tatsächlich um <i>Benutzer B</i> handelt, der die Nachricht gesendet hat), indem er ein digitales Zertifikat mit dem privaten Schlüssel von <i>Benutzer B</i> verschlüsselt. Wenn <i>Benutzer A</i> ihn empfängt, kann <i>Benutzer A</i> den öffentlichen Schlüssel von <i>Benutzer B</i> verwenden, um ihn zu entschlüsseln.</p>

Erläuterung zu Begriff oder Problem (Fortsetzung)	
<i>Wer stellt die Infrastruktur bereit?</i>	<p>Es werden eine Reihe von Produkten angeboten, mit denen ein Unternehmen oder eine Unternehmensgruppe eine PKI implementieren kann. Die Beschleunigung von E-Commerce und Business-to-Business-Commerce über das Internet hat die Nachfrage nach PKI-Lösungen erhöht. Ähnliche Ideen sind das Virtual Private Network (VPN) und der IP Security-Standard (IPsec). Zu den führenden PKI-Anbietern gehören:</p> <ul style="list-style-type: none"> • RSA, das die wichtigsten Algorithmen entwickelt hat, die von PKI-Anbietern verwendet werden. • VeriSign, das als Zertifizierungsstelle fungiert und Software verkauft, die es einem Unternehmen ermöglicht, eigene Zertifizierungsstellen zu erstellen. • GTE CyberTrust, das eine PKI-Implementierungsmethodik und einen Beratungsservice bietet, den es anderen Unternehmen zum Festpreis bieten soll. • Xcert, dessen Web Sentry-Produkt den Sperrstatus von Zertifikaten auf einem Server mithilfe des OCSP (Online Certificate Status Protocol) überprüft. • Netscape, dessen Directory Server angeblich 50 Millionen Objekte unterstützt und 5.000 Abfragen pro Sekunde verarbeitet; Secure E-Commerce, mit dem ein Unternehmen oder Extranet-Manager digitale Zertifikate verwalten kann; und Meta-Directory, das alle Unternehmensverzeichnisse zur Sicherheitsverwaltung in einem einzigen Verzeichnis verbinden kann.
<p>Die folgenden Themenreferenzen stammen aus: http://searchsecurity.techtarget.com/</p> <ul style="list-style-type: none"> • PKI (Public-Key-Infrastruktur) • Kryptografie für öffentliche/private Schlüssel • Wer stellt die Infrastruktur bereit? • Digitales Zertifikat • DH-Schlüssel • Man-in-the-Middle-Angriff <p>Verweis zum Thema RSA-Schlüsselpaar: http://en.wikipedia.org/wiki/RSA</p>	

4.2. Vom ICDM-RX verwendete TCP- und UDP-Socket-Ports

Die folgende Liste enthält alle logischen TCP- und UDP-Socket-Ports, die im ICDM-RX implementiert sind.

Beschreibung der Socket-Portnummern	
22 SSH 23 Telnet	Die TCP-Ports 22 (ssh) und 23 (telnet) werden für Verwaltungs- und Diagnosezwecke verwendet und für die normale Verwendung nicht benötigt. Sie sind standardmäßig aktiviert. Port 23 kann deaktiviert werden.
80 HTTP 443 SSL oder HTTPS	Die TCP-Ports 80 (http) und 443 (https) werden vom Webserver für die Verwaltung und Konfiguration verwendet und sind standardmäßig aktiviert. Sie können nicht deaktiviert werden.
161 SNMP	UDP-Port 161 wird vom SNMP-Agenten verwendet, wenn SNMP aktiviert ist. Dies ist die Standardeinstellung.
4606	TCP-Port 4606 wird benötigt, wenn Sie die Webschnittstelle oder PortVision DX verwenden und die Firmware aktualisieren möchten, ohne einen TFTP-Server einzurichten. Dieser Port kann nicht deaktiviert werden.
4607	TCP-Port 4607 wird nur zu Diagnosezwecken verwendet und wird für den normalen Betrieb nicht benötigt. Dieser Port kann nicht deaktiviert werden.
TCP 8000 - 8xxx	Erhöht sich pro serieller Schnittstelle auf dem ICDM-RX. Beispiel: Ein ICDM-RX mit 4 Ports hätte die Ports 8000 bis 8003.
UDP 7000 - 7xxx	Erhöht sich pro serieller Schnittstelle auf dem ICDM-RX. Beispiel: Ein ICDM-RX mit 4 Ports hätte die Ports 7000 bis 7003.

4.3. ICDM-RX-Sicherheitsfunktionen

Die folgenden Unterabschnitte enthalten Informationen zu den ICDM-RX-Sicherheitsfunktionen.

4.3.1. Secure Config Mode

ICDM-RX unterstützt den Secure Config Mode.

Sicherheitsmodus-Informationen	
Secure Config	Verschlüsselt/authentifiziert Konfigurations- und Administrationsvorgänge (Webserver, IP-Einstellungen, Laden der Software usw.). Secure Config mode: <ul style="list-style-type: none"> • Deaktiviert Administratorbefehle im MAC-Modus mit Ausnahme der ID-Anforderung†. • Deaktiviert TCP/IP-Admin-Befehle mit Ausnahme der ID-Anforderung†. • Deaktiviert den Telnet-Konsolenzugriff (Port 23)†. • Deaktiviert den unverschlüsselten http://-Zugriff über Port 80. • Deaktiviert E-Mail-Benachrichtigungen und SNMP-Funktionen. • Zwei Werte für http-Befehle READ und WRITE: A3: Enable.
† wirkt sich sowohl auf RedBoot als auch auf die Standardanwendung für Ihr Protokoll aus.	

4.3.2. Sicherheitsvergleich

In dieser Tabelle werden zusätzliche Informationen zum Vergleich der Sicherheitsfunktionen angezeigt.

	Sehr schwach				Sehr stark	
	0	1	2	3	3	4
Unterstützt von	Keine	Passwort	Authentifizierung	Secure Config	Secure Data	Schlüssel und Zertifikat
RedBoot	ja	ja	ja	nein	ja	nein
TCP zu seriellen Ports	ja	ja	ja	nein	nein	nein
SSH zu seriellen Ports	nein	nein	nein	ja	ja	ja
UDP zu seriellen Ports	ja	ja	ja	deaktiviert	deaktiviert	deaktiviert
Telnet/Port 23	ja	ja	ja	deaktiviert	ja †	deaktiviert
SSH Telnet/Port 22	ja	ja	ja	ja	ja	ja
Telnet Port 4607	ja	ja	ja	deaktiviert	ja	ja
SSH (PuTTY) 4607	nein	nein	nein	ja	deaktiviert	deaktiviert
HTTP (Port 80)	ja	ja	ja	deaktiviert	deaktiviert	deaktiviert
HTTPS (Port 443)	nein	nein	nein	ja	ja	ja
E-Mail	ja	ja	ja	deaktiviert	deaktiviert	deaktiviert
SNMP	ja	ja	ja	deaktiviert	deaktiviert	deaktiviert

3/26/20

4.3.3. SSH-Server

Der SSH-Server des ICDM-RX weist die folgenden Merkmale auf:

- Erfordert eine Passwortauthentifizierung, auch wenn das Passwort leer ist.
- Wird unabhängig vom **Secure Config Mode** zusammen mit dem Telnet-Zugriff aktiviert/deaktiviert.
- Der ICDM-RX verwendet externe MatrixSSH-Bibliotheken von PeerSec Networks: <http://www.peersec.com/>.

4.3.4. SSL-Übersicht

ICDM-RX-SSL bietet die folgenden Funktionen:

- Verschlüsselung und Authentifizierung.
 - Durch die Verschlüsselung wird verhindert, dass Lauscher die übertragenen Daten abrufen können.
 - Die Authentifizierung ermöglicht es dem Client (Webbrowser) und dem Server (ICDM-RX) sicherzustellen, dass nur die gewünschten Parteien Verbindungen herstellen dürfen. Dies verhindert unbefugte Zugriffe und Man-in-the-Middle-Angriffe auf den Kommunikationskanal.
- Mehrere leicht unterschiedliche SSL-Protokolle werden vom ICDM-RX unterstützt: SSLv3, TLSv1.0, TLS1.1 und TLS1.2.
- Der ICDM-RX verwendet externe MatrixSSL-Bibliotheken von PeerSec Networks: <http://www.peersec.com/matrixssl.html>.

4.3.5. SSL-Authentifizierung

Die ICDM-RX-SSL-Authentifizierung hat folgende Funktionen:

- Authentifizierung bedeutet, dass die Identität der Partei am anderen Ende eines Kommunikationskanals überprüft werden kann. Ein Benutzername/Passwort ist ein gängiges Beispiel für die Authentifizierung.
- SSL/TLS-Protokolle ermöglichen die Authentifizierung mit RSA-Zertifikaten oder DSS-Zertifikaten. Der ICDM-RX unterstützt nur RSA-Zertifikate.
- Jede Partei (Client und Server) kann der anderen Partei ein ID-Zertifikat vorlegen.
- Jedes ID-Zertifikat wird von einem anderen *Zertifizierungsstellen*-Zertifikat oder Schlüssel signiert.
- Eine Partei kann dann die Gültigkeit des ID-Zertifikats der jeweils anderen Partei überprüfen, indem sie bestätigt, dass es von einer vertrauenswürdigen Stelle signiert wurde. Diese Überprüfung erfordert, dass jede Partei Zugriff auf das Zertifikat/den Schlüssel hat, das/der zum Signieren des ID-Zertifikats der anderen Partei verwendet wurde.

4.3.5.1. Server-Authentifizierung

Die *Server-Authentifizierung* ist der Mechanismus, mit dem der ICDM-RX seine Identität beweist.

- Der ICDM-RX (in der Regel ein SSL-Server) kann konfiguriert werden, indem ein ID-Zertifikat hochgeladen wird, das den Clients angezeigt wird, wenn sie eine Verbindung zum ICDM-RX herstellen.
- Der private Schlüssel, der zum Signieren des Zertifikats verwendet wird, muss auch in den ICDM-RX hochgeladen werden.
Hinweis: *Durch den Besitz dieses privaten Schlüssels können Lauscher den gesamten Datenverkehr zum und vom ICDM-RX entschlüsseln.*
- Der entsprechende öffentliche Schlüssel kann zur Überprüfung des ID-Zertifikats verwendet werden, jedoch nicht zum Entschlüsseln des Datenverkehrs.

- Alle ICDM-RX-Einheiten werden ab Werk mit identischen selbstsignierten ID-Zertifikaten und privaten Schlüsseln geliefert. Das bedeutet, dass jemand (mit etwas Aufwand) den werkseitig voreingestellten privaten Schlüssel aus der ICDM-RX-Firmware extrahieren und damit den Datenverkehr von einem anderen ICDM-RX belauschen kann, der mit dem privaten Standardschlüssel verwendet wird.
- Die öffentlichen/privaten Schlüsselpaare und die ID-Zertifikate können mithilfe von **openssl**-Befehlszeilenprogrammen erstellt werden.
- Wenn das Server-Authentifizierungszertifikat im ICDM-RX nicht von einer dem Client bekannten Zertifizierungsstelle signiert ist (bei Auslieferung nicht der Fall), wird der Benutzer durch interaktive SSL-Clients (z. B. Webbrowser) in der Regel gewarnt.
- Wenn der Name im Server-Authentifizierungszertifikat nicht mit dem *Hostnamen* übereinstimmt, der für den Zugriff auf den Server verwendet wurde, wird der Benutzer durch interaktive SSL-Clients (z. B. Webbrowser) in der Regel gewarnt.

4.3.5.2. Client-Authentifizierung

Die *Client-Authentifizierung* ist der Mechanismus, mit dem der ICDM-RX die Identität von Clients (Webbrowser usw.) überprüft.

- Clients können generell so konfiguriert werden, dass sie ein bestimmtes unbekanntes Serverzertifikat akzeptieren, sodass der Benutzer nicht später gewarnt wird.
- Der ICDM-RX (in der Regel ein SSL-Server) kann durch Hochladen eines Zertifikats einer vertrauenswürdigen *Zertifizierungsstelle* konfiguriert werden; das Zertifikat wird zur Überprüfung der ID-Zertifikate verwendet, die dem ICDM-RX von den SSL-Clients vorgelegt werden. Auf diese Weise können Sie den Zugriff auf den ICDM-RX auf eine begrenzte Anzahl von Clients beschränken, die mit entsprechenden ID-Zertifikaten konfiguriert wurden.
- Die ICDM-RX-Einheiten werden ohne Autoritätszertifikat versandt und erfordern von Clients kein Vorlegen von ID-Zertifikaten. Dadurch können alle SSL-Clients eine Verbindung zum ICDM-RX herstellen.

4.3.5.3. Zertifikate und Schlüssel

Um den Zugriff auf die geschützten SSL/TLS-Ressourcen des ICDM-RX zu steuern, sollten Sie ein eigenes benutzerdefiniertes CA-Zertifikat erstellen und anschließend autorisierte Client-Anwendungen mit Identitätszertifikaten konfigurieren, die vom benutzerdefinierten CA-Zertifikat signiert wurden.

Dieses hochgeladene CA-Zertifikat, das zur Validierung der Identität eines Clients dient, wird manchmal als *Trusted Root Certificate*, *Trusted Authority Certificate* oder *Trusted CA Certificate* bezeichnet. Dieses CA-Zertifikat kann ein vertrauenswürdiges kommerzielles Zertifikat oder ein privat generiertes Zertifikat sein, das ein Unternehmen intern erstellt, um einen Mechanismus zur Steuerung des Zugriffs auf Ressourcen bereitzustellen, die durch die SSL/TLS-Protokolle geschützt sind.

Die folgende Liste enthält zusätzliche Informationen zu Zertifikaten und Schlüsseln:

- Standardmäßig wird der ICDM-RX ohne Zertifizierungsstelle (CA, Certificate Authority) geliefert und ermöglicht daher Verbindungen mit jedem SSL/TLS-Cliet. Falls gewünscht, kann der kontrollierte Zugriff auf SSL/TLS-geschützte Funktionen konfiguriert werden, indem ein Client-Authentifizierungszertifikat in den ICDM-RX hochgeladen wird.
- Zertifikate sind bei kommerziellen Zertifizierungsstellen (VeriSign, Thawte, Entrust usw.) erhältlich.
- Zertifikate können von Benutzern mithilfe von **openssl**-Befehlszeilenprogrammen oder anderen Anwendungen zur eigenen Verwendung erstellt werden.
- Zertifikate und Schlüssel, die auf den ICDM-RX hochgeladen werden sollen, müssen im Binärdateiformat **.DER** und nicht im ASCII-Dateiformat **.PEM** vorliegen. (Die **openssl**-Programme können Dateien in beiden Formaten erstellen und Dateien zwischen den beiden Formaten hin und her konvertieren.)
- Die Konfiguration von Zertifikaten und Schlüsseln erfolgt durch vier hochgeladene Dateien im unteren Teil *Key and Certificate Management* der Website *Edit Security Configuration*.

- **RSA Key Pair used by SSL and SSH servers**

Hierbei handelt es sich um ein privates/öffentliches Schlüsselpaar, das für zwei Zwecke verwendet wird:

- Es wird von einigen Verschlüsselungssammlungen verwendet, um die SSL/TLS-Handshake-Nachrichten zu verschlüsseln. Der Besitz des privaten Teils dieses Schlüsselpaars ermöglicht es einem Lauscher, den Datenverkehr auf SSL/TLS-Verbindungen zu entschlüsseln, die beim Handshake die RSA-Verschlüsselung verwenden.
- Er wird zum Signieren des RSA-Serverzertifikats verwendet, um zu überprüfen, ob der ICDM-RX zur Verwendung des RSA-Serveridentitätszertifikats autorisiert ist. Durch den Besitz des privaten Teils dieses Schlüsselpaars kann sich jemand als ICDM-RX ausgeben.

Wenn der serverseitige RSA-Schlüssel ersetzt wird, muss auch ein entsprechendes RSA-Serverzertifikat erstellt und als übereinstimmender Satz hochgeladen werden, da die Clients das Identitätszertifikat andernfalls nicht verifizieren können.

- **RSA Server Certificate used by SSL servers**

- Dies ist das RSA-Identitätszertifikat, das vom ICDM-RX beim SSL/TLS-Handshake verwendet wird, um sich zu identifizieren. Es wird im ICDM-RX am häufigsten vom SSL-Servercode verwendet, wenn die Clients Verbindungen mit dem sicheren Webserver des ICDM-RX oder anderen sicheren TCP-Ports öffnen. Wenn die ICDM-RX-Konfiguration mit seriellem Port so eingerichtet ist, dass eine TCP-Verbindung (als Client) zu einem anderen Servergerät hergestellt wird, verwendet der ICDM-RX dieses Zertifikat auch, um sich selbst als SSL-Client zu identifizieren, sofern dies vom Server angefordert wird.
- Um ordnungsgemäß zu funktionieren, muss dieses Zertifikat mit dem Server-RSA-Schlüssel signiert werden. Das bedeutet, dass das RSA-Serverzertifikat und der RSA-Serverschlüssel als Paar ersetzt werden müssen.

- **DH Key pair used by SSL servers**

Hierbei handelt es sich um ein privates/öffentliches Schlüsselpaar, das von einigen Verschlüsselungssammlungen verwendet wird, um die SSL/TLS-Handshake-Nachrichten zu verschlüsseln.

Der Besitz des privaten Teils des Schlüsselpaars ermöglicht es einem Lauscher, den Datenverkehr auf SSL/TLS-Verbindungen zu entschlüsseln, die beim Handshake die DH-Verschlüsselung verwenden.

- **Client Authentication Certificate used by SSL servers**

Wenn der ICDM-RX mit einem CA-Zertifikat konfiguriert ist, müssen alle SSL/TLS-Clients ein RSA-Identitätszertifikat vorlegen, das vom konfigurierten CA-Zertifikat signiert wurde. Der ICDM-RX ist bei Auslieferung nicht mit einem CA-Zertifikat konfiguriert, und alle SSL/TLS-Clients sind zulässig.

4.3.6. SSL-Leistung

Der ICDM-RX verfügt über die folgenden SSL-Leistungskenngrößen:

- Die Ver- und Entschlüsselung ist ein CPU-intensiver Prozess, und die Verwendung verschlüsselter Datenströme begrenzt die Anzahl der Ports, die bei einem bestimmten seriellen Durchsatz verwaltet werden können. Die folgende Tabelle zeigt beispielsweise die Anzahl der Ports, die bei 100 % Durchsatz von SocketServer für verschiedene Chiffrensammlungen und Baudraten verwaltet werden können.

	9600	38400	57600	115200
RC4-MD5	32	16	10	5
RC4-SHA	32	13	9	4
AES128-SHA	28	7	5	2
AES256-SHA	26	7	4	2
DES3-SHA	15	3	2	1

Hinweis: Diese Durchsätze erfordern eine CPU-Auslastung von 100 %, sodass andere Funktionen wie der Webserver bei den oben gezeigten Durchsätzen sehr langsam arbeiten. Um eine nutzbare Weboberfläche beizubehalten, sollte die oben angegebene maximale Durchsatzrate/Port-Anzahl deutlich unterschritten werden.

- Der für die Einrichtung einer SSL-Verbindung benötigte Overhead ist erheblich. Die benötigte Zeit zum Öffnen einer Verbindung mit SocketServer ist abhängig vom Verschlüsselungsschema des öffentlichen Schlüssels, das für den ersten Handshake verwendet wird. Typische Einrichtungszeiten für die drei Verschlüsselungsschemata mit öffentlichen Schlüsseln beim ICDM-RX sind:
 - RSA 0,66 Sekunden
 - DHE 3,84 Sekunden
 - DHA 3,28 Sekunden
- Da für jeden Datenblock, der über eine SSL-Verbindung gesendet/empfangen wird, ein gewisser Overhead entsteht, haben die SocketServer-Abfragerate und die Größe der auf SocketServer geschriebenen Blöcke auch spürbare Auswirkungen auf die CPU-Auslastung. Das Schreiben größerer Datenblöcke und eine langsamere SocketServer-Abfragerate verringern die CPU-Auslastung und ermöglichen einen etwas höheren Durchsatz.

4.3.7. SSL-Chiffrensammlungen

Dieser Unterabschnitt enthält Informationen zu SSL-Chiffrensammlungen.

- Eine SSL-Verbindung verwendet vier verschiedene Funktionen, von denen jede eine von mehreren verschiedenen Chiffren oder Algorithmen verwenden kann. Eine bestimmte Kombination aus vier Chiffren/Algorithmen wird als Chiffrensammlung bezeichnet.
- Umfang einer Chiffrensammlung:
 - Verschlüsselungsalgorithmus des öffentlichen Schlüssels
 - Dient zum Schutz des ersten Handshake und der Verbindungseinrichtung.
 - Typische Optionen sind RSA, DH, DHA, DHE, EDH, SRP, PSK. Der ICDM-RX unterstützt RSA, DHA und DHE.
 - Authentifizierungsalgorithmus
 - Wird verwendet, um die Identitäten der beiden Parteien untereinander zu überprüfen.
 - Typische Optionen sind RSA, DSA, ECDSA. Der ICDM-RX unterstützt nur RSA.
 - Stromverschlüsselung
 - Dient zur Verschlüsselung der zwischen den beiden Parteien ausgetauschten Benutzerdaten.
 - Typische Optionen: RC4, DES, 3DES, AES, IDEA, Camellia, NULL. Der ICDM-RX unterstützt RC4, 3DES und AES.
 - Message Authentication Code (Nachrichtenauthentifizierungscode)
 - Hash-Funktion (Prüfsumme), mit der sichergestellt wird, dass kein Nachrichten-Frame bei der Übertragung beschädigt oder geändert wurde.
 - Zu den typischen Optionen gehören MD5, SHA, MD2, MD4. Der ICDM-RX unterstützt MD5 und SHA.
- Bei der Entwicklung der SSL/TLS-Protokolle sind die vier oben genannten Optionen nicht voneinander unabhängig: Nur bestimmte Kombinationen werden durch die Standards definiert. Die Standardkombinationen der Protokolle (SSL oder TLS) und Chiffrensammlungen, die vom ICDM-RX unterstützt werden, sind in der folgenden Tabelle aufgeführt.

4.3.8. Vom ICDM-RX unterstützte Chiffrensammlungen

Der ICDM-RX unterstützt folgende Chiffrensammlungen:

Protokoll	Öffentlicher Schlüssel	Authentifizierung	Chiffre	MAC
SSL	RSA	RSA	3DES	SHA
SSL	RSA	RSA	RC4	SHA
SSL	RSA	RSA	RC4	MD5
SSL	DHE	RSA	3DES	SHA
SSL	DHA	RSA	RC4	MD5
SSL	RSA	RSA	NULL	MD5
SSL	RSA	RSA	NULL	SHA
TLS	RSA	RSA	AES128	SHA
TLS	RSA	RSA	AES256	SHA
TLS	DHE	RSA	AES128	SHA
TLS	DHE	RSA	AES256	SHA
TLS	DHA	RSA	AES128	SHA
TLS	DHA	RSA	AES256	SHA

4.3.8.1. SSL-Ressourcen

Weitere Informationen finden Sie in den folgenden SSL-Ressourcen:

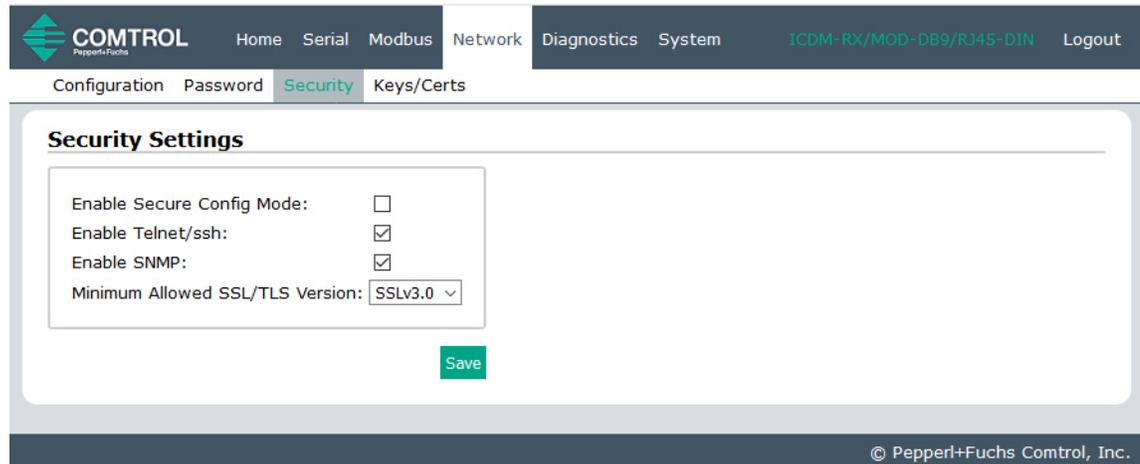
- Die Standardreferenz ist „SSL and TLS“ von Eric Rescorla.
- Die Wikipedia-Seite zu SSL/TLS bietet einen guten Überblick: <http://en.wikipedia.org/wiki/TLS>
- **openssl** enthält Befehlszeilenprogramme für die folgenden Zwecke. Weitere Informationen finden Sie unter: <http://www.openssl.org/>
 - Schlüssel/Zertifikate erstellen/überprüfen
 - Als Client oder Server agieren
- **ssldump** ist ein Befehlszeilenprogramm, das einen visuell lesbaren Auszug aus Handshake und Datenverkehr einer SSL-Verbindung anzeigt. Weitere Informationen finden Sie unter: <http://www.rtfm.com/ssldump/>.
 - Kann den Datenstrom entschlüsseln, wenn der private Schlüssel des Servers bereitgestellt wird
 - Kann decodierte Datenströme in ASCII/Hex anzeigen
 - Kann Inhalte von Handshake-Paketen anzeigen (einschließlich ID-Zertifikate)

4.4. Konfigurieren/Aktivieren der Sicherheitsfunktionen – Übersicht

Sie können die ICDM-RX-Sicherheitsfunktionen auf der Webseite aktivieren. Die *Schlüssel- und Zertifikatsverwaltung* muss über die Registerkarte *Security* auf den ICDM-RX-Webseiten erfolgen.

