

Handbuch | DE

TwinCAT/BS

Betriebssystem



Inhaltsverzeichnis

1	Hinweise zur Dokumentation	7
1.1	Symbolerklärung	8
1.2	Ausgabestände der Dokumentation	8
2	Erste Schritte	10
2.1	Erster Systemstart.....	10
2.2	IP-Adresse ermitteln.....	10
2.3	Zugriff über SSH, webbasierte Konsole oder Webinterface.....	12
2.4	Standardpasswort ändern	14
3	Beckhoff TwinCAT/BSD-Installer.....	15
3.1	Partitionen und Ordnerstruktur	16
3.2	Einrichtung und Installation	19
3.2.1	Bootfähigen USB-Stick erstellen	19
3.2.2	BIOS-Einstellungen überprüfen	21
3.2.3	TwinCAT/BSD installieren.....	21
3.3	Remote-Zugriff auf den TwinCAT/BSD-Installer über SSH.....	22
3.4	Automatisierung von Prozessen – Skripte in der Praxis einsetzen.....	23
4	TwinCAT/BSD	24
4.1	Zugangsdaten	25
4.2	ZFS-Eigenschaften	26
4.3	Verzeichnisstruktur.....	28
4.4	Write Filter	29
4.4.1	Write Filter aktivieren bzw. deaktivieren.....	29
4.4.2	Ausnahmen definieren	29
4.5	Texteditoren	29
5	Netzwerkeinstellungen	31
5.1	Einstellungen für Systeme mit dhcpd	32
5.1.1	Dhcpd nachinstallieren und aktivieren.....	32
5.1.2	IP-Adresse einstellen (dhcpd)	32
5.2	IP-Adresse einstellen für Systeme mit dhclient.....	34
5.3	Hostnamen ändern.....	35
5.4	Firewall.....	35
5.4.1	Firewall aktivieren und deaktivieren	36
5.4.2	Port freigeben.....	36
5.5	WLAN-Konfiguration	37
5.5.1	Mit WLAN verbinden	37
5.5.2	Als Accesspoint konfigurieren	38
5.5.3	DHCP-Server einrichten.....	39
5.6	Verbindung mit Beckhoff LTE-Stick herstellen.....	40
5.7	HTTPS-Zertifikate.....	42
5.7.1	Automatische Zertifikatserstellung deaktivieren.....	42
5.7.2	HTTPS-Zertifikat anfordern oder erstellen	42
5.7.3	Zertifikat importieren	43
6	Systemaktualisierung	44

6.1	TwinCAT/BSD aktualisieren	46
6.2	Major-Version aktualisieren.....	46
6.3	CPU-Mikrocode aktualisieren.....	47
7	Package-Server	49
7.1	Auf chinesischen Server wechseln	49
7.2	Auf FreeBSD-Repository umschalten	50
7.3	Package-Verwaltung	50
7.3.1	Suchen	51
7.3.2	Installieren.....	51
7.3.3	Aktualisieren.....	52
7.3.4	Deinstallieren	52
7.3.5	Sperren	53
7.4	Lokales Repository einrichten	53
7.4.1	Repository auf USB-Stick bereitstellen	53
7.4.2	Eigenen Package-Server einrichten.....	55
8	Konfiguration.....	57
8.1	Systeminformationen	57
8.2	Benutzer und Rechteverwaltung	58
8.2.1	Neuen Benutzer anlegen	59
8.2.2	Benutzerinformationen editieren	60
8.2.3	Benutzer löschen	61
8.3	USB-Stick einbinden	62
8.4	Automount für externe Datenträger aktivieren	63
8.5	USV-Software konfigurieren.....	64
8.6	Realtime-Ethernet deaktivieren	64
8.7	Dienste automatisch starten (Autostart).....	66
8.8	Shell ändern	66
8.9	Tastatursprache umstellen	66
8.10	Uhrzeit mit NTP synchronisieren.....	67
9	Remote-Zugriff.....	69
9.1	Beckhoff Device Manager: Webinterface	69
9.2	Remote-Zugriff mit SSH	71
9.3	Dateien mit dem WinSCP-Client verwalten.....	73
9.3.1	WinSCP-Client starten und einsetzen.....	73
9.3.2	WinSCP als root.....	74
9.3.3	Dateien öffnen und editieren	75
9.4	SSH-Einstellungen bearbeiten	76
10	TwinCAT/BSD Hypervisor	77
10.1	Geräte- und Funktionsunterstützung.....	77
10.2	Virtuelle Maschinen starten und verwalten	77
10.3	Shell-Skripte einsetzen	80
10.4	Autostart von Shell-Skripten.....	82
10.5	Erweiterte VM-Konfiguration	83
10.5.1	ZFS-Datasets als Speicherort für virtuelle Maschinen.....	83
10.5.2	UEFI-basierte virtuelle Maschinen	83

10.5.3	VNC-basierte Interaktion mit virtuellen Maschinen	84
10.5.4	Virtuelle Laufwerke.....	85
10.5.5	Netzwerkconfiguration von virtuellen Maschinen	87
10.5.6	PCI-Device-Passthrough.....	94
10.5.7	Durchreichen von Eingabegeräten.....	96
10.6	Debian Linux als Gastbetriebssystem installieren.....	97
10.7	Windows als Gastbetriebssystems	102
10.7.1	C9900-S620: Windows 10 vorinstalliert mit Device-Passthrough	103
10.7.2	C9900-S621: Windows 10 vorinstalliert ohne Device-Passthrough.....	104
10.7.3	Windows VM mit vm-installer nachinstallieren	105
10.7.4	Anpassen der Windows VM Konfiguration.....	106
11	C/C++ Projekte für TwinCAT/BSD.....	107
11.1	Unter TwinCAT/BSD kompilieren	107
11.2	Remote-Debugging von Applikationen mit Visual Studio Code (VSC)	107
12	TwinCAT 3.....	111
12.1	Zielsysteme suchen	111
12.2	Geräte scannen.....	113
12.3	AMS NetID ändern	114
12.4	TwinCAT in den Run- oder Config Modus versetzen	114
12.5	ADS-Routen manuell anlegen oder löschen	115
12.6	Heap-Speicher erhöhen	116
12.7	Router-Speicher anpassen	117
12.8	Isolierte Kerne zuweisen	118
13	Wiederherstellungsoptionen.....	119
13.1	Wiederherstellungspunkt.....	120
13.1.1	Auf Werkseinstellungen zurücksetzen	120
13.1.2	Wiederherstellungspunkt erstellen	121
13.1.3	Auf Wiederherstellungspunkt zurücksetzen	121
13.1.4	Restore-Bootumgebung einsetzen.....	122
13.2	Backup und Restore.....	123
13.2.1	Backup erstellen.....	123
13.2.2	Backup wiederherstellen	124
13.2.3	Backup aus Live-System erstellen und wiederherstellen.....	124
14	Fehlerbehandlung und Diagnose	126
14.1	Kernelmeldungen für Diagnose nutzen	126
14.2	Logdateien	126
14.3	Dumps	127
14.3.1	Automatischen Prozess-Dump nutzen.....	127
14.3.2	Prozess-Dump manuell erzeugen.....	127
14.3.3	Systeminformationen zur Analyse bereitstellen	127
14.4	ADS-Monitor einsetzen	128
14.5	Netzwerkverkehr mit Wireshark analysieren	129
14.6	Systemreparatur.....	130
14.6.1	Vom USB-Installer Stick booten.....	130
14.6.2	Single-User Modus starten.....	131

15 Anhang	132
15.1 Wichtige Befehle	132
15.1.1 TwinCAT	132
15.1.2 Shell	132
15.1.3 Datei- und Verzeichnisverwaltung.....	134
15.1.4 Systemadministration.....	136
15.1.5 Wichtige Dateien und Verzeichnisse.....	138
15.1.6 Texteditoren	139
15.1.7 Dokumentation	140
15.2 Literaturverzeichnis	141
15.3 FreeBSD Copyright	141
15.4 Support und Service.....	142
Tabellenverzeichnis	143
Abbildungsverzeichnis	144

1 Hinweise zur Dokumentation

Diese Beschreibung wendet sich ausschließlich an ausgebildetes Fachpersonal der Steuerungs- und Automatisierungstechnik, das mit den geltenden nationalen Normen vertraut ist.

Zur Installation und Inbetriebnahme der Komponenten ist die Beachtung der Dokumentation und der nachfolgenden Hinweise und Erklärungen unbedingt notwendig.

Das Fachpersonal ist verpflichtet, stets die aktuell gültige Dokumentation zu verwenden.

Das Fachpersonal hat sicherzustellen, dass die Anwendung bzw. der Einsatz der beschriebenen Produkte alle Sicherheitsanforderungen, einschließlich sämtlicher anwendbaren Gesetze, Vorschriften, Bestimmungen und Normen erfüllt.

Disclaimer

Diese Dokumentation wurde sorgfältig erstellt. Die beschriebenen Produkte werden jedoch ständig weiterentwickelt.

Wir behalten uns das Recht vor, die Dokumentation jederzeit und ohne Ankündigung zu überarbeiten und zu ändern.

Aus den Angaben, Abbildungen und Beschreibungen in dieser Dokumentation können keine Ansprüche auf Änderung bereits gelieferter Produkte geltend gemacht werden.

Marken

Beckhoff®, ATRO®, EtherCAT®, EtherCAT G®, EtherCAT G10®, EtherCAT P®, MX-System®, Safety over EtherCAT®, TC/BSD®, TwinCAT®, TwinCAT/BSD®, TwinSAFE®, XFC®, XPlanar® und XTS® sind eingetragene und lizenzierte Marken der Beckhoff Automation GmbH.

Die Verwendung anderer in dieser Dokumentation enthaltenen Marken oder Kennzeichen durch Dritte kann zu einer Verletzung von Rechten der Inhaber der entsprechenden Kennzeichnungen führen.



EtherCAT® ist eine eingetragene Marke und patentierte Technologie, lizenziert durch die Beckhoff Automation GmbH, Deutschland.

Copyright

© Beckhoff Automation GmbH & Co. KG, Deutschland.

Weitergabe sowie Vervielfältigung dieses Dokuments, Verwertung und Mitteilung seines Inhalts sind verboten, soweit nicht ausdrücklich gestattet.

Zuwiderhandlungen verpflichten zu Schadenersatz. Alle Rechte für den Fall der Patent-, Gebrauchsmuster- oder Geschmacksmustereintragung vorbehalten.

Fremdmarken

In dieser Dokumentation können Marken Dritter verwendet werden. Die zugehörigen Markenvermerke finden Sie unter: <https://www.beckhoff.com/trademarks>.

1.1 Symbolerklärung

In der Dokumentation werden folgende Warnhinweise verwendet. Lesen und befolgen Sie die Warnhinweise.

Warnhinweise, die vor Sach- oder Umweltschäden warnen:

HINWEIS

Es besteht eine mögliche Gefährdung für Umwelt und Geräte.

Hinweise, die weitere Informationen oder Tipps anzeigen:



Dieser Hinweis gibt wichtige Informationen, die beim Umgang mit dem Produkt oder der Software helfen. Es besteht keine unmittelbare Gefahr für Produkt, Mensch und Umwelt.

1.2 Ausgabestände der Dokumentation

Tab. 1: Änderungshinweise für die Dokumentation.

Version	Änderungen
1.0	<ul style="list-style-type: none"> • Erste Version
1.1	<ul style="list-style-type: none"> • Kapitel TwinCAT/BSD, Netzwerkeinsellungen, Package Server, Konfiguration, TwinCAT 3, Wiederherstellungsoptionen und Fehlerbehandlung und Diagnose überarbeitet
1.2	<ul style="list-style-type: none"> • Kapitel Systemaktualisierung, Systeminformation, Beckhoff Device Manager und Uhrzeit mit NTP synchronisieren hinzugefügt. • TwinCAT Kapitel überarbeitet.
1.3	<ul style="list-style-type: none"> • Kapitel TwinCAT/BSD Hypervisor hinzugefügt.
1.4	<ul style="list-style-type: none"> • Kapitel „Remote-Debugging von Applikationen mit Visual Studio Code (VSC)“ hinzugefügt.
1.5	<ul style="list-style-type: none"> • Kapitel „Systemaktualisierung“ überarbeitet. • Kapitel „IPv6 deaktivieren“ entfernt • Kapitel „Netzwerkeinstellungen“ um Angaben zum neuen dhcpcd-Client erweitert. • Kapitel „Dienste automatisch starten“ angepasst. • Kapitel „Remote-Debugging von Applikationen mit Visual Studio Code (VSC) überarbeitet“
1.6	<ul style="list-style-type: none"> • Kapitel „WLAN-Konfiguration“ und „TwinCAT/BSD Hypervisor“ überarbeitet. • Kapitel „Erste Schritte“, „Beckhoff TwinCAT/BSD-Installer“ und „CPU-Mikrocode aktualisieren“ hinzugefügt.
1.7	<ul style="list-style-type: none"> • Kapitel „Eigenen Package-Server einrichten“ hinzugefügt.
1.8	<ul style="list-style-type: none"> • Kapitel „Automount für externe Datenträger aktivieren“ und „USV-Software konfigurieren“ hinzugefügt. • Änderung des Home-Verzeichnisses von TwinCAT/BSD-Version 13 auf 14. Alle Angaben angepasst von <code>/usr/home</code> auf <code>/home</code> • Kapitel „Backup und Restore“, „Remote-Zugriff mit SSH“, und „Lokales Repository aufsetzen“ angepasst.
1.9	<ul style="list-style-type: none"> • Kapitel „TwinCAT/BSD Hypervisor“ überarbeitet.
2.0	<ul style="list-style-type: none"> • Kapitel „HTTPS-Zertifikate“ hinzugefügt.

Tab. 2: Änderungshinweise für das Betriebssystem.

Repository-Version	TwinCAT/BSD-Version	Änderungen
89449	13.2.0.6	<ul style="list-style-type: none">• dhcpcd(8) als Standard DHCP-Client ausgeliefert und löst den älteren Client ab
126815	14.0.4.1	<ul style="list-style-type: none">• Home-Verzeichnis liegt jetzt direkt unter <code>/home</code> (kein Symlink mehr) und nicht mehr unter <code>/usr/home</code>• Automount wird unterstützt• USV-Software ist verfügbar• Wi-Fi 6 wird unterstützt

2 Erste Schritte

Das nachfolgende Kapitel beschreibt die grundlegenden ersten Schritte mit TwinCAT/BSD. Vorausgesetzt wird, dass ein Industrie-PC mit vorinstalliertem TwinCAT/BSD-Betriebssystem von Beckhoff erworben wurde. Das Vorhandensein einer solchen Installation ist anhand des TwinCAT/BSD-Lizenzaufklebers auf dem Gerät identifizierbar.

2.1 Erster Systemstart

Verbinden Sie sämtliche Netzkabel mit dem Industrie-PC und schalten Sie die Spannungsversorgung ein. Wenn Sie einen Bildschirm an das Gerät angeschlossen haben, sehen Sie den BIOS-Boot-Bildschirm und danach den TwinCAT/BSD-Bootloader.

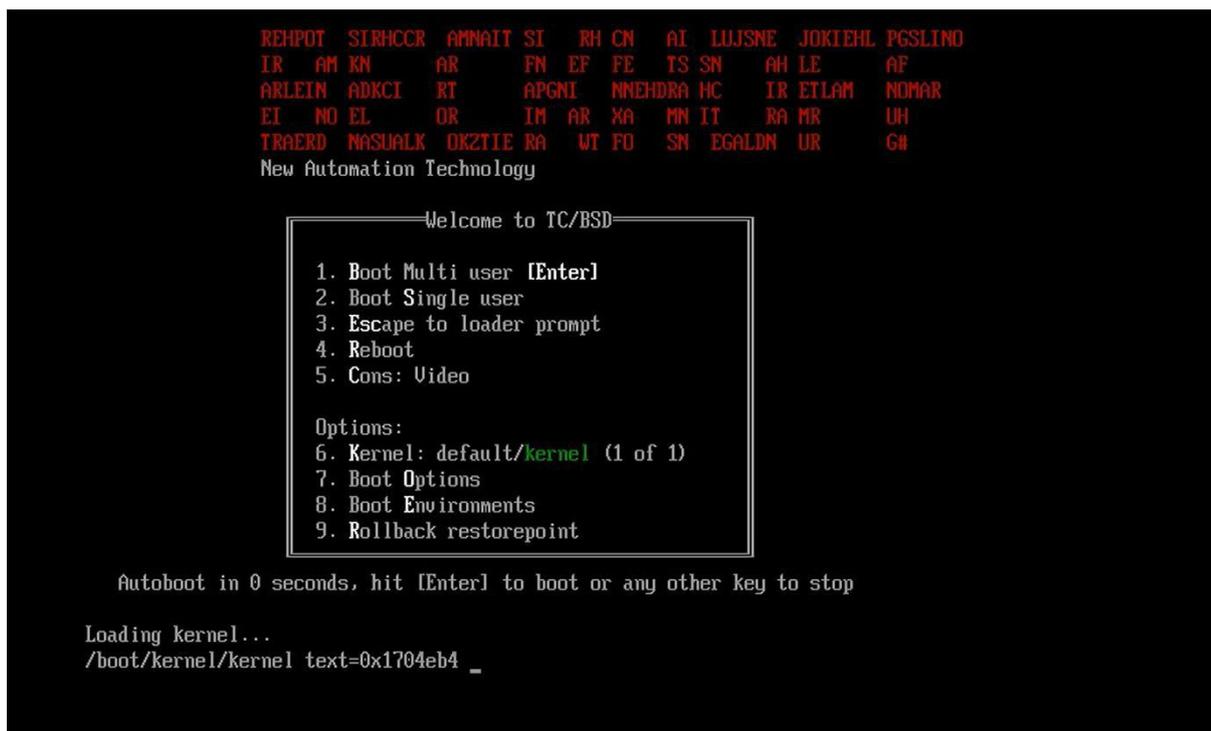


Abb. 1: TwinCAT/BSD-Bootloader während des Starts.