Wenn Sie sichere COM-Ports wünschen, müssen Sie auch den SSL-Modus aktivieren (**Enable SSL Mode**) und alle zutreffenden Server- oder Client-Zertifikate im NS-Link-Gerätetreiber für Windows eingeben.

Die folgende Abbildung zeigt die Seite **Security Settings** im Menü **Network**. Sie wird in der folgenden Tabelle erläutert.



Hinweis: Die Seite Sicherheitseinstellungen ist für alle Protokolle gleich, in diesem Beispiel handelt es sich um ein Modbus-Produkt.

Beschreibung der Sicherheitsoptionen	
Enable Secure Config Mode	<p>Wenn der Secure Config Mode aktiviert ist, wird damit der unverschlüsselte Zugriff auf Verwaltungs- und Diagnosefunktionen deaktiviert. Der Secure Config Mode ändert das ICDM-RX-Verhalten wie folgt:</p> <ul style="list-style-type: none"> • Der Telnet-Zugriff auf Verwaltungs- und Diagnosefunktionen ist deaktiviert. Der SSH-Zugriff ist weiterhin zulässig. • Der unverschlüsselte Zugriff auf den Webserver über Port 80 (http://URLs) ist deaktiviert. • Der verschlüsselte Zugriff auf den Webserver über Port 443 (https://URLs) ist weiterhin zulässig. • Administrative Befehle, die die Konfiguration oder den Betriebszustand ändern und über das proprietäre TCP-Treiberprotokoll von Pepperl + Fuchs an TCP-Port 4606 eingehen, werden ignoriert. • Administrative Befehle, die die Konfiguration oder den Betriebszustand ändern und mit der proprietären Ethernet-Protokollnummer 0x11FE von Pepperl + Fuchs im MAC-Modus empfangen werden, werden ignoriert.
Enable Telnet/ssh	<p>Mit dieser Option wird die Telnet-Sicherheitsfunktion aktiviert oder deaktiviert, nachdem Sie auf Save geklickt haben und der ICDM-RX neu gestartet wurde. <i>Diese Option ist standardmäßig aktiviert.</i></p>
Enable SNMP	<p>Mit dieser Option wird die SNMP-Sicherheitsfunktion aktiviert oder deaktiviert, nachdem Sie auf Save geklickt haben und der ICDM-RX neu gestartet wurde. <i>Diese Option ist standardmäßig aktiviert.</i></p>

3/26/20

Beschreibung der Sicherheitsoptionen (Fortsetzung)	
Minimum Allowed SSL/TLS Version	Sie können die entsprechende Version für Ihre Umgebung auswählen. <ul style="list-style-type: none">• SSLv3.0• TLSv1.0 (default)• TLSv1.1• TLSv1.2

4.4.1. Schlüssel- und Zertifikatsverwaltung

Die Schlüssel- und Zertifikatsverwaltung ist nur auf der Webseite **Network | Keys/Cert** verfügbar.

The screenshot shows the CONTROL web interface. The top navigation bar includes 'CONTROL Pepperl+Fuchs', 'Home', 'Serial', 'Ethernet', 'Network', 'Diagnostics', 'System', 'ICDM-RX/PN-ST/RJ45-DIN', and 'Logout'. Below this, a secondary navigation bar shows 'Configuration', 'Password', 'Security', 'Keys/Certs', and 'PROFINET IO'. The main content area is titled 'Key and Certificate Management' and contains a table with three rows of key/certificate information, each with 'Browse' and 'Delete' buttons. A 'Save' button is located below the table. A 'Note' section follows, providing instructions on the effect of changes and the required file format (DER). The footer of the interface reads '© Pepperl+Fuchs Control, Inc.'.

Key/Certificate Type	Current Value	Actions
RSA Key pair used by SSL and SSH servers:	Factory	Browse Delete
RSA Server Certificate used by SSL servers:	Factory	Browse Delete
DH Key pair used by SSL servers:	Factory	Browse Delete

Note

Key and certificate changes will take effect after a reboot.

Files must be in DER format.

The RSA key and RSA certificate are used together by clients to authenticate the identity of the server. If you update one without updating the other, clients will be unable to authenticate the server and you will receive warnings from the web browser and other SSL clients.

Beschreibung der Optionen für die Schlüssel- und Zertifikatsverwaltung	
RSA Key pair used by SSL and SSH servers	<p>Hierbei handelt es sich um ein privates/öffentliches Schlüsselpaar, das für zwei Zwecke verwendet wird:</p> <p>Es wird von einigen Verschlüsselungssammlungen verwendet, um die SSL/TLS-Handshake-Nachrichten zu verschlüsseln. Der Besitz des privaten Teils dieses Schlüsselpaars ermöglicht es einem Lauscher, den Datenverkehr auf SSL/TLS-Verbindungen zu entschlüsseln, die beim Handshake die RSA-Verschlüsselung verwenden.</p> <p>Er wird zum Signieren des RSA-Serverzertifikats verwendet, um zu überprüfen, ob der ICDM-RX zur Verwendung des RSA-Serveridentitätszertifikats autorisiert ist. Durch den Besitz des privaten Teils dieses Schlüsselpaars kann sich jemand als ICDM-RX ausgeben.</p> <p>Wenn der Server-RSA-Schlüssel ersetzt werden soll, muss auch ein entsprechendes RSA-Identitätszertifikat erstellt und hochgeladen werden, sonst können die Clients das Identitätszertifikat nicht überprüfen.</p>
RSA Server Certificate used by SSL servers	<p>Dies ist das RSA-Identitätszertifikat, das vom ICDM-RX beim SSL/TLS-Handshake verwendet wird, um sich zu identifizieren. Es wird im ICDM-RX am häufigsten vom SSL-Servercode verwendet, wenn die Clients Verbindungen mit dem sicheren Webserver des ICDM-RX oder anderen sicheren TCP-Ports öffnen. Wenn die ICDM-RX-Konfiguration mit seriellen Port so eingerichtet ist, dass eine TCP-Verbindung (als Client) zu einem anderen Servergerät hergestellt wird, verwendet der ICDM-RX dieses Zertifikat auch, um sich selbst als SSL-Client zu identifizieren, sofern dies vom Server angefordert wird.</p> <p>Um ordnungsgemäß zu funktionieren, muss dieses Zertifikat mit dem Server-RSA-Schlüssel signiert werden. Das bedeutet, dass das RSA-Serverzertifikat und der RSA-Serverschlüssel als Paar ersetzt werden müssen.</p>
DH Key pair used by SSL servers	<p>Hierbei handelt es sich um ein privates/öffentliches Schlüsselpaar, das von einigen Verschlüsselungssammlungen verwendet wird, um die SSL/TLS-Handshake-Nachrichten zu verschlüsseln.</p> <p>Hinweis: <i>Der Besitz des privaten Teils des Schlüsselpaars ermöglicht es einem Lauscher, den Datenverkehr auf SSL/TLS-Verbindungen zu entschlüsseln, die beim Handshake die DH-Verschlüsselung verwenden.</i></p>
Von SSL-Servern verwendetes Client-Authentifizierungszertifikat	<p>Wenn der ICDM-RX mit einem CA-Zertifikat konfiguriert ist, müssen alle SSL/TLS-Clients ein RSA-Identitätszertifikat vorlegen, das vom konfigurierten CA-Zertifikat signiert wurde. Der ICDM-RX ist bei Auslieferung nicht mit einem CA-Zertifikat konfiguriert, und alle SSL/TLS-Clients sind zulässig.</p> <p>Weitere Informationen finden Sie unter <i>Client-Authentifizierung</i> auf Seite 40.</p>
<ul style="list-style-type: none"> • <i>Alle ICDM-RX-Einheiten werden ab Werk mit identischer Konfiguration ausgeliefert. Alle haben identische, selbstsignierte Server-RSA-Zertifikate, Server-RSA-Schlüssel, Server-DH-Schlüssel von Pepperl + Fuchs und keine Client-Authentifizierungszertifikate.</i> • <i>Für maximale Daten- und Zugriffssicherheit sollten Sie alle ICDM-RX-Einheiten mit benutzerdefinierten Zertifikaten und Schlüsseln konfigurieren.</i> 	

4.5. Verwendung eines Webbrowsers zum Festlegen von Sicherheitsfunktionen

Die folgenden Verfahren werden im Folgenden erläutert:

- *Ändern der Sicherheitskonfiguration*
- *Ändern von Schlüsseln und Zertifikaten* auf Seite 48

4.5.1. Ändern der Sicherheitskonfiguration

Gehen Sie wie folgt vor, um die Sicherheitseinstellungen des ICDM-RX zu ändern.

1. Geben Sie die IP-Adresse des ICDM-RX in das Feld *Address* Ihres Webbrowsers ein, und drücken Sie **Enter**.
2. Klicken Sie auf **Network | Security**.
3. Aktivieren Sie die entsprechenden Kontrollkästchen, um die Sicherheit für Ihre Umgebung zu aktivieren oder zu deaktivieren.

Weitere Informationen finden Sie im Hilfesystem oder unter *Konfigurieren/Aktivieren der Sicherheitsfunktionen – Übersicht* auf Seite 44.

4. Nachdem Sie die Änderungen vorgenommen haben, klicken Sie auf **Save**.

4.5.2. Ändern von Schlüsseln und Zertifikaten

Gehen Sie wie folgt vor, um die Sicherheitsschlüssel und Zertifikate des ICDM-RX zu aktualisieren. Weitere Informationen finden Sie im Hilfesystem oder unter *Schlüssel- und Zertifikatsverwaltung* auf Page 48.

1. Geben Sie bei Bedarf die IP-Adresse des ICDM-RX in das Feld *Address* Ihres Webbrowsers ein, und drücken Sie **Enter**.
2. Klicken Sie auf **Network | Keys/Certs**.
3. Klicken Sie auf **Browse**, um die Schlüssel- oder Zertifikatsdatei zu suchen. Markieren Sie die Datei, und klicken Sie auf **Open**.
4. Klicken Sie auf **Upload**.
5. Klicken Sie auf **Save**; die Änderungen werden jedoch erst nach einem Neustart des ICDM-RX wirksam.

Hinweis: Die Schlüssel- oder Zertifikatsschreibweise ändert sich von *factory* oder *none* in **User**, sobald der ICDM-RX sicher ist.

Sie können den ICDM-RX neu starten, indem Sie auf **System | Reboot** klicken oder die PortVision DX-Neustartoption verwenden.

4.6. Kennwortauthentifizierung

In diesem Abschnitt werden drei Methoden zur Konfiguration der Kennwortauthentifizierung beschrieben.

- Über die Webseite
- Über Telnet oder SSH

4.6.1. Über die Webseite

Sie können problemlos ein Kennwort einrichten, um den ICDM-RX zu sichern. Gehen Sie wie folgt vor, um ein Kennwort über die Webseite zu konfigurieren.

Hinweis: *Es wurde kein werkseitiges Kennwort festgelegt.*

Verwenden Sie die folgenden Informationen, um ein Kennwort für den ICDM-RX zu konfigurieren.

1. Melden Sie sich beim ICDM-RX über Ihren Webbrowser mit der IP-Adresse von ICDM-RX an.
2. Klicken Sie auf **Network | Password**.
3. Wenn Sie ein vorhandenes Kennwort ändern, geben Sie dieses in das Feld **Old Password** ein.
4. Geben Sie ein neues Passwort und das Bestätigungspasswort ein.
5. Klicken Sie auf die Schaltfläche **Save**.

Wenn jemand versucht, sich beim ICDM-RX anzumelden, muss er Folgendes eingeben:

- Admin für den Benutzernamen
- Das konfigurierte Kennwort als Kennwort

4.6.2. Über Telnet oder SSH

Wenn Sie dies noch nicht getan haben, installieren Sie PortVision DX. Das ist eine Windows-Anwendung. Bei Bedarf können Sie von <https://www.pepperl-fuchs.com> die neueste Version von PortVision DX herunterladen und diese Version installieren.

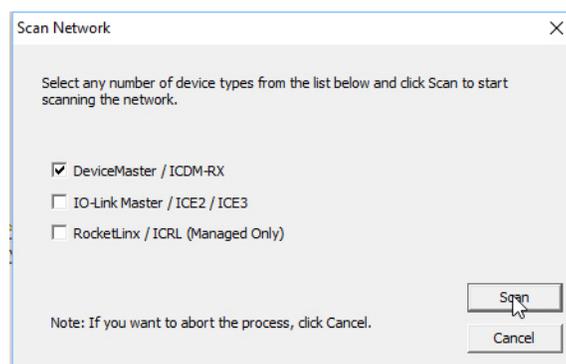
In diesem Unterabschnitt werden die folgenden Themen behandelt:

- *Anmeldeauthentifizierung* auf Seite 49
- *Konfigurieren von Passwörtern* auf Seite 52
- *Telnet-Befehle* auf Seite 54

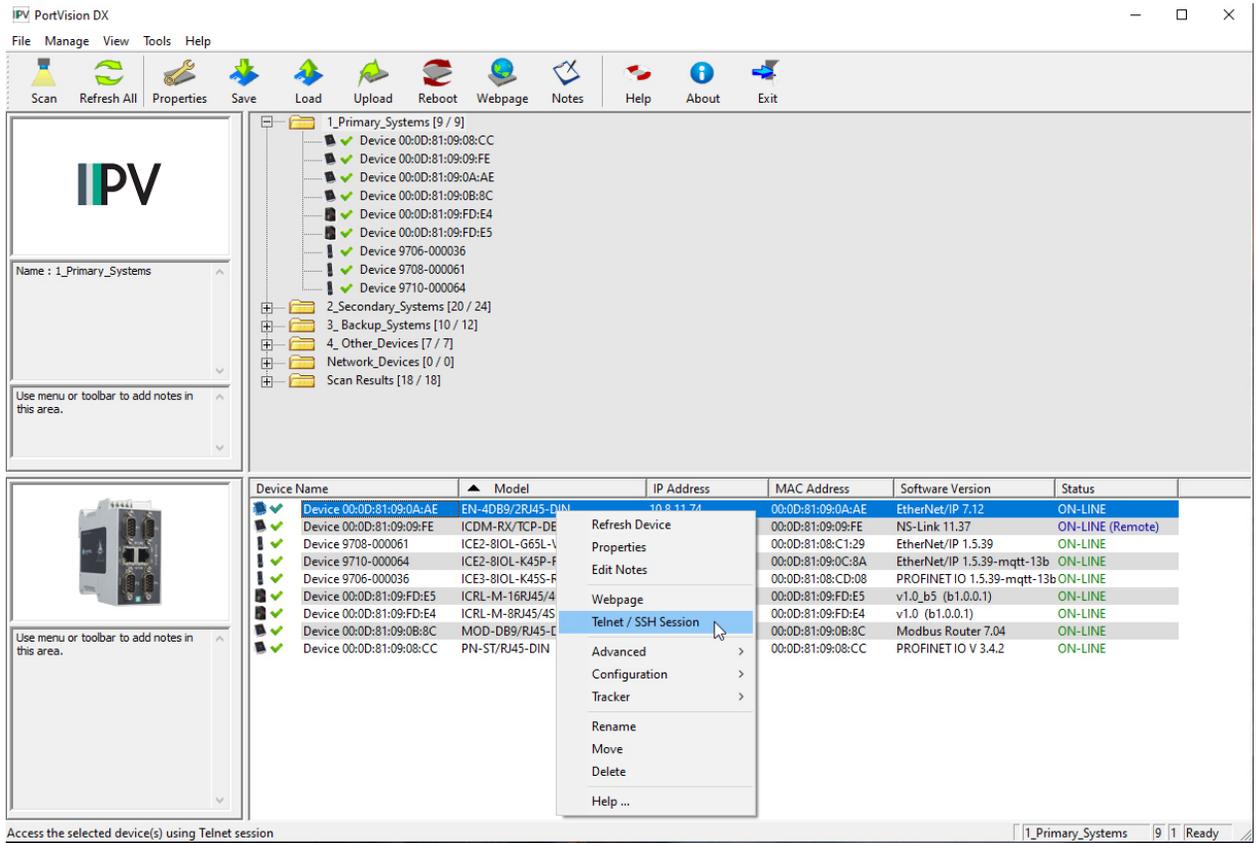
4.6.2.1. Anmeldeauthentifizierung

Führen Sie die folgenden Schritte aus, um auf eine Telnet-Sitzung in PortVision DX zuzugreifen, damit Sie die Anmeldeauthentifizierung festlegen können.

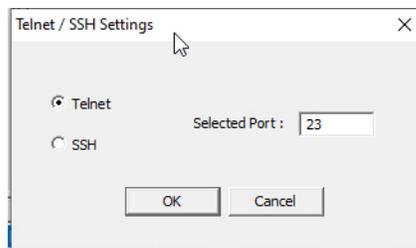
1. Starten Sie PortVision DX.
2. Beim erstmaligen Start von PortVision DX:
 - a. Klicken Sie in der Symbolleiste auf die Schaltfläche **Scan**, um den ICDM-RX zu finden, für den Sie die Kennwortauthentifizierung konfigurieren möchten.
 - b. Klicken Sie auf die ICDM-RX-Option oder andere entsprechende Modelle.
 - c. Klicken Sie auf die Schaltfläche **Scan**.



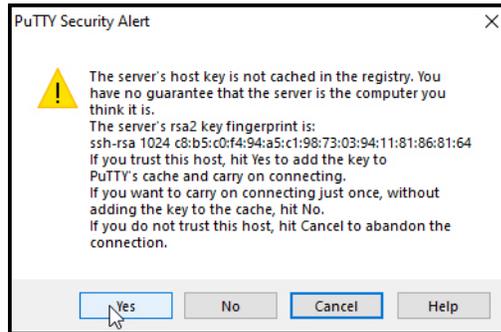
- Markieren Sie den ICDM-RX im Teilfenster Device List (unten), den Sie für die Kennwortauthentifizierung konfigurieren möchten, und klicken Sie auf **Telnet / SSH Session**.



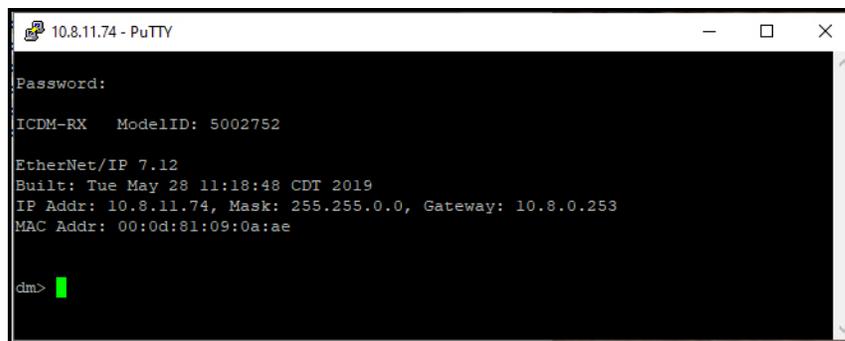
- Wählen Sie **Telnet** oder **SSH**. Lassen Sie die Nummer **Selected Port** unverändert bei 23 oder 22, und klicken Sie auf **Ok**.



5. Wenn Sie **SSH** auswählen, klicken Sie auf **Yes** beim *PuTTY Security Alert*.

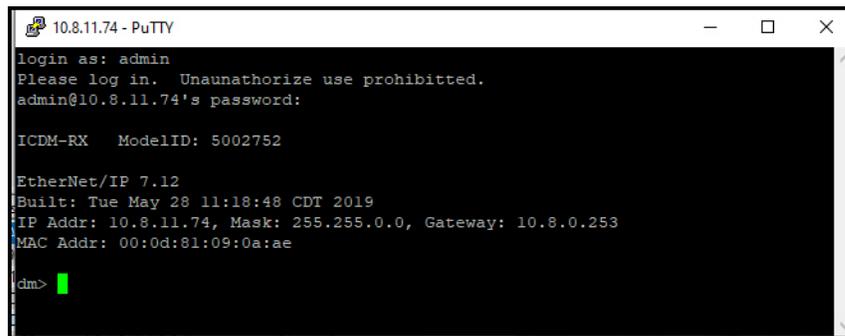


6. Wenn es sich um eine Telnet-Sitzung handelt und für den ICDM-RX ein Kennwort konfiguriert wurde, geben Sie das Kennwort ein und drücken Sie die Eingabetaste.

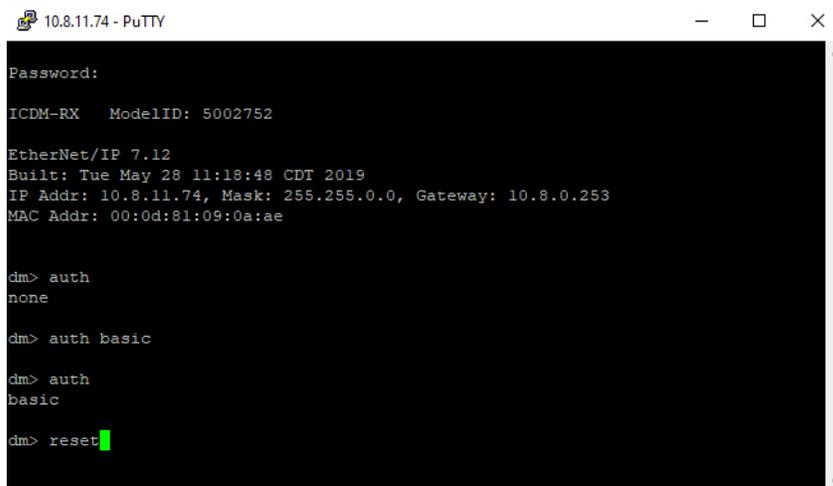


Hinweis: Wenn kein Kennwort festgelegt wurde, drücken Sie die Eingabetaste.