Dann erscheinen während der Boot-Phase von TwinCAT/BSD verschiedene Meldungen, die mit der Anmeldeaufforderung enden. Melden Sie sich mit Benutzer „Administrator“ und dem Passwort „1“ in der Konsole an. Das Passwort sollte sofort nach der Anmeldung geändert werden (siehe: [Standardpasswort ändern \[► 14\]](#)).

```

login: Administrator
Password:
Last login: Thu Sep 14 13:53:41 on ttyv0
FreeBSD 13.2-RELEASE-p1 n254639-8330e4d7c03- BHF

The software licenses can be found in this folder: /usr/local/etc/TwinCAT/3.1/System/Legal/
TcOsSys.dll: 4026.1.20
TwinCAT Build: 3.1.4026.0
AMS Net Id: 5.61.105.18.1.1
TC/BSD: 13.2.1.1,2

```

Wenn Sie keinen Bildschirm angeschlossen haben, ist der einfachste Weg, um zu sehen, ob das Gerät ordnungsgemäß gebootet hat, eine TwinCAT-LED, die blau aufleuchtet.

2.2 IP-Adresse ermitteln

Für alle anschließenden Arbeiten mit dem Industrie-PC und dem System ist die IP-Adresse des Systems erforderlich. Mithilfe der IP-Adresse ist beispielsweise ein Remote-Zugriff über SSH, den Beckhoff Device-Manager (Webinterface) oder die Arbeit mit TwinCAT möglich.

IP-Adresse ermitteln mit Bildschirm

Es gibt mehrere Möglichkeiten, die IP-Adresse zu ermitteln, um über das Netzwerk auf das Gerät zuzugreifen. Wenn Sie einen lokalen Bildschirm angeschlossen haben, können Sie sich mit dem Benutzer "Administrator" und dem Passwort "1" anmelden.

Geben Sie den Befehl `ifconfig` in der Konsole ein, damit alle verfügbaren Ethernet-Schnittstellen im System ausgegeben werden:

```
Administrator@CX-3D6912:~ $ ifconfig
igb0: flags=8863<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
  options=4a024a9<RXCSUM,VLAN_MTU,JUMBO_MTU,VLAN_HWCSUM,LRO,WOL_MAGIC,RXCSUM_IPV6,NOMAP>
  ether 00:01:05:3d:69:12
  inet6 fe80::78ff:f9f9:ef31:454d%igb0 prefixlen 64 scopeid 0x1
  inet 169.254.228.5 netmask 0xffff0000 broadcast 169.254.255.255
  media: Ethernet autoselect
  status: no carrier
  nd6 options=1<PERFORMNUD>
igb1: flags=8863<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
  options=4a024a9<RXCSUM,VLAN_MTU,JUMBO_MTU,VLAN_HWCSUM,LRO,WOL_MAGIC,RXCSUM_IPV6,NOMAP>
  ether 00:01:05:3d:69:13
  inet6 fe80::d2c1:31fd:a18e:e1c3%igb1 prefixlen 64 scopeid 0x2
  inet 172.17.40.26 netmask 0xfffffc00 broadcast 172.17.43.255
  media: Ethernet autoselect (100baseTX <full-duplex>)
  status: active
  nd6 options=1<PERFORMNUD>
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
  options=680003<RXCSUM,TXCSUM,LINKSTATE,RXCSUM_IPV6,TXCSUM_IPV6>
  inet6 ::1 prefixlen 128
  inet6 fe80::1%lo0 prefixlen 64 scopeid 0x3
  inet 127.0.0.1 netmask 0xff000000
  groups: lo
  nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
Administrator@CX-3D6912:~ $
```

Standardmäßig sind die Ethernet-Schnittstellen so konfiguriert, dass sie eine IP-Adresse von einem lokalen DHCP-Server erhalten. In diesem Beispiel ist das die IP-Adresse: 172.17.40.26 die für die Schnittstelle `igb1` vergeben wurde, über die der Industrie-PC mit dem Netzwerk verbunden wurde.

IP-Adresse ermitteln ohne Bildschirm

Verwenden Sie die Funktion Broadcast-Search unter TwinCAT, wenn kein Bildschirm angeschlossen ist, um die IP-Adresse eines TwinCAT/BSD-Zielsystems zu ermitteln.

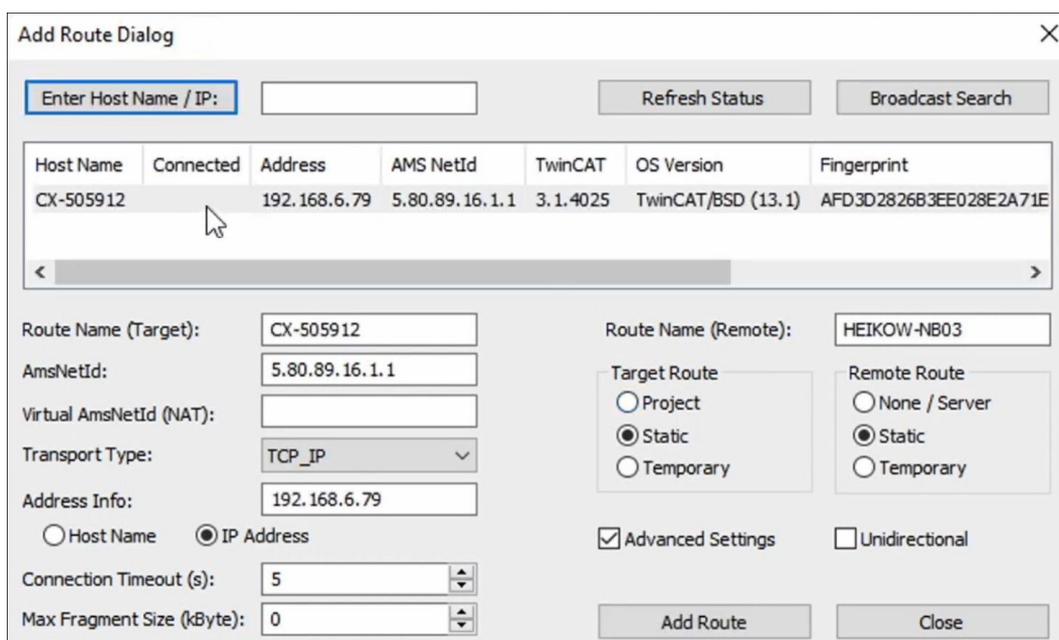


Abb. 2: Add-Route-Dialog mit einem TwinCAT/BSD-Zielsystem und dazugehöriger IP-Adresse.

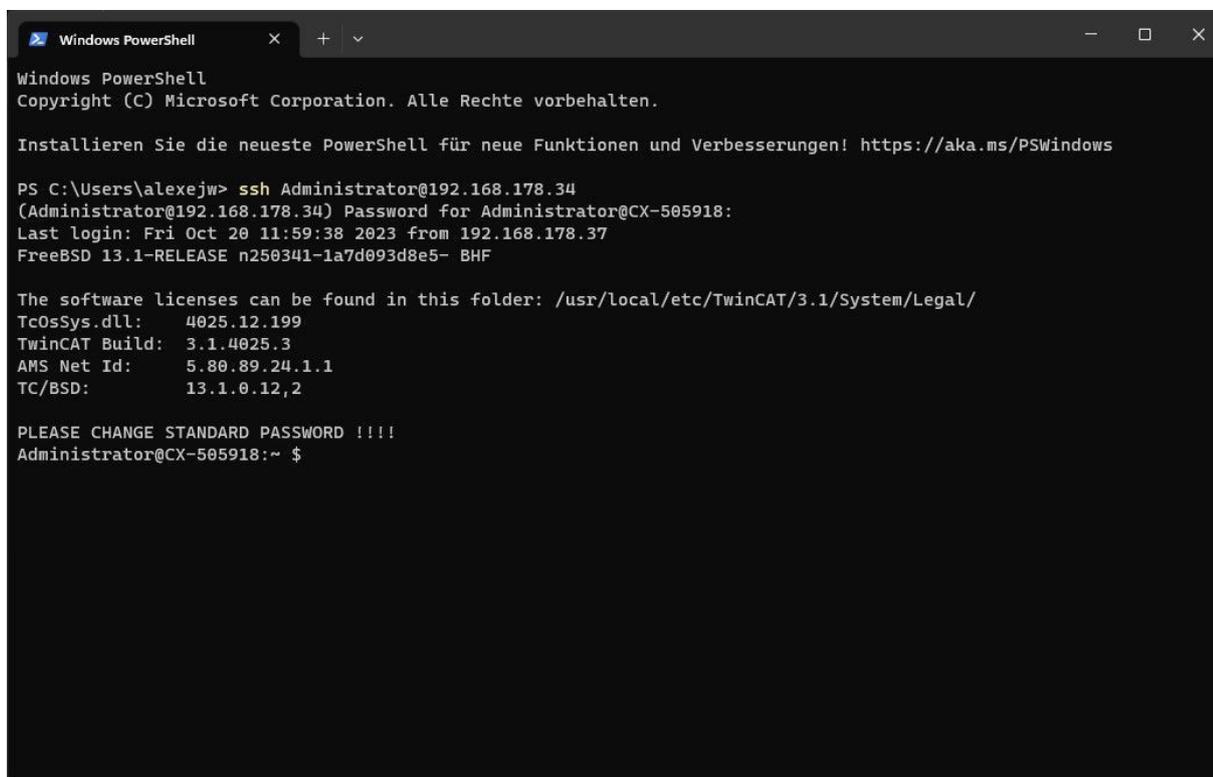
Wenn Sie mehrere Steuerungen haben, können Sie diese anhand des Namens oder des Betriebssystems identifizieren. Beachten Sie, dass unter TwinCAT/BSD standardmäßig nur Secure-ADS aktiviert ist. Eine detaillierte Beschreibung, wie die Funktion Broadcast-Search verwendet und wie nach einem TwinCAT/BSD-Zielsystem gesucht werden kann, finden Sie unter: [Zielsysteme suchen](#) [► 111].

Wenn Sie eine direkte Verbindung zu Ihrem Laptop ohne DHCP haben, weist sich das TwinCAT/BSD-Gerät selbst eine Auto-IP-Adresse aus dem Bereich 169.254 zu, und die letzten beiden Bytes werden dann von den letzten beiden Bytes der MAC-Adresse (169.254.{MAC5}.{MAC6}) abgeleitet, die auf dem Typenschild aufgedruckt ist.

2.3 Zugriff über SSH, webbasierte Konsole oder Webinterface

SSH-Zugriff

Wenn Sie einen SSH-Client auf Ihrem Laptop haben, können Sie diesen für die Verbindung verwenden. Bei den aktuellen Windows 10-Versionen ist dies beispielsweise eine Windows-Funktion, die über PowerShell verwendet werden kann. Benutzen Sie dafür den Befehl `ssh Administrator@<bsd-ip>`.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

Installieren Sie die neueste PowerShell für neue Funktionen und Verbesserungen! https://aka.ms/PSWindows

PS C:\Users\alexejw> ssh Administrator@192.168.178.34
(Administrator@192.168.178.34) Password for Administrator@CX-505918:
Last login: Fri Oct 20 11:59:38 2023 from 192.168.178.37
FreeBSD 13.1-RELEASE n250341-1a7d093d8e5- BHF

The software licenses can be found in this folder: /usr/local/etc/TwinCAT/3.1/System/Legal/
TcOsSys.dll:      4025.12.199
TwinCAT Build:   3.1.4025.3
AMS Net Id:      5.80.89.24.1.1
TC/BSD:          13.1.0.12,2

PLEASE CHANGE STANDARD PASSWORD !!!!
Administrator@CX-505918:~ $
```

Abb. 3: Remote-Zugriff über SSH mit Hilfe der Windows PowerShell.

Webbasierte Konsole

Wenn Sie nicht über einen SSH-Client verfügen, ist auf dem Gerät eine webbasierte Konsole verfügbar, auf die Sie mit einem Browser über HTTPS und die IP-Adresse des Geräts zugreifen können. Mit der Eingabe von `https://<ip-adress>/console` im Browser gelangen Sie auf die webbasierte Konsole.

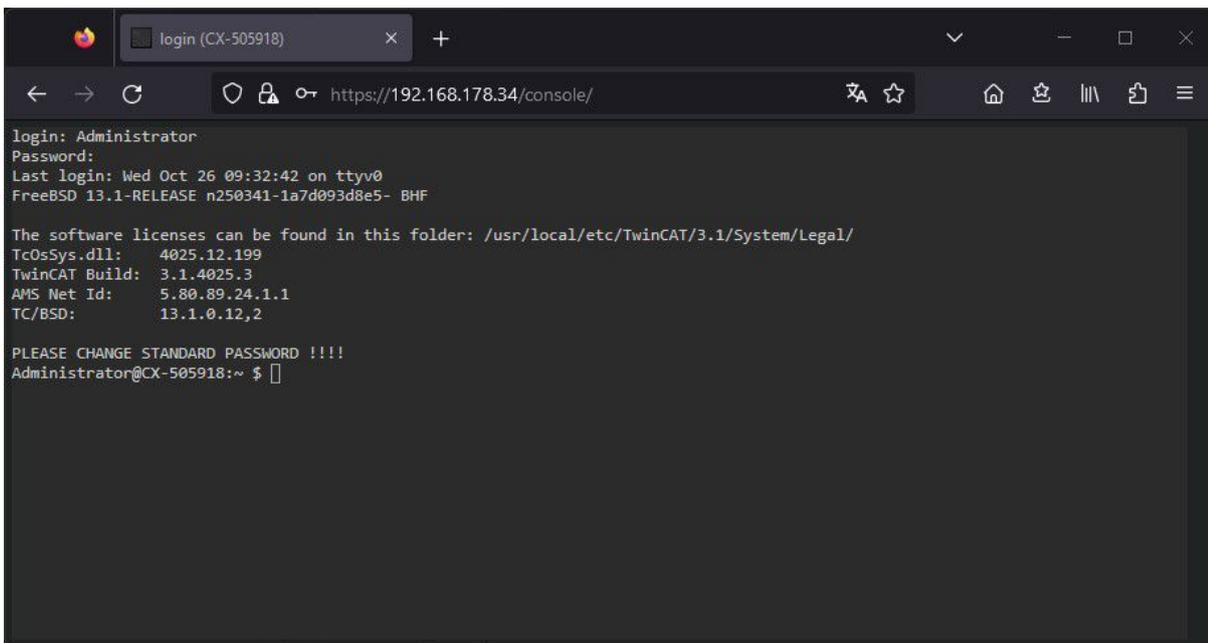


Abb. 4: Zugriff über die webbasierte Konsole eines TwinCAT/BSD-Systems.

Da das Gerät über ein selbstsigniertes Zertifikat verfügt, zeigt der Browser eine Warnung an, dass er das Zertifikat nicht verifizieren konnte. Sie können dies einfach ignorieren und fortfahren. Sie sehen nun eine Konsole in Ihrem Webbrowser

Beckhoff Device Manager: Webinterface

Wenn Sie eine grafische Oberfläche bevorzugen und kein Terminal verwenden möchten, können Sie auch auf die Website des Beckhoff Device Managers zugreifen, was der einfachste Weg ist, das Gerät zu konfigurieren. Geben Sie dazu einfach die IP-Adresse in den Browser ein. Weitere Informationen siehe: [Beckhoff Device Manager: Webinterface \[► 69\]](#).

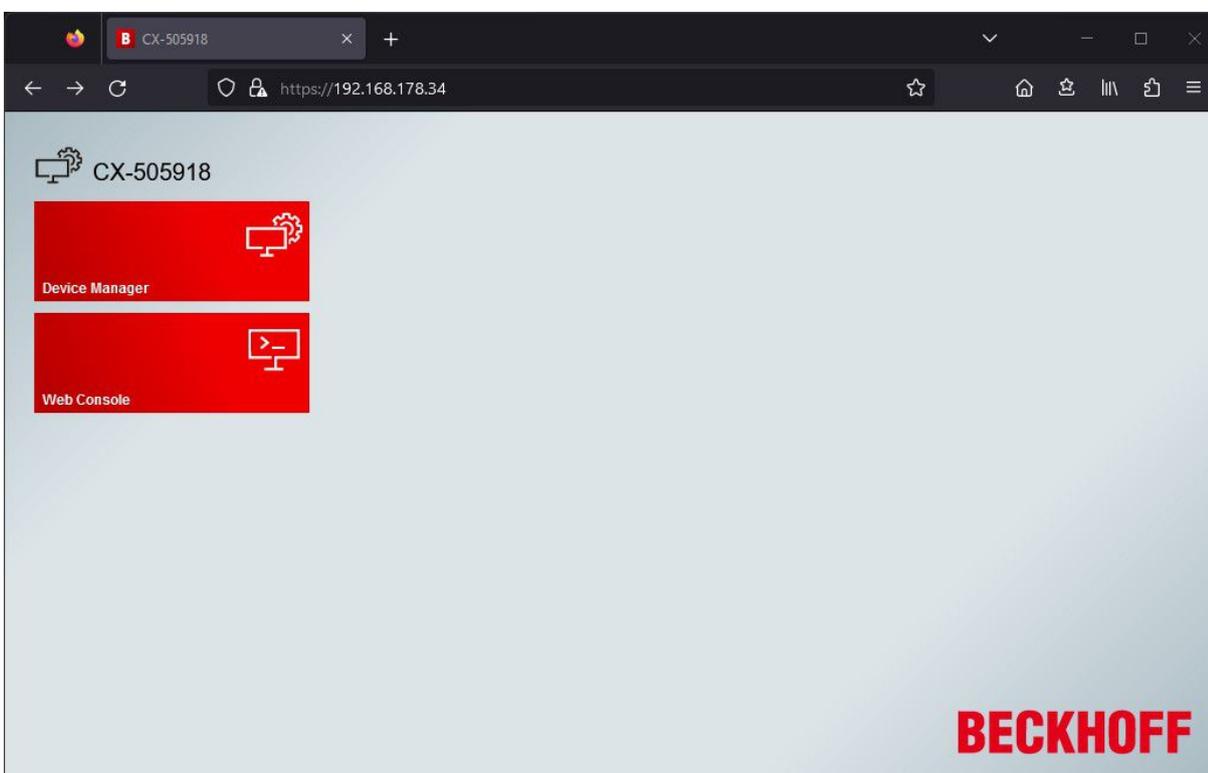


Abb. 5: Zugriff auf den Gerätemanager eines TwinCAT/BSD-Systems.

2.4 Standardpasswort ändern

Ändern Sie das Passwort für das Administratorkonto, was immer einer der ersten Schritte sein sollte, wenn Sie ein neues System erhalten. Abhängig davon, ob Sie einen Bildschirm angeschlossen haben, kann das Standardpasswort in der Konsole oder im Webinterface des Beckhoff Device Managers geändert werden.

Passwort in der Konsole ändern

Das Passwort des jeweils eingeloggten Benutzers ändern Sie mit dem Befehl `passwd`. Bei Auslieferung von TwinCAT/BSD ist standardmäßig ein Benutzer (Administrator) vorhanden, mit dem Sie sich in der Konsole anmelden können. Er besitzt keine klassischen Administrator-Rechte wie unter Windows-Systemen, hat jedoch die Berechtigung, sich für bestimmte Zwecke Root-Rechte zu beschaffen.

1. Starten Sie TwinCAT/BSD.
2. Loggen Sie sich mit dem Benutzernamen `Administrator` und dem Passwort `1` ein.
3. Nach erfolgreicher Anmeldung werden der Benutzer und der Hostname des Industrie-PCs angezeigt. Zum Beispiel: `CX-1D7BD4`.
4. Geben Sie den Befehl `passwd` ein, um ein neues Passwort für TwinCAT/BSD festzulegen. Folgen Sie den weiteren Anweisungen.

⇒ Sie haben erfolgreich ein neues Passwort für TwinCAT/BSD und den Benutzer Administrator festgelegt.

Passwort im Beckhoff Device Manager ändern

Das Webinterface des Beckhoff Device Managers kann über einen Standard-Webbrowser aufgerufen werden. Geben Sie dazu in die Suchleiste die IP-Adresse oder den Hostnamen des Industrie-PCs ein. Ändern Sie das Standardpasswort unter **Security > Login**.

The screenshot shows the Beckhoff Device Manager web interface. On the left is a navigation menu with icons and labels for 'Device', 'Hardware', 'Software', 'TwinCAT', and 'Security'. The 'Security' menu item is highlighted in red. The main content area is titled 'Login' and contains a 'Change User Passwords' section with four input fields: 'Username', 'Password', 'New Password', and 'New Password (confirm)'. Below this is a 'User Management' section with three sub-sections: 'Add User' (with three input fields), 'Add Local Group' (with one input field), and 'Set Local Group Membership' (with a radio button for 'Add' and 'Delete', and two input fields for 'Username' and 'Groupname'). Each sub-section has a confirmation icon (checkmark) and a cancel icon (X).

Abb. 6: Passwort ändern im Webinterface des Beckhoff Device Managers.

3 Beckhoff TwinCAT/BSD-Installer

Der Beckhoff TwinCAT/BSD-Installer bietet eine breite Palette von Funktionen und Anwendungsfällen, die weit über die einfache Installation des TwinCAT/BSD-Betriebssystems auf einem Industrie-PC hinausgehen. Hier sind die verschiedenen Möglichkeiten im Detail:

1. [Installation von TwinCAT/BSD](#) [► 19]: Wie bereits erwähnt, ist die primäre Funktion des TwinCAT/BSD-Installer die Installation des TwinCAT/BSD-Betriebssystems auf einem Industrie-PC.
2. [Backup-Erstellung](#) [► 123]: Mit dem TwinCAT/BSD-Installer können Sie Backups erstellen, um Daten und Konfigurationen zu sichern. Diese Backups können später verwendet werden, um das System im Falle eines Ausfalls oder einer Störung schnell wiederherzustellen.
3. [Backup-Wiederherstellung](#) [► 124]: Falls ein Problem auftritt oder eine Wiederherstellung erforderlich ist, ermöglicht der TwinCAT/BSD-Installer die Wiederherstellung von zuvor erstellten Backups. Dies gewährleistet die Kontinuität des Betriebs und minimiert Ausfallzeiten.
4. [Starten einer Shell](#) [► 130]: Der TwinCAT/BSD-Installer ermöglicht auch das Starten einer Shell. Diese Shell bietet Zugriff auf ein vollwertiges FreeBSD-System, welches auf dem USB-Stick installiert ist. Dies ist äußerst nützlich für Wartungs- und Diagnosezwecke, da Sie direkt vom USB-Stick auf das FreeBSD-System zugreifen können, ohne die Hauptinstallation zu beeinträchtigen.
5. [Automatisierung von Prozessen mit Skripten](#) [► 23]: Der TwinCAT/BSD-Installer ermöglicht das Speichern und Ausführen von Skripten zur Automatisierung von Prozessen. Diese Skripte bieten die Flexibilität, benutzerdefinierte Automatisierungsprozesse durchzuführen, um wiederkehrende Aufgaben zu automatisieren und den Installations- und Konfigurationsprozess weiter zu optimieren.

Zusammenfassend bietet der Beckhoff TwinCAT/BSD-Installer eine umfassendes Werkzeug für die Installation, Sicherung, Verwaltung und Automatisierung von TwinCAT/BSD-Systemen auf Industrie-PCs. Von der Erstinstallation bis zur Wiederherstellung und der Möglichkeit zur direkten Systemverwaltung sowie der Automatisierung von Prozessen.

Download und Installation

Der TwinCAT/BSD-Installer, inklusive der aktuellen TwinCAT/BSD-Version, steht als bootfähige ISO-Datei auf der [Beckhoff-Homepage](#) zum Download bereit. Mit der ISO-Datei kann ein bootfähiger USB-Stick [► 19] erstellt und von diesem ein Industrie-PC gebootet werden, um anschließend eine grafische Benutzeroberfläche mit interaktivem Menü zu starten.

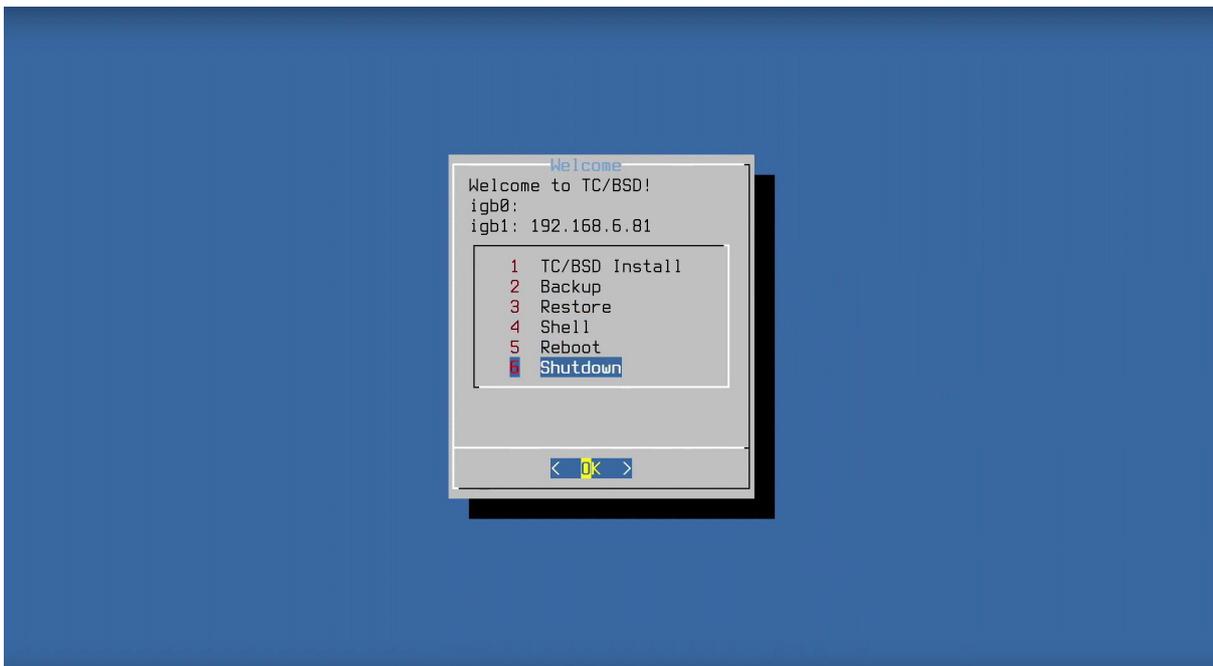


Abb. 7: Beckhoff TwinCAT/BSD-Installer: Startseite mit interaktivem Menü.

Benutzen Sie dafür ein Flashtool wie beispielsweise [Rufus](#), um die bootfähige ISO-Datei auf einen USB-Stick zu übertragen, wodurch der USB-Stick erst zu einem tragbaren TwinCAT/BSD-Installer wird.

Software und Lizenzierung

Die TwinCAT/BSD-Installation beinhaltet eine TwinCAT-3-Runtime, mit der Möglichkeit, weitere Software und TwinCAT-3-Functions zu installieren. Diese Software beinhaltet keine separate kommerzielle Lizenz und ist nur für Testzwecke vorgesehen. Für eine kommerzielle Nutzung des Produkts ist eine separate Lizenz sowie ein Lizenzaufkleber erforderlich. Eine TwinCAT/BSD-Lizenz kann für vorhandene Geräte beim Service angefragt werden.

3.1 Partitionen und Ordnerstruktur

Auf dem Beckhoff TwinCAT/BSD-Installer-Stick befinden sich zwei Partitionen, eine FreeBSD-Partition mit einem read-only Unix-Dateisystem (UFS) und eine FAT-Partition zur Speicherung von Backups und Skripten, die zur Automatisierung von Prozessen verwendet werden können. Achten Sie darauf, dass die FAT-Partition erst nach dem ersten Booten des USB-Sticks eingerichtet wird.

Wenn Sie den USB-Stick direkt nach der Erstellung in einen Industrie-PC einstecken, heißt die FAT-Partition zunächst BHF-PREOP. Erst wenn Sie das erste Mal vom USB-Stick booten, wird die FAT-Partition in BHF umbenannt.

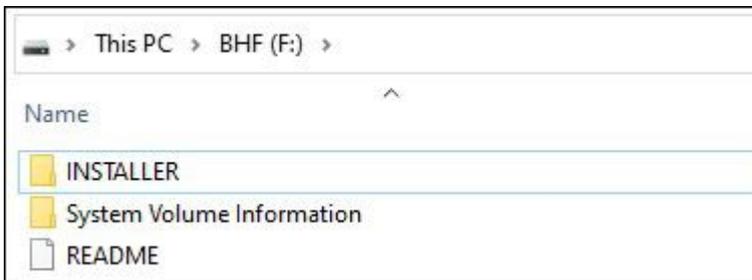


Abb. 8: FAT-Partition und Ordnerstruktur des TwinCAT/BSD-Installer-Sticks unter Windows.

Auf der FAT-Partition befinden sich zwei Ordner und eine Readme-Datei mit kurzer Beschreibung aller Ordner. Der Installer-Ordner enthält Ordner für SSH-Keys, Logs und alles zur Automatisierung von Prozessen mit dem TwinCAT/BSD-Installer-Stick.

Backups, die mit dem TwinCAT/BSD-Installer-Stick erstellt werden, werden in einem eigenen Ordner mit der Dateiendung *.tcbkp00 gespeichert. Da es sich um eine FAT-Partition handelt, beträgt die maximale Größe einer einzelnen Datei 4 GB. Wenn das Backup die 4 GB überschreitet, wird das Backup in mehrere Teile von 4 GB aufgeteilt.

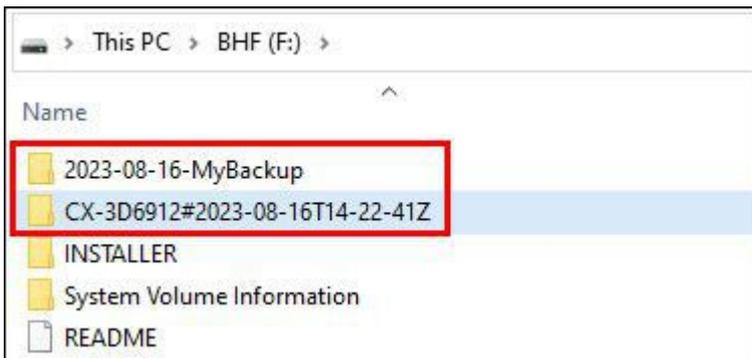


Abb. 9: Ordnerstruktur des TwinCAT/BSD-Installer-Sticks mit zwei Backup-Ordnern.

Um bereits vorhandene Backups, beispielsweise aus einem Archiv, auf den TwinCAT/BSD-Installer-Stick zu kopieren, gehen Sie wie folgt vor: Erstellen Sie auf dem Stick einen Ordner mit einem beliebigen Namen. Legen Sie das Backup mit der Dateiendung *.tcbkp00 in diesem Ordner ab.

Hinweis Wenn der TwinCAT/BSD-Installer-Stick initial erstellt wurde, muss einmal vom Stick gebootet werden, damit die notwendigen Partitionen angelegt werden.

Der Installer-Ordner enthält weitere Unterordner, die einerseits Beispielskripte enthalten und andererseits dazu verwendet werden können, eigene Skripte zur Automatisierung von Prozessen mit dem TwinCAT/BSD-Installer-Stick zu speichern. So können z. B. Skripte erstellt werden, die sofort nach der Installation

ausgeführt werden, um ein frisch installiertes Image an die eigenen Bedürfnisse anzupassen. Oder es können Skripte verwendet werden, die automatisch ein TwinCAT/BSD-System sichern oder wiederherstellen, sobald der TwinCAT/BSD-Installer-Stick eingesteckt ist.

Die aufgeführten Beispiele sind nicht vollständig und es sind weitere Szenarien für den Einsatz von Skripten denkbar. Die folgende Tabelle beschreibt, in welchem Verzeichnis die Skripte für die jeweilige Aufgabe abgelegt werden müssen, um ordnungsgemäß zu funktionieren.

Tab. 3: Beschreibung der Verzeichnisse im Installer-Ordner.

Verzeichnis	Beschreibung
/INSTALLER	Basisverzeichnis für Dateien, die keine Backup-Daten sind.
/INSTALLER/.ssh	Kopieren Sie Ihren Public-Key hierher, um eine Verbindung zum TwinCAT/BSD-Installer über SSH herzustellen. Sie müssen das Beispiel „start_ssh_server“ aktivieren, um eine Verbindung herzustellen. Das Beispiel befindet sich bereits standardmäßig im Autorun-Ordner.
/INSTALLER/autorun	Skripte, die hier abgelegt sind, werden nach dem Booten automatisch in alphabetischer Reihenfolge ausgeführt.
/INSTALLER/logs	Hier finden Sie Log-Dateien von Autorun-Skripten.
/INSTALLER/autorun_samples	Ordner mit fertigen Beispielen. Alle Skripte aus dem Beispielordner müssen in das Verzeichnis <code>/INSTALLER/autorun/</code> kopiert werden, um eine spezifische Aufgabe auszuführen (z.B. <code>start_ssh_server</code>).
/INSTALLER/autorun_samples/start_ssh_server	Dieses Beispiel startet den SSH-Daemon, um SSH-Verbindungen zu ermöglichen und wird standardmäßig ausgeführt.
/INSTALLER/autorun_samples/autoinstall_tcbsd	Beispiel für die automatische Installation von TwinCAT/BSD. Das System wird standardmäßig auf der größten verfügbaren Festplatte installiert. Eine bestimmte Festplatte kann als Parameter im Skript konfiguriert werden. Das Standardpasswort für das installierte System wird als Umgebungsvariable bereitgestellt und kann im Skript angepasst werden.
/INSTALLER/autorun_samples/auto_backup	Beispiel für die automatische Sicherung eines TwinCAT/BSD-Systems. Das Skript sucht nach einem TwinCAT/BSD-System, indem es nach einer Festplatte sucht, die einen Pool „zroot“ enthält. Es wird ein Backup mit einem Dateinamen aus dem Hostnamen des Systems und dem aktuellen Zeitstempel generiert und im Verzeichnis <code>\INSTALLER</code> abgelegt.
/INSTALLER/autorun_samples/auto_restore	Beispiel für die automatische Wiederherstellung einer TwinCAT/BSD-Sicherung. Sie können die Zielfestplatte durch einen Parameter im Skript auswählen. Zusätzlich können Sie eine Sicherungsdatei anhand ihres Namens als Muster auswählen (z.B. „.tcbkp“ für jede Sicherung oder „backup1.tcbkp00“ für eine bestimmte Sicherung). Standardmäßig werden verfügbare Sicherungen nach ihrer Dateiendung alphabetisch aufgelistet. Die erste wird zur Wiederherstellung ausgewählt und auf der größten verfügbaren Festplatte wiederhergestellt, wenn keine Festplatte angegeben wurde.
/INSTALLER/post_install.d	Dieser Ordner enthält Skripte, die dazu bestimmt sind, das installierte System zu ändern. Die Skripte müssen einen der folgenden Namen haben: <ul style="list-style-type: none"> • *.installer: Skripte, die auf „.installer“ enden, werden im Rahmen des TwinCAT/BSD-Installers ausgeführt. Der Pfad zum Ordner, auf dem das installierte System gemountet ist, wird als Argument \$1 bereitgestellt. Dies ist nützlich, wenn Sie z.B. Dateien in das System kopieren wollen, da Sie in diesem Fall auf das Dateisystem des TwinCAT/BSD-Installers zugreifen. • *.chroot: Skripte, die auf „.chroot“ enden, werden im Rahmen des installierten Systems ausgeführt. Dies bietet eine bequemere Methode zur Modifizierung von Benutzerkonten oder zur Installation von Paketen.
/INSTALLER/runonce.d	Der Inhalt dieses Ordners wird in den Ordner „runonce“ im installierten System kopiert. Skripte im Runonce-Ordner werden einmalig ausgeführt und dann deaktiviert, indem sie entweder in „runonce.d/succeeded“ oder „runonce.d/failed“ verschoben werden. Das ist hilfreich, wenn der Industrie-PC einmal gebootet werden muss, beispielsweise wenn bestimmte Kernelmodule benötigt werden, die erst nach dem Booten geladen werden können.
/autorun_preop.sh	Wird beim ersten Booten des TwinCAT/BSD-Installers ausgeführt, um gerätespezifische Anpassungen vorzunehmen.

3.2 Einrichtung und Installation

Dieses Kapitel bieten eine detaillierte Anleitung zur Installation von TwinCAT/BSD auf einem Industrie-PC. Im ersten Abschnitt werden die Schritte zur Erstellung eines bootfähigen USB-Sticks unter Verwendung des Rufus-Tools erläutert, einschließlich der erforderlichen Voraussetzungen. Im zweiten Abschnitt werden die notwendigen Schritte zur Konfiguration der BIOS-Einstellungen beschrieben, um sicherzustellen, dass der Industrie-PC von diesem USB-Stick booten kann. Schließlich wird im dritten Abschnitt der gesamte Installationsprozess behandelt.

3.2.1 Bootfähigen USB-Stick erstellen

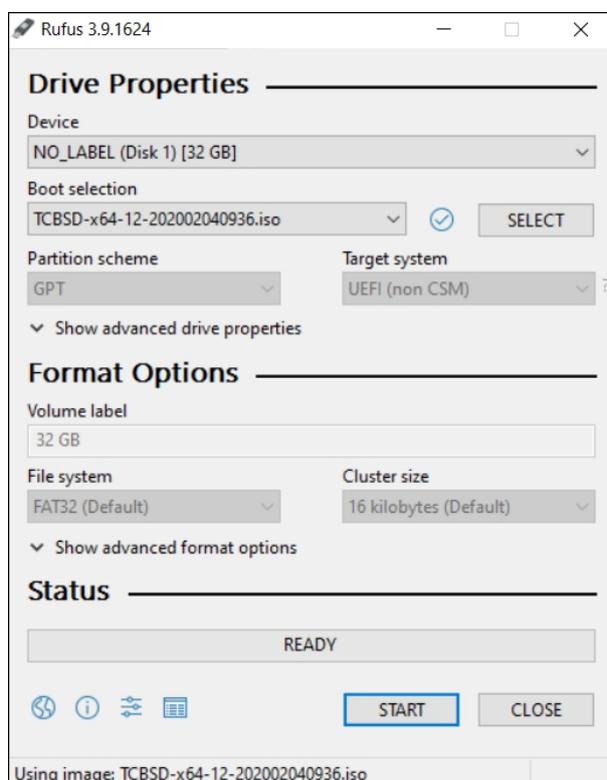
Bevor Sie TwinCAT/BSD auf einem Industrie-PC installieren können, müssen Sie einen bootfähigen USB-Stick erstellen und das aktuelle Image auf den USB-Stick aufspielen. Benutzen Sie dafür ein Flashtool wie beispielsweise Rufus. Anschließend können Sie den Industrie-PC vom USB-Stick starten und TwinCAT/BSD installieren.

Voraussetzungen für diesen Arbeitsschritt:

- Rufus-Tool heruntergeladen unter <https://rufus.ie/>
Hinweis: Beachten Sie, dass neuere Versionen von rufus möglicherweise nicht mit Tools für Festplattenverschlüsselung kompatibel sind. Empfohlen wird daher die Verwendung von Rufus 3.13.
- [Bootfähige ISO-Datei](#) für die Installation von TwinCAT/BSD
- USB-Stick mit mindestens 2 GB Speicherplatz.

Gehen Sie wie folgt vor:

1. Starten Sie das Rufus-Tool auf einem PC mit Windows Betriebssystem.
2. Klicken Sie auf **Select** und wählen Sie das Image aus, welches Sie auf den USB-Stick aufspielen möchten.



3. Wählen Sie unter **Device** einen USB-Stick als Ziellaufwerk aus. Wenn nur ein externes Laufwerk mit ihrem PC verbunden ist, dann wird der USB-Stick automatisch ausgewählt.
Hinweis: Daten auf dem USB-Stick werden unwiderruflich gelöscht.
4. Klicken Sie auf **Start**, um das Image auf den USB-Stick aufzuspielen.

- ⇒ Der Vorgang kann einige Minuten dauern. Brechen Sie den Vorgang nicht ab, bis die Meldung **Ready** erscheint. Sie haben erfolgreich einen bootfähigen USB-Stick erstellt und können im nächsten Schritt TwinCAT/BSD auf dem Industrie-PC installieren.

3.2.2 BIOS-Einstellungen überprüfen

Überprüfen Sie die BIOS Einstellungen, um den Industrie-PC von dem zuvor erstellten USB-Stick starten zu können. Für TwinCAT/BSD muss der Bootmodus im BIOS auf UEFI oder Dual Boot stehen. Wählen Sie Dual Boot, wenn Sie zwischen Speichermedien mit unterschiedlichen Betriebssystemen wechseln wollen.

Starten Sie das BIOS-Setup und passen Sie den Bootmodus an, wenn die Einstellungen auf Ihrem Industrie-PC abweichen.

Gehen Sie wie folgt vor:

1. Starten Sie Ihren Industrie-PC neu und drücken Sie **[Entf]**, um das BIOS-Setup zu starten.
Das Fenster BIOS-Setup erscheint.
 2. Stellen Sie unter **Boot > Boot mode select** die Option **UEFI** oder **DUAL** ein.
 3. Drücken Sie **[F4]**, um die Einstellungen zu speichern und das BIOS-Setup zu verlassen.
Das Gerät wird neu gestartet.
- ⇒ Sie haben das BIOS erfolgreich konfiguriert und können im nächsten Schritt TwinCAT/BSD installieren.

3.2.3 TwinCAT/BSD installieren

Schließen Sie den bootfähigen USB-Stick mit TwinCAT/BSD Image an einen Industrie-PC an und starten das Gerät.

Voraussetzungen:

- Bootfähiger USB-Stick mit TwinCAT/BSD Image.
- Min. 4 GB freien Speicherplatz.

Gehen Sie wie folgt vor:

1. Schließen Sie den USB-Stick mit TwinCAT/BSD Image an den Industrie-PC an.
2. Starten Sie den Industrie-PC und drücken Sie **[F7]**, um in das Bootmenü zu gelangen.
3. Wählen Sie den UEFI-Eintrag für den USB-Stick aus und bestätigen mit **[Enter]**.
Der Industrie-PC bootet vom USB-Stick und der Beckhoff TwinCAT/BSD-Installer wird ausgeführt.
4. Wählen Sie die Option **TC/BSD Install**, um TwinCAT/BSD zu installieren.



5. Vergeben Sie ein Passwort und folgen Sie den weiteren Installationsanweisungen.
- ⇒ Starten Sie den Industrie-PC neu. TwinCAT/BSD wird geladen.

3.3 Remote-Zugriff auf den TwinCAT/BSD-Installer über SSH

SSH steht für Secure Shell und ist eine Methode zur Herstellung einer sicheren Verbindung zwischen zwei Computern. SSH funktioniert durch Authentifizierung basierend auf einem Schlüsselpaar, wobei sich der private Schlüssel auf einem entfernten Server oder Industrie-PC und der entsprechende öffentliche Schlüssel auf einem lokalen Computer befindet. Wenn die Schlüssel übereinstimmen, wird dem Benutzer Zugriff gewährt.

In diesem Kapitel wird gezeigt, wie Sie eine SSH-Verbindung von einem lokalen PC zu einem Industrie-PC mit einem TwinCAT/BSD-Installer herstellen und auf dessen Shell zugreifen können. Dadurch haben Sie Zugriff auf ein vollwertiges TwinCAT/BSD-System, was Sie zur Reparatur oder Datenrettung nutzen können, wenn beispielsweise ein fehlerhafter Prozess einen Systemstart verhindert oder ein fehlerhaftes TwinCAT-Projekt eine Bootschleife verursacht.

Voraussetzungen:

- Bevor Sie eine Remote-Verbindung über SSH herstellen können, müssen Sie sicherstellen, dass der TwinCAT/BSD-Installer auf dem USB-Stick eingerichtet ist.
- Der SSH-Server muss aktiv sein. Das Skript „start_ssh_server“ befindet sich dafür bereits auf dem USB-Stick im Ordner */INSTALLER/autorun*.

Gehen Sie wie folgt vor:

1. Bevor Sie eine SSH-Verbindung herstellen können, müssen Sie ein SSH-Schlüsselpaar auf Ihrem lokalen PC generieren. Dieses Schlüsselpaar besteht aus einem privaten und einem öffentlichen Schlüssel.

Unter Windows 10 kann das SSH-Schlüsselpaar mit OpenSSH generiert werden. Öffnen Sie die Eingabeaufforderung (Command Prompt) als Administrator auf Ihrem Windows 10-PC und führen Sie folgenden Befehl aus:

```
ssh-keygen -t ed25519
```

2. Sie werden aufgefordert, einen Speicherort anzugeben und optional ein Kennwort festzulegen. Das generierte Schlüsselpaar wird standardmäßig im Verzeichnis *C:\Users*Ihr Benutzername*\.ssh* gespeichert.

```
Generating public/private ed25519 key pair.  
Enter file in which to save the key (C:\Users\username\.ssh\id_ed25519):
```

3. Jetzt haben Sie einen öffentlichen und privaten Schlüssel an dem angegebenen Speicherort. Die *.pub*-Dateien sind öffentliche Schlüssel, und Dateien ohne Erweiterung sind private Schlüssel.
4. Verwenden Sie den Befehl `ssh-add`, um den privaten Schlüssel in den SSH-Agenten zu laden. Dadurch wird die SSH-Authentifizierung einfacher und sicherer, da der private Schlüssel verschlüsselt im SSH-Agenten gespeichert ist. Öffnen Sie dazu die Eingabeaufforderung auf Ihrem lokalen PC und geben Sie den folgenden Befehl ein:

```
ssh-add %env:USERPROFILE\.ssh\id_ed25519
```

5. Der Inhalt des öffentlichen Schlüssels (*.ssh\id_ed25519.pub*) muss auf dem TwinCAT/BSD-Installer in einer Datei namens *authorized_keys* unter *\INSTALLER\.ssh* abgelegt werden.
6. Ab jetzt können Sie von ihrem lokalen PC oder von jedem Client aus, der über den privaten Schlüssel verfügt, eine Verbindung mit dem TwinCAT/BSD-Installer herstellen. Öffnen Sie die Eingabeaufforderung auf Ihrem lokalen PC und verwenden Sie den folgenden Befehl:

```
ssh root@<IP of TwinCAT/BSD installer>
```

7. Die IP-Adresse des TwinCAT/BSD-Installers wird nach dem Booten in der grafischen Benutzeroberfläche angezeigt. Zusätzlich kann im Vorfeld mit Hilfe der Shell eine feste IP-Adresse für den USB-Stick konfiguriert werden.
- ⇒ Nach erfolgreicher Authentifizierung über SSH haben Sie Zugriff auf den TwinCAT/BSD-Installer und damit auf die Shell des darauf installierten TwinCAT/BSD-Systems. Sie können nun die erforderlichen Aufgaben ausführen, wie die Installation oder Wartung des Betriebssystems.

3.4 Automatisierung von Prozessen – Skripte in der Praxis einsetzen

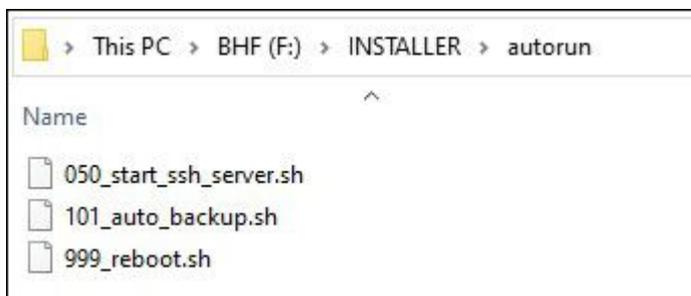
In diesem Kapitel wird an einem Beispiel beschrieben, wie Skripte in Verbindung mit dem TwinCAT/BSD-Installer eingesetzt werden können. Skripte sind äußerst nützlich, um verschiedene Aufgaben im Zusammenhang mit TwinCAT/BSD-Systemen und dem TwinCAT/BSD-Installer zu automatisieren. Sie können verwendet werden, um Backups zu erstellen, Backups wiederherzustellen, das System zu konfigurieren, automatische Installationen durchzuführen und vieles mehr.

In diesem Kapitel beschränken wir uns auf ein Szenario, indem ein Backup automatisch von einem TwinCAT/BSD-System mit Hilfe eines TwinCAT/BSD-Installers erstellt wird.

Es sind weitere Szenarien für den Einsatz von Skripten denkbar. Zur Erinnerung: die folgende [Tabelle \[► 18\]](#) beschreibt, in welchem Verzeichnis die Skripte für die jeweilige Aufgabe abgelegt werden müssen, um ordnungsgemäß zu funktionieren.

Gehen Sie wie folgt vor:

1. Kopieren Sie die Skripte `auto_backup.sh` und `reboot.sh` aus dem Verzeichnis `\INSTALLER\autorun_samples\auto_backup` in das Verzeichnis `\INSTALLER\autorun`.



2. Stecken Sie den so präparierten USB-Stick in einen Industrie-PC.
 3. Starten Sie den Industrie-PC neu und drücken Sie **[F7]**, um in das Bootmenü zu gelangen. Wählen Sie im Bootmenü den USB-Stick aus, vom dem Sie booten möchten.
 4. Der TwinCAT/BSD-Installer wird gestartet und anschließend automatisch ein Backup erstellt. Es wird ein Backup mit einem Dateinamen aus dem Hostnamen des Systems und dem aktuellen Zeitstempel generiert und im Verzeichnis `\INSTALLER` abgelegt. Eine Interaktion mit der grafischen Benutzeroberfläche ist nicht erforderlich.
 5. Im letzten Schritt wird der Industrie-PC nach dem Backup mit Hilfe des Skript `reboot.sh` neu gestartet.
- ⇒ Das Backup wird auf dem USB-Stick im Verzeichnis `\INSTALLER` gespeichert. Wird für diese Aufgabe ein Beckhoff-Stick verwendet, so ist es nicht notwendig, das Bootmenü mit **[F7]** aufzurufen. Im BIOS sind Beckhoff USB-Sticks standardmäßig als erstes Bootmedium eingerichtet und werden automatisch erkannt. Beim Einstecken eines Beckhoff-USB-Sticks wird der USB-Stick also direkt gebootet.

4 TwinCAT/BSD

TwinCAT/BSD kombiniert die TwinCAT Runtime mit FreeBSD, einem industriell erprobten und zuverlässigen Open-Source-Betriebssystem. Neben Multicore-Unterstützung und einem kleinen Footprint bietet TwinCAT/BSD mit dem Beckhoff Package Server eine einfache Möglichkeit, um TwinCAT Functions und FreeBSD-Applikationen zu installieren oder das ganze System zu aktualisieren.

Was ist FreeBSD

FreeBSD ist ein Unix-kompatibles Open-Source-Betriebssystem, welches direkt von der Berkeley Software Distribution (BSD) abstammt. Als Open-Source-Projekt wird FreeBSD von einer großen Entwicklergruppe kontinuierlich weiterentwickelt, verbessert und optimiert. Beckhoff hat sich aufgrund der freizügigen BSD Lizenz für FreeBSD entschieden, welche die Integration von TwinCAT ohne lizenzrechtliche Probleme ermöglicht.

FreeBSD erfreut sich einer großen Beliebtheit und wird weltweit von namhaften Unternehmen eingesetzt. Eine ausführliche Auflistung der Nutzer finden Sie unter:

<https://www.freebsdoundation.org/freebsd/#whois>

FreeBSD unterstützt sowohl x86 als auch X64 Plattformen und ermöglicht skalierbare Systeme mit ARM-CPU's bis hin zu leistungsstarken Xeon-CPU's.

Weitere Informationen zu FreeBSD finden Sie auf der Homepage der FreeBSD-Foundation oder des FreeBSD Projektes:

<https://www.freebsdoundation.org/>

<https://www.freebsd.org/>

TwinCAT

TwinCAT/BSD unterstützt alle TwinCAT-3-Runtime-Funktionen. Die Programmierung erfolgt weiterhin mit dem bekannten TwinCAT XAE auf Basis von Visual Studio® auf einem Windows-Entwicklungsrechner. TwinCAT/BSD bietet Multicore-Unterstützung, wodurch auch einzelne Kerne für die exklusive Nutzung von TwinCAT reserviert werden können.

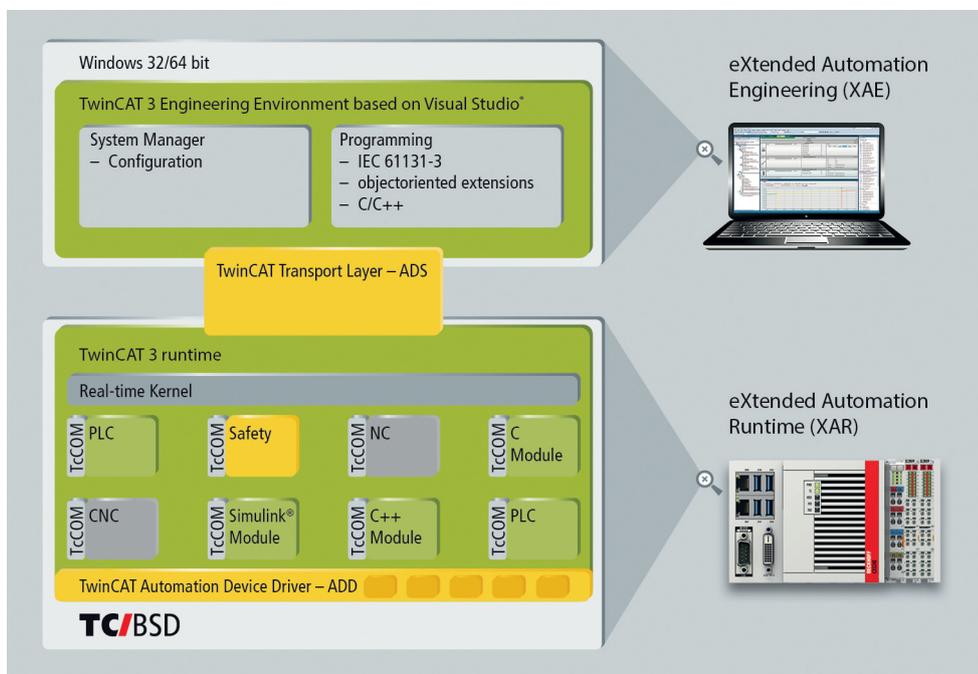


Abb. 10: Aufbau der TwinCAT 3 Runtime unter TwinCAT/BSD.

Neben dem TwinCAT HMI Server kann ein HTML5 Webbrowser als Client für TwinCAT HMI genutzt werden. Die Konfiguration erfolgt wie gewohnt über den grafischen Editor der Entwicklungsumgebung TwinCAT XAE.

Software und Updates

Neben einer Vielzahl von FreeBSD-Programmen lassen sich über den Beckhoff Package-Server auch TwinCAT Functions installieren. Über diesen Weg ist darüber hinaus das unkomplizierte Updaten des Betriebssystems sowie der TwinCAT Runtime über das Netzwerk möglich. Die Installation von Softwarepaketen kann auch offline erfolgen. Hierbei werden die Softwarepakete zuvor auf einen Entwicklungsrechner mit Netzwerkanschluss geladen und später direkt auf dem Beckhoff Industrie-PC installiert. Auch das kundenseitige Hosten eines eigenen Package-Servers ist möglich. Neben FreeBSD-Programmen, die auf diese Weise angeboten werden können, stehen ebenfalls viele von Linux bekannte Programme zur Verfügung:

<https://www.freebsd.org/ports/>

Write Filter

Wie von Windows Betriebssystemen bekannt, stellt auch TwinCAT/BSD einen Write Filter bereit, der das System vor persistenten Änderungen schützt. Nach einem Neustart befindet sich das System bei aktiviertem Write Filter wieder in einem zuvor definierten Zustand.

Sichern und Wiederherstellen

Das Sichern und Wiederherstellen eines TwinCAT/BSD-Systems kann über einen USB-Stick erfolgen, der ähnliche Funktionen wie der Beckhoff Service Stick für Windows-Betriebssysteme bietet. Auch aus dem Live-System heraus kann ein Backup erstellt werden, welches lokal oder über das Netzwerk auf einem entfernten System gesichert wird.

4.1 Zugangsdaten

● Standardpasswort ändern

I Ändern Sie aus Sicherheitsgründen das Standardpasswort nach der ersten Anmeldung.

Bei Auslieferung von TwinCAT/BSD ist standardmäßig ein Benutzer (`Administrator`) vorhanden, mit dem Sie sich in der Konsole anmelden können. Er besitzt keine klassischen Administrator-Rechte wie unter Windows-Systemen, hat jedoch die Berechtigung, sich für bestimmte Zwecke Root-Rechte zu beschaffen. Verwenden Sie den Befehl `doas`, um Root-Rechte zu erhalten. Dabei entspricht `doas` dem Befehl `sudo`, einem Befehl der aus anderen unixartigen Betriebssystemen bekannt ist.

Anmeldedaten:

- Login: `Administrator`
- Passwort: `1`

Gehen Sie wie folgt vor:

1. Starten Sie den Industrie-PC.
2. Loggen Sie sich mit dem Benutzernamen `Administrator` und dem Passwort `1` ein.
3. Nach erfolgreicher Anmeldung wird der Benutzer und der Hostname des Industrie-PCs angezeigt. Zum Beispiel: `CX-1D7BD4`.