Wenn es sich um eine SSH-Sitzung mit Typ „admin“ für die Anmeldung handelt und für den ICDM-RX ein Kennwort konfiguriert wurde, geben Sie das Kennwort ein, und drücken Sie die Eingabetaste



7. Geben Sie **auth** ein, und drücken Sie die Eingabetaste, um den Authentifizierungsstatus anzuzeigen. „None“ gibt an, dass keine Authentifizierung festgelegt ist.
8. Geben Sie **auth basic** ein, und drücken Sie die Eingabetaste, um die Erzwingung der Anmeldefunktion zu aktivieren.
9. Geben Sie **reset** ein, und drücken Sie die Eingabetaste.
10. Schließen Sie das PuTTY-Fenster.



```
10.8.11.74 - PuTTY
Password:
ICDM-RX ModelID: 5002752
EtherNet/IP 7.12
Built: Tue May 28 11:18:48 CDT 2019
IP Addr: 10.8.11.74, Mask: 255.255.0.0, Gateway: 10.8.0.253
MAC Addr: 00:0d:81:09:0a:ae

dm> auth
none

dm> auth basic

dm> auth
basic

dm> reset
```

PortVision DX zeigt bis zum

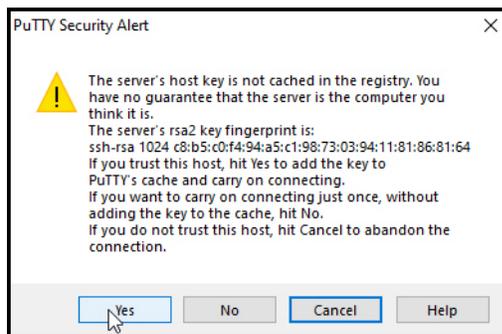
nächsten Abfragezyklus vorübergehend ICDM-RX als OFF-LINE an, da ICDM-RX neu gestartet wird.

Um die erzwungene Anmeldefunktion zu deaktivieren, geben Sie **auth none** ein.

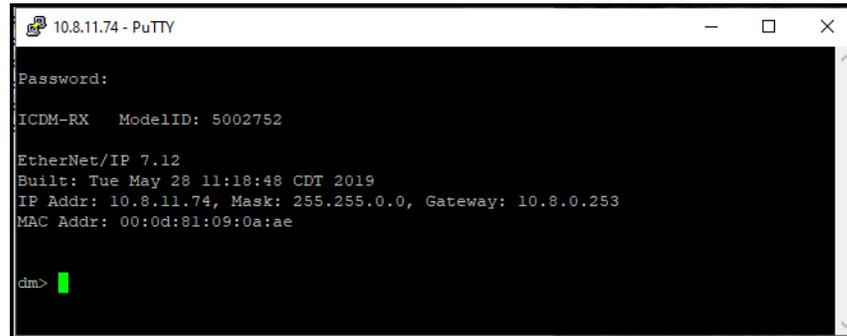
4.6.2.2. Konfigurieren von Passwörtern

Gehen Sie wie folgt vor, um ein ICDM-RX-Kennwort zu konfigurieren.

1. Markieren Sie im Teilfenster Device List (unten) den ICDM-RX, für den Sie ein Kennwort konfigurieren möchten, und klicken Sie auf **Telnet / SSH Session**.
2. Wählen Sie Telnet oder SSH. Lassen Sie die Nummer Selected Port unverändert auf 23, und klicken Sie auf **Ok**.
3. Wenn Sie **SSH** auswählen, klicken Sie auf **Yes** beim *PuTTY Security Alert*.



4. Wenn es sich um eine Telnet-Sitzung handelt und für den ICDM-RX ein Kennwort konfiguriert wurde, geben Sie das Kennwort ein und drücken Sie die Eingabetaste.

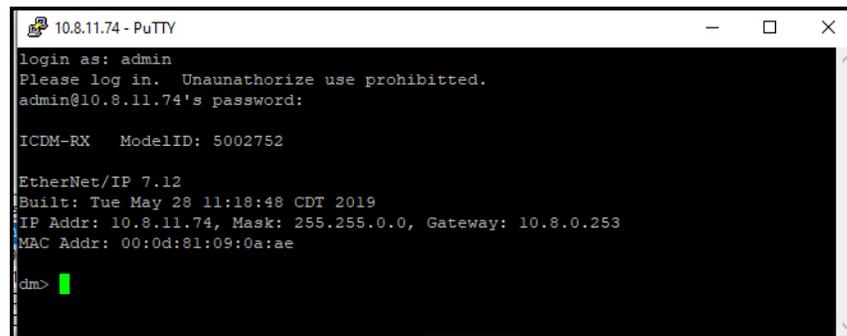


```
10.8.11.74 - PuTTY
Password:
ICDM-RX ModelID: 5002752
EtherNet/IP 7.12
Built: Tue May 28 11:18:48 CDT 2019
IP Addr: 10.8.11.74, Mask: 255.255.0.0, Gateway: 10.8.0.253
MAC Addr: 00:0d:81:09:0a:ae

dm>
```

Hinweis: Wenn kein Kennwort festgelegt wurde, drücken Sie die Eingabetaste.

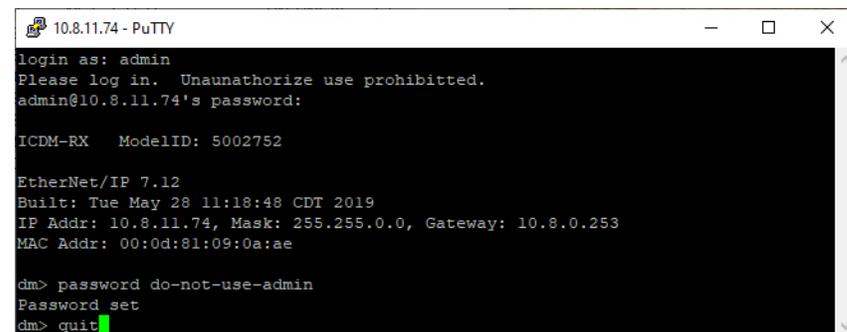
Wenn es sich um eine SSH-Sitzung mit Typ „admin“ für die Anmeldung handelt und für den ICDM-RX ein Kennwort konfiguriert wurde, geben Sie das Kennwort ein, und drücken Sie die Eingabetaste



```
10.8.11.74 - PuTTY
login as: admin
Please log in. Unauthorize use prohibited.
admin@10.8.11.74's password:
ICDM-RX ModelID: 5002752
EtherNet/IP 7.12
Built: Tue May 28 11:18:48 CDT 2019
IP Addr: 10.8.11.74, Mask: 255.255.0.0, Gateway: 10.8.0.253
MAC Addr: 00:0d:81:09:0a:ae

dm>
```

5. Geben Sie „password“ ein und das Kennwort, das Sie festlegen möchten. Das folgende Beispiel zeigt, wie das Kennwort auf „do-not-use-admin“ festgelegt wird.



```
10.8.11.74 - PuTTY
login as: admin
Please log in. Unauthorize use prohibited.
admin@10.8.11.74's password:
ICDM-RX ModelID: 5002752
EtherNet/IP 7.12
Built: Tue May 28 11:18:48 CDT 2019
IP Addr: 10.8.11.74, Mask: 255.255.0.0, Gateway: 10.8.0.253
MAC Addr: 00:0d:81:09:0a:ae

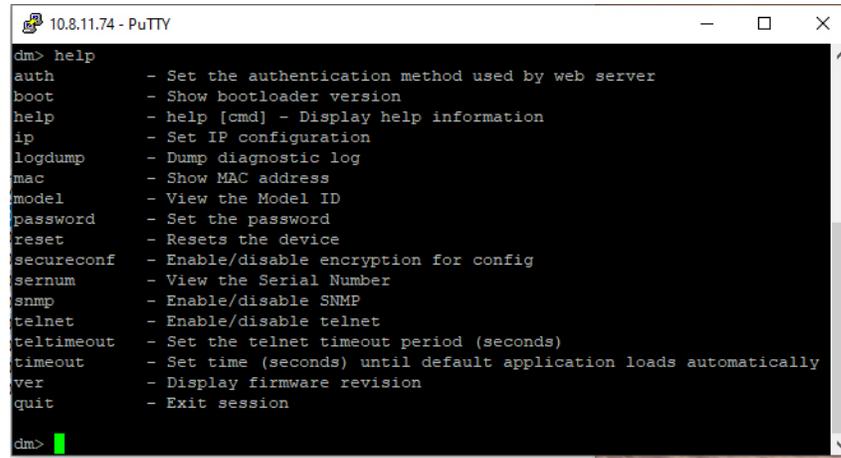
dm> password do-not-use-admin
Password set
dm> quit
```

Hinweis: Stellen Sie sicher, dass Sie das Kennwort nicht vergessen, da Sie nach der Konfiguration von ICDM-RX mit dem Secure Config Mode das Kennwort nicht wiederherstellen können und es auf die Werkseinstellungen zurücksetzen müssen, damit die Standardeinstellung geladen wird.

6. Geben Sie **quit** ein, und drücken Sie die Eingabetaste.

4.6.2.3. Telnet-Befehle

Um auf die Telnet-Hilfe zuzugreifen, geben Sie „help“ ein.



```
10.8.11.74 - PuTTY
dm> help
auth          - Set the authentication method used by web server
boot         - Show bootloader version
help         - help [cmd] - Display help information
ip           - Set IP configuration
logdump      - Dump diagnostic log
mac          - Show MAC address
model        - View the Model ID
password     - Set the password
reset        - Resets the device
secureconf   - Enable/disable encryption for config
sernum       - View the Serial Number
snmp         - Enable/disable SNMP
telnet       - Enable/disable telnet
teltimeout   - Set the telnet timeout period (seconds)
timeout      - Set time (seconds) until default application loads automatically
ver          - Display firmware revision
quit         - Exit session

dm>
```

4.6.3. Webseitenkennwort-Zugriff

Wenn für die Authentifizierung ein Kennwort, wie bei „basic“, erforderlich ist, müssen Sie sich bei jeder Webserver-Sitzung anmelden, unabhängig davon, ob Sie PortVision DX oder einen Webbrowser verwenden. Führen Sie die folgenden Schritte aus, um sich anzumelden:

1. Tragen Sie keinen Benutzernamen ein.
2. Geben Sie Ihr Kennwort ein. Wenn kein Kennwort konfiguriert ist, tragen sie keines ein.
3. Klicken Sie auf OK.

The screenshot shows a web browser interface for a login page. At the top left is the 'CONTROL' logo with 'Pepperl+Fuchs' underneath. To the right of the logo, the device model 'ICDM-RX/EN-4DB9/2R345-D1N' and a 'Logout' link are visible. The main content area is titled 'Login' and contains two input fields: 'username' with the value 'admin' and 'password' with five dots. A green 'login' button is positioned below the password field. The footer displays the URL 'http://10.8.11.74/goform/login' and the copyright notice '© Pepperl+Fuchs Control, Inc.'

Nach der Anmeldung haben Sie vollständigen Lese-/Schreibzugriff auf den Webseiten.

5. Anschließen von seriellen Geräten

In diesem Abschnitt wird erläutert, wie Sie Ihre seriellen Geräte an den ICDM-RX anschließen. Außerdem erhalten Sie Informationen zum Konfektionieren von seriellen Kabeln oder Testkabeln und Loopback-Steckverbindern zum Testen der seriellen Anschlüsse.

- *DB9-Steckverbinder* auf Seite 57
- *RJ45-Steckverbinder* auf Seite 60
- *Vier Schraubklemmen (ICDM-RX/xxx-2ST/RJ45-DIN)* auf Seite 63
- *Neun Schraubklemmen (ICDM-RX/xxx-ST/RJ45-DIN)* auf Seite 66



Vorsicht

Stellen Sie sicher, dass Sie die Ports für den richtigen Kommunikationsmodus konfiguriert haben, bevor Sie Geräte anschließen. Der Standardmodus ist RS-232. In seltenen Fällen kann es geschehen, dass ein seriellcs Gerät beim Anschließen im falschen Modus beschädigt wird.



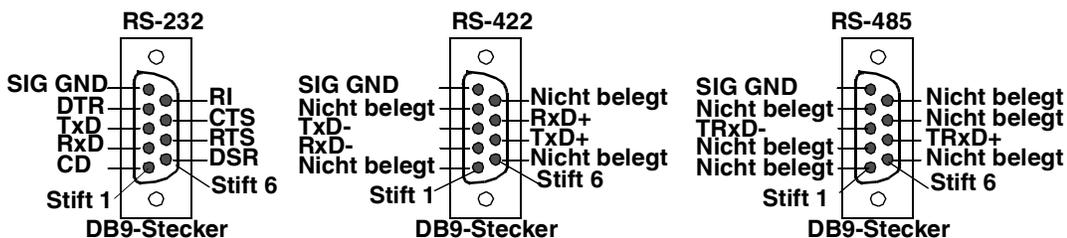
5.1. DB9-Steckverbinder

Dieser Unterabschnitt enthält die folgenden Informationen:

- Stiftbelegung (unten)
- DB9-Nullmodemkabel (RS-232) auf Seite 58
- DB9-Nullmodemkabel (RS-422) auf Seite 58
- Nicht gekreuzte DB9-Netzwerkkabel (RS-232/485) auf Seite 58
- DB9-Loopback-Stecker auf Seite 59
- Anschließen von seriellen DB9-Geräten auf Seite 59

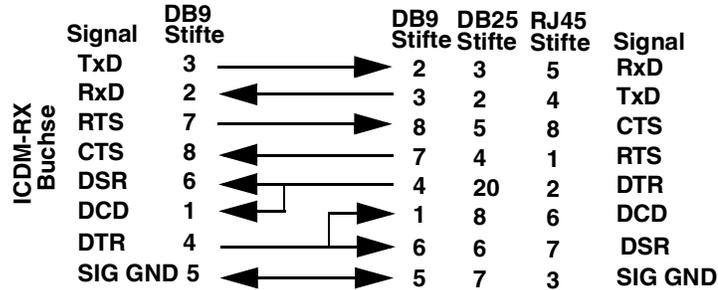
Stiftbelegung im DB9-Steckverbinder			
Stift	RS-232	RS-422 und RS-485 Vollduplex (Master/Slave)†	RS-485 Halbduplex
1	DCD	Nicht belegt	Nicht belegt
2	RxD	RxD-	Nicht belegt
3	TxD	TxD-	TRxD-
4	DTR	Nicht belegt	Nicht belegt
5	Signalmasse	Signalmasse	Signalmasse
6	DSR	Nicht belegt	Nicht belegt
7	RTS	TxD+	TRxD+
8	CTS	RxD+	Nicht belegt
9	RI	Nicht belegt	Nicht belegt
† Hutschienenmodelle unterstützen RS-485 Vollduplex.			

Wenn Sie Hilfe bei der Stiftbelegung oder Verkabelung des seriellen Geräts benötigen, lesen Sie die Installationsdokumentation des Hardwareherstellers. Dort sind die Signale des DB9-Steckverbinders dargestellt.



5.1.1. DB9-Nullmodemkabel (RS-232)

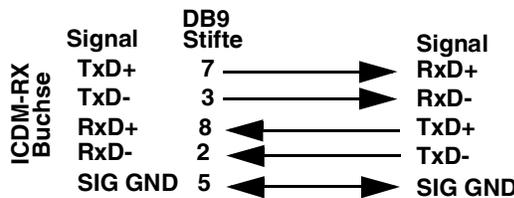
Verwenden Sie die folgende Abbildung, wenn Sie ein RS-232-Nullmodemkabel konfektionieren müssen. Für den Anschluss von DTE-Geräten wird ein Nullmodemkabel benötigt.



Note: Sie sollten ein nicht gekreuztes Netzwerkkabel erwerben oder konfektionieren und einen Nullmodem-Adapter erwerben.

5.1.2. DB9-Nullmodemkabel (RS-422)

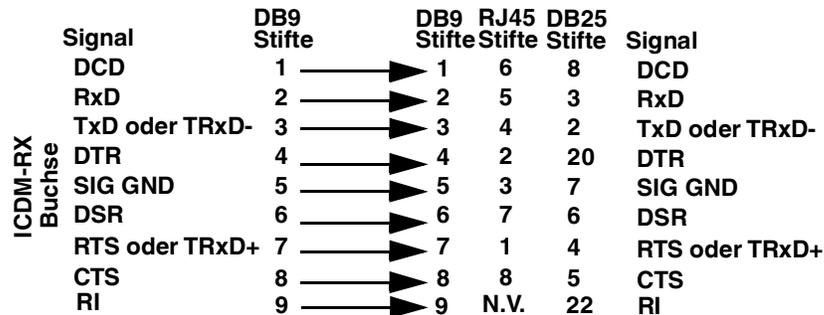
Verwenden Sie die folgende Abbildung, wenn Sie ein RS-422-Nullmodemkabel konfektionieren müssen.



Note: Die RS-422-Stiftbelegung ist nicht genormt. Jeder Peripheriehersteller verwendet unterschiedliche Stiftbelegungen. Informationen zur Stiftbelegung für die oben genannten Signale finden Sie in der Dokumentation zum Peripheriegerät.

5.1.3. Nicht gekreuzte DB9-Netzwerkkabel (RS-232/485)

Verwenden Sie die folgende Abbildung, wenn Sie ein nicht gekreuztes Netzwerkkabel des Typs RS-232 oder RS-485 konfektionieren müssen. Nicht gekreuzte Kabel werden zum Anschließen von Modems und anderen DCE-Geräten verwendet. Etwa kann ein nicht gekreuztes Kabel verwendet werden, um COM2 mit einem Modem zu verbinden.



5.1.4. DB9-Loopback-Stecker

Loopback-Steckverbinder sind Stecker für serielle DB9-Ports mit zusammenverdrahteten Stiften, die in Verbindung mit der Anwendungssoftware zum Testen serieller Anschlüsse verwendet werden. Der ICDM-RX wird mit einem Loopback-Steckverbinder (RS-232/422) geliefert.

Verdrahten Sie die folgenden Stifte miteinander, um zusätzliche Steckverbinder zu konfektionieren oder einen fehlenden RS-232-Loopback-Stecker zu ersetzen:

- Stift 1 an 4 an 6
- Stift 2 an 3
- Stift 7 an 8 an 9



Verkabeln Sie die folgenden Stifte als RS-422-Loopback-Stecker:

- Stift 2 an 3
- Stift 7 an 8



5.1.5. Anschließen von seriellen DB9-Geräten

Mit diesen Informationen können Sie serielle Geräte an DB9-Steckverbinder anschließen.

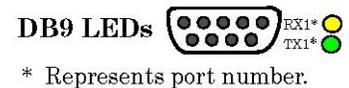
1. Schließen Sie Ihre seriellen Geräte mit dem passenden Kabel am entsprechenden seriellen Port des ICDM-RX an.

Note: Wenn Sie Hilfe bei der Stiftbelegung oder Verkabelung des Peripheriegeräts benötigen, lesen Sie die Installationsdokumentation des Hardwareherstellers.

2. Stellen Sie sicher, dass die Geräte ordnungsgemäß kommunizieren.

Note: ICDM-RX-DIN-Modelle haben keine TX/RX-LEDs.

Die LEDs für RX (gelb) und TX (grün) funktionieren entsprechend, wenn das Kabel ordnungsgemäß an ein serielles Gerät angeschlossen ist.



- Nach dem Aus- und Einschalten des ICDM-RX (entsprechende Modelle) sind die RX/TX-LEDs ausgeschaltet.
- Die LEDs funktionieren erst wie beschrieben, nachdem der Port von einer Anwendung geöffnet wurde.

Modus	LEDs
RS-232	RX-LEDs (gelb) leuchten während des Empfangens von Daten
RS-422	
RS-485	TX-LEDs (grün) leuchten während des Empfangens von Daten

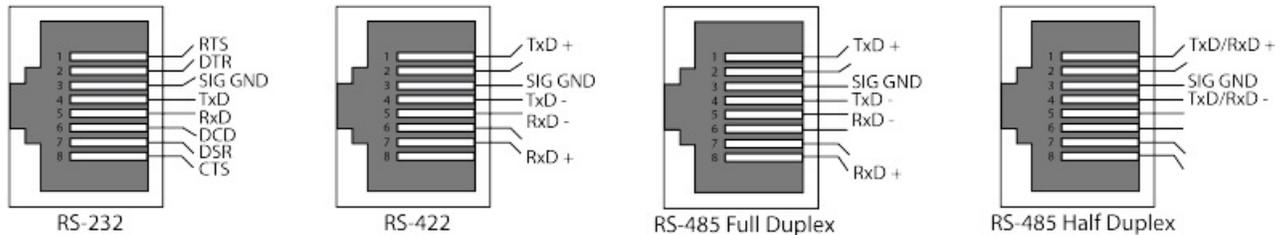
3. Informationen zu den verbleibenden LEDs finden Sie unter *ICDM-RX LEDs* auf Seite 102.

5.2. RJ45-Steckverbinder

Dieser Unterabschnitt enthält die folgenden Informationen:

- Stiftbelegung (unten)
- *RJ45-Nullmodemkabel (RS-232)*
- *RJ45-Nullmodemkabel (RS-422)* auf Seite 61
- *Nicht gekreuzte RJ45-Netzwerkkabel (RS-232/485)* auf Seite 61
- *RJ45-Loopback-Stecker* auf Seite 61
- *RJ45-RS-485-Testkabel* auf Seite 61
- *Anschließen von RJ45-Geräten* auf Seite 62

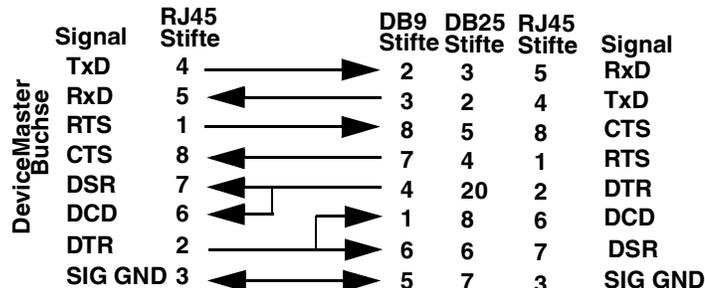
Sie können Ihr eigenes Nullmodem oder ein nicht gekreuztes serielles RJ45-Kabel konfektionieren, wenn Sie die DB9-zu-RJ45-Adapter wie in den folgenden Unterabschnitten angegeben verwenden.



Stift	RS-232	RS-422	RS-485
1	RTS	TxD+	TRxD+
2	DTR	Nicht belegt	Nicht belegt
3	Signalmasse	Signalmasse	Signalmasse
4	TxD	TxD-	TRxD-
5	RxD	RxD-	Nicht belegt
6	DCD	Nicht belegt	Nicht belegt
7	DSR	Nicht belegt	Nicht belegt
8	CTS	RxD+	Nicht belegt

5.2.1. RJ45-Nullmodemkabel (RS-232)

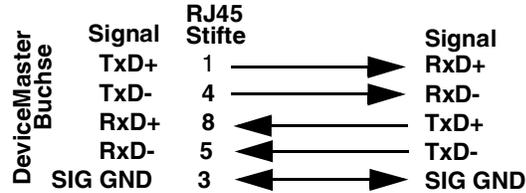
Verwenden Sie die folgende Abbildung, wenn Sie ein RS-232-Nullmodemkabel konfektionieren müssen. Für den Anschluss von DTE-Geräten wird ein Nullmodemkabel benötigt.



Note: Sie sollten ein nicht gekreuztes Netzwerkkabel erwerben oder konfektionieren und einen Nullmodem-Adapter erwerben. Beispielsweise kann ein Nullmodemkabel verwendet werden, um COM2 eines PCs mit COM2 eines anderen PCs zu verbinden.

5.2.2. RJ45-Nullmodemkabel (RS-422)

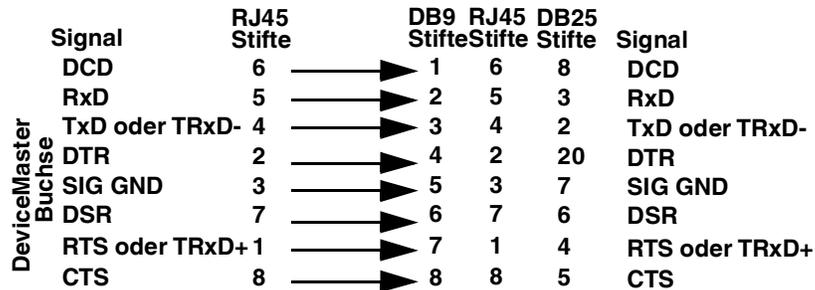
Verwenden Sie die folgende Abbildung, wenn Sie ein RS-422-Nullmodem-RJ45-Kabel konfektionieren müssen. Für den Anschluss von DTE-Geräten wird ein Nullmodemkabel benötigt.



Note: Die RS-422-Stiftbelegung ist nicht genormt. Jeder Peripheriehersteller verwendet unterschiedliche Stiftbelegungen. Informationen zur Bestimmung der Stiftbelegung für die oben genannten Signale finden Sie in der Dokumentation zum Peripheriegerät.

5.2.3. Nicht gekreuzte RJ45-Netzwerkkabel (RS-232/485)

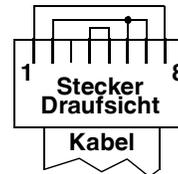
Verwenden Sie die folgende Abbildung, wenn Sie ein nicht gekreuztes Netzwerkkabel des Typs RS-232 oder RS-485 konfektionieren müssen. Nicht gekreuzte Kabel werden zum Anschließen von Modems und anderen DCE-Geräten verwendet.



5.2.4. RJ45-Loopback-Stecker

Loopback-Steckverbinder sind Stecker für serielle RJ45-Ports mit zusammenverdrahteten Stiften, die in Verbindung mit der Anwendungssoftware zum Testen serieller Anschlüsse verwendet werden. Der ICDM-RX wird mit einem Loopback-Steckverbinder (RS-232/422) geliefert.

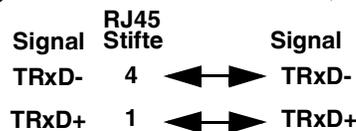
- Stift 4 an 5
- Stift 1 an 8
- Stift 2 an 6 an 7



Der RS-232-Loopback-Stecker funktioniert auch für RS-422.

5.2.5. RJ45-RS-485-Testkabel

Sie können wie zuvor gezeigt ein nicht gekreuztes Kabel verwenden, oder ein eigenes Kabel konfektionieren.



Note: Die RS-422-Stiftbelegung ist nicht genormt. Jeder Peripheriehersteller verwendet unterschiedliche Stiftbelegungen. Informationen zur Bestimmung der Stiftbelegung für die oben genannten Signale finden Sie in der Dokumentation zum Peripheriegerät.

5.2.6. Anschließen von RJ45-Geräten

Mit diesen Informationen können Sie serielle Geräte an RJ45-Steckverbinder anschließen.

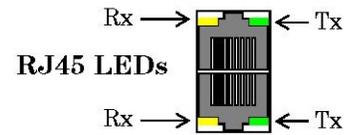
1. Schließen Sie Ihre seriellen Geräte mit dem passenden Kabel am entsprechenden seriellen Port des ICDM-RX an.

Note: Wenn Sie Hilfe bei der Stiftbelegung oder Verkabelung des Peripheriegeräts benötigen, lesen Sie die Installationsdokumentation des Hardwareherstellers.

2. Wenn der ICDM-RX über RX/TX-LEDs verfügt, überprüfen Sie, ob die Geräte ordnungsgemäß kommunizieren.

Die LEDs für RX (gelb) und TX (grün) funktionieren entsprechend, wenn das Kabel ordnungsgemäß an ein serielles Gerät angeschlossen ist.

- Nach dem Aus- und Einschalten des ICDM-RX sind die RX/TX-LEDs ausgeschaltet.
- Die LEDs funktionieren erst wie beschrieben, nachdem der Port von einer Anwendung geöffnet wurde.



Modus	LED-Funktionen
RS-232	RX-LEDs (gelb) leuchten während des Empfangens von Daten
RS-422	
RS-485	TX-LEDs (grün) leuchten während des Empfangens von Daten

3. Informationen zu den verbleibenden LEDs finden Sie unter *ICDM-RX LEDs* auf Seite 102.

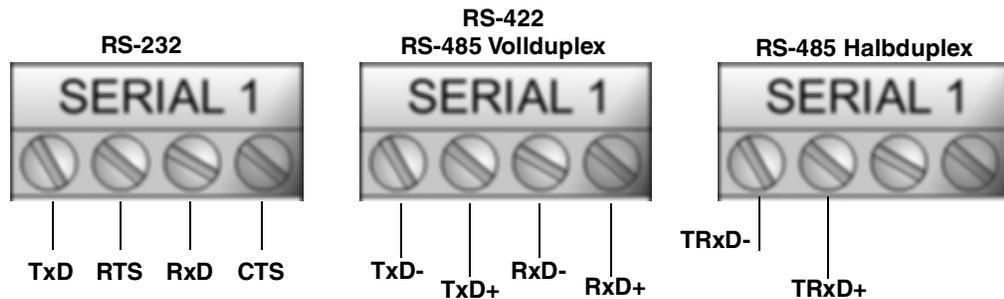
5.3. Vier Schraubklemmen (ICDM-RX/xxx-2ST/RJ45-DIN)

In diesem Unterabschnitt werden die folgenden Themen für den ICDM-RX/xxx-2ST/RJ45-DIN mit 4 seriellen Schraubklemmen behandelt.

- *Serielle 4-fach-Anschlussklemme für Steckverbinder auf Seite 63*
- *Serielle 4-fach-Anschlussklemme für Nullmodemkabel (RS-232) auf Seite 64*
- *Serielle 4-fach-Anschlussklemme für Nullmodemkabel (RS-422) auf Seite 64*
- *Serielle 4-fach-Anschlussklemme für nicht gekreuzte Kabel (RS-232/485) auf Seite 65*
- *Serielle 4-fach-Anschlussklemme für Loopback-Signale auf Seite 65*
- *Anschließen von seriellen Geräten auf Seite 65*

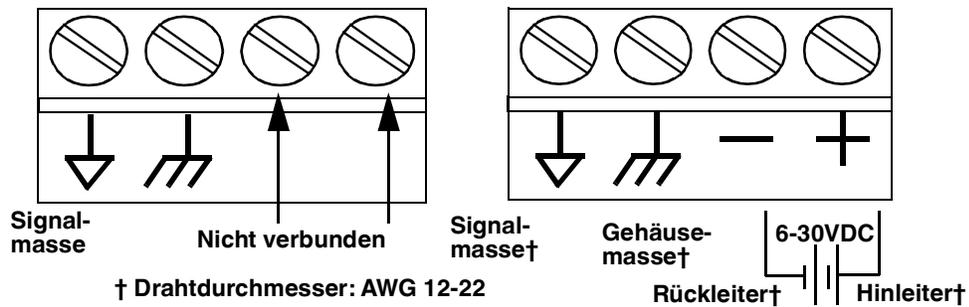
5.3.1. Serielle 4-fach-Anschlussklemme für Steckverbinder

Die folgende Tabelle und die folgenden Zeichnungen dienen zur Information über die Signale. Die Signale für **SERIAL2** sind identisch mit **SERIAL1**.



† Masse muss mit der entsprechenden Signalmasse verbunden sein.

RS-232: Herstellen der Masseverbindung

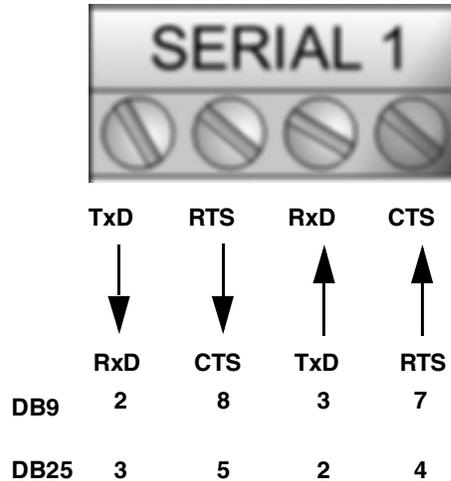


RS-232†	TxD	RTS	RxD	CTS
RS-422/RS-485 Vollduplex	TxD-	TxD+	RxD-	RxD+
RS-485 Halbduplex	TRxD-	TRxD+		
† RS-232-Masse muss mit der Signalmasse verbunden sein.				

5.3.2. Serielle 4-fach-Anschlussklemme für Nullmodemkabel (RS-232)

Für den Anschluss von DTE-Geräten wird ein RS-232-Nullmodemkabel benötigt.

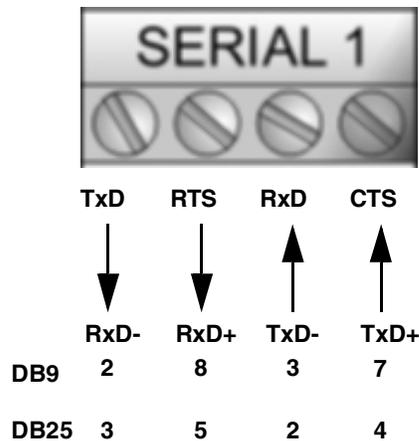
RS-232-Nullmodemkabel



5.3.3. Serielle 4-fach-Anschlussklemme für Nullmodemkabel (RS-422)

Für den Anschluss von DTE-Geräten wird ein RS-422-Nullmodemkabel benötigt.

RS-422-Nullmodemkabel

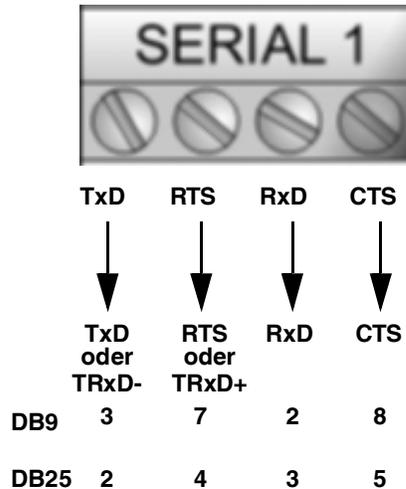


Note: Die RS-422-Stiftbelegung ist nicht genormt. Jeder Peripheriehersteller verwendet unterschiedliche Stiftbelegungen. Informationen zur Bestimmung der Stiftbelegung für die oben genannten Signale finden Sie in der Dokumentation zum Peripheriegerät.

5.3.4. Serielle 4-fach-Anschlussklemme für nicht gekreuzte Kabel (RS-232/485)

Nicht gekreuzte RS-232- oder RS-485-Kabel werden zum Anschließen von Modems und anderen DCE-Geräten verwendet.

Nicht gekreuztes RS-232/422-Kabel

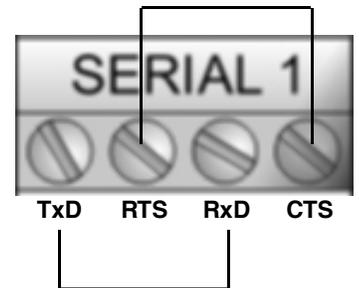


5.3.5. Serielle 4-fach-Anschlussklemme für Loopback-Signale

Verwenden Sie diese Zeichnung, um ein Loopback zu verkabeln, das in Verbindung mit einer Anwendungssoftware zum Testen serieller Ports verwendet wird.

Verkabeln Sie die Anschlussklemmen miteinander, um einen Loopback zu erstellen.

- TxD an RxD
- RTS an CTS



5.3.6. Anschließen von seriellen Geräten

Verwenden Sie die folgenden Informationen, um den ICDM-RX/xxx-2ST/RJ45-DIN mit seriellen Anschlussklemmen zu verbinden.

1. Schließen Sie Ihre seriellen Geräte mit dem passenden Kabel am entsprechenden seriellen Port des ICDM-RX/xxx-2ST/RJ45-DIN an. Sie können Ihre eigenen Kabel oder Loopbacks anhand der entsprechenden Vorgaben konfektionieren.

Note: Wenn Sie Hilfe bei der Stiftbelegung oder Verkabelung des seriellen Geräts benötigen, lesen Sie die Installationsdokumentation des Hardwareherstellers.

2. Informationen zu den LEDs finden Sie unter *ICDM-RX LEDs* auf Seite 102.

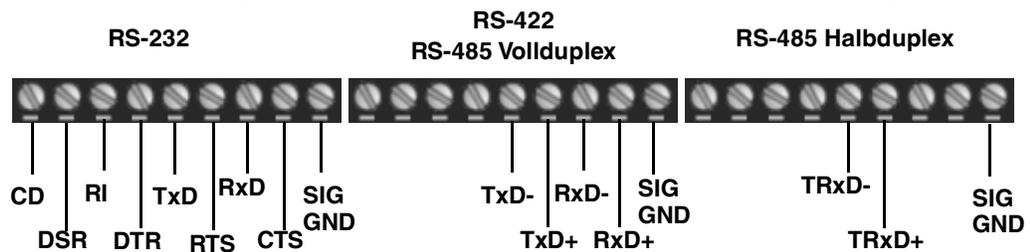
5.4. Neun Schraubklemmen (ICDM-RX/xxx-ST/RJ45-DIN)

In diesem Unterabschnitt werden die folgenden Themen für den ICDM-RX/xxx-ST/RJ45-DIN mit 9 seriellen Schraubklemmen behandelt.

- 9-fach-Schraubklemmen auf Seite 66
- 9-fach-Schraubklemme für RS-232-Nullmodemkabel auf Seite 67
- 9-fach-Schraubklemme für RS-422-Nullmodemkabel auf Seite 67
- 9-fach-Schraubklemme für nicht gekreuzte RS-232/485-Kabel auf Seite 68
- 9-fach-Schraubklemme für Loopback-Signale auf Seite 68
- Anschließen von seriellen Geräten auf Seite 68

5.4.1. 9-fach-Schraubklemmen

Die folgende Tabelle und die folgenden Zeichnungen dienen zur Information über die Signale.



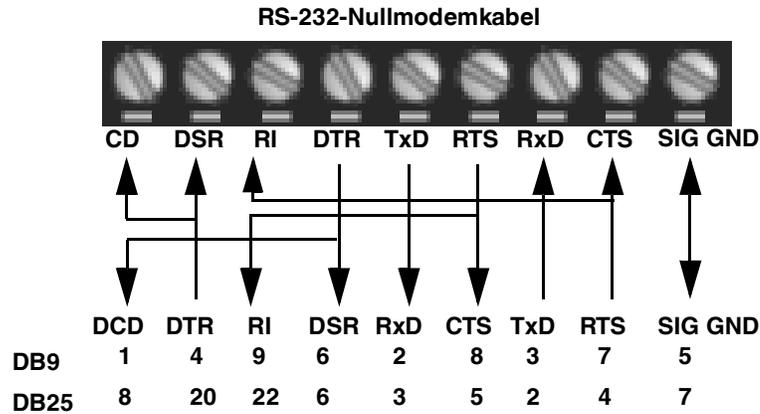
† Masse muss mit der Signalmasse verbunden sein.

	1	2	3	4	5	6	7	8	9
RS-232	CD	DSR	RI	DTR	TxD	RTS	RxD	CTS	Signalmasse
RS-422/RS-485 Vollduplex	N.V.	N.V.	N.V.	N.V.	TxD-	TxD+	RxD-	RxD+	Signalmasse
RS-485 Halbduplex	N.V.	N.V.	N.V.	N.V.	TRxD-	TRxD+	N.V.	N.V.	Signalmasse

† Masse muss mit der Signalmasse verbunden sein.

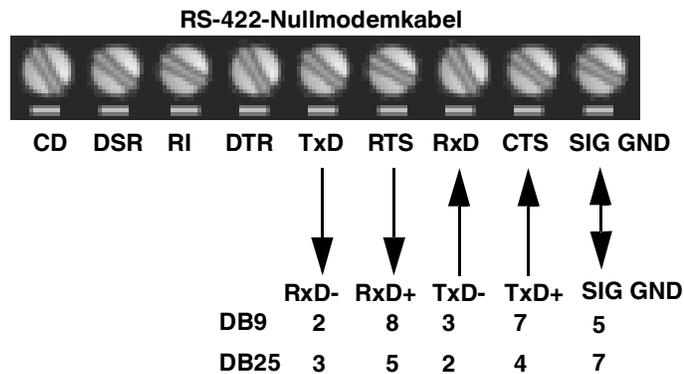
5.4.2. 9-fach-Schraubklemme für RS-232-Nullmodemkabel

Für den Anschluss von DTE-Geräten wird ein RS-232-Nullmodemkabel benötigt.



5.4.3. 9-fach-Schraubklemme für RS-422-Nullmodemkabel

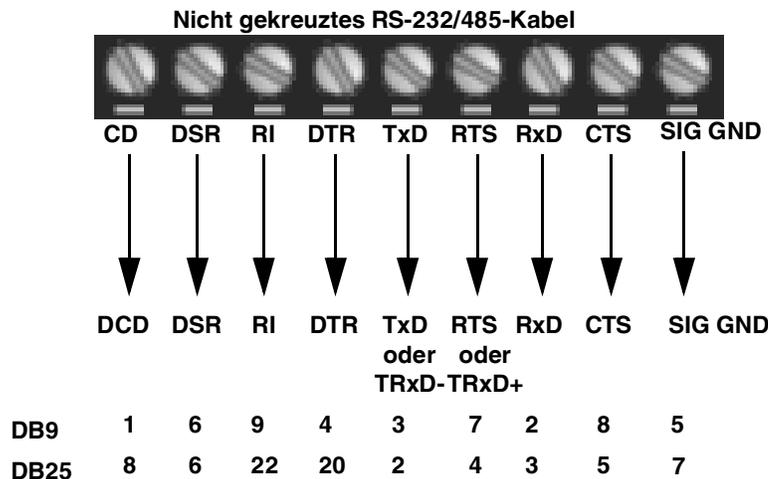
Für den Anschluss von DTE-Geräten wird ein RS-422-Nullmodemkabel benötigt.



Note: Die RS-422-Stiftbelegung ist nicht genormt. Jeder Peripheriehersteller verwendet unterschiedliche Stiftbelegungen. Informationen zur Bestimmung der Stiftbelegung für die oben genannten Signale finden Sie in der Dokumentation zum Peripheriegerät.

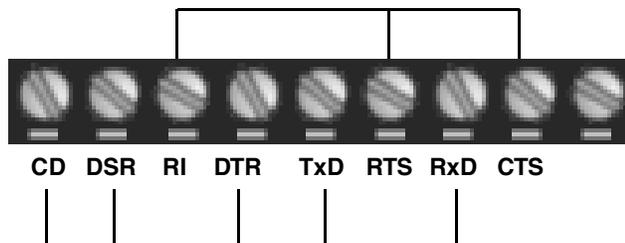
5.4.4. 9-fach-Schraubklemme für nicht gekreuzte RS-232/485-Kabel

Nicht gekreuzte RS-232- oder RS-485-Kabel werden zum Anschließen von Modems und anderen DCE-Geräten verwendet.



5.4.5. 9-fach-Schraubklemme für Loopback-Signale

Verwenden Sie diese Zeichnung, um ein Loopback zu verkabeln, das in Verbindung mit einer Anwendungssoftware zum Testen serieller Ports verwendet wird.



Verkabeln Sie die Anschlussklemmen miteinander, um einen Loopback zu erstellen.

- TxD an RxD
- RTS an CTS an RI
- DTR an CD an DSR

5.4.6. Anschließen von seriellen Geräten

Verwenden Sie die folgenden Informationen, um den ICDM-RX mit seriellen Anschlussklemmen zu verbinden.

1. Schließen Sie Ihre seriellen Geräte mit dem passenden Kabel am entsprechenden seriellen Port des ICDM-RX an. Sie können Ihre eigenen Kabel oder Loopbacks anhand der entsprechenden Vorgaben konfektionieren.

Note: Wenn Sie Hilfe bei der Stiftbelegung oder Verkabelung des seriellen Geräts benötigen, lesen Sie die Installationsdokumentation des Hardwareherstellers.

2. Informationen zu den LEDs finden Sie unter *ICDM-RX LEDs* auf Seite 102.

6. Verwalten des ICDM-RX

In diesem Abschnitt werden die folgenden ICDM-RX-Instandhaltungsverfahren behandelt:

- *Neustarten des ICDM-RX*
 - *Hochladen der Firmware auf mehrere ICDM-RX-Einheiten* auf Seite 70
 - *Konfigurieren mehrerer ICDM-RX-Netzwerkadressen* auf Seite 71

Note: Sie können die Netzwerkadressen für mehrere ICDM-RX-Einheiten konfigurieren, allgemeine Einstellungen für die ICDM-RX-Einheiten konfigurieren und die Einstellungen in einer Konfigurationsdatei speichern, mit der Sie Einstellungen für alle oder ausgewählte ICDM-RX-Einheiten laden können.
 - *Neues Gerät in PortVision DX hinzufügen* auf Seite 71
 - *Ändern der Bootloader-Zeitüberschreitung* auf Seite 73: Hier wird das Ändern des Bootloader-Timeouts beschrieben.
 - *Verwalten des Bootloaders* auf Seite 75: Hier wird erläutert, wie Sie die Bootloader-Version überprüfen und den neuesten Bootloader herunterladen.
 - *Wiederherstellen der Werkseinstellungen (spezifische Modelle – Reset-Schaltfläche)* auf Seite 78
 - *Wiederherstellen der Standardwerte* auf Seite 80
 - *Zugreifen auf RedBoot-Befehle in Telnet-/SSH-Sitzungen (PortVision DX)* auf Seite 81
- Note:** Sie können optional unter RedBoot-Verfahren auf Seite 85 nachsehen, wenn Sie Verfahren auf RedBoot-Ebene durchführen möchten.

6.1. Neustarten des ICDM-RX

Es gibt viele Möglichkeiten, den ICDM-RX neu zu starten.

Methode	Vorgehensweise
PortVision DX	Klicken Sie mit der rechten Maustaste auf den ICDM-RX oder die ICDM-RX-Einheiten im Teilfenster <i>Device List</i> . Klicken Sie auf Advanced >Reboot und dann auf Yes . Note: Wenn die Sicherheitsfunktion auf der Webseite aktiviert wurde, müssen Sie den ICDM-RX auf der Webseite neu starten.
Webseite	System I Reboot: Sie haben 10 Sekunden Zeit zum Abbrechen, bevor der ICDM-RX automatisch neu startet. Optional können Sie auf Reboot Now klicken.
Telnet	Geben Sie reset ein.
ICDM-RX Hutschienenmodelle	Die Hutschienenmodelle des ICDM-RX haben einen Reset/Restore -Schalter. <ul style="list-style-type: none"> • Wenn der Schalter Reset/Restore weniger als 2 Sekunden gedrückt wird, startet der ICDM-RX neu. • Wenn der Schalter Reset/Restore länger als etwa 5 Sekunden gedrückt wird, werden die Werkseinstellungen des ICDM-RX wiederhergestellt.

6.2. Hochladen der Firmware auf mehrere ICDM-RX-Einheiten

Sie können dieses Verfahren anwenden, wenn Ihr ICDM-RX mit dem Host-PC oder Laptop verbunden ist, oder wenn sich der ICDM-RX im lokalen Netzwerksegment befindet.

1. Wenn Sie dies nicht getan haben, installieren Sie PortVision DX (*Installation von PortVision DX* auf Seite 22), und scannen Sie mit **Scan** das Netzwerk.
2. Klicken Sie auf dem Bildschirm **Main** bei gedrückter Umschalttaste auf alle ICDM-RX, die Sie aktualisieren möchten, und gehen Sie dann anhand einer der folgenden Methoden vor:
 - Klicken Sie auf die Schaltfläche **Upload**.
 - Klicken Sie mit der rechten Maustaste, und klicken Sie dann auf **Advanced > Upload Firmware**.
 - Klicken Sie im Menü **Manage** auf **Advanced > Upload Firmware**.

Device Name	Model	IP Address	MAC Address	Software Version	Status
Device 00:0D:81:09:08:E1	PN-ST/RJ45-DIN	10.8.11.72	00:0D:81:09:08:E1	PROFINET IO V 3.4.2	ON-LINE
Device 00:0D:81:09:09:FE	TCP-DB9/RJ45-PM	10.8.11.73	00:0D:81:09:09:FE	NS-Link 11.37	ON-LINE
Device 00:0D:81:09:0A:AE	EN-4DB9/2RJ45-DIN	10.8.11.74	00:0D:81:09:0A:AE	EtherNet/IP 7.12	ON-LINE
Device 00:0D:81:09:0B:9E	MOD-DB9/RJ45-DIN	10.8.11.71	00:0D:81:09:0B:9E	Modbus Router 7.05	ON-LINE
Device 00:0D:81:09:0E:C3	EN-DB9/RJ45-DIN	10.8.11.70	00:0D:81:09:0E:C3	EtherNet/IP 7.14	OFF-LINE
Device 00:0D:81:09:61:0B	PN-4DB9/2RJ45-DIN	10.8.0.187	00:0D:81:09:61:0B	PROFINET IO V 3.4.2	ON-LINE
Device 9706-000036	ICE3		00:0D:81:08:CD:08	PROFINET IO 1.5.37	ON-LINE
Device 9708-000061	ICE2		00:0D:81:08:C1:29	EtherNet/IP 1.5.37	ON-LINE
Device 9710-000064	ICE2		00:0D:81:09:0C:8A	EtherNet/IP 1.5.37	ON-LINE

3. Suchen Sie die Firmware-Datei (**.cmtl**). Klicken Sie auf **Open** (*neue Firmware suchen*), und klicken Sie dann auf **Yes** (*Firmware hochladen*).
Es kann einige Minuten dauern, bis die Firmware auf den ICDM-RX hochgeladen wird. Der ICDM-RX startet beim Hochladen neu.
4. Klicken Sie in der Hinweismeldung auf **Ok** (gibt vor, dass Sie mit der Verwendung des Geräts warten sollen, bis der Status **ON-LINE** lautet).