```
Administrator@CX-1D7BD4$
```

4. Geben Sie den Befehl `passwd` ein, um ein neues Passwort für TwinCAT/BSD festzulegen. Folgen Sie den weiteren Anweisungen.

⇒ Sie haben sich erfolgreich angemeldet und ein neues Passwort für TwinCAT/BSD festgelegt.

4.2 ZFS-Eigenschaften

ZFS ist ein Dateisystem, welches die Rollen eines Volumenmanagers und Dateisystems miteinander kombiniert. Das Besondere ist, dass ZFS die Struktur der Speichermedien kennt und auf diese Weise ein zusammenhängender Speicher-Pool (zpool) zur Verfügung steht. Der Speicher-Pool wird unter den verfügbaren Dateisystemen aufgeteilt. Sobald weitere Speichermedien zum Pool hinzugefügt werden, wachsen die existierenden Dateisysteme automatisch mit und der neue Speicherplatz wird allen Dateisystemen zur Verfügung gestellt.

Herkömmliche Dateisysteme, wie beispielsweise NTFS, ext3 oder UFS verhalten sich anders. Hier werden Festplatten, RAID-Controller, Volumenmanager und Dateisystem voneinander getrennt. Dateisysteme können nur auf einer Festplatte gleichzeitig angelegt werden. Sobald eine zweite Festplatte eingefügt wird, müssen zwei separate Dateisysteme erstellt werden.

Weitere Vorteile von ZFS sind:

- RAID-Funktionalität ist standardmäßig verfügbar.
- Ausschaltsicher durch Copy-on-Write
- Automatische Datenfehlererkennung durch Prüfsummen
- Einfache Sicherungsmöglichkeiten durch Snapshots

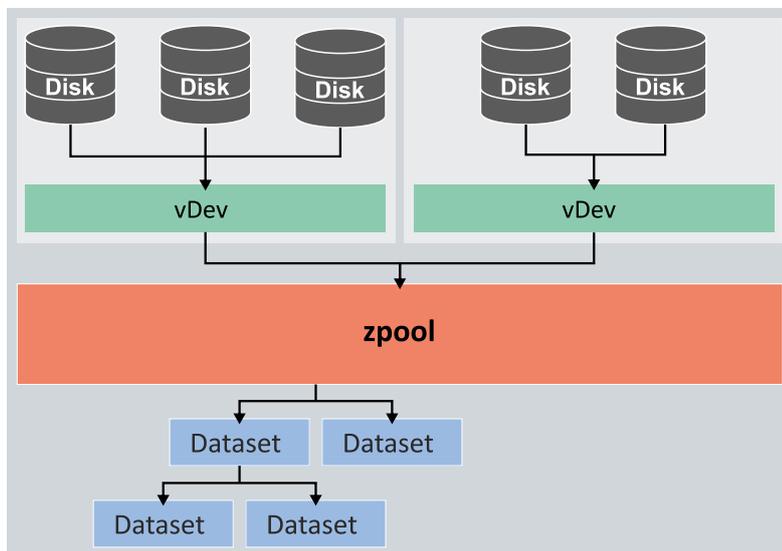


Abb. 11: Übersicht zum Aufbau des Speicher-Pools inklusive Speichermedien und Datensets.

vDev

Die vDevs repräsentieren die zugrundeliegende Hardware, wie beispielsweise HDDs, SSDs oder CFast-Karten. Es gibt verschiedene vDev-Arten. Ein vDev kann aus einer Festplatte, einer Gruppe von Festplatten, einem File, einem Mirror aus zwei oder mehreren Festplatten oder verschiedenen RAID-Z-Konfigurationen bestehen.

Wenn mehrere vDevs eingesetzt werden, dann werden die Daten unter den verfügbaren vDevs aufgeteilt, um die Geschwindigkeit zu steigern und den Speicherplatz optimal auszunutzen. Wenn ein vdev ausfällt sind die Daten des gesamten Pools verloren. Daher ist eine entsprechende Redundanz (z.B. RAID1) bei einem vdev sinnvoll.

Speicher-Pool (zpool)

Ein Speicher-Pool (zpool) wiederum besteht aus einem oder mehreren vDevs. Ein Speicher-Pool (zpool) ist die Basis von ZFS und ist im Grunde eine Ansammlung von vDevs. Die vDevs repräsentieren ihrerseits die zugrundeliegende Hardware, wie beispielsweise HDDs, SSDs oder CFast-Karten, die die Daten speichern.

Die vDevs werden zu einem Speicher-Pool zusammengefasst. Ein Speicher-Pool wird dann verwendet, um ein oder mehrere Dateisysteme (Datasets) oder Blockgeräte (Volumes) zu erstellen. Diese Datasets und Volumes teilen sich den im Pool verfügbaren Speicherplatz.

Datasets

Dataset ist der allgemeine Begriff für ein ZFS-Dateisystem, Volume, Snapshot oder Klon. Es können beliebig viele Datasets angelegt werden, die ihrerseits auf einem Speicher-Pool aufsetzen und Verzeichnisse und Dateien beibehalten. Datasets bauen hierarchisch aufeinander auf. Es gibt ein Wurzel-Dataset, mit darauffolgenden Eltern-Datasets, Kind-Datasets und weiterführende Abstufungen.

Die Datasets erben alle Eigenschaften von den Eltern und Großeltern. Es ist aber möglich, die geerbten Standardwerte der Eltern und Großeltern zu ändern und zu überschreiben. Grundsätzlich können für jedes Dataset Eigenschaften, wie beispielsweise Komprimierung, Schreib- und Lesezugriff, Speicherplatzreservierung (quotas) oder Netzwerkfreigaben festgelegt werden.

Beispiel für ein Dataset:

`zroot/tmp`

In diesem Beispiel ist `zroot/` das Wurzel-Dataset und gleichzeitig die Bezeichnung für den Speicher-Pool (zpool) unter TwinCAT/BSD. Sie können sich alle vorhandenen Datasets mit dem Befehl `zfs list` anzeigen lassen.

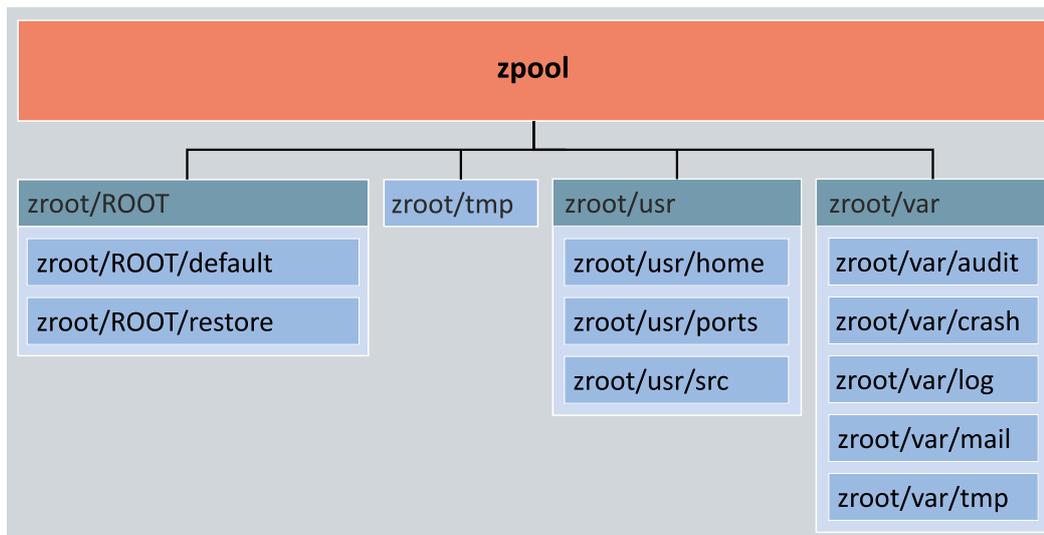


Abb. 12: Datasets des TwinCAT/BSD-Betriebssystems.

Das Dataset `zroot/ROOT/default` beinhaltet das Basissystem, alle Programme und TwinCAT. Das Dataset `zroot/ROOT/restore` ist eine Bootumgebung die zum Wiederherstellen von Wiederherstellungspunkten und dem Zurücksetzen auf Werkseinstellungen genutzt wird (siehe: [Wiederherstellungsoptionen](#) [► 119]). Die anderen Datasets werden in ihren jeweiligen Mountpoints gemountet und sind über die Dateisystemhierarchie zu erreichen (siehe: [Verzeichnisstruktur](#) [► 28]). Datasets ermöglichen das individuelle Definieren von Optionen wie Lese- und Schreibrechten für ganze Speicherbereiche oder die Begrenzung von Speicherplatz für beispielsweise Logdateien oder das Home-Verzeichnis. Darüber hinaus lassen sich einzelne Datasets durch Snapshots sichern.

Zusätzlich dazu, wird mit `zfs list` zu jedem Dataset der Standard-Mountpoint angegeben, also der Punkt in der Dateisystemhierarchie des Betriebssystems, über den auf das Dataset zugegriffen werden kann, sofern es gemountet ist. Die meisten Datasets werden direkt nach dem Systemstart automatisch gemountet. Mit dem Befehl `zfs mount` lassen sich die aktuell tatsächlich gemounteten Datasets anzeigen. Erst durch gemountete Datasets wird ein Dateisystem, Verzeichnis oder Gerät für den Benutzer zugänglich gemacht. Der Speicher-Pool (zpool) und die dazugehörigen Datasets werden in TwinCAT/BSD direkt nach dem Booten gemountet.

Volumes

Ein Volume ist ein spezieller Typ von Dataset. Es wird nicht als Dateisystem eingehängt und ist stattdessen ein Blockgerät unter `/dev/zvol/poolname/dataset`. Dies erlaubt es das Volume für andere Dateisysteme zu verwenden, die Festplatten einer virtuellen Maschine bereitzustellen oder über Protokolle wie iSCSI oder HAST (Highly Available Storage) exportiert zu werden. Ein Volume kann mit einem beliebigen Dateisystem formatiert werden oder als reiner Datenspeicher fungieren. Für den Benutzer erscheint ein Volume als eine gewöhnliche Platte mit einer fixen Größe.

4.3 Verzeichnisstruktur

Die Verzeichnisstruktur von TwinCAT/BSD basiert auf dem Filesystem-Hierarchy-Standard (FHS).

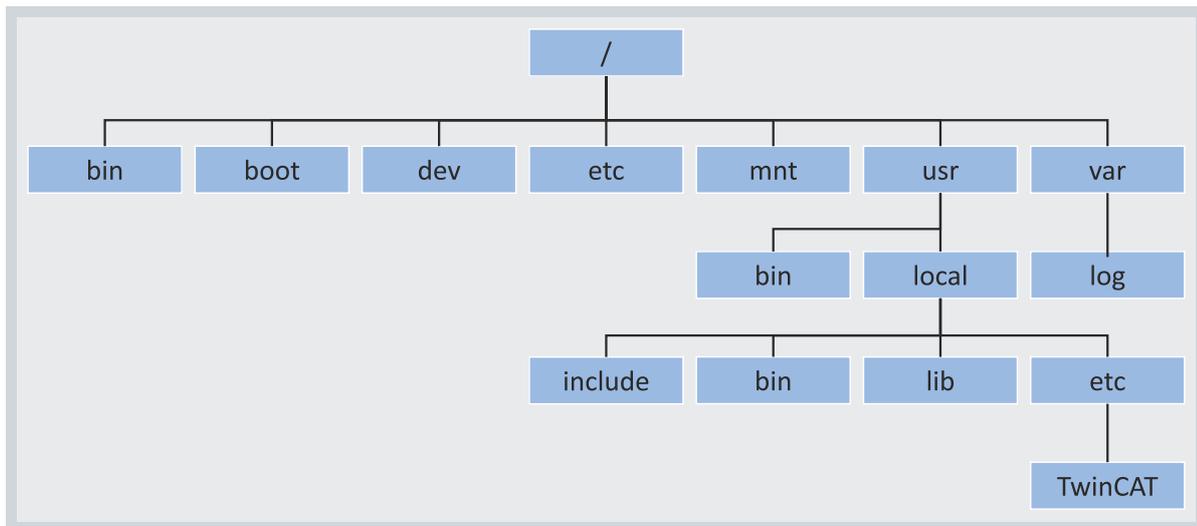


Abb. 13: TwinCAT/BSD-Verzeichnisstruktur.

Mit `cd` kann das Verzeichnis gewechselt werden. `cd ..` wechselt in der Verzeichnishierarchie eine Stufe nach oben, `cd /bin` in das Verzeichnis `/bin`. Mit `ls` werden Dateien im aktuellen Verzeichnis aufgelistet.

Tab. 4: Überblick über wichtige TwinCAT/BSD-Verzeichnisse.

Verzeichnis	Beschreibung
/	Wurzelverzeichnis und oberste Verzeichnishierarchie.
/bin/	Grundlegende Benutzeranwendungen für Single-/ und Multiuser-Umgebung.
/boot/	Kernel, Treiber, Programme und Konfigurationsdateien für den Bootprozess.
/dev/	Device-Nodes, über die beispielsweise direkt auf Hardware zugegriffen werden kann.
/etc/	Systemrelevante Skripte und Konfigurationsdateien.
/home/	Hier liegen die Home-Verzeichnisse der Benutzer.
/mnt/	Leeres Verzeichnis, dient in der Regel als Mountpoint beispielsweise für USB-Sticks.
/root/	Home-Verzeichnis des Superusers <code>root</code> .
/sbin/	Grundlegende Systemanwendungen für Single-/ und Multiuser-Umgebung.
/usr/	Unix-System-Resources, beinhaltet den Großteil der Benutzeranwendungen.
/usr/bin	Allgemeine Anwendungen.
/usr/include/	Beinhaltet Headerdateien für C-Compiler.
/usr/local/	Lokale Programme und Bibliotheken, d.h. Software die ein Benutzer selbst installiert hat, beispielsweise Software die nichts mit dem eigentlichen FreeBSD Basissystem zu tun hat.
/usr/local/bin/	Vor allem Beckhoff-Anwendungen
/usr/local/etc/	Konfigurationsdateien, TwinCAT-Verzeichnis mit TwinCAT Functions und SPS-Projekt .
/usr/local/include/	Unter anderem ADS-Headerdateien TcAdsDef.h und TcAdsAPI.h
/usr/sbin/	Systemanwendungen die vom Benutzer ausgeführt werden.
/var/	Variable Dateien, d.h. temporäre, sich ändernde Dateien wie beispielsweise Logdateien.
/var/log/	Beinhaltet Logdateien des Systems.

Programme, die in einem der bin- oder/sbin-Verzeichnisse liegen, können in der Regel ohne Pfadangabe über die Kommandozeile aufgerufen werden. Sie sind in den Shells als Umgebungsvariablen definiert.

4.4 Write Filter

TwinCAT/BSD verfügt über einen Write Filter, der bestimmte Datasets vor Schreibzugriffen schützt. Der Vorteil eines Write Filters ist, dass der Benutzer ein System in einem vorkonfigurierten Zustand sichern kann. Nach einem Neustart wird das System automatisch in den ursprünglich definierten Zustand zurückgesetzt.

Das Dataset `zroot/ROOT/default`, das den Großteil des Systems und TwinCAT beinhaltet, ist bei aktivem Write Filter vor Schreibzugriffen geschützt. Alle anderen Datasets werden nicht vom Write Filter erfasst. So können beispielsweise weiterhin Benutzerdateien unter `/home` oder Logdateien unter `/var/log` persistent gespeichert werden, auch wenn der Rest des Systems nach einem Neustart zurückgesetzt wird.

4.4.1 Write Filter aktivieren bzw. deaktivieren

In diesem Schritt wird gezeigt, wie Sie einen Write Filter unter TwinCAT/BSD aktivieren bzw. deaktivieren können. Beachten Sie, dass die Änderungen am Write Filter erst nach einem Neustart wirksam werden.

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `doas service bwf enable` in der Konsole ein, um den Write Filter zu aktivieren.
2. Bestätigen Sie den Befehl mit dem Administrator-Passwort.