Im nächsten Abfragezyklus aktualisiert PortVision DX das Teilfenster *Device List* und zeigt die neue Firmwareversion an.

3/26/20

6.3. Konfigurieren mehrerer ICDM-RX-Netzwerkadressen

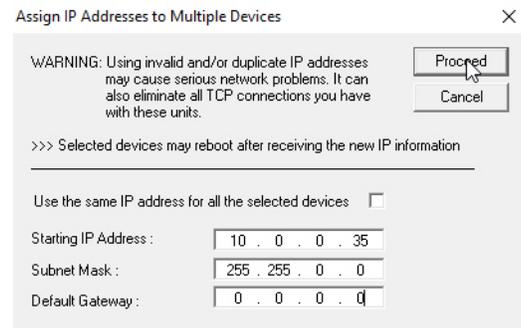
Sie können die Netzwerkadressen für mehrere ICDM-RX-Einheiten mit der Option **Assign IP to Multiple Devices** konfigurieren.

Darüber hinaus können Sie allgemeine Einstellungen für die ICDM-RX -Webseite konfigurieren und die Einstellungen in einer Konfigurationsdatei speichern, die Sie in alle oder ausgewählte ICDM-RX-Einheiten laden können.

Damit dieses Verfahren funktioniert, müssen sich die ICDM-RX-Einheiten im selben Netzwerksegment befinden. Gehen Sie wie folgt vor, um mehrere ICDM-RX-Einheiten zu konfigurieren.

1. Wenn Sie dies nicht getan haben, installieren Sie PortVision DX (*Installation von PortVision DX* auf Seite 22), und scannen Sie mit **Scan** das Netzwerk.
2. Klicken Sie bei gedrückter Umschalttaste auf die ICDM-RX-Einheiten, deren Netzwerkinformationen Sie programmieren möchten. Klicken Sie mit der rechten Maustaste, und klicken Sie dann auf **Advanced > Assign IP to Multiple Devices**.
3. Geben Sie die Start-IP-Adresse, die Subnetzmaske und das IP-Gateway ein. Klicken Sie auf **Proceed**.

PortVision DX zeigt die programmierten IP-Adressen nach dem nächsten Aktualisierungszyklus im Teilfenster *Device List* an.



6.4. Neues Gerät in PortVision DX hinzufügen

Sie können einen neuen ICDM-RX manuell hinzufügen, wenn Sie das Netzwerk nicht nach neuen ICDM-RX-Einheiten durchsuchen möchten. In bestimmten Fällen können Sie jedoch das Fenster *Add New Device* verwenden, um Folgendes zu tun:

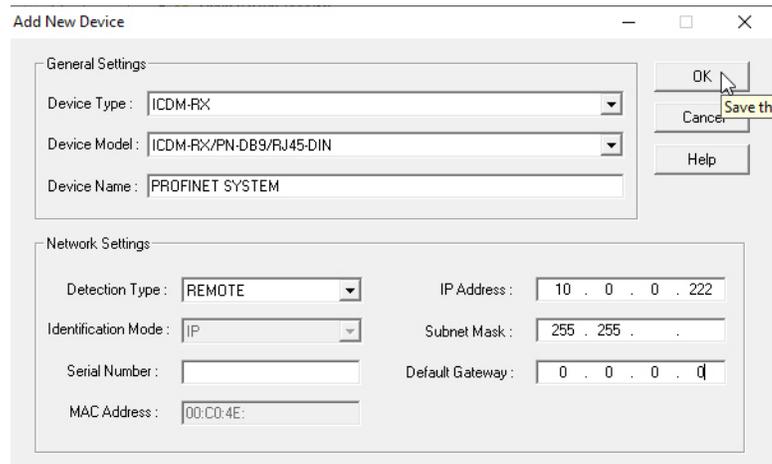
- Konfigurieren Sie die ICDM-RX-Einheiten, die sich nicht im lokalen Netzwerk (Remote) befinden, gemäß *Remote-Einheit mit IP-Adresse* auf Seite 71.
- Vorkonfigurieren Sie einen ICDM-RX in PortVision DX (lokal) gemäß *Lokale Einheit mit IP-Adresse oder MAC-Adresse* auf Seite 72.

6.4.1. Remote-Einheit mit IP-Adresse

Gehen Sie wie folgt vor, um eine ICDM-RX-Remote-Einheit in PortVision DX hinzuzufügen.

1. Öffnen Sie das Fenster *New Device* anhand einer der folgenden Methoden:
 - Klicken Sie im Menü *Manage* auf **Add New > Device**.
 - Klicken Sie mit der rechten Maustaste auf einen Ordner oder einen RocketLinx-Switch im Teilfenster *Device Tree* (an einem beliebigen Punkt, sofern kein ICDM-RX markiert ist und Sie sich in einem gültigen Ordner befinden), und klicken Sie auf **Add New > Device**.
2. Wählen Sie den entsprechenden ICDM-RX in der Drop-Down-Liste **Device Type** aus.
3. Wählen Sie das entsprechende Modell in der Drop-Down-Liste **Device Model** aus.
4. Geben Sie einen Gerätenamen in das Listenfeld **Device Name** ein.
5. Wählen Sie **REMOTE** als *Detection Type*.
6. Geben Sie optional die Seriennummer in das Listenfeld **Serial Number** ein.

7. Geben Sie die IP-Adresse für den ICDM-RX ein. Es ist nicht nötig, die Subnetzmaske und das Standard-Gateway einzugeben.

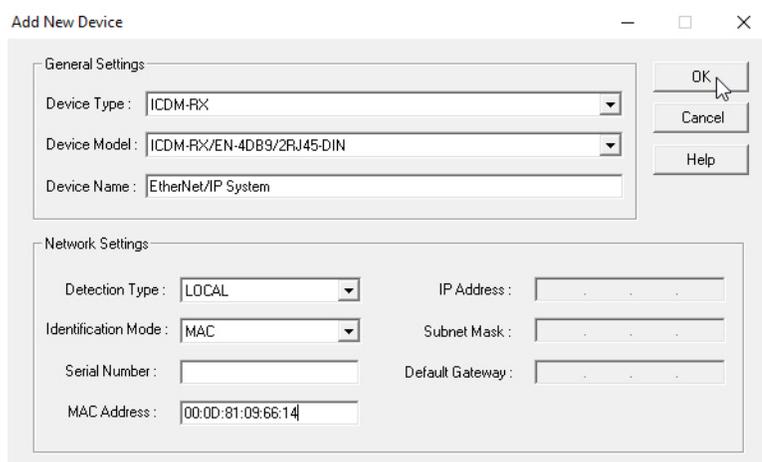


8. Klicken Sie auf **Ok**, um das Fenster *Add New Device* zu schließen. Es kann einige Minuten dauern, bis der ICDM-RX gespeichert wird.
9. Klicken Sie bei Bedarf auf **Refresh**, damit der neue ICDM-RX im Teilfenster *Device Tree* oder *Device List* angezeigt wird. Der ICDM-RX zeigt „OFF-LINE“ an, wenn er nicht mit dem Netzwerk verbunden ist oder eine falsche IP-Adresse eingegeben wurde.

6.4.2. Lokale Einheit mit IP-Adresse oder MAC-Adresse

Gehen Sie wie folgt vor, um eine lokale ICDM-RX-Einheit in PortVision DX hinzuzufügen, sofern Sie das Netzwerk nicht scannen möchten.

1. Suchen Sie die Netzwerkinformationen oder die MAC-Adresse des ICDM-RX, den Sie hinzufügen möchten.
2. Öffnen Sie das Fenster *New Device* anhand einer der folgenden Methoden:
 - Klicken Sie im Menü *Manage* auf **Add New > Device**.
 - Klicken Sie mit der rechten Maustaste auf einen Ordner oder einen RocketLinx-Switch im Teilfenster *Device Tree* (an einem beliebigen Punkt, sofern kein ICDM-RX markiert ist und Sie sich in einem gültigen Ordner befinden), und klicken Sie auf **Add New > Device**.
3. Wählen Sie den entsprechenden ICDM-RX in der Drop-Down-Liste **Device Type** aus.



4. Wählen Sie das entsprechende Modell in der Drop-Down-Liste **Device Model** aus.
5. Geben Sie einen Gerätenamen in das Listenfeld **Device Name** ein.
6. Wählen Sie **LOCAL** als *Detection Type*.
7. Geben Sie die MAC-Adresse oder die Netzwerkinformationen ein.
Note: *An allen ICDM-RX-Einheiten ist ein MAC-Adressenschild angebracht.*
8. Geben Sie optional die Seriennummer in das Listenfeld **Serial Number** ein.
9. Klicken Sie auf **Ok**.
10. Klicken Sie bei Bedarf auf **Refresh**, damit der neue ICDM-RX im Teilfenster *Device Tree* oder *Device List* angezeigt wird. Der ICDM-RX zeigt „OFF-LINE“ an, wenn er nicht mit dem Netzwerk verbunden ist oder eine falsche IP-Adresse eingegeben wurde.

6.5. Ändern der Bootloader-Zeitüberschreitung

Gehen Sie wie folgt vor, um die Bootloader-Zeitüberschreitung auf 45 Sekunden zu ändern. Mit diesem Verfahren können Sie nach dem erfolgreichen Hochladen von SocketServer die Bootloader-Zeitüberschreitung auf 15 Sekunden zurücksetzen.

1. Verwenden Sie bei Bedarf Ihren Browser, um über die IP-Adresse auf den ICDM-RX zuzugreifen.
2. Klicken Sie auf **Network**.
3. Geben Sie in das Feld **Boot Timeout** den Wert 45 ein, und klicken Sie auf **Save**.

The screenshot shows the web interface for the ICDM-RX. The top navigation bar includes 'CONTROL', 'Home', 'Serial', 'Ethernet', 'Network', 'Diagnostics', 'System', 'ICDM-RX/PN-DB9/RJ45-DIN', and 'Logout'. Below this, a secondary navigation bar has 'Configuration', 'Password', 'Security', 'Keys/Certs', and 'PROFINET IO'. The main content area is titled 'Network Configuration' and is divided into two panels: 'General' and 'IPv4'. In the 'General' panel, the 'Device Name' is 'icdmr1p1e', 'TCP Keepalive' is 60 s, 'Boot Timeout' is 15 s (highlighted with a red box), and 'Telnet Timeout' is 300 s. In the 'IPv4' panel, 'Use DHCP' and 'Use PLC assigned' are unselected, while 'Use static config below' is selected. Below this, the 'Address' is 10.8.9.185, 'Subnet Mask' is 255.255.0.0, and 'Default Gateway' is empty. A green 'Save' button is located at the bottom right of the configuration area. The footer of the page reads '© Pepper+Fuchs Control, Inc.'.

Note: Sie sollten den Wert für die Bootloader-Zeitüberschreitung nach dem Hochladen der Firmware wieder auf 15 Sekunden zurücksetzen.

6.6. Verwenden von Konfigurationsdateien

In diesem Unterabschnitt ist beschrieben, wie Sie ICDM-RX-Konfigurationsdateien erstellen (speichern) und laden können. ICDM-RX-Konfigurationsdateien können aus folgenden Gründen erstellt werden:

- Speichern der ICDM-RX-Konfigurationseinstellungen, um diese in ähnliche ICDM-RX-Einheiten laden zu können und Zeit bei der Konfiguration von ICDM-RX zu sparen.
- Speichern der ICDM-RX-Konfigurationseinstellungen, weil Sie eine neue Firmwareversion installieren müssen und die alten Konfigurationseinstellungen mit der neuen Firmwareversion laden möchten.

6.6.1. Speichern von Konfigurationsdateien

Hier ist beschrieben, wie Sie Konfigurationsdateien speichern können.

1. Geben Sie die IP-Adresse in Ihren Browser ein, um die Webschnittstelle zu öffnen.
2. Klicken Sie auf **System | Configuration File**.
3. Klicken Sie auf die Schaltfläche **Save Configuration**.

The screenshot shows the 'Configuration File' page of the ICDM-RX web interface. The top navigation bar includes 'CONTROL Pepperl+Fuchs', 'Home', 'Serial', 'Ethernet', 'Network', 'Diagnostics', 'System', and 'Logout'. Below the navigation bar, there are tabs for 'Update Firmware', 'Configuration File', 'System Snapshot', 'Restore Defaults', and 'Reboot'. The main content area is titled 'Configuration File' and contains two sections: 'Save Configuration' and 'Load Configuration'. The 'Save Configuration' section has a text box with the instruction 'To save this ICDM-RX's configuration to a file on your PC, click "Save Configuration"' and a 'Save Configuration' button. The 'Load Configuration' section has a text box with the instruction 'To load a configuration file to this ICDM-RX, select the file, and then click "Load Configuration"', a 'Configuration file:' label, a text input field, a 'Browse' button, and a 'Load Configuration' button. The footer of the page reads '© Pepperl+Fuchs Control, Inc.'.

4. Je nach Browser müssen Sie auf „Speichern“ klicken oder zu einem bestimmten Ablageort navigieren.

6.6.2. Laden von Konfigurationsdateien

Verwenden Sie das folgende Verfahren, um Konfigurationsdateien zu laden.

1. Geben Sie bei Bedarf die IP-Adresse in Ihren Browser ein.
2. Klicken Sie auf **System | Configuration File**.
3. Klicken Sie auf die Schaltfläche **Browse**, und wählen Sie die Konfigurationsdatei aus. Der voreingestellte Name der Konfigurationsdatei lautet:
dm_xxx.xxx.xxx.xxx.ds
Dabei steht *xxx.xxx.xxx.xxx* für die IP-Adresse, und *.ds* ist die Dateierweiterung.
4. Klicken Sie auf die Schaltfläche **Load Configuration**.

The screenshot shows the web interface for ICDM-RX hardware configuration. At the top, there is a navigation bar with the 'CONTROL' logo and menu items: Home, Serial, Ethernet, Network, Diagnostics, System, ICDM-RX/PN-089/R345-DIN, and Logout. Below this is a secondary menu with 'Update Firmware', 'Configuration File' (highlighted), 'System Snapshot', 'Restore Defaults', and 'Reboot'. The main content area is titled 'Configuration File' and is divided into two sections: 'Save Configuration' and 'Load Configuration'. The 'Save Configuration' section contains a text box with instructions and a 'Save Configuration' button. The 'Load Configuration' section contains a text box with instructions, a text input field with the value 'dm_icdmt1p1e.ds', a 'Browse' button, and a 'Load Configuration' button. Red annotations with numbers 1 and 2 point to the 'Browse' and 'Load Configuration' buttons respectively. The footer of the page reads '© Pepperl+Fuchs Control, Inc.'

6.7. Verwalten des Bootloaders

Bootloader bezieht sich auf das Betriebssystem, das während der Einschaltphase auf der ICDM-RX-Hardware ausgeführt wird und dann die Standardanwendung (z. B. EtherNET/IP, Ethernet/IP zu Modbus, Modbus-Router, PROFINET IO, oder PROFINET IO zu Modbus-Firmware) lädt.

Note: In der Regel sollten Sie den Bootloader nur aktualisieren, wenn Sie vom technischen Pepperl + Fuchs-Support dazu aufgefordert werden.

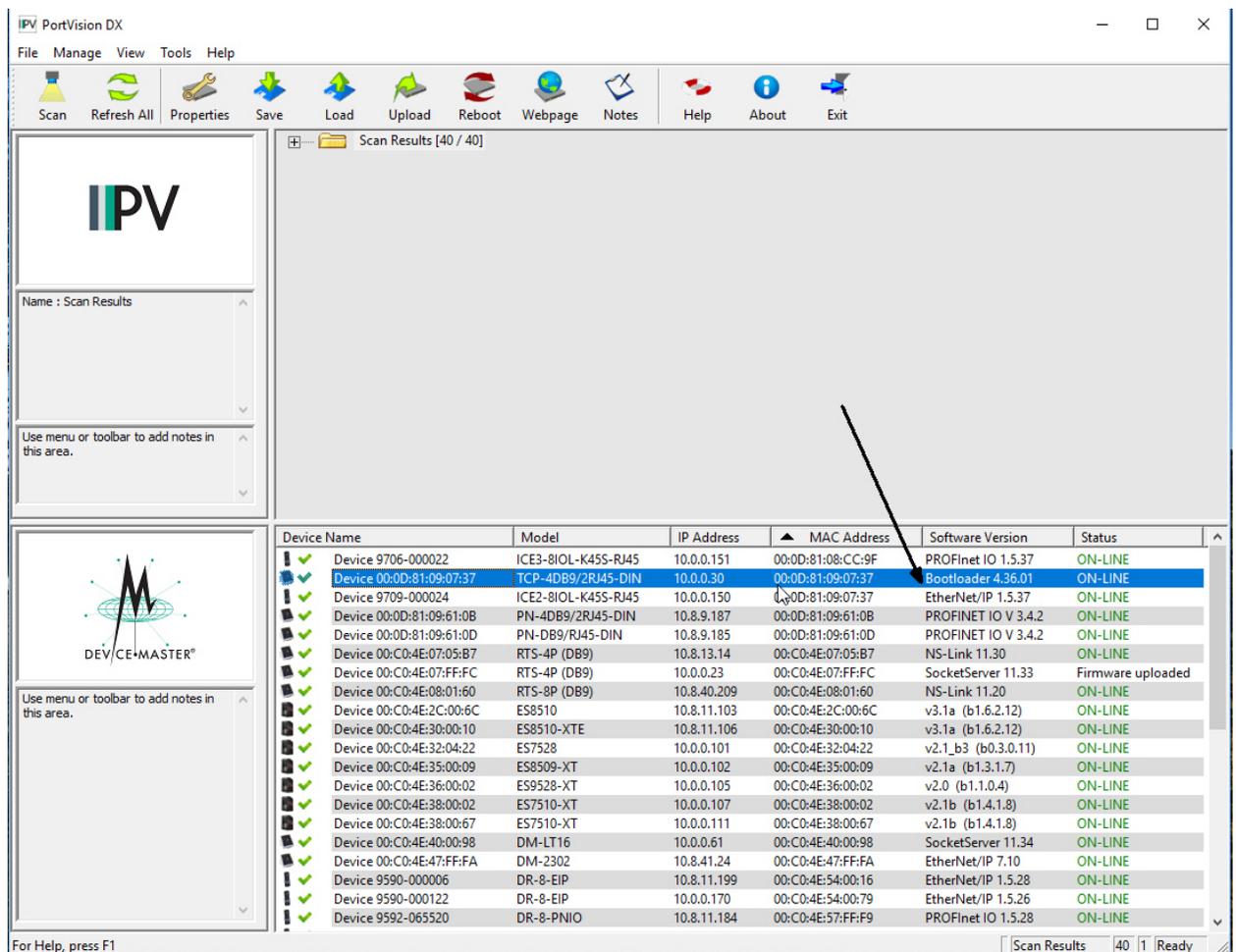
Es gibt verschiedene Methoden und Tools, mit denen Sie die Bootloader-Version überprüfen oder den Bootloader aktualisieren können.

- **PortVision DX** ist die einfachste Möglichkeit, die Bootloader-Version zu überprüfen und die neueste Version hochzuladen.
- Optional kann RedBoot verwendet werden, um die Bootloader-Version zu überprüfen und den Bootloader zu aktualisieren. Weitere Informationen finden Sie unter *RedBoot-Verfahren* auf Seite 85.

6.7.1. Überprüfen der Bootloader-Version

Im folgenden Verfahren wird die Bootloader-Version mit PortVision DX überprüft. Optional können Sie RedBoot verwenden, siehe *Ermitteln der Bootloader-Version* auf Seite 89.

1. Wenn Sie dies nicht getan haben, installieren Sie PortVision DX (*Installation von PortVision DX* auf Seite 22), und scannen Sie mit **Scan** das Netzwerk.
2. Klicken Sie mit der rechten Maustaste auf den ICDM-RX im Teilfenster *Device List*. Klicken Sie dann auf **Advanced > Reboot**.
3. Klicken Sie auf **Yes**, um die Abfrage *Confirm Reboot* zu bestätigen.
4. Klicken Sie mit der rechten Maustaste im Teilfenster *Device List* auf den ICDM-RX. Klicken Sie auf **Refresh**. Sie müssen dies möglicherweise mehrmals tun, bis Sie den Neustartzyklus im Teilfenster *Device List* sehen. Die Bootloader-Version wird beim Neustartvorgang kurz vor dem Laden der Anwendung (z. B. EtherNET/IP, Ethernet/IP zu Modbus, Modbus-Router, PROFINET IO, oder PROFINET IO zu Modbus-Firmware) angezeigt.
5. Überprüfen Sie auf der Website <https://www.pepperl-fuchs.com>, ob eine neuere Version des Bootloaders verfügbar ist.



6. Gehen Sie zum nächsten Unterabschnitt, wenn Sie eine neue Version des Bootloaders hochladen müssen.

6.7.2. Hochladen des Bootloaders

Gehen Sie wie folgt vor, um den Bootloader in den ICDM-RX hochzuladen. In der Regel sollten Sie den Bootloader nur aktualisieren, wenn Sie vom technischen Pepperl + Fuchs-Support dazu aufgefordert werden oder auf <https://www.pepperl-fuchs.com> eine Benachrichtigung mit der Firmware veröffentlicht wurde.

Note: Der technische Support rät davon ab, den Bootloader über ein WAN zu aktualisieren. Die besten Ergebnisse erzielen Sie, wenn Sie den ICDM-RX direkt an einen PC oder Laptop anschließen, um den Bootloader hochzuladen.



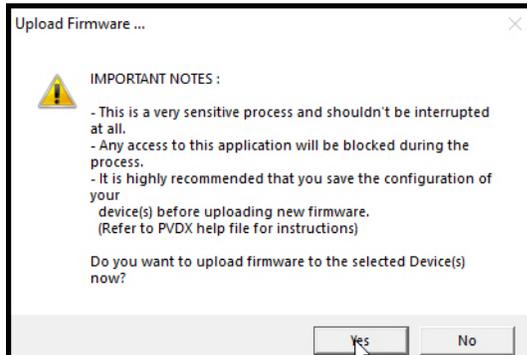
Stellen Sie sicher, dass die Stromversorgung beim Hochladen des Bootloaders nicht unterbrochen wird. Nach einer Unterbrechung der Stromversorgung beim Hochladen des Bootloaders muss der ICDM-RX an Pepperl + Fuchs gesendet werden, damit er neu programmiert werden kann.

Wenn Sie die Firmware nicht in den ICDM-RX hochladen können, laden Sie den Bootloader nicht hoch.

1. Wenn Sie dies nicht getan haben, installieren Sie PortVision DX (*Installation von PortVision DX* auf Seite 22), und scannen Sie mit **Scan** das Netzwerk.
2. Überprüfen Sie bei Bedarf die Bootloader-Version (*Überprüfen der Bootloader-Version* auf Seite 76), und laden Sie die neueste Version herunter.
3. Klicken Sie mit der rechten Maustaste auf den ICDM-RX, den Sie aktualisieren möchten. Klicken Sie auf **Advanced > Upload Firmware**. Navigieren Sie zur Bootloader-Datei **.cmtl**, und klicken Sie dann auf **Open**.

Device Name	Model	IP Address	MAC Address	Software Version	Status
Device 9706-000022	ICE3-BIOL-K455-RJ45	10.0.0.151	00:0D:81:08:CC:9F	PROFINET IO 1.5.37	ON-LINE
Device 00:0D:81:09:07:37		10.0.0.30	00:0D:81:09:07:37	SocketServer 11.37	ON-LINE
Device 9709-000024		10.0.0.150	00:0D:81:09:07:37	EtherNet/IP 1.5.37	ON-LINE
Device 00:0D:81:09:06	Refresh Device	10.8.9.187	00:0D:81:09:61:08	PROFINET IO V 3.4.2	ON-LINE
Device 00:0D:81:09:06	Properties	10.8.9.185	00:0D:81:09:61:0D	PROFINET IO V 3.4.2	ON-LINE
Device 00:0D:81:09:06	Edit Notes	10.8.13.14	00:C0:4E:07:05:B7	NS-Link 11.30	ON-LINE
Device 00:C0:4E:07:05	Webpage	10.0.0.23	00:C0:4E:07:FF:FC	SocketServer 11.33	ON-LINE
Device 00:C0:4E:08:00	Telnet / SSH Session	10.8.40.209	00:C0:4E:08:01:60	NS-Link 11.20	ON-LINE
Device 00:C0:4E:2C:00		10.8.11.103	00:C0:4E:2C:00:6C	v3.1a (b1.6.2.12)	ON-LINE
Device 00:C0:4E:30:00	Advanced >			3.1a (b1.6.2.12)	ON-LINE
Device 00:C0:4E:32:00	Configuration >			2.1_b3 (b0.3.0.11)	ON-LINE
Device 00:C0:4E:35:00	Tracker >			2.1a (b1.3.1.7)	ON-LINE
Device 00:C0:4E:36:00				2.0 (b1.1.0.4)	ON-LINE
Device 00:C0:4E:38:00	Rename			2.1b (b1.4.1.8)	ON-LINE
Device 00:C0:4E:38:00	Move			2.1b (b1.4.1.8)	ON-LINE
Device 00:C0:4E:40:00	Delete			SocketServer 11.34	ON-LINE
Device 00:C0:4E:47:FF		10.8.41.24	00:C0:4E:47:FF:FA	EtherNet/IP 7.10	ON-LINE
Device 9590-000006		10.8.11.199	00:C0:4E:54:00:16	EtherNet/IP 1.5.28	ON-LINE
Device 9590-000122		10.0.0.170	00:C0:4E:54:00:79	EtherNet/IP 1.5.26	ON-LINE
Device 9592-065520	DR-8-PNIO	10.8.11.184	00:C0:4E:57:FF:F9	PROFINET IO 1.5.28	ON-LINE

- Klicken Sie auf **Yes** in der Meldung *Upload Firmware*, die Sie darauf hinweist, dass es sich um einen sensiblen Prozess handelt.



- Klicken Sie in der zweiten Meldung *Upload Firmware* auf **Ok**.
- Klicken Sie mit der rechten Maustaste auf den ICDM-RX, und klicken Sie auf **Refresh**, bis die Bootloader-Version im Teilfenster *Device List* angezeigt wird. Überprüfen Sie, ob die neue Version geladen wurde.

6.8. Wiederherstellen der Werkseinstellungen (spezifische Modelle – Reset-Schaltfläche)

Gehen Sie wie folgt vor, um die ICDM-RX-Hutschienenmodelle auf die Werkseinstellungen zurückzusetzen. Informationen zum Wiederherstellen der Port-Standard Einstellungen siehe *Wiederherstellen der Standardwerte* auf Seite 80.

Wenn Sie vom technischen Support aufgefordert werden, die ICDM-RX-Werkseinstellungen wiederherzustellen, drücken Sie den Schalter **Reset/Restore** länger als 5 Sekunden.

Modell	Position zurücksetzen
ICDM-RX/xxx-DB9/RJ45-DIN ICDM-RX/xxx-ST/RJ45-DIN	Loch für die Taste zum Zurücksetzen links neben der STATUS-LED.



Modell	Position zurücksetzen
ICDM-RX/ xxx -2DB9RJ45-DIN	<p>Loch für die Taste zum Zurücksetzen unter dem Logo auf der linken oberen Seite.</p> 
ICDM-RX/ xxx -2ST/RJ45-DIN	<p>Loch für die Taste zum Zurücksetzen unterhalb des Ethernet-Ports und über dem Logo.</p> 
ICDM-RX/ xxx -4DB9/2RJ45-DIN	<p>Loch für die Taste zum Zurücksetzen unter dem Logo auf der linken oberen Seite.</p> 

3/26/20

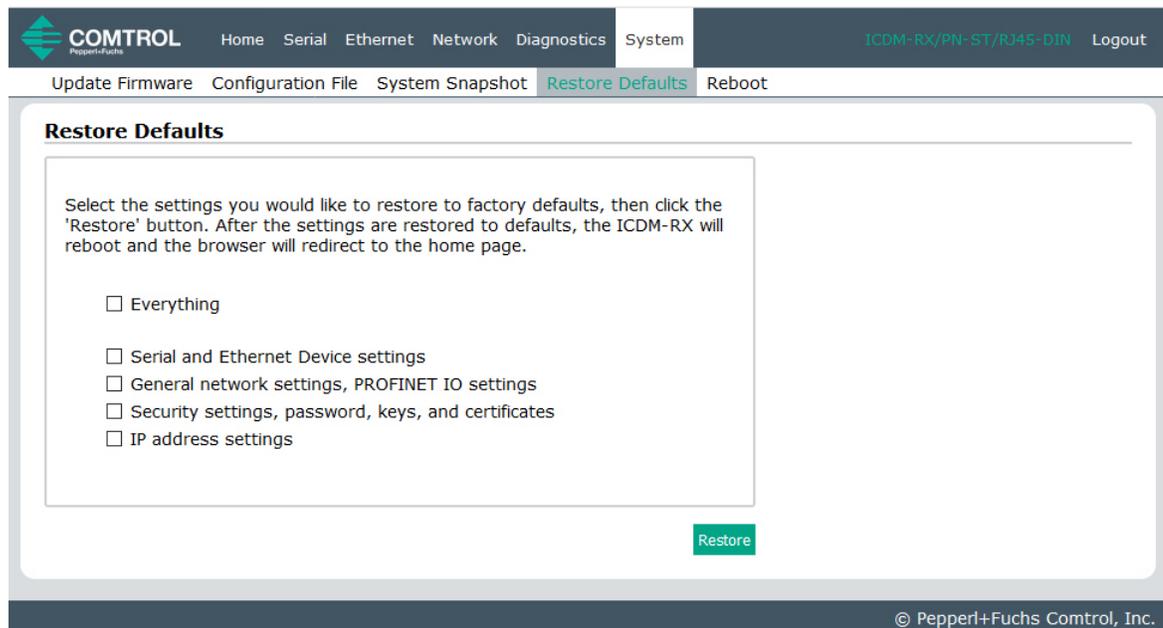
Beim Wiederherstellen der ICDM-RX-Hutschienenmodelle werden die folgenden Einstellungen auf die Werkseinstellungen zurückgesetzt:

- Port-Einstellungen
- Netzwerkeinstellungen
- Password
- Telnet-Aktivierung
- Zeitüberschreitung beim Start
- SSL-Aktivierung
- Telnet-Zeitüberschreitung

6.9. Wiederherstellen der Standardwerte

Mit dem folgenden Verfahren können Sie einige oder alle ICDM-RX-Einstellungen auf die Werkseinstellungen zurücksetzen.

1. Öffnen Sie die Webschnittstelle, indem Sie die IP-Adresse in Ihren Browser eingeben.
2. Klicken Sie auf **System | Restore Defaults**.
3. Wählen Sie aus, welche Elemente Sie auf Werkseinstellungen zurücksetzen möchten.
4. Klicken Sie auf die Schaltfläche **Restore**.

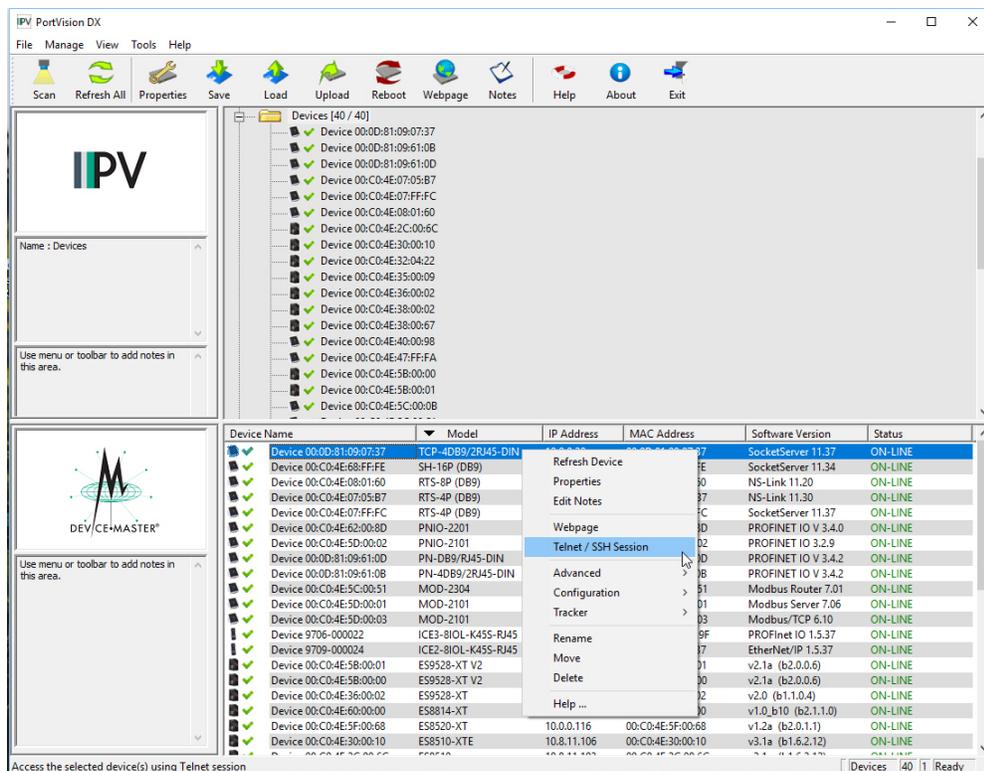


Note: Dieser Screenshot zeigt die wiederherzustellenden Standardwerte für PROFINET IO, jedes ICDM-RX Industrial Gateway enthält protokollspezifische Einstellungen.

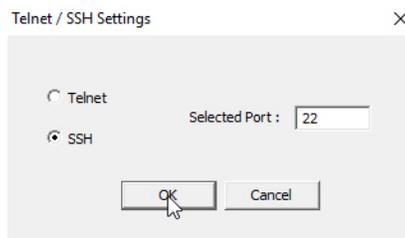
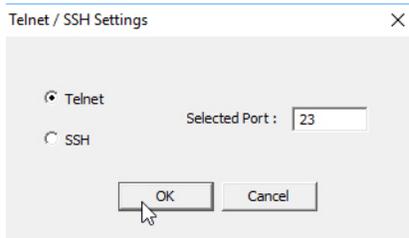
6.10. Zugreifen auf RedBoot-Befehle in Telnet-/SSH-Sitzungen (PortVision DX)

Sie können eine Telnet- oder SSH-Sitzung mit PortVision DX öffnen, um auf RedBoot-Befehle zuzugreifen. Gehen Sie wie folgt vor, um mit PortVision DX auf eine Telnet- oder SSH-Sitzung zuzugreifen.

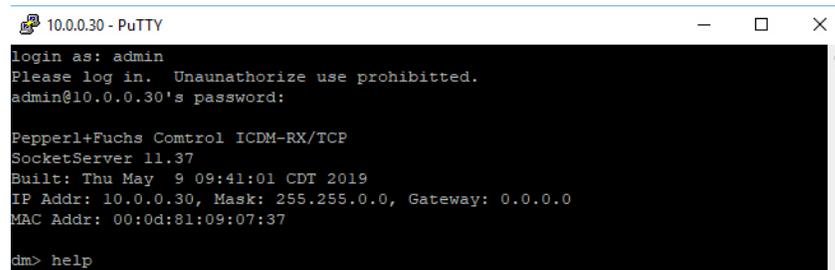
1. Klicken Sie in PortVision DX, PortVision DX, mit der rechten Maustaste im Teilfenster *Device List* auf den ICDM-RX, für den Sie eine Telnet-Sitzung öffnen möchten. Klicken Sie dann auf **Telnet/SSH Session**.



2. Wählen Sie **Telnet** oder **SSH**. Lassen Sie die Nummer **Selected Port** unverändert, und klicken Sie auf **Ok**.



3. Geben Sie ggf. das Passwort ein, und drücken Sie **Enter**. Wenn kein Passwort festgelegt wurde, drücken Sie **Enter**. Wenn Sie eine SSH-Sitzung verwenden, geben Sie **admin** als Anmeldedaten ein, und drücken Sie **Enter**.



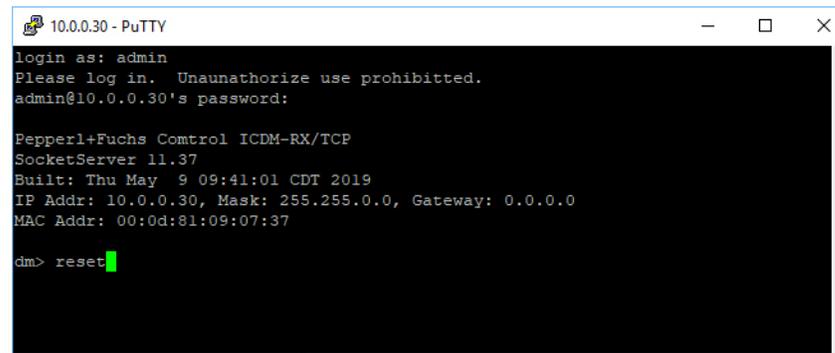
```
10.0.0.30 - PuTTY
login as: admin
Please log in.  Unaunauthorize use prohibited.
admin@10.0.0.30's password:

Pepperl+Fuchs Control ICDM-RX/TCP
SocketServer 11.37
Built: Thu May  9 09:41:01 CDT 2019
IP Addr: 10.0.0.30, Mask: 255.255.0.0, Gateway: 0.0.0.0
MAC Addr: 00:0d:81:09:07:37

dm> help
```

Wenn der PuTTY-Bildschirm im Hintergrund blinkt und nicht wie oben dargestellt angezeigt wird, stellen Sie sicher, dass **Enable Telnet/ssh** auf der Webseite nicht deaktiviert wurde. Um dies zu überprüfen, kehren Sie zu PortVision DX zurück, klicken Sie mit der rechten Maustaste auf den ICDM-RX im Teilfenster *Device List*, und klicken Sie auf **Webpage**. Klicken Sie auf **Network | Security**, und überprüfen Sie, ob die Option **Enable Telnet/ssh** aktiviert ist. Ist dies nicht der Fall, klicken Sie auf die Option und dann auf **Save**. Schließen Sie die Webschnittstelle.

4. Geben Sie **Reset** ein, drücken Sie **Enter**, und schließen Sie die Telnet-Sitzung.

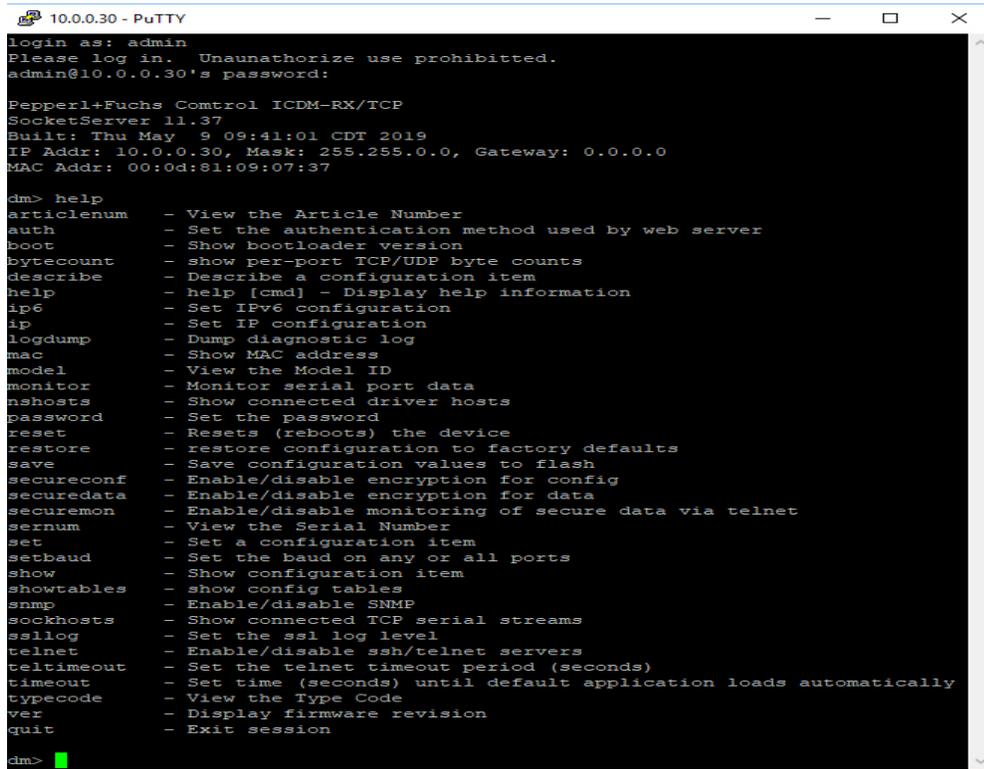


```
10.0.0.30 - PuTTY
login as: admin
Please log in.  Unaunauthorize use prohibited.
admin@10.0.0.30's password:

Pepperl+Fuchs Control ICDM-RX/TCP
SocketServer 11.37
Built: Thu May  9 09:41:01 CDT 2019
IP Addr: 10.0.0.30, Mask: 255.255.0.0, Gateway: 0.0.0.0
MAC Addr: 00:0d:81:09:07:37

dm> reset
```

5. Öffnen Sie die Telnet- oder SSH-Sitzung rasch erneut, indem Sie die vorherigen Schritte ausführen.



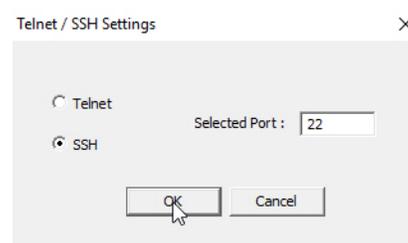
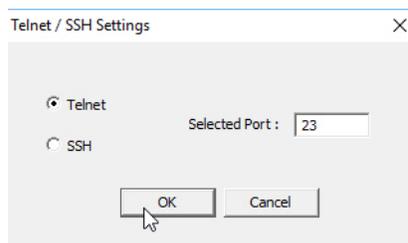
```
10.0.0.30 - PuTTY
login as: admin
Please log in. Unauthenticated use prohibited.
admin@10.0.0.30's password:

Pepperl+Fuchs Control ICDM-RX/TCP
SocketServer 11.37
Built: Thu May  9 09:41:01 CDT 2019
IP Addr: 10.0.0.30, Mask: 255.255.0.0, Gateway: 0.0.0.0
MAC Addr: 00:0d:81:09:07:37

dm> help
articlenum - View the Article Number
auth       - Set the authentication method used by web server
boot       - Show bootloader version
bytecount  - show per-port TCP/UDP byte counts
describe   - Describe a configuration item
help       - help [cmd] - Display help information
ip6        - Set IPv6 configuration
ip         - Set IP configuration
logdump    - Dump diagnostic log
mac        - Show MAC address
model      - View the Model ID
monitor    - Monitor serial port data
nshosts    - Show connected driver hosts
password   - Set the password
reset      - Resets (reboots) the device
restore    - restore configuration to factory defaults
save       - Save configuration values to flash
secureconf - Enable/disable encryption for config
securedata - Enable/disable encryption for data
securemon  - Enable/disable monitoring of secure data via telnet
sernum     - View the Serial Number
set        - Set a configuration item
setbaud    - Set the baud on any or all ports
show       - Show configuration item
showtables - show config tables
snmp       - Enable/disable SNMP
sockhosts  - Show connected TCP serial streams
ssllog     - Set the ssl log level
telnet     - Enable/disable ssh/telnet servers
telnetout  - Set the telnet timeout period (seconds)
timeout    - Set time (seconds) until default application loads automatically
typecode   - View the Type Code
ver        - Display firmware revision
quit      - Exit session

dm>
```

6. Wählen Sie **Telnet** oder **SSH**. Lassen Sie die Nummer **Selected Port** unverändert, und klicken Sie auf **Ok**.



7. Drücken Sie **Enter**. Sie können **help** eingeben, um die RedBoot-Befehle zu überprüfen. Weitere Informationen finden Sie unter *RedBoot-Befehlsübersicht* auf Seite 91.

```
10.0.0.30 - PuTTY
ver
*****
**
**  Comtrol DeviceMaster and ICDM-RX Bootloader 4.36.01
**  Platform: Comtrol DeviceMaster (Cortex-M3)
**  RedBoot(tm) environment - built 15:00:45, Jun  6 2019
**  Portions Copyright (C) 2000, Red Hat, Inc.
**  Portions Copyright (C) Pepperl+Fuchs Comtrol, Inc.
**
*****

RAM: 0x10000000-0x10018000 [0x100018d4-0x1000bc6a available]
      0x10080000-0x1008a000 [0x10080000-0x1008a000 available]
      0x20000000-0x20010000 [0x20000000-0x20010000 available]
      0x28000000-0x29000000 [0x28000000-0x29000000 available]
FLASH: 0x14000000-0x147fffff, 2048 x 0x1000 blocks
RedBoot> help
Set/show web authentication
  auth [noaccess,none,basic,md5,invalid]
Set/Query the system console baud rate
  baudrate [-b <rate>]
Show/set Board revision
  boardrev [rev-number]
Manage machine caches
  cache [ON | OFF]
Show/set catalog number
  catalognum [catalog number]
Display/switch console channel
  channel [-1|<channel number>]
Show chassis features
  chassis
Compute a 32bit checksum [POSIX algorithm] for a range of memory
  cksum -b <location> -l <length>
Clear application configuration
  clearconfig
Show/Set CPU clock frequency
  cpufreq
Calibrate SDRAM clock delay
  delaycal <passes>
Show/set Device Id
  deviceid [device id]
Disable program loading
  disable
Display (hex dump) a range of memory
  dump -b <location> [-l <length>] [-s] [-1|-2|-4]
Show/set eeprom version
  eepromvers [ver]
Manage FLASH images
  fis {cmds}
Show flash info
  flash
Execute code at a location
  go [-w <timeout>] [-c] [-n] [entry]
Help about help?
  help [<topic>]
Display command history
  history
Show/set HW feature flags
  hwflags [flags]
Show/set IP address config
```

Note: Die *dm*-Eingabeaufforderung sollte durch eine RedBoot-Eingabeaufforderung ersetzt werden. Falls nicht, können Sie die Bootloader-Zeitüberschreitung für eine längere Zeitdauer zurücksetzen und dieses Verfahren wiederholen.

7. RedBoot-Verfahren

Sie können diesen Abschnitt als Referenz verwenden, wenn Sie Aufgaben in RedBoot ausführen möchten.

- *Zugreifen auf die RedBoot-Übersicht* auf Seite 85
- *Einrichten einer seriellen Verbindung* auf Seite 86
- *Einrichten einer Telnet-Verbindung* auf Seite 87
- *Festlegen der Netzwerkeinstellungen* auf Seite 88
- *Konfigurieren der Netzwerkeinstellungen* auf Seite 88
- *Ändern der Bootloader-Zeitüberschreitung* auf Seite 89
- *Ermitteln der Bootloader-Version* auf Seite 89
- *Zurücksetzen des ICDM-RX* auf Seite 90
- *Konfigurieren von Passwörtern* auf Seite 90
- *RedBoot-Befehlsübersicht* auf Seite 91

Optional können Sie PortVision DX auf einem Windows-System im Netzwerk installieren und alle diese Aufgaben ausführen. PortVision DX stellt eine Telnet/SSH-Sitzung bereit, die unter *Zugreifen auf RedBoot-Befehle in Telnet-/SSH-Sitzungen (PortVision DX)* auf Seite 81 beschrieben ist.