```
Administrator@CX-3D6912:~ $ doas service bwf enable
Password:
bwf_enable: NO -> YES
writefilter enabled, please reboot to make your changes take effect.
```

3. Starten Sie den Industrie-PC mit `shutdown -r now neu`, damit die Einstellungen übernommen werden.
- ⇒ Der Write Filter ist nach dem Neustart aktiv. Mit dem Befehl `doas service bwf disable` wird der Write Filter wieder deaktiviert.

4.4.2 Ausnahmen definieren

Durch das Erstellen neuer Datasets lassen sich Ausnahmen für den Write Filter definieren, da nur das Dataset `zroot/ROOT/default` vor Schreibzugriffen geschützt wird und alle übrigen Datasets des Systems, auch die neu erstellen, vom Schutz ausgenommen sind.

In diesem Kapitel wird beispielhaft gezeigt, wie ein eigenes Dataset für das TwinCAT-Boot-Verzeichnis erstellt und dieses Verzeichnis dadurch vom Schutz des Write Filters ausgenommen werden kann.

Voraussetzungen:

- Sichern Sie im Vorfeld das TwinCAT-Boot-Verzeichnis, wenn Sie dieses Beispiel nachstellen.
- Deaktivieren Sie den Write Filter (siehe: [Write Filter aktivieren bzw. deaktivieren \[► 29\]](#)).

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `doas rm -rf /usr/local/etc/TwinCAT/3.1/Boot/*` ein.
2. Das Verzeichnis `usr/local/etc/TwinCAT/3.1/Boot` wird aus der Dateihierarchie herausgelöst.
3. Geben Sie den Befehl `doas zfs create -o mountpoint=/usr/local/etc/TwinCAT/3.1/Boot zroot/usr/TwinCAT-Boot` ein, damit das neue Dataset `zroot/usr/TwinCAT-Boot` gemountet wird.

⇒ Sie haben erfolgreich ein neues Dataset für das TwinCAT-Boot-Verzeichnis erstellt. Mit `zfs mount` werden alle gemounteten Datasets angezeigt, darunter auch das neue Dataset `zroot/usr/TwinCAT-Boot`. Alle darunterliegenden Verzeichnisse werden ab jetzt nicht mehr durch einen aktiven Write Filter vor Schreibzugriffen geschützt.

4.5 Texteditoren

Der Einsatz von Texteditoren ist die einfachste Methode, um TwinCAT/BSD ohne zusätzliche Programme zu konfigurieren. Dabei werden Textdateien in der Konsole mit Hilfe eines Texteditors geöffnet und bearbeitet.

Easy-Editor (ee)

Unter TwinCAT/BSD kann der Easy-Editor (ee) für diese Aufgabe verwendet werden. Geben Sie den Befehl `ee` in die Konsole ein, um den Easy-Editor zu starten. Verwenden Sie `ee filename`, um die zu editierende Datei mit dem Namen `filename` zu öffnen.

Systemdateien sind aus Sicherheitsgründen geschützt und können unter TwinCAT/BSD nur von Benutzern mit erweiterten Rechten (Root-Rechten) geöffnet werden. Verwenden Sie `(doas) doas ee filename`, um Systemdateien mit Root-Rechten zu öffnen.

Nach dem Öffnen des Editors, werden die wichtigsten Funktionen oben im Display aufgelistet.

```
^[ (escape) menu    ^y search prompt  ^k delete line    ^p prev li    ^g prev page
^o ascii code      ^x search         ^l undelete line  ^n next li    ^v next page
^u end of file     ^a begin of line  ^w delete word    ^b back 1 char
^t top of text     ^e end of line    ^r restore word   ^f forward 1 char
^c command         ^d delete char    ^j undelete char  ^z next word
=====line 1 col 0 lines from top 1 =====
```

Das Zeichen (^) steht für die **[Strg]** Taste. Wenn Sie also die Funktion `^c` verwenden möchten, müssen Sie die Tastenkombination **[Strg] + [c]** drücken.

Weitere Informationen und Funktionen zum Easy-Editor finden Sie unter:

<https://www.freebsd.org/cgi/man.cgi?query=ee&sektion=1&manpath=freebsd-release-ports>

vi-Editor

TwinCAT/BSD verfügt auch über leistungsfähigere Texteditoren wie den vi-Editor, der von erfahrenen Benutzern eingesetzt werden kann. Dieser Texteditor bieten mehr Funktionalität im Vergleich zum Easy-Editor (ee), ist aber weniger intuitiv.

Weitere Informationen und Funktionen zum vi-Editor finden Sie unter:

<https://www.freebsd.org/cgi/man.cgi?query=vi&sektion=1>

5 Netzwerkeinstellungen

Dieses Kapitel beschreibt die Netzwerkeinstellungen unter TwinCAT/BSD und führt Sie durch die erforderlichen Schritte zur Konfiguration Ihres Systems. Themen wie die IP-Adresszuweisung, die Anpassung des Hostnamens und die Aktivierung der Firewall mit Portfreigabe werden hier behandelt.

- **IP-Adresse einstellen:** In diesem Abschnitt erfahren Sie, wie Sie eine feste IP-Adresse einstellen oder dynamisch per DHCP beziehen können.
- **Hostnamen ändern:** Der Hostname identifiziert Ihr System im Netzwerk. Hier wird erklärt, wie Sie den Hostnamen anpassen können, um eine eindeutige Identifikation zu ermöglichen.
- **Firewall:** In diesem Abschnitt erfahren Sie, wie Sie die Firewall auf Ihrem System aktivieren und konfigurieren können. Zusätzlich wird gezeigt, wie Sie bestimmte Ports freigeben können, um den Zugriff auf spezifische Anwendungen zu ermöglichen.
- **WLAN:** In diesem Abschnitt wird gezeigt, wie Sie sich mit einem WLAN-Netzwerk verbinden und Ihr System als Accesspoint konfigurieren können. Des Weiteren zeigen wir Ihnen, wie Sie einen DHCP-Server einrichten können, um eine automatische IP-Adresszuweisung in Ihrem WLAN-Netzwerk zu ermöglichen.

DHCP-Client

Unter TwinCAT/BSD wurde bisher der `dhclient(8)` als DHCP-Client verwendet. Ab Version 13.2.0.6 / 89449 wird `dhcpcd(8)` als Standard DHCP-Client ausgeliefert und löst den älteren Client ab. Aus Gründen der Vollständigkeit wird weiterhin beschrieben, wie beim alten DHCP-Client (siehe: [IP-Adresse einstellen für Systeme mit dhclient \[► 34\]](#)) und wie im Vergleich dazu beim `dhcpcd` (siehe: [IP-Adresse einstellen \(dhcpcd\) \[► 32\]](#)) eine feste IP-Adresse eingestellt werden kann.

Der neue DHCP-Client bietet folgende Vorteile:

- Schnellere Auto-IP-Vergabe (169.254.x.x).
- Verkürzte Bootzeiten.
- Moderner und schneller Daemon.
- Weitere Features, unter anderem die Verwaltung von mehreren IP-Adressen auf einer Netzwerkschnittstelle.

Wenn Sie den `dhcpcd` auch unter älteren TwinCAT/BSD-Versionen nutzen möchten, muss das Paket `dhcpcd` manuell nachinstalliert und anschließend unter `/etc/rc.conf` konfiguriert werden (siehe: [Dhcpcd nachinstallieren und aktivieren \[► 32\]](#)). **Hinweis** Beachten Sie, dass der ältere `dhclient` und `dhcpcd` nicht gleichzeitig konfiguriert sein dürfen, da sich die beiden Services gegenseitig stören.

DHCP ist weiterhin für jede Netzwerkschnittstelle voreingestellt und die IP-Adresse wird automatisch bezogen. Um eine statische IP-Adresse einzustellen, kann weiterhin `ifconfig` verwendet werden.

5.1 Einstellungen für Systeme mit dhcpcd

Ab Version 13.2.0.6 / 89449 wird `dhcpcd(8)` als Standard DHCP-Client ausgeliefert und löst den älteren Client ab. In diesem Kapitel wird beschrieben, wie unter TwinCAT/BSD mit `dhcpcd` eine feste IP-Adresse eingestellt werden kann.

Zusätzlich wird gezeigt, wie das Paket `dhcpcd` für ältere TwinCAT/BSD-Versionen nachinstalliert und der bisherige DHCP-Client deaktiviert werden kann.

5.1.1 Dhcpcd nachinstallieren und aktivieren

● Wiederherstellungspunkt erstellen

i Erstellen Sie einen Wiederherstellungspunkt, bevor Sie eine größere Systemänderung vornehmen oder Programme installieren (siehe: [Wiederherstellungsoptionen \[► 119\]](#)).

In diesem Kapitel wird beschrieben, wie `dhcpcd` auch unter älteren TwinCAT/BSD-Versionen nachinstalliert und aktiviert werden kann. Dazu muss die Datei `/etc/rc.conf` um einige Einträge erweitert bzw. bestimmte Einträge entfernt werden. Bei jeder Installation prüft das Programm `pkg`, ob der lokale Datenbestand, mit dem auf dem Package-Server übereinstimmt und wird bei Bedarf aktualisiert.

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `doas pkg install dhcpcd` in der Konsole ein.
2. Bestätigen Sie die Installation mit **[y]**, damit das Package aus dem Repository abgerufen und auf dem System installiert wird.
3. Geben Sie in der Konsole `doas ee /etc/rc.conf` ein.
Die Datei `rc.conf` wird im Editor geöffnet.
4. Entfernen Sie die Zeile `ifconfig_DEFAULT="DHCP"`, um den älteren DHCP-Client zu deaktivieren.

Hinweis Der ältere `dhclient` und `dhcpcd` dürfen nicht gleichzeitig konfiguriert sein, da sich die beiden Services gegenseitig stören.

5. Entfernen Sie den Eintrag `background_dhclient="YES"` und bereinigen Sie so weiter die Konfigurationsdatei.
6. Fügen Sie folgende Zeilen in die Konfigurationsdatei ein.

```
dhcpcd_enable="YES"
dhcpcd_flags="--waitip"
```

7. Drücken Sie **[Esc]** und wählen Sie die Option a) `leave editor` und anschließend a) `save changes`.

⇒ Starten Sie das System mit `shutdown -r now` neu, damit die Änderungen wirksam werden. Damit ist `dhcpcd` einsatzbereit. Wenn die IP-Adresse nicht über DHCP bezogen werden soll, dann kann im nächsten Schritt eine feste IP-Adresse eingestellt werden (siehe: [IP-Adresse einstellen \(dhcpcd\) \[► 32\]](#)).

5.1.2 IP-Adresse einstellen (dhcpcd)

DHCP ist im Auslieferungszustand standardmäßig aktiv. Wenn im Netzwerk kein DHCP-Server vorhanden ist, vergibt TwinCAT/BSD automatisch nach einem Timeout von fünf Sekunden eine IP-Adresse (169.254.x.x). Die Alternative ist eine feste IP-Adresse. In diesem Arbeitsschritt wird gezeigt, wie Sie in einem System mit `dhcpcd` eine feste IP-Adresse in der Konsole einstellen.

Diese Einstellungen sind alternativ über das Webinterface des Beckhoff Device Managers möglich (siehe: [Beckhoff Device Manager: Webinterface \[► 69\]](#)).

Gehen Sie wie folgt vor:

1. Geben Sie in der Konsole `ifconfig` ein, um die Netzwerkkonfiguration abzufragen. In diesem Beispiel werden die Ethernet-Schnittstellen `igb0` und `igb1` eines Industrie-PCs mit zwei Schnittstellen aufgelistet. Die Schnittstelle `igb1` ist aktiv und mit einem Netzwerk verbunden.

```
igb0: flags=8863<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=4a024a9<RXCSUM,VLAN_MTU,JUMBO_MTU,VLAN_HWCSUM,LRO,WOL_MAGIC,RXCSUM_IPV6,NOMAP>
ether 00:01:05:3d:69:12
```

```

inet6 fe80::25b2:4227:1a65:b77a%igb0 prefixlen 64 scopeid 0x1
inet 169.254.228.5 netmask 0xffff0000 broadcast 169.254.255.255
media: Ethernet autoselect
status: no carrier
nd6 options=1<PERFORMNUD>
igb1: flags=8863<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=4a024a9<RXCSUM,VLAN_MTU,JUMBO_MTU,VLAN_HWCSUM,LRO,WOL_MAGIC,RXCSUM_IPV6,NOMAP>
ether 00:01:05:3d:69:13
inet6 fe80::4207:801c:e08a:9ede%igb1 prefixlen 64 scopeid 0x2
inet 172.17.42.57 netmask 0xfffffc00 broadcast 172.17.43.255
media: Ethernet autoselect (100baseTX <full-duplex>)
status: active
nd6 options=1<PERFORMNUD>

```

2. Geben Sie in der Konsole `doas ee /etc/rc.conf` ein.

Die Datei `rc.conf` wird im Editor geöffnet.

3. Navigieren Sie mit den Pfeiltasten mindestens unter den Eintrag `dhcpcd_enable="YES"` und ergänzen Sie die folgende Zeile:

```
ifconfig_igb1="inet 192.168.25.25 netmask 255.255.255.0"
```

4. Beachten Sie die Reihenfolge der Einträge in der Konfigurationsdatei. Konfigurationsdateien werden vom System von oben nach unten gelesen. Mit der Konfiguration einer statischen IP-Adresse nach der DHCP-Konfiguration überschreiben Sie die vorangegangene DHCP-Konfiguration.

5. Definieren Sie mit `inet` die IP-Adresse und mit `netmask` die Subnetzmaske für die Ethernet-Schnittstelle `igb1`.

6. Fügen Sie dem Eintrag `dhcpcd_flags` den Parameter `--denyinterfaces igb1` hinzu, damit DHCP für diese Schnittstelle deaktiviert wird. Andernfalls erhält die Schnittstelle zwei IP-Adressen. Eine feste IP-Adresse, die Sie definiert haben und zusätzlich eine IP-Adresse vom DHCP-Server. Sie könne diesen Schritt überspringen, wenn dieses Verhalten gewünscht ist.

```
dhcpcd_flags="--waitip --denyinterfaces igb1"
```

7. Soll DHCP für mehrere Schnittstellen deaktiviert werden, können diese mit Komma getrennt aufgelistet werden.

```
dhcpcd_flags="--waitip --denyinterfaces igb1,igb0"
```

8. Drücken Sie **[Esc]** und wählen Sie die Option `a) leave editor` und anschließend `a) save changes`.

⇒ Sie haben erfolgreich `192.168.25.25` als feste IP-Adresse eingestellt. Geben Sie den Befehl `doas service netif restart && doas service dhcpcd restart` in der Konsole ein, damit die Einstellungen übernommen werden. Verwenden Sie den Befehl `doas sh -c "service netif restart && service dhcpcd restart"`, wenn Sie über SSH auf das System zugreifen. Überprüfen Sie anschließend mit dem Befehl `ifconfig` die Netzwerkeinstellungen.

5.2 IP-Adresse einstellen für Systeme mit dhclient

DHCP ist im Auslieferungszustand standardmäßig aktiv. Wenn im Netzwerk kein DHCP-Server vorhanden ist, vergibt TwinCAT/BSD automatisch nach einem Timeout von fünf Sekunden eine IP-Adresse (169.254.x.x). Die Alternative ist eine feste IP-Adresse. In diesem Arbeitsschritt wird gezeigt, wie Sie eine feste IP-Adresse in der Konsole einstellen.

Diese Einstellungen sind alternativ über das Webinterface des Beckhoff Device Managers möglich (siehe: [Beckhoff Device Manager: Webinterface](#) [► 69]).

Gehen Sie wie folgt vor:

1. Geben Sie in der Konsole `ifconfig` ein, um die Netzwerkkonfiguration abzufragen. In diesem Beispiel werden die Ethernet-Schnittstellen `igb0` und `igb1` eines Industrie-PCs mit zwei Schnittstellen aufgelistet. Die Schnittstelle `igb1` ist aktiv und mit einem Netzwerk verbunden.