7.1. Zugreifen auf die RedBoot-Übersicht

Für den Zugriff auf RedBoot können Sie eine der folgenden Methoden verwenden:

- Eine *serielle* Verbindung zwischen Port 1 am ICDM-RX und einem COM-Port an einem PC (Seite 86). Wenn Sie die serielle Methode verwenden möchten, benötigen Sie ein Nullmodemkabel, ein auf dem PC installiertes und konfiguriertes Terminalprogramm und einen **Bootloader-Timeout**-Wert von mehr als 15 Sekunden. Wenn der Wert **Bootloader Timeout** auf 1 Sekunde reduziert wurde, ist dieses Verfahren NICHT möglich.

Note: *Verwenden Sie die serielle Verbindungsmethode, wenn sich der ICDM-RX nicht im selben Ethernet-Netzwerksegment wie der PC befindet.*

Wenn Sie die IP-Adresse des ICDM-RX nicht kennen, müssen Sie eine serielle Verbindung verwenden, um mit dem ICDM-RX zu kommunizieren.

- Eine *Telnet-Verbindung* (Seite 87), wenn der ICDM-RX lokal über Ethernet zugänglich ist. Für eine *Telnet-Verbindung* müssen Sie die IP-Adresse kennen. Darüber hinaus muss die IP-Adresse auch für das Netzwerk gültig sein, mit dem sie verbunden ist.

Beispiel: Wenn Sie die IP-Adresse nicht geändert haben, um in Ihrem Netzwerk zu arbeiten, muss das Netzwerksegment 192.168.250.x sein, um Telnet zur Standard-IP-Adresse des ICDM-RX zu führen.

7.2. Einrichten einer seriellen Verbindung

Gehen Sie wie folgt vor, um eine serielle Verbindung mit einem Terminalserverprogramm einzurichten. Sie können PuTTY (Windows) verwenden, oder von PortVision DX über **Tools > Applications > PuTTY** optional auf PuTTY zugreifen.

1. Schließen Sie ein Nullmodemkabel von einem verfügbaren COM-Port Ihres PCs an **Port 1** des ICDM-RX an.

Note: Wenn Sie ein Nullmodemkabel konfektionieren müssen, siehe *Anschließen von seriellen Geräten auf Seite 56*.

2. Konfigurieren Sie das Terminalserverprogramm auf die folgenden Werte:

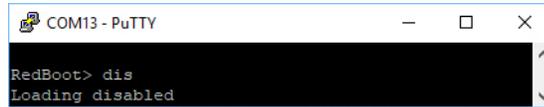
- Bits pro Sekunde = 57.600
- Datenbits = 8
- Parität = keine
- Stoppbits = 1
- Flusssteuerung = keine

Note: Wenn Sie das Laden des Bootloaders (Schritt 3 bis 5) nicht vor der Zeitüberschreitung deaktivieren (Default = 15 Sekunden), wird eine Anwendung aus dem Flash geladen und gestartet. Wiederholen Sie in diesem Fall Schritt 3 bis 5. Der Befehl **#!DM** ist der einzige Befehl, bei dem Groß- und Kleinschreibung beachtet wird. Er muss in Großbuchstaben eingegeben werden.

3. Setzen Sie den ICDM-RX zurück.

Note: Trennen Sie je nach Modell das Netzkabel, und schließen Sie es wieder an (externes Netzteil und kein Netzschalter), oder schalten Sie den Netzschalter ein und wieder aus (internes Netzteil).

4. Geben Sie sofort **#!DM** ein, und drücken Sie **Enter** im Terminalprogramm.



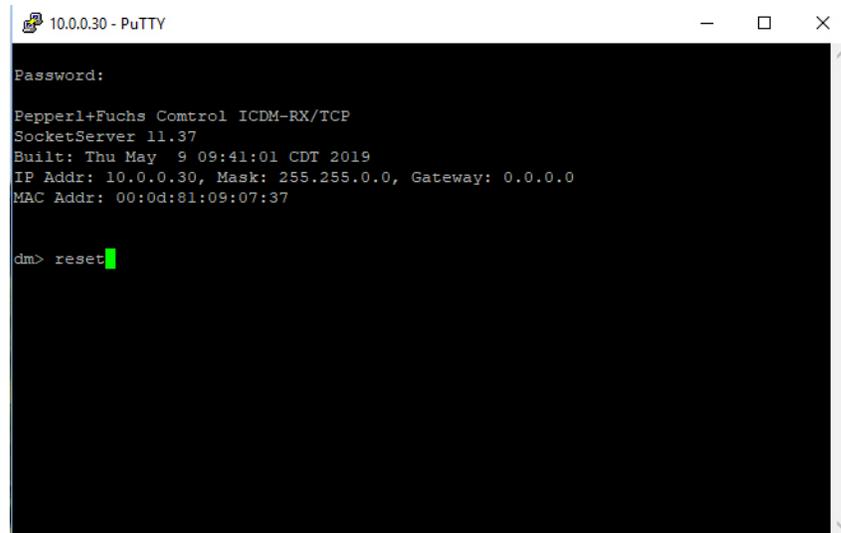
```
COM13 - PuTTY
RedBoot> dis
Loading disabled
```

5. Geben Sie **dis** bei der Eingabeaufforderung **RedBoot>** ein, und drücken Sie **Enter**.
6. Vergewissern Sie sich, dass das Laden deaktiviert wurde.
7. Sie können die gewünschte Aufgabe mit dem Verfahren auf Seite 85 oder gemäß *RedBoot-Befehlsübersicht* auf Seite 91 ausführen.

7.3. Einrichten einer Telnet-Verbindung

Gehen Sie wie folgt vor, um eine Telnet-Verbindung zum ICDM-RX herzustellen.

1. Öffnen Sie eine Telnet-Sitzung, und geben Sie die IP-Adresse des ICDM-RX ein.
Unter Windows können Sie PortVision DX verwenden, siehe *Zugreifen auf RedBoot-Befehle in Telnet-/SSH-Sitzungen (PortVision DX)* auf Seite 81.
2. Drücken Sie **Enter**, wenn Sie kein Passwort programmiert haben, oder geben Sie das Passwort ein, und drücken Sie **Enter**.

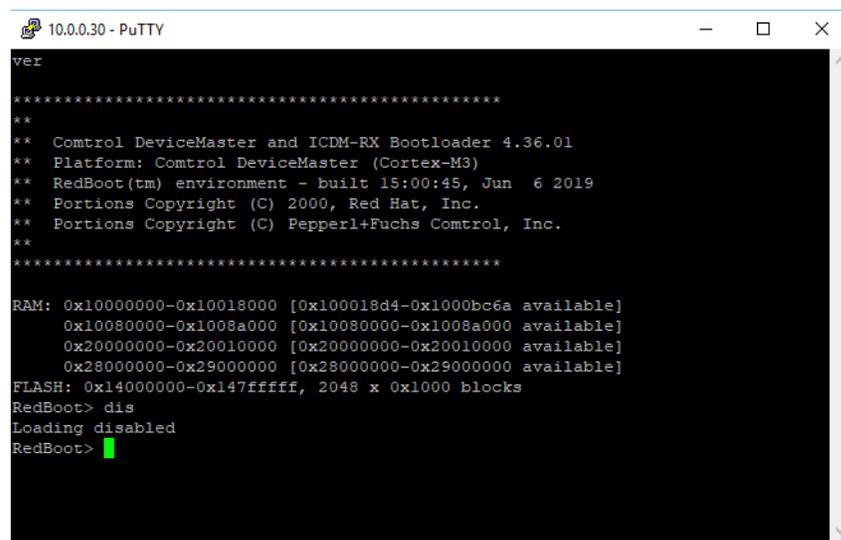


```
10.0.0.30 - PuTTY
Password:
Pepperl+Fuchs Control ICDM-RX/TCP
SocketServer 11.37
Built: Thu May 9 09:41:01 CDT 2019
IP Addr: 10.0.0.30, Mask: 255.255.0.0, Gateway: 0.0.0.0
MAC Addr: 00:0d:81:09:07:37

dm> reset
```

Note: Der ICDM-RX ist nicht mit einem Passwort vorprogrammiert.

3. Geben Sie **reset** ein, und schließen Sie die Sitzung.
4. Öffnen Sie eine neue Telnet-Sitzung. Geben Sie die IP-Adresse des ICDM-RX und das Passwort ein.
5. Geben Sie **dis** ein, um den Bootloader zu deaktivieren.
6. Vergewissern Sie sich, dass das System mit der Meldung **Loading disabled** reagiert.



```
10.0.0.30 - PuTTY
ver
*****
**
** Control DeviceMaster and ICDM-RX Bootloader 4.36.01
** Platform: Control DeviceMaster (Cortex-M3)
** RedBoot(tm) environment - built 15:00:45, Jun 6 2019
** Portions Copyright (C) 2000, Red Hat, Inc.
** Portions Copyright (C) Pepperl+Fuchs Control, Inc.
**
*****

RAM: 0x10000000-0x10018000 [0x100018d4-0x1000bc6a available]
0x10080000-0x1008a000 [0x10080000-0x1008a000 available]
0x20000000-0x20010000 [0x20000000-0x20010000 available]
0x28000000-0x29000000 [0x28000000-0x29000000 available]
FLASH: 0x14000000-0x147fffff, 2048 x 0x1000 blocks
RedBoot> dis
Loading disabled
RedBoot>
```

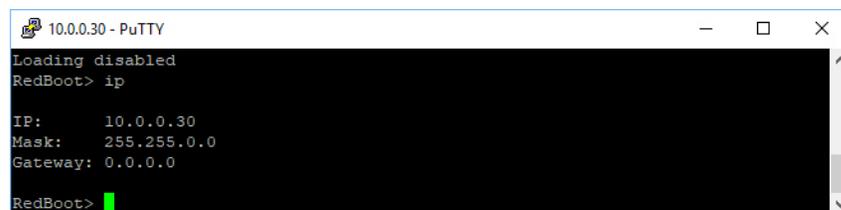
7.4. Festlegen der Netzwerkeinstellungen

Wenn Sie sich nicht sicher sind, welche Netzwerkinformationen auf dem ICDM-RX vorhanden sind, können Sie das folgende Verfahren durchführen.

Standardnetzwerkeinstellungen:

- IP-Adresse: 192.168.250.250
 - Subnetzmaske: 255.255.0.0
 - Gateway-Adresse: 192.168.250.1
1. Stellen Sie die Kommunikation zum ICDM-RX mithilfe der seriellen Methode (Seite 86) oder der Telnet-Methode (Seite 87) her.
 2. Geben Sie **ip** bei der Aufforderung **RedBoot** ein.

Die Werte für IP-Adresse, Subnetzmaske und IP-Gateway werden angezeigt.



```
10.0.0.30 - PuTTY
Loading disabled
RedBoot> ip
IP:      10.0.0.30
Mask:    255.255.0.0
Gateway: 0.0.0.0
RedBoot>
```

Note: Optional können Sie PortVision DX auf einem Windows-System im Netzwerk installieren und die IP-Informationen im Fenster Geräteliste abrufen.

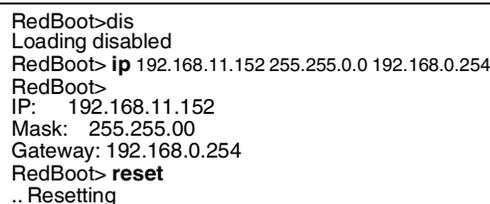
7.5. Konfigurieren der Netzwerkeinstellungen

Gehen Sie wie folgt vor, um die IP-Adresse mit RedBoot zu programmieren.

1. Stellen Sie die Kommunikation zum ICDM-RX mithilfe der seriellen Methode (Seite 86) oder der Telnet-Methode (Seite 87) her.
2. Geben Sie **ip [addr mask gateway]** ein, und drücken Sie **Enter**, um die IP-Adresse zu konfigurieren. *Wobei gilt:*

- addr** = IP-Adresse, die Sie verwenden möchten
- mask** = Subnetzmaske Ihres Netzwerks
- gateway** = vom Netzwerkadministrator zugewiesen

Stellen Sie sicher, dass jeder Wert durch ein Leerzeichen abgetrennt ist.



```
RedBoot>dis
Loading disabled
RedBoot> ip 192.168.11.152 255.255.0.0 192.168.0.254
RedBoot>
IP:      192.168.11.152
Mask:    255.255.00
Gateway: 192.168.0.254
RedBoot> reset
.. Resetting
```

3. Überprüfen Sie, ob RedBoot mit Ihren konfigurierten Netzwerkinformationen antwortet, oder führen Sie den Befehl erneut aus.
4. Wenn Sie keine weiteren zugehörigen RedBoot-Aufgaben haben, geben Sie **reset** ein, um den ICDM-RX zurückzusetzen.

7.6. Ändern der Bootloader-Zeitüberschreitung

Gehen Sie wie folgt vor, um die Bootloader-Zeitüberschreitung zu ändern.

1. Stellen Sie die Kommunikation zum ICDM-RX mithilfe der seriellen Methode (Seite 86) oder der Telnet-Methode (Seite 87) her.
2. Geben Sie **timeout** bei der Aufforderung **RedBoot** ein.

```
RedBoot> dis
Loading disabled
RedBoot> timeout
Timeout 15 seconds
RedBoot> timeout 45
timeout 45 seconds
RedBoot>_
```

RedBoot antwortet mit dem aktuellen Bootloader-Zeitüberschreitungswert.

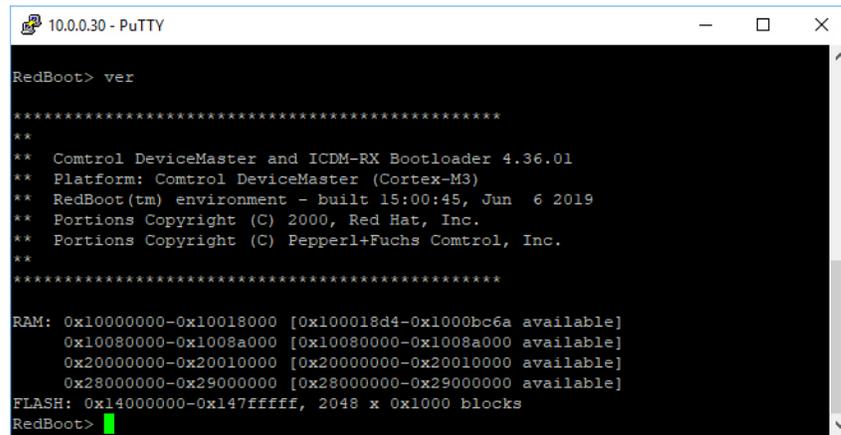
3. Geben Sie **timeout** und einen Wert ein, um die Zeitüberschreitung zu ändern. Beispiel **Timeout 45**: So wird die Bootloader-Zeitüberschreitung auf 45 Sekunden geändert.

7.7. Ermitteln der Bootloader-Version

Gehen Sie wie folgt vor, um festzustellen, welche Bootloader-Version im ICDM-RX geladen ist.

1. Stellen Sie die Kommunikation zum ICDM-RX mithilfe der seriellen Methode (Seite 86) oder der Telnet-Methode (Seite 87) her.
2. Geben Sie **version** bei der Eingabeaufforderung **RedBoot** ein.

Die Bootloader-Informationen werden angezeigt.



```
10.0.0.30 - PuTTY
RedBoot> ver
*****
**
** Control DeviceMaster and ICDM-RX Bootloader 4.36.01
** Platform: Control DeviceMaster (Cortex-M3)
** RedBoot(tm) environment - built 15:00:45, Jun 6 2019
** Portions Copyright (C) 2000, Red Hat, Inc.
** Portions Copyright (C) Pepperl+Fuchs Control, Inc.
**
*****
RAM: 0x10000000-0x10018000 [0x100018d4-0x1000bc6a available]
      0x10080000-0x1008a000 [0x10080000-0x1008a000 available]
      0x20000000-0x20010000 [0x20000000-0x20010000 available]
      0x28000000-0x29000000 [0x28000000-0x29000000 available]
FLASH: 0x14000000-0x147fffff, 2048 x 0x1000 blocks
RedBoot>
```

3. Wenn Sie keine weiteren zugehörigen RedBoot-Aufgaben haben, geben Sie **reset** ein, um den ICDM-RX zurückzusetzen.

Note: Optional können Sie PortVision DX auf einem Windows-System im Netzwerk installieren und die Bootloader-Version im Fenster „Device List“ abrufen. Starten Sie den ICDM-RX neu, klicken Sie mit der rechten Maustaste auf den ICDM-RX, und klicken Sie auf „Refresh Device“, bis die Bootloader-Version angezeigt wird. Die Bootloader-Version wird nur für einen Moment angezeigt.

7.8. Zurücksetzen des ICDM-RX

Wenn Sie Ihre Aufgaben in RedBoot abgeschlossen haben, müssen Sie einen **reset**-Befehl in der Eingabeaufforderung **RedBoot>** eingeben, damit der ICDM-RX mit dem Vorgang beginnen kann.

Note: Die LEDs am ICDM-RX durchlaufen die Einschaltsequenz. Der ICDM-RX hat den Reset-Zyklus abgeschlossen, wenn die **PWR**- oder **Status-LED** leuchtet und nicht mehr blinkt.

```
RedBoot> dis
Loading disabled
RedBoot> reset
```

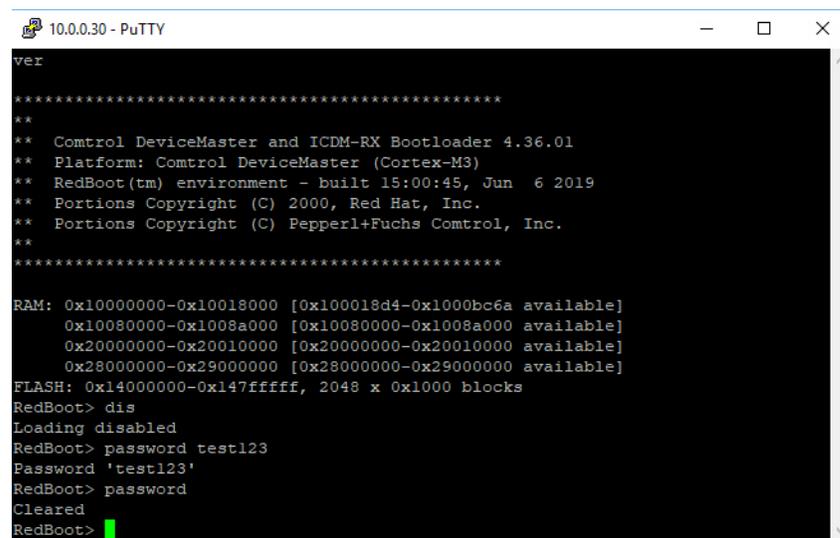
7.9. Konfigurieren von Passwörtern

In diesem Abschnitt wird beschrieben, wie Sie ein Passwort für den Web- und Telnet-Server konfigurieren.

Gehen Sie wie folgt vor, um das ICDM-RX-Passwort für den Web- und Telnet-Server einzurichten. Durch die Einrichtung eines Passworts werden unbefugte Änderungen an der ICDM-RX-Konfiguration verhindert.

1. Stellen Sie die Kommunikation zum ICDM-RX mithilfe der seriellen Methode (Seite 86) oder der Telnet-Methode (Seite 87) her.
2. Geben Sie **password [Ihr_Passwort]** ein, und drücken Sie **Enter**.

Note: Wenn Sie Ihr Passwort vergessen haben, können Sie es mit der seriellen Methode neu programmieren, die das Passwort umgeht.



```
10.0.0.30 - PuTTY
ver
*****
**
** Control DeviceMaster and ICDM-RX Bootloader 4.36.01
** Platform: Control DeviceMaster (Cortex-M3)
** RedBoot(tm) environment - built 15:00:45, Jun  6 2019
** Portions Copyright (C) 2000, Red Hat, Inc.
** Portions Copyright (C) Pepperl+Fuchs Control, Inc.
**
*****
RAM: 0x10000000-0x10018000 [0x100018d4-0x1000bc6a available]
      0x10080000-0x1008a000 [0x10080000-0x1008a000 available]
      0x20000000-0x20010000 [0x20000000-0x20010000 available]
      0x28000000-0x29000000 [0x28000000-0x29000000 available]
FLASH: 0x14000000-0x147fffff, 2048 x 0x1000 blocks
RedBoot> dis
Loading disabled
RedBoot> password test123
Password 'test123'
RedBoot> password
Cleared
RedBoot>
```

Note: Die Bootloader-Version auf Ihrem ICDM-RX kann sich von der in dieser Grafik gezeigten Version unterscheiden.

Wenn Sie die Webbrowser-Authentifizierung einrichten möchten, lesen Sie über den Befehl **auth** in *RedBoot-Befehlsübersicht* auf Seite 91 nach.

7.10. RedBoot-Befehlsübersicht

Die folgende Tabelle bietet einen Überblick über die verfügbaren RedBoot-Befehle. Nach dem Zugriff auf RedBoot können Sie die Liste der Befehle online anzeigen, indem Sie **help** eingeben und **Enter** drücken.

RedBoot-Befehle	
auth {noaccess, none, basic, md5, invalid}	Legt die Webauthentifizierung fest oder zeigt sie an. Die Standardeinstellung ist none , d. h., es wird keine Authentifizierung für den Zugriff auf den Webserver benötigt. Um den Zugriff auf den Webserver zu verweigern, klicken Sie auf noaccess oder invalid . Bei einem Zugriffsversuch wird eine Meldung angezeigt, die den Benutzer darüber informiert, dass der Zugriff verweigert wird. Um den Webserver so zu konfigurieren, dass er ein unverschlüsseltes Passwort anfordert, klicken Sie auf basic . Um den Webserver für die Anforderung eines verschlüsselten Passworts zu konfigurieren, klicken Sie auf md5 . (Einige Browser unterstützen den Befehl md5 nicht.)
baudrate [-b <rate>]	Baudrate der Systemkonsole festlegen/abfragen.
boardrev†	Zeigt die Platinenversion an.
cache [ON OFF]	Verwaltet die Caches der Maschine.
catalognum [catalog number]†	Zeigt die Katalognummer an.
channel [-1 <channel number>]	Zeigt den Konsolenkanal an oder schaltet ihn um.
chassist†	Zeigt Gehäuseinformationen an.
cksum -b <location> -l <length>	Berechnet eine 32-Bit-Prüfsumme [POSIX-Algorithmus] für einen Speicherbereich.
clearconfig	Löscht die Anwendungskonfiguration.
cpufreq†	Zeigt die CPU-Taktfrequenz an.
delaycal <passes>†	Kalibriert die SDRAM-Taktverzögerung.
deviceid [device id]†	Zeigt die Geräte-ID an.
disable	Deaktiviert das automatische Laden der Standardanwendung.
dump -b <location> [-l <length>] [-s] [-1 2 4]	Zeigt einen Speicherbereich an (Hexadezimal-Speicherauszug).
eepromvers [ver]†	Zeigt die eeprom-Version an.
fis {cmds}	Verwaltet Flash-Images.
flash	Zeigt Flash-Informationen an.
go [-w <timeout>] [-c] [-n] [entry]	Führt Codes an einer Position aus.
help <topic>	Zeigt die verfügbaren RedBoot-Befehle an.
history	Zeigt den Befehlsverlauf an.
hwflagst†	Zeigt die HW-Feature-Flags an.
ip [addr mask gateway]	Zeigt die IP-Adresskonfiguration an oder legt sie fest.
load [-r] [-v] [-h <host>] [-p <TCP port>] [-m <varies>] [-c <channel_number>] [-b <base_address>] <file_name>	Lädt eine Datei.