```
igb0: flags=8863<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=4a024a9<RXCSUM,VLAN_MTU,JUMBO_MTU,VLAN_HWCSUM,LRO,WOL_MAGIC,RXCSUM_IPV6,NOMAP>
ether 00:01:05:3d:69:12
inet6 fe80::25b2:4227:1a65:b77a%igb0 prefixlen 64 scopeid 0x1
inet 169.254.228.5 netmask 0xffff0000 broadcast 169.254.255.255
media: Ethernet autoselect
status: no carrier
nd6 options=1<PERFORMNUD>
igb1: flags=8863<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=4a024a9<RXCSUM,VLAN_MTU,JUMBO_MTU,VLAN_HWCSUM,LRO,WOL_MAGIC,RXCSUM_IPV6,NOMAP>
ether 00:01:05:3d:69:13
inet6 fe80::4207:801c:e08a:9ede%igb1 prefixlen 64 scopeid 0x2
inet 172.17.42.57 netmask 0xfffffc00 broadcast 172.17.43.255
media: Ethernet autoselect (100baseTX <full-duplex>)
status: active
nd6 options=1<PERFORMNUD>
```

2. Geben Sie in der Konsole `doas ee /etc/rc.conf` ein. Die Datei `rc.conf` wird im Editor geöffnet.
3. Navigieren Sie mit den Pfeiltasten mindestens unter den Eintrag `ifconfig_default="DHCP"` und ergänzen Sie die folgende Zeile:

```
ifconfig_igb1="inet 172.17.40.30 netmask 255.255.255.0"
```

4. Beachten Sie die Reihenfolge der Einträge in der Konfigurationsdatei. Konfigurationsdateien werden vom System von oben nach unten gelesen. Mit der Konfiguration einer statischen IP-Adresse nach der DHCP-Konfiguration überschreiben Sie die vorangegangene DHCP-Konfiguration. Das `default` in `ifconfig_default` bedeutet, dass diese Konfiguration für alle Schnittstellen gilt. Mit nachfolgenden Einträgen können Sie diese Konfiguration zum Teil oder auch ganz überschreiben.
 5. Definieren Sie mit `inet` die IP-Adresse und mit `netmask` die Subnetzmaske für die Ethernet-Schnittstelle `igb1`.
 6. Drücken Sie **[Esc]** und wählen Sie die Option a) `leave editor` und anschließend a) `save changes`.
- ⇒ Sie haben erfolgreich `172.17.40.30` als feste IP-Adresse eingestellt. Geben Sie den Befehl `doas service netif restart` in der Konsole ein, damit die Einstellungen übernommen werden. Überprüfen Sie anschließend mit dem Befehl `ifconfig` die Netzwerkeinstellungen.

5.3 Hostnamen ändern

In diesem Arbeitsschritt wird gezeigt, wie Sie den Hostnamen eines Industrie-PCs ändern. Beachten Sie, dass Sie damit auch die eindeutige Bezeichnung des Industrie-PCs in einem Netzwerk ändern.

Hostnamen bei Beckhoff Industrie-PCs bei Auslieferung

Der Hostname wird bei älteren Industrie-PCs automatisch aus dem Präfix CX-, CP- oder BK_IPC- und den letzten 3 Byte der MAC-Adresse gebildet. Die MAC-Adresse ist 6 Byte lang, wobei die ersten 3 Byte die Beckhoff-Herstellerkennzeichnung 00 01 05 ist.

Im Gegensatz dazu, wird bei aktuellen Geräten der Hostname aus der Beckhoff Traceability Number (BTN) gebildet, die auf allen neuen Geräten verwendet und auf dem Typenschild als Seriennummer abgedruckt wird. Die BTN ist eine eindeutige, aus acht Zeichen bestehende Seriennummer, die langfristig alle anderen Seriennummern-Systeme bei Beckhoff ersetzen und zum Zwecke der Vereinheitlichung schrittweise eingeführt wird.

Maßgeblich ist die Information auf dem Typenschild des Industrie-PCs. Wenn keine BTN-Nummer vorhanden ist, wird der Hostname aus der MAC-Adresse gebildet. Wenn eine BTN-Nummer vorhanden ist, wird stattdessen die BTN-Nummer für die Bildung des Hostnamens verwendet. Beispiele für Hostnamen bei Industrie-PCs, die aus der MAC-Adresse oder BTN-Nummer gebildet werden:

- Embedded-PC mit MAC-Adresse „00-01-05-12-24-A3“ erhält den Hostnamen CX-1224A3.
- Industrie-PC mit BTN-Nummer „000fgyeg“ erhält den Hostnamen BTN-000fgyeg.

Diese Einstellungen sind alternativ über das Webinterface des Beckhoff Device Managers möglich (siehe: [Beckhoff Device Manager: Webinterface \[► 69\]](#)).

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `doas ee /etc/rc.conf` in der Konsole ein.
Die Datei `rc.conf` wird geöffnet.

```
zfs_enable="YES"
# network services and TwinCAT settings
pf_enable="YES"
sshd_enable="YES"
TcSystemService_enable=YES
# custom settings
hostname="CX-1D7BD4"
ifconfig_igb0="DHCP"
ifconfig_igb1="DHCP"
allscreens_kbdflags="-b quiet.off"
# Debugging settings
syslogd_flags="-ss"
#keymap="de.noacc.kbd"
```

2. Ändern Sie den Hostnamen unter dem Eintrag `hostname="CX-112233"`.
Drücken Sie **[Esc]** und speichern Sie die Änderungen.

⇒ Der neue Hostname wird erst nach einem Neustart durch den Befehl `shutdown -r now` übernommen.

5.4 Firewall

TwinCAT/BSD stellt mit dem Package-Filter (PF) eine komplette und voll ausgestattete Firewall bereit. Die Firewall ist ab Werk restriktiv eingestellt und erlaubt nur wenige ein- und ausgehende Verbindungen. Die Regeln für die Firewall werden in einer Konfigurationsdatei gespeichert. Sie können die Konfigurationsdatei mit dem Befehl `doas ee /etc/pf.conf` öffnen.

Die Regeln für Ports, die von Beckhoff-Diensten genutzt werden, werden durch „anchor bhf“ in der Datei `pf.conf` inkludiert und werden für TwinCAT Functions dynamisch erstellt. Eigene Regeln für die Firewall sollten weiterhin in der Datei `pf.conf` eingefügt werden.

Beachten Sie, dass der unverschlüsselte ADS-Port 48898 standardmäßig deaktiviert ist. Nutzen Sie stattdessen Secure-ADS oder schalten Sie den ADS-Port 48898 mit folgendem Eintrag in der Firewall frei:

Tab. 5: Firewall-Regel für unverschlüsselte ADS-Kommunikation.

Regel	Beschreibung
pass in quick proto tcp to port 48898 synproxy state	TCP-Verbindungen auf ADS-Port 48898 (ADS/TCP), standardmäßig deaktiviert.

5.4.1 Firewall aktivieren und deaktivieren

Die Firewall ist standardmäßig aktiv. Eine inaktive Firewall kann in vielen Fällen, z.B. in einer Testumgebung, nützlich oder sogar notwendig sein. In diesem Schritt wird gezeigt, wie Sie die Firewall deaktivieren können. Beachten Sie, dass ohne Firewall die eingehenden und ausgehenden Verbindungen nicht mehr geprüft werden. Deaktivieren Sie die Firewall nie dauerhaft.

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `doas service pf stop` in der Konsole ein.
Die Firewall wird deaktiviert.
 2. Geben Sie den Befehl `doas service pf start` in der Konsole ein, um die Firewall wieder zu aktivieren.
- ⇒ Die Firewall wird nach jedem Neustart automatisch wieder aktiviert. Dieses Verhalten wird durch den Eintrag `pf_enable="YES"` in der Datei `rc.conf` sichergestellt.

5.4.2 Port freigeben

● Automatische Portfreigabe für TwinCAT Functions

I Ports, die für TwinCAT Functions erforderlich sind, werden nach der Installation der TwinCAT Functions automatisch freigegeben.

In diesem Schritt wird gezeigt, wie Sie einen TCP-Port freigeben können. Als Beispiel wird eine eingehende Verbindung für den TCP-Port 502 erstellt, die für die Modbus/TCP-Kommunikation erforderlich ist.

Geben Sie einen Port wie folgt frei:

1. Geben Sie den Befehl `doas ee /etc/pf.conf` in der Konsole ein.
Die Konfigurationsdatei `pf.conf` wird geöffnet.
 2. Erstellen Sie die Regel `pass in quick proto tcp to port 502 keep state` um den TCP-Port 502 freizugeben.
 3. Drücken Sie **[Esc]** und speichern Sie die Änderungen.
 4. Geben Sie den Befehl `doas pfctl -f /etc/pf.conf` ein, um die Regeln neu zu laden. Hierfür muss die Firewall aktiviert sein.
- ⇒ Sie haben erfolgreich einen Port freigegeben. Benutzen Sie den Befehl `doas pfctl -f /etc/pf.conf` um die Regeln sofort zu aktivieren. Andernfalls greift die Regel nach dem nächsten Neustart der Firewall.

5.5 WLAN-Konfiguration

In diesem Kapitel werden verschiedene Aspekte der WLAN-Konfiguration unter TwinCAT/BSD beschrieben und beinhaltet Schritt-für-Schritt Anleitungen wie ein Industrie-PC mit einem WLAN verbunden, als Accesspoint konfiguriert oder wie ein DHCP-Server eingerichtet werden kann.

Im ersten Abschnitt wird gezeigt, wie eine WLAN-Verbindung hergestellt wird, inklusive der Suche nach Netzwerken und der Zuweisung einer IP-Adresse über einen DHCP-Server. Der zweite Abschnitt erklärt die Konfiguration des Industrie-PCs als Accesspoint mit dem Packet `hostapd`. Der dritte Abschnitt widmet sich der Installation und Konfiguration eines DHCP-Servers, der je nach Netzwerk-Infrastruktur erforderlich sein kann.

5.5.1 Mit WLAN verbinden

In diesem Arbeitsschritt wird gezeigt, wie Sie unter TwinCAT/BSD eine WLAN-Verbindung mit einem Access-Point herstellen. Zusätzlich erfahren Sie, wie Sie nach WLAN-Netzwerken suchen und die SSID ermitteln.

Das WLAN wird mit WPA2 verschlüsselt und die IP-Adresse wird automatisch von einem DHCP-Server zugewiesen.

Voraussetzungen:

- Beckhoff WLAN-Sticks: CU8210-D001-0101 oder CU8210-D001-0102
- SSID und Passwort eines bestehenden WLANs.

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `sysctl net.wlan.devices` in der Konsole ein, um den Gerätenamen zu ermitteln. Bei einem Beckhoff WLAN-Stick wird beispielsweise `rtwn0` als GeräteName ausgegeben.
2. Öffnen Sie die Datei `rc.conf` mit `doas ee /etc/rc.conf` und ergänzen Sie folgende Zeilen:

```
# wireless
wlans_rtwn0="wlan0"    #wlan0 is now your network interface
create_args_wlan0="country DE"
ifconfig_wlan0="up scan WPA DHCP"
```

3. Folgende Zeilen müssen ergänzt werden, wenn `dhcpcd` (Standard ab Version 13.2.0.6 / 89449) eingesetzt wird.

```
# wireless
wlans_rtwn0="wlan0"    #wlan0 is now your network interface
create_args_wlan0="country DE"
ifconfig_wlan0="up scan WPA"
```

4. Wenn DHCP nicht aktiv oder gewünscht ist, wird mit folgendem Eintrag eine feste IP-Adresse festgelegt.

```
# wireless
wlans_rtwn0="wlan0"    #wlan0 is now your network interface
create_args_wlan0="country DE"
ifconfig_wlan0="WPA inet 192.168.0.100 netmask 255.255.255.0 up scan"
```

5. Starten Sie den Netzwerk-Service mit `doas service netif restart neu`, um die Einstellungen in der `rc.conf`-Datei zu übernehmen.
6. Suchen Sie mit `doas ifconfig wlan0 up scan` nach neuen WLAN-Netzwerken. Mit dem Befehl `doas ifconfig wlan0 list scan` werden bereits bekannte Netzwerke angezeigt.
7. Speichern Sie die Zugangsdaten zu einem WLAN-Netzwerk mit dem Befehl `doas ee /etc/wpa_supplicant.conf` indem Sie folgende Zeilen in der Datei `wpa_supplicant.conf` ergänzen.

```
network={
    ssid="myssid"      #for myssid specify the name of the network
    psk="mypsk"       #for mypsk enter password of network
}
```

8. Geben Sie `doas service netif restart` ein, um den Netzwerk-Service neu zu starten.

⇒ Die WLAN-Verbindung wird aufgebaut. Mit `ifconfig` wird der Netzwerkstatus zur WLAN-Schnittstelle angezeigt.

Weitere Informationen unter: <https://www.freebsd.org/doc/handbook/network-wireless.html>

5.5.2 Als Accesspoint konfigurieren

Sie können einen Industrie-PC unter TwinCAT/BSD als Accesspoint konfigurieren. Für diese Funktion wird das Paket `hostapd` benötigt und muss nachinstalliert werden. Installieren Sie das Paket `hostapd` mit:

```
doas pkg install hostapd
```

Der Daemon `hostapd` kümmert sich um die Client-Authentifizierung und Schlüsselverwaltung auf dem WPA2-fähigen Accesspoint.

Stellen Sie sicher, dass die richtige Regulatory-Domain für das jeweilige Land benutzt wird. Diese beinhaltet beispielsweise die erlaubten Kanäle, erlaubte Sendeleistung und DFS-Aktivierung für bestimmte 5GHz-Kanäle.

Voraussetzungen:

- Paket `hostapd` installieren.
- Internetverbindung.
- Wenn der WLAN-Stick beim Hochfahren bereits gesteckt war, muss er einmal erneut gesteckt werden.

Gehen Sie wie folgt vor:

1. Öffnen Sie mit `doas ee /etc/rc.conf` die Datei `rc.conf` und ergänzen Sie folgende Zeilen.

Beispiel:

```
hostapd_enable="YES"      #starts the hostapd daemon automatically after boot
wlans_rtwn0="wlan0"      #wireless interface used for access point
create_args_wlan0="wlanmode hostap ssid yourSSIDname authmode WPA2"
ifconfig_wlan0="inet 192.168.0.1 netmask 255.255.255.0 country DE"
```

2. Öffnen Sie mit `doas ee /etc/hostapd.conf` die Datei `hostapd.conf` und ergänzen Sie folgende Zeilen.

Beispiel:

```
interface=wlan0
debug=1
ctrl_interface=/var/run/hostapd
ctrl_interface_group=wheel
ssid=yourSSIDname
wpa=2
wpa_passphrase=freebsdmail #password for wlan network
wpa_key_mgmt=WPA-PSK
wpa_pairwise=CCMP
channel=6 #Channel for the desired radio band (default: 0 stands for ACS, automatic Channel Selection)
hw_mode=g #Operation mode, in this case g=IEEE802.11g (2.4 GHz)
country_code=DE #used to set the right regulatory domain for your country
ieee80211d=1 #advertises the country_code an the set of allowed channels and transmit power levels based on the regulatory limits (default=0)
```

3. Geben Sie den Befehl `doas service hostapd forcestart` ein, um den Accesspoint zu starten.

⇒ Sie haben den Industrie-PC erfolgreich als Accesspoint konfiguriert. Mit der SSID und dem Passwort aus der Datei `hostapd.conf` kann ab jetzt ein WLAN-Teilnehmer eine Verbindung zum Netzwerk herstellen.

Weitere Informationen unter: <https://www.freebsd.org/doc/handbook/network-wireless.html>

5.5.3 DHCP-Server einrichten

Abhängig von der Netzwerk-Infrastruktur kann es vorkommen, dass Sie einen DHCP-Server benötigen. In diesem Arbeitsschritt wird gezeigt, wie Sie einen DHCP-Server installieren und konfigurieren können.

Voraussetzungen:

- Internetverbindung.
- Passen Sie die Firewall an und wenden Sie die Regeln auf die WLAN-Schnittstelle an (Siehe: [Firewall \[▶ 35\]](#))

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `doas pkg install dhcpd` in die Konsole ein, um den DHCP-Server zu installieren.
2. Öffnen Sie mit `doas ee /usr/local/etc/dhcpd.conf` die Datei `dhcpd.conf` und bearbeiten Sie die Konfiguration nach Ihren Anforderungen..

Beispiel:

```
subnet 192.168.0.0 netmask 255.255.255.0 {  
  range 192.168.0.10 192.168.0.20;  
  default-lease-time 600;  
  max-lease-time 72400;  
  option subnet-mask 255.255.255.0;  
}
```

3. Öffnen Sie mit `doas ee /etc/rc.conf` die Datei `rc.conf` und ergänzen Sie folgende Zeilen:

```
dhcpd_enable="YES"  
dhcpd_flags="wlan0"  
dhcpd_ifaces="wlan0"
```

4. Geben Sie den Befehl `doas service dhcpd start` ein, um den DHCP-Dienst zu starten. Nach einem Neustart wird der DHCP-Dienst wegen des entsprechenden Eintrags in der `rc.conf` automatisch gestartet.
 5. Mit dem Befehl `ee /var/db/dhcpd.leases` können Sie sich aktuelle und abgelaufene Leases ansehen.
- ⇒ Der DHCP-Server ist damit aktiv und hört nur auf Anfragen auf der Schnittstelle `wlan0`.

Weitere Informationen unter: https://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/network-dhcp.html oder <https://man.openbsd.org/dhcpd.8>

5.6 Verbindung mit Beckhoff LTE-Stick herstellen

In diesem Kapitel wird gezeigt, wie Sie eine Netzwerkverbindung mit dem LTE-Stick (CU8210-D004-0200) herstellen und die serielle Schnittstelle des LTE-Sticks nutzen können.

Voraussetzungen:

- LTE-Stick CU8210-D004-0200
- SIM-Karte und entsprechende Zugangsdaten eines Netzproviders

Gehen Sie wie folgt vor:

1. Schließen Sie den LTE-Stick an den Industrie-PC an.
2. Eine neue Netzwerkschnittstelle (standardmäßig ue0) wird erkannt. Mit `ifconfig` werden die verfügbaren Schnittstellen angezeigt.