3/26/20

RedBoot-Befehle (Fortsetzung)	
loop 232 422 int port-number	Führt einen Loopback-Test auf dem Port aus.
mac†	Zeigt die Ethernet-MAC-Adresse an.
mcmp -s <location> -d <location> -l <length> [-1 2 4]	Vergleicht zwei Speicherblöcke.
mcopy -s <location> -d <location> -l <length> [-1 2 4]	Kopiert den Speicher von einer Adresse auf eine andere.
mem_read <start_addr> (<end_addr>)	Liest den Speicher aus.
mem_write <value> <start_addr> (<end_addr>)	Schreibt in den Speicher.
mfill -b <location> -l <length> -p <pattern> [-1 2 4]	Füllt einen Speicherblock mit einem Muster.
model [model-number]†	Zeigt die Modellnummer an.
modelname [model name]†	Zeigt den Modellnamen an.
numether [num]†	Zeigt die Anzahl der Ethernet-Ports an.
numserial [num]†	Zeigt die Anzahl der seriellen Ports an.
oemid [id]†	Zeigt die OEM-ID an.
password {password}	Legt das Passwort fest oder löscht es.
ping [-v] [-n <count>] [-l <length>] [-t <timeout>] [-r <rate>] [-i <IP_addr>] -h <IP_addr>	Netzwerkverbindungstest.
ramtest <passes>	Testet den RAM.
ramtime [reg [<value>]]	Zeigt die RAM-Timing-Registerwerte an.
reset	Setzt den ICDM-RX zurück.
secureconf [disable enable]	Legt die Aktivierung der sicheren Konfiguration fest oder zeigt sie an.
securedata [disable enable]	Legt die Aktivierung sicherer Daten fest oder zeigt sie an.
sernum [prefix] [serial_number] sernum [serial_number]†	Zeigt die Seriennummer des Geräts an (falls verfügbar).
?	Zeigt kurz gefasste Hilfethemen an.
snmp [disable enable]	Legt die SNMP-Aktivierung fest oder zeigt sie an.
summary	Zeigt eine Zusammenfassung mit Bootloader-Version, Netzwerkadressinformationen, MAC-Adresse und Sicherheitseinstellungen an.
telnet [disable enable]	Legt die Aktivierung des Telnet-servers fest oder zeigt sie an. Deaktiviert Telnet.
timeout [seconds]	Zeigt eine Telnet-Zeitüberschreitung an oder legt sie fest.
terse	Antwortmodus für den TERSE-Befehl.
t485 port #1 port #2	Führt Port-zu-Port-RS-485-Tests durch. Die Portnummerierung ist Port 0 bis 15. Sie müssen ein nicht gekreuztes Netzwerkkabel, z. B. ein Ethernet-Patchkabel, anschließen.
timeout {seconds}	Zeigt den Zeitüberschreitungswert für den Bootloader an oder legt ihn fest.

3/26/20



RedBoot-Befehle (Fortsetzung)	
vendorid [vendor id]†	Zeigt die Hersteller-ID an.
version	Zeigt die Versionsinformationen zu RedBoot an.
x -b <location> [-l <length>] [-s] [-1 -2 -4]	Zeigt einen Speicherbereich an (Hexadezimal-Speicherauszug).
kszdump	Speicherauszug eines vordefinierten Satzes von KSZ8863-Registern.
kszrd <r1> [r2]	Angegebene KSZ8863-Register lesen.
kszrestart	KSZ8863 neu starten.
kszwr <r1> <val>	Angegebene KSZ8863-Register lesen.
† Schreibgeschützte Elemente, die in RedBoot nicht geändert werden können.	

8. Spezifikationen des externen Netzteils

Dieser Abschnitt enthält Informationen, die Sie möglicherweise benötigen, wenn Sie Ihre eigenen externen Netzteile verwenden möchten.

- **ICDM-RX/xxx-DB9/RJ45-PM Netzteil** auf Seite 94
- **ICDM-RX/xxx-DB9/RJ45-DIN oder ICDM-RX/xxx-ST/RJ45-DIN Netzteil** auf Seite 95
- **ICDM-RX/xxx-2ST/RJ45-DIN Netzteil** auf Seite 96
- **ICDM-RX/xxx-2DB9RJ45-DIN Netzteil** auf Seite 97
- **ICDM-RX/xxx-4DB9/2RJ45-DIN Netzteil** auf Seite 98

8.1. ICDM-RX/xxx-DB9/RJ45-PM Netzteil

Diese Tabelle enthält Spezifikationen für das Netzteil, das mit dem ICDM-RX 1-Port-Schalttafeleinbau geliefert wird. In dieser Tabelle sind die Spezifikationen für das optionale Netzteil von Pepperl + Fuchs aufgeführt.

Pepperl + Fuchs Netzteil: ICDM-RX/xxx-DB9/RJ45-PM	
Frequenz Eingangsleitung	43–63 Hz
Spannung Eingangsleitung	90–260 V AC
Ausgangsspannung	24VDC
Ausgangsstrom	500 mA bei 24 V DC

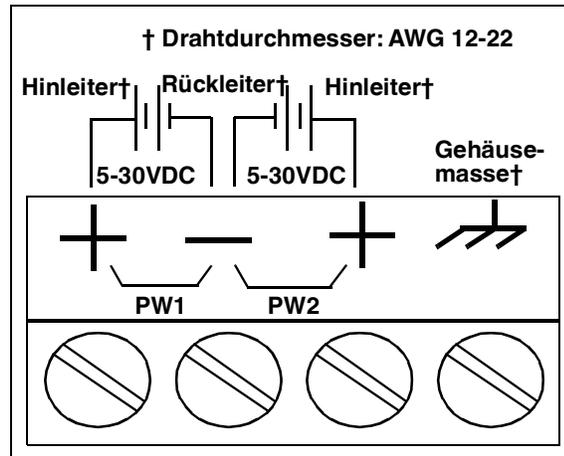
Diese Tabelle enthält die Vorgaben für die Verwendung eines eigenen Netzteils.

ICDM-RX/xxx-DB9/RJ45-PM Externes Netzteil	
Ausgangsspannung†	5-30VDC
Stromstärke†	100 mA (min.) bei 24 V DC
Leistung	2,5 W
† Es kann jedes Netzteil verwendet werden, das die Anforderungen an Stromverbrauch, Spannung, Stromversorgung und Stiftbelegung erfüllt.	



8.2. ICDM-RX/xxx-DB9/RJ45-DIN oder ICDM-RX/xxx-ST/RJ45-DIN Netzteil

Diese Tabelle enthält die Vorgaben beim Erwerb eines Netzteils für einen ICDM-RX/xxx-DB9/RJ45-DIN oder ICDM-RX/xxx-ST/RJ45-DIN.

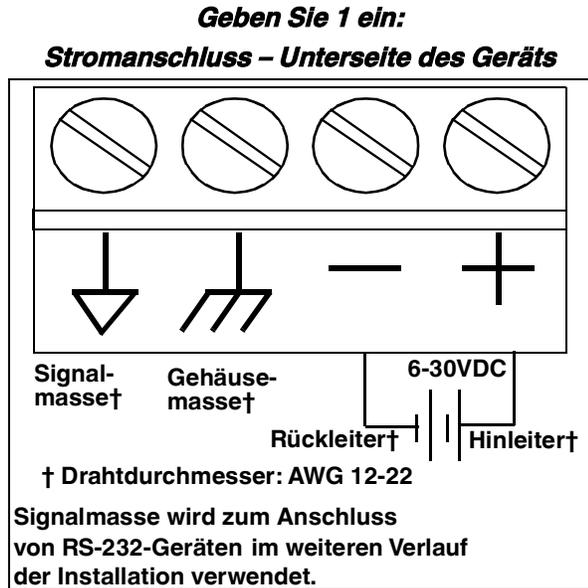


Diese Tabelle enthält die Vorgaben für die Verwendung eines eigenen Netzteils.

ICDM-RX/xxx-DB9/RJ45-DIN oder ICDM-RX/xxx-ST/RJ45-DIN Externes Netzteil	
Ausgangsspannung †	5-30VDC
Stromstärke †	100 mA (min.) bei 24 V DC
Leistung	2,5 W
† Es kann jedes Netzteil verwendet werden, das die Anforderungen an Stromverbrauch, Spannung, Stromversorgung und Stiftbelegung erfüllt.	

8.3. ICDM-RX/xxx-2ST/RJ45-DIN Netzteil

Diese Tabelle enthält die Vorgaben beim Erwerb eines Netzteils für einen ICDM-RX/xxx-2ST/RJ45-DIN.



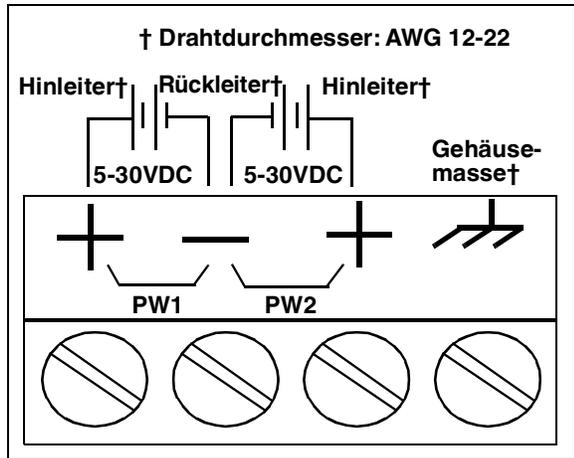
Diese Tabelle enthält die Vorgaben für die Verwendung eines eigenen Netzteils.

ICDM-RX/xxx-2ST/RJ45-DIN Externes Netzteil	
Ausgangsspannung†	6-30VDC
Stromstärke†	100 mA (min.) bei 24 V DC
Leistung	2,5 W
† Es kann jedes Netzteil verwendet werden, das die Anforderungen an Stromverbrauch, Spannung, Stromversorgung und Stiftbelegung erfüllt.	



8.4. ICDM-RX/xxx-2DB9RJ45-DIN Netzteil

Diese Tabelle enthält die Vorgaben für den Erwerb eines Netzteils für einen ICDM-RX/xxx-2DB9RJ45-DIN.

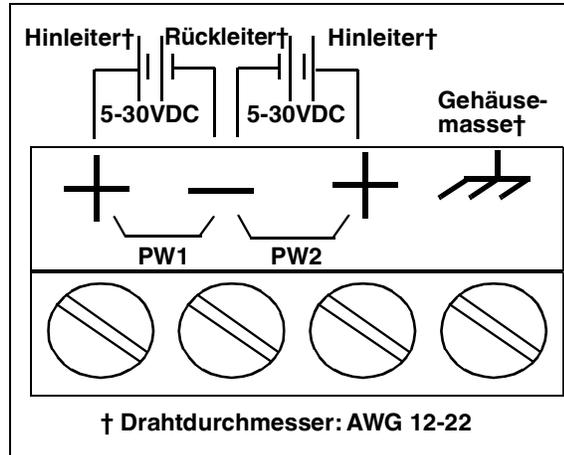


Diese Tabelle enthält die Vorgaben für die Verwendung eines eigenen Netzteils.

ICDM-RX/xxx-2DB9RJ45-DIN Externes Netzteil	
Ausgangsspannung† Stromstärke† Leistung	5-30VDC 100 mA (min.) bei 24 V DC 2,5 W
† Es kann jedes Netzteil verwendet werden, das die Anforderungen an Stromverbrauch, Spannung, Stromversorgung und Stiftbelegung erfüllt.	

8.5. ICDM-RX/xxx-4DB9/2RJ45-DIN Netzteil

Diese Tabelle enthält die Vorgaben für den Erwerb eines Netzteils für einen ICDM-RX/xxx-4DB9/2RJ45-DIN.



Diese Tabelle enthält die Vorgaben für die Verwendung eines eigenen Netzteils.

ICDM-RX/xxx-4DB9/2RJ45-DIN Externes Netzteil	
Ausgangsspannung†	5-30VDC
Stromstärke†	100 mA (min.) bei 24 V DC
Leistung	2,5 W
† Es kann jedes Netzteil verwendet werden, das die Anforderungen an Stromverbrauch, Spannung, Stromversorgung und Stiftbelegung erfüllt.	

9. Fehlerbehandlung und technischer Support

Dieser Abschnitt enthält Informationen zur Fehlerbehandlung für Ihren ICDM-RX. Bevor Sie den technischen Support anrufen, sollten Sie die folgenden Unterabschnitte durchlesen, da Sie viele Verfahren oder Prüfungen durchführen müssen, bevor man Ihnen bei der Diagnose eines Problems helfen kann.

- *Checkliste zur Fehlerbehandlung* auf Seite 99
- *Allgemeine Fehlerbehandlung* auf Seite 100
- *Verkettung des ICDM-RX mit zwei Ethernet-Ports* auf Seite 101
- *ICDM-RX LEDs* auf Seite 102

Wenn Sie das Problem nicht diagnostizieren können, wenden Sie sich an den technischen Support.

9.1. Checkliste zur Fehlerbehandlung

Die folgende Checkliste kann Ihnen bei der Diagnose Ihres Problems helfen:

- Stellen Sie sicher, dass Sie die richtigen Kabeltypen an den richtigen Anschlüssen verwenden und dass alle Kabel fest angeschlossen sind.

Note: Die meisten Kundenprobleme, die dem technischen Support von Pepperl + Fuchs gemeldet werden, sind letztendlich auf Verkabelungs- oder Netzwerkprobleme zurückzuführen.

Modell	Verbunden mit	Ethernetkabel	Steckverbindernamen
ICDM-RX/ xxx -DB9/RJ45-PM	Ethernet-Hub oder NIC	Standard	10/100 ETHERNET
ICDM-RX/ xxx -DB9/RJ45-DIN ICDM-RX/ xxx -ST/RJ45-DIN ICDM-RX/ xxx -2DB9RJ45-DIN ICDM-RX/ xxx -2ST/RJ45-DIN	Ethernet-Hub oder NIC	Standard	10/100
ICDM-RX/ xxx -4DB9/2RJ45-DIN	Ethernet-Hub oder NIC	Standard	10/100 - E1/E2

- Überprüfen Sie, ob Netzwerk-IP-Adresse, Subnetzmaske und Gateway stimmen und für das Netzwerk geeignet sind. Stellen Sie sicher, dass die im ICDM-RX programmierte IP-Adresse mit der vom Systemadministrator zugewiesenen eindeutigen, reservierten, konfigurierten IP-Adresse übereinstimmt.
 - Wenn eine IP-Adressierung verwendet wird, sollte das System in der Lage sein, den ICDM-RX anzupingen.
 - Bei Verwendung von DHCP muss das Hostsystem die Subnetzmaske und das Gateway bereitstellen.
- Stellen Sie sicher, dass der Ethernet-Hub und alle anderen Netzwerkgeräte zwischen System und ICDM-RX eingeschaltet und in Betrieb sind.
- Starten Sie das System neu, setzen Sie dann die Stromversorgung am ICDM-RX zurück, und beobachten Sie die Aktivität der **PWR-** oder **Status-LED** (Seite 102).

PWR- oder Status-LED	Beschreibung
5 Sek. Aus, 3x Blinken, 5 Sek. Aus, 3x Blinken...	Redboot™-Prüfsummenfehler.
5 Sek. Aus, 4x Blinken, 5 Sek. Aus, 4x Blinken...	SREC-Ladefehler.

Nur PROFINET IO:

Status- oder PWR-LED	Beschreibung
----------------------	--------------

Blinkt alle 10 Sekunden	Keine SPS-Verbindung.
Leuchtet (durchgehend)	Mindestens eine SPS-Verbindung wurde hergestellt.
Blinkt	<ul style="list-style-type: none"> • LED-Blinkmodus ist aktiviert. • Fehler erkannt oder Diagnoseinformationen verfügbar.

- Wenn Sie ein ICDM-RX-Ersatzgerät haben, tauschen Sie das Gerät versuchsweise aus.

9.2. Allgemeine Fehlerbehandlung

In dieser Tabelle sind Tipps zur allgemeinen Fehlerbehandlung aufgeführt.

Note: Vergewissern Sie sich, dass Sie die Checkliste zur Fehlerbehandlung auf Seite 99 gelesen haben.

Allgemeiner Zustand	Erklärung/Handlungsanweisung
PWR- oder Status-LED blinkt	<p>Zeigt an, dass das Bootprogramm nicht auf das Gerät heruntergeladen wurde.</p> <ol style="list-style-type: none"> 1. Starten Sie das System neu. 2. Stellen Sie sicher, dass Sie die aktuelle Firmware für Ihr Protokoll heruntergeladen haben. <p>Note: Wenn die PWR- oder Status-LED weiterhin blinkt, wenden Sie sich an den technischen Support.</p>
PWR- oder Status-LED leuchtet nicht und blinkt nicht alle 10 Sekunden Nur PROFINET IO	<p>Zeigt an, dass die Stromversorgung nicht eingeschaltet wurde oder ein Hardwarefehler vorliegt. Wenden Sie sich an den technischen Support.</p>
Gerät kann nicht über Ethernet-Hub angepingt werden	<p>Trennen Sie den ICDM-RX vom Netzwerk. Verbinden Sie das Gerät direkt mit der NIC im Hostsystem.</p>
Ping oder Verbindung mit dem ICDM-RX nicht möglich	<p>Auf die Standard-IP-Adresse des ICDM-RX kann aufgrund der Subnetzmaske eines anderen Netzwerks oft nicht zugegriffen werden, es sei denn, im Netzwerk wird 192.168 verwendet.</p> <p>In den meisten Fällen ist es erforderlich, eine Adresse einzugeben, die Ihrem Netzwerk entspricht.</p>
Bei Verbindung mit einigen Ethernet-Switches oder -Routern wird der ICDM-RX immer wieder neu gestartet.	<p>Ungültige IP-Informationen können auch dazu führen, dass der Schalter oder Router nach einer Gateway-Adresse sucht. Das Fehlen einer Gateway-Adresse ist eine häufige Ursache.</p>

9.3. Verkettung des ICDM-RX mit zwei Ethernet-Ports

Die ICDM-RX-Modelle mit zwei Ethernet-Ports entsprechen den IEEE-Spezifikationen für standardmäßige Ethernet 10/100BASE-TX-Topologien.

Bei Verwendung der Ports **E1** und **E2** ist der ICDM-RX als Switch einzustufen. Wenn nur der Port **UP** verwendet wird, handelt es sich um ein einfaches Endknotengerät.

Die maximale Anzahl der verketteten ICDM-RX-Einheiten und die maximale Entfernung zwischen den Einheiten basieren auf den Ethernet-Standards und werden durch Ihre eigene Umgebung und die Konformität Ihres Netzwerks mit diesen Standards bestimmt.

Pepperl + Fuchs hat sieben verkettete ICDM-RX-Geräte mit CAT5-Kabeln von 3 m Länge getestet; dies ist jedoch nicht die theoretische Grenze. Es kann vorkommen, dass die Leistung der Geräte am Ende der Kette beeinträchtigt wird. Es wird daher empfohlen, Ihre Umgebung zu überlasten und die Leistung zu testen. Auch das Betriebssystem und die Anwendung können die Gesamtanzahl der Ports begrenzen, die installiert werden können.

Im Folgenden finden Sie einige kurze Richtlinien und URLs mit zusätzlichen Informationen. Beachten Sie, dass sich Normen und URLs gelegentlich ändern.

- Regeln für Ethernet 10BASE-T
 - Es sind maximal vier Repeater-Hops möglich.
 - Sie können 10BASE-T-Twisted-Pair-Kabel der Kategorie 3 oder 5 verwenden.
 - Die maximale Länge jedes Kabels beträgt 100 m.

Note: *Twisted-Pair-Kabel nach CAT3 oder 5 sehen wie Telefonkabel aus, sind jedoch nicht identisch. Das Netzwerk funktioniert nicht, wenn Telefonkabel zum Anschließen des Geräts verwendet werden.*
- Regeln für Fast Ethernet 100BASE-TX
 - Es sind maximal zwei Repeater-Hops möglich (für einen Hub der Klasse II). Ein Hub der Klasse II kann direkt an einen anderen Fast-Ethernet-Hub der Klasse II angeschlossen werden. Ein Hub der Klasse I kann nicht direkt mit einem anderen Fast-Ethernet-Hub verbunden werden.
 - Sie müssen 100BASE-TX-Twisted-Pair-Kabel der Kategorie 5 verwenden.
 - Die maximale Länge jedes Twisted-Pair-Kabels beträgt 100 m.
 - Die Gesamtlänge der Twisted-Pair-Verkabelung (über direkt angeschlossene Hubs) darf 205 m nicht überschreiten.

Note: *Twisted-Pair-Kabel nach CAT5 sehen wie Telefonkabel aus, sind jedoch nicht identisch. Das Netzwerk funktioniert nicht, wenn Telefonkabel zum Anschließen des Geräts verwendet werden.*
- IEEE 802.3-Spezifikation: Ein Netzwerk mit Leistungsverstärkern zwischen den Kommunikationsstationen (PCs) unterliegt der 5-4-3-Regel für die Leistungsverstärker-Anordnung im Netzwerk:
 - Fünf Segmente, die mit dem Netzwerk verbunden sind
 - Vier Repeater
 - An drei Segmente der 5 Segmente können Stationen angeschlossen sein. Die anderen beiden Segmente müssen Inter-Leistungsverstärker-Link-Segmente ohne angeschlossene Stationen sein.

Weitere Informationen finden Sie im Internet.

9.4. ICDM-RX LEDs

Die LEDs zeigen an, dass die ICDM-RX-Standardanwendung ausgeführt wird. Wenn Sie PortVision DX geladen haben, können Sie den ICDM-RX-Status online überprüfen.

Modell	Netzwerk-LEDs
ICDM-RX/ xxx -DB9/RJ45-PM	<ul style="list-style-type: none"> • Wenn die Status-LED an der Vorderseite des Geräts leuchtet, wird das Gerät mit Strom versorgt und hat den Startvorgang abgeschlossen. Die Status-LED blinkt während des Startvorgangs. Es dauert ca. 15 Sekunden, bis der Bootloader den Zyklus abgeschlossen hat. Wenn der Bootloader den Zyklus abgeschlossen hat, leuchtet die LED durchgehend und blinkt nur etwa alle 10 Sekunden. Nur PROFINET IO: Wenn der Bootloader den Zyklus beendet, blinkt die LED mehrmals schnell, erlischt dann, und blinkt ca. alle 10 Sekunden, wenn keine SPS-Verbindung besteht. • Wenn die rote LED Link Act leuchtet, ist die Ethernet-Verbindung betriebsbereit. • Wenn die rote Duplex-LED leuchtet, weist dies auf Vollduplex-Aktivität hin. • Wenn die rote 100-LED leuchtet, weist dies auf eine funktionierende 100-MB-Ethernet-Verbindung hin (nur 100-MB-Netzwerk).
ICDM-RX/ xxx -DB9/RJ45-DIN ICDM-RX/ xxx -ST/RJ45-DIN ICDM-RX/ xxx -2DB9RJ45-DIN ICDM-RX/ xxx -2ST/RJ45-DIN ICDM-RX/ xxx -4DB9/2RJ45-DIN	<ul style="list-style-type: none"> • Wenn die STATUS-LED an der Vorderseite des Geräts leuchtet, wird das Gerät mit Strom versorgt und hat den Startvorgang abgeschlossen. Die STATUS-LED blinkt während des Startvorgangs. Es dauert ca. 15 Sekunden, bis der Bootloader den Zyklus abgeschlossen hat. Wenn der Bootloader den Zyklus abgeschlossen hat, leuchtet die LED durchgehend und blinkt nur etwa alle 10 Sekunden. Nur PROFINET IO: Wenn der Bootloader den Zyklus beendet, blinkt die LED mehrmals schnell, erlischt dann, und blinkt ca. alle 10 Sekunden, wenn keine SPS-Verbindung besteht. • Wenn die LED LINK (grün) leuchtet, weist dies auf eine funktionierende Ethernet-Verbindung hin. • Wenn die LED ACT (gelb) blinkt, weist dies auf Netzwerkaktivität hin.

FACTORY AUTOMATION – SENSING YOUR NEEDS



Worldwide Headquarters

Pepperl+Fuchs Group
68307 Mannheim · Germany
Tel. +49 621 776-0
E-mail: info@de.pepperl-fuchs.com

USA Headquarters

Pepperl+Fuchs Inc.
Twinsburg, Ohio 44087 · USA
Tel. +1 330 4253555
E-mail: sales@us.pepperl-fuchs.com

Asia Pacific Headquarters

Pepperl+Fuchs Pte Ltd.
Company Registration No. 199003130E
Singapore 139942
Tel. +65 67799091
E-mail: sales@sg.pepperl-fuchs.com

www.pepperl-fuchs.com

 **PEPPERL+FUCHS**
SENSING YOUR NEEDS

Subject to modifications
Copyright PEPPERL+FUCHS • Printed in Germany

TDOCT-6548_ENG

3/26/20