```
Administrator@CX-3D6912:~ $ ifconfig
---snipped---
ue0: flags=1008843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST,LOWER_UP> metric 0 mtu 1500
    options=80000<LINKSTATE>
    ether 76:ae:02:ec:c9:45
    inet 192.168.225.40 netmask 0xfffff00 broadcast 192.168.225.255
    inet6 fe80::8f92:e7ea:ed:1a66%ue0 prefixlen 64 scopeid 0x4
    inet6 2a01:599:640:6862:c05:263b:b3a4:385f prefixlen 64 autoconf
    media: Ethernet autoselect
    status: active
    nd6 options=1<PERFORMNUD>
---snipped---
```

3. Wenn der `dhclient` verwendet wird, muss einen Eintrag in der Konfigurationsdatei `rc.conf` vorgenommen werden, damit der LTE-Stick eine IP-Adresse erhält. Öffnen Sie die Konfigurationsdatei mit `doas ee /etc/rc.conf` und fügen Sie die Zeile `ifconfig_ue0="SYNCDHCP"` hinzu.

Dieser Eintrag sorgt dafür, dass der LTE-Stick entweder eine IP-Adresse von einem vorhandenen DHCP-Server erhält oder selbstständig eine vergibt. Hier bekommt der LTE-Stick eine IP-Adresse vom Provider.

4. Wenn stattdessen `dhcpcd` (Standard ab Version 13.2.0.6 / 89449) eingesetzt wird, ist diese Konfiguration nicht erforderlich und erfolgt über die Standardeinstellungen.
5. Überprüfen Sie mit `ls /dev` welche virtuelle COM-Schnittstelle vom TwinCAT/BSD erkannt wurde. Im Normalfall ist neu hinzugekommen: `ttYU0`
6. Mit dem Befehl `doas cu -l /dev/ttYU0` bauen wir eine serielle Verbindung zu dem LTE-Stick auf, um die SIM-Pin und die Zugangsdaten des Netzproviders (APN, Access Point Name) eingeben zu können. Nach erfolgreicher Verbindung wird `Connected` in der Konsole ausgegeben.

```
Administrator@CX-505918:~ $ doas cu -l /dev/ttYU0
Password:
Connected
```

7. Im nächsten Schritt können AT-Kommandos mit dem LTE-Stick ausgetauscht werden, um die SIM-PIN einzugeben bzw. dem LTE-Stick seinen APN mitzuteilen. Der APN muss initial bei der ersten Einrichtung des Sticks eingetragen werden und wird auf dem Stick hinterlegt.
8. Tragen Sie die SIM-Pin ein, sofern die SIM-Karte über eine PIN verfügt. Die SIM-Pin muss natürlich nach jedem Reboot des Gerätes erneut eingegeben werden.

```
AT+CPIN=<your pin>
```

9. Wenn es Ihre Richtlinien erlauben, können Sie die SIM-PIN über folgenden Befehl deaktivieren:

```
AT+CLCK="SC",0,"<your pin>"
```

10. Verwenden Sie folgenden Befehl, um den APN einzutragen:

```
AT+CGDCONT=APN#,"IPV4V6","your_new_apn"
```

11. So führt beispielsweise der Befehl `AT+CGDCONT=1,"IPV4V6","internet.t-mobile"` dazu, dass als erster priorisierter Zugangspunkt (APN1) "internet.t-mobile" verwendet wird.

12. Die angelegten APNs können mit `AT+CGDCONT?` angezeigt werden.

```
AT+CGDCONT?
+CGDCONT: 1,"IPV4V6","internet.t-mobile","0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0",0,0,0,0
```

13. Falsche oder nicht mehr benötigte APNs kann man mit `AT+CGDCONT=<select Index>` löschen.

14. Um die oben genannten Änderungen (bei der Verwendung vom dhclient) an der rc.conf zu übernehmen, muss TwinCAT/BSD einmal neu gestartet werden.

⇒ Nach dem Neustart erhält die Schnittstelle ue0 eine IP-Adresse und hat bei aktivem Datentarif auch eine Verbindung ins Internet. Der die LED des LTE-Sticks blinkt bei entsperrter SIM-Karte und erreichbarem Mobilfunknetz mit aktivem Datentarif "blau". Ist die SIM-Karte nicht entsperrt oder gibt es Probleme beim Erreichen des Mobilfunknetzes, blinkt die LED "rot".

Die Kommunikation nach außen ist standardmäßig möglich, so dass z.B. ein Ping an Google (ping: 8.8.8.8) zum Testen gesendet werden kann. Gegebenenfalls müssen Einstellungen an der Firewall vorgenommen werden, wenn Sie restriktivere Firewall-Regeln definiert haben, damit ue0 auch nach außen kommunizieren kann.

Randnotiz: SMS-Versand über den LTE Stick

Wenn Sie den SMS-Funktionsbaustein (SendSMS) von TwinCAT nutzen wollen, kann hierfür die oben genannte serielle Schnittstelle ttyU0 verwendet werden. Denn über den ADS-Server der TF6340 (Serial Communication) ist es möglich, USB-Geräte über eine virtuelle serielle Schnittstelle anzusprechen.

Voraussetzungen:

- TF6340: TwinCAT 3 Serial Communication
- TF6350: TwinCAT 3 SMS/SMTP

Der virtuelle serielle Schnittstelle kann in dem Fall über die TwinCAT 3 Function TF6340 (Serial Communication) verbunden werden. Die TwinCAT 3 Function TF6340 muss ebenfalls auf dem TwinCAT/ BSD-System installiert werden. Die TwinCAT 3 Function TF6350 (SMS/SMTP) ermöglicht es anschließend, SMS mithilfe von Funktionsbausteinen an einen Empfänger zu senden. Ein ausführliches Beispiel, wie eine SMS über den LTE-Stick versendet werden kann, finden Sie hier: https://infosys.beckhoff.com/content/1031/tf6350_tc3_sms_sntp/373331083.html?id=3466585722444011586

Wenn Sie z. B. den SMS-Funktionsbaustein von TwinCAT verwenden wollen, muss für die Schnittstelle ttyU0 im Funktionsbaustein entsprechend Port "0" eingetragen werden.

Ausdruck	Datentyp	Wert
fbSendSMS	SendSMS	
sText	STRING	'Please check machine #5, threshold is reached'
sSend	BOOL	FALSE
sNumber	STRING	'123456'
sBusy	BOOL	FALSE
sError	INT	0
RxBuffer	ComBuffer	
TxBuffer	ComBuffer	
fbLineCtrlAds	SerialLineControlADS	
bAdsError	BOOL	FALSE
nAdsErrorID	UDINT	0
bConnect	BOOL	TRUE
sNetId	T_AmsNetId	"
stSerialCfg	ComSerialConfig	
ComPort	UDINT	0
Baudrate	UDINT	9600
Parity	COMPARITY_T	PARITY_NONE
DataBits	INT	8

Abb. 14: Beispiel für die Verwendung des SMS-Funktionsbausteins in TwinCAT 3.

5.7 HTTPS-Zertifikate

Dieses Kapitel beschreibt, wie Sie eigene HTTPS-Zertifikate erstellen und importieren können, falls die von Beckhoff standardmäßig für das Webinterface (Device Manager) bereitgestellten Zertifikate für Ihre Anwendung nicht geeignet sind.

In der Informationstechnologie sind Zertifikate ein Mittel, um Identitäten sicher nachzuweisen. Dadurch können Nachrichten oder Dokumente verschlüsselt werden, sodass nur der gewünschte Empfänger den Inhalt wieder entschlüsseln kann. Diese Technik wird unter anderem von jedem Webbrowser beim Abrufen einer Seite über das HTTPS-Protokoll genutzt.

Dabei erfragt ein Netzwerkteilnehmer beim Aufbau einer Kommunikationsverbindung zu einem anderen Teilnehmer dessen Zertifikat. Das Zertifikat wird geprüft und ob der andere Teilnehmer sich mit Hilfe des dazugehörigen Schlüssels authentisiert. Sobald die Identität nachgewiesen wurde, lässt sich der nachfolgende Nachrichtenaustausch über die Verbindung gegen unbefugte Manipulation und wahlweise auch gegen unbefugte Einsichtnahme schützen.

Um eigens generierte HTTPS-Zertifikate zu nutzen, muss:

- die automatische Generierung eines Zertifikats für Industrie-PCs deaktiviert,
- ein Zertifikat bei einer Zertifizierungsstelle (Certificate Authority, CA) angefordert
- und anschließend das HTTPS-Zertifikat importiert werden.

Der genaue Ablauf und die notwendigen Schritte werden in diesem Kapitel beschrieben.

5.7.1 Automatische Zertifikatserstellung deaktivieren

In manchen Anwendungsfällen ist es für den Anwender nicht sinnvoll, die von TwinCAT/BSD generierten Zertifikate für den Webserver wiederzuverwenden. In diesem Anwendungsfall kann die automatische Synchronisation deaktiviert und eigene Zertifikate für den TwinCAT/BSD-Webserver (nginx) verwendet werden.

Dafür muss zunächst die automatische Zertifikatserstellung deaktiviert werden, damit die eigenen Zertifikate installiert und nicht durch das Standard-Beckhoff-Zertifikat überschrieben werden.

Gehen Sie wie folgt vor:

1. Deaktivieren Sie den Dienst `IPCDiagnostics`, damit das Zertifikat nicht durch das Standard-Beckhoff-Zertifikat überschrieben wird.
2. Geben Sie dazu den Befehl `doas service IPCDiagnostics disable` in der Konsole ein.
⇒ Die automatische Generierung von Zertifikaten wurde deaktiviert. Im nächsten Schritt kann ein Zertifikat bei einer Zertifizierungsstelle (Certificate Authority, CA) angefordert werden (siehe: [HTTPS-Zertifikat anfordern oder erstellen](#) ▶ 42).

5.7.2 HTTPS-Zertifikat anfordern oder erstellen

Üblicherweise stellt eine Zertifizierungsstelle (Certificate Authority, CA) Installationsanweisungen zur Verfügung, wie ein von ihr ausgestelltes Zertifikat zu installieren ist. Die Zertifizierungsstelle stellt sogar Anweisungen zur Verfügung, wie das Zertifikat zu beantragen ist. Bitte befolgen Sie in erster Linie die Anweisungen der Zertifizierungsstelle.

Zunächst müssen Sie eine Zertifikatsanforderung (Certificate Signing Request, CSR) erstellen und die Zertifikatsanforderung gemäß den Anweisungen der Zertifizierungsstelle an diese weiterleiten. Die Zertifizierungsstelle wird Ihnen dann das Serverzertifikat und die Zwischenzertifikate zur Verfügung stellen, um eine Zertifikatsanforderung zu erstellen

Wenn Sie kein Zertifikat von einer offiziellen Zertifizierungsstelle (CA) haben, können Sie zu Testzwecken ein selbstsigniertes Zertifikat erstellen.

Gehen Sie wie folgt vor:

1. Generieren Sie zu Testzwecken ein selbstsigniertes Zertifikat mit dem folgenden Befehl:

```
doas openssl req -x509 -newkey rsa:4096 -nodes -sha256 -days 3650 \
    -keyout IPCDiagnostics.key \
    -out IPCDiagnostics.crt \
    -subj '/CN=<hostname>' \
    -addext 'subjectAltName=DNS:<hostname>,IP:<ipaddress>'
```

2. Der Befehl erstellt einen privaten Schlüssel `IPCDiagnostics.key` und ein selbstsigniertes Zertifikat `IPCDiagnostics.crt`.

`openssl req`: Der Befehlssteil `req` erstellt und bearbeitet Zertifikatsanfragen (CSR – Certificate Signing Request). Mit `-x509` wird stattdessen direkt ein selbstsigniertes Zertifikat erstellt.

`-newkey rsa:4096`: Erstellt ein neues Schlüsselpaar mit dem RSA-Algorithmus und einer Schlüssellänge von 4096 Bit.

`-nodes`: Bedeutet "no DES". Der private Schlüssel wird nicht verschlüsselt gespeichert, d. h., es wird kein Passwort benötigt, um den Schlüssel zu verwenden.

`-sha256`: Verwendet den sicheren Hash-Algorithmus SHA-256, um die Zertifikatsnatur zu erstellen.

`-keyout IPCDiagnostics.key`: Speichert den privaten Schlüssel in der Datei `IPCDiagnostics.key`.

`-out IPCDiagnostics.crt`: Speichert das erstellte Zertifikat in der Datei `IPCDiagnostics.crt`.

`-subj '/CN=<hostname>'`: Gibt die Daten für das Zertifikat an, ohne eine interaktive Abfrage. `/CN=<hostname>` legt den Common-Name (CN) fest, der normalerweise der Hostname oder die Domain ist, die durch das Zertifikat geschützt wird.

`-addext 'subjectAltName=DNS:<hostname>,IP:<ipaddress>'`: Fügt eine Erweiterung (Extension) zum Zertifikat hinzu. `subjectAltName (SAN)` erlaubt zusätzliche Namen und IP-Adressen, die das Zertifikat abdecken soll.

3. Ersetzen Sie `<hostname>` durch den Hostnamen und `<ipaddress>` durch die IP-Adresse Ihres TwinCAT/BSD-Geräts.

⇒ Im nächsten Schritt kann das Zertifikat importiert werden (siehe: [Zertifikat importieren](#) [► 43]).

5.7.3 Zertifikat importieren

Sobald Sie ein Zertifikat von einer offiziellen Zertifizierungsstelle (CA) erhalten haben, können Sie dieses in Ihr TwinCAT/BSD-System importieren. Alternativ können Sie auch das selbstsignierte Zertifikat verwenden, das Sie zu Testzwecken erstellt haben.

Gehen Sie wie folgt vor:

1. Ersetzen Sie den vorhandenen privaten Schlüssel für nginx durch Ihren privaten Schlüssel:

```
doas cp IPCDiagnostics.key /usr/local/etc/TwinCAT/3.1/Target/PrivateKeys/IPCDiagnostics.key
```

2. Ersetzen Sie das vorhandene Zertifikat für nginx durch Ihr Zertifikat:

```
doas cp IPCDiagnostics.crt /usr/local/etc/TwinCAT/3.1/Target/Certificates/IPCDiagnostics.crt
```

3. Starten Sie den nginx-Webserver neu:

```
doas service nginx restart
```

4. Das Zertifikat ist nach dem Neustart des Dienstes einsatzbereit.

⇒ Wenn Sie kein Zertifikat einer offiziellen Zertifizierungsstelle (CA) verwenden, zeigt Ihr Browser eine Sicherheitswarnung an. Sie können Ihren Browser so konfigurieren, dass er das Zertifikat automatisch akzeptiert, indem Sie das Server-Zertifikat in den Zertifikatsspeicher Ihres Browsers importieren. Weitere Informationen hierzu finden Sie unter: [Selbstsignierte Zertifikate für https-Verbindung](#)

Da einige Browser (z.B. Mozilla Firefox) eigene Zertifikatsspeicher verwenden, kann es erforderlich sein, das Zertifikat direkt im Browser zu importieren.

6 Systemaktualisierung

TwinCAT/BSD Release-Prozess

Die Systemaktualisierung erfolgt standardmäßig über den voreingestellten Beckhoff Package-Server bzw. das Beckhoff-Repository, welches alle benötigten Packages bereitstellt (siehe: [Package-Server \[► 49\]](#)).

In der Regel wird am ersten Dienstag eines jeden Monats eine neue Version des Beckhoff-Repositorys veröffentlicht. Vorausgesetzt, dass alle internen Tests erfolgreich bestanden werden. Wenn die internen Tests fehlschlagen, wird die Veröffentlichung auf den nächsten Monat verschoben.

Es wird nur das Beckhoff-Repository aktualisiert, was nicht unbedingt bedeutet, dass in jeder neuen Repository-Version automatisch eine neue TwinCAT/BSD oder TwinCAT-Version veröffentlicht wird. Es könnten auch einfach einzelne Packages sein, Packages von Drittanbietern oder Packages, die Sie nicht mal auf ihrem System installiert haben. Wenn Sie eine Aktualisierung durchführen, ist es empfehlenswert das gesamte System und nicht nur einzelne Packages auf den neusten Stand zu bringen. Das liegt daran, dass die Packages im Beckhoff-Repository in jedem Release als Gesamtsystem getestet werden, wodurch Inkompatibilitäten vermieden werden.

Es besteht jederzeit die Möglichkeit, einen getesteten Versionstand des Beckhoff-Repositorys als lokales Repository runterzuladen und zu speichern. Dadurch können Sie ihr System in einem getesteten Stand einfrieden und beispielsweise für den Serienmaschinenbau nutzen. Das lokale Repository und alle darin enthaltenen Packages, können in diesem Fall über einen Server im lokalen Netzwerk oder über einen USB-Stick bereitgestellt werden (siehe: [Repository auf USB-Stick bereitstellen \[► 53\]](#)).

TwinCAT/BSD-Version aufrufen

Die TwinCAT/BSD-Version kann mit dem Befehl `TcSysExe.exe` aufgerufen werden. Es gibt verschiedene Versionsinformationen, die Sie vom System erhalten können. Unter dem Eintrag TC/BSD wird die aktuelle Version aufgelistet:

```
Administrator@CX-0C8432:~ $ TcSysExe.exe

The software licenses can be found in this folder: /usr/local/etc/TwinCAT/3.1/System/Legal/
TcOsSys.dll: TcOsSys_Rel131_4024_20210804.2
TwinCAT Build: 3.1.4024.19
AMS Net Id: 5.12.132.50.1.1
TC/BSD: 13.0.8.2,2
Administrator@CX-0C8432:~ $
```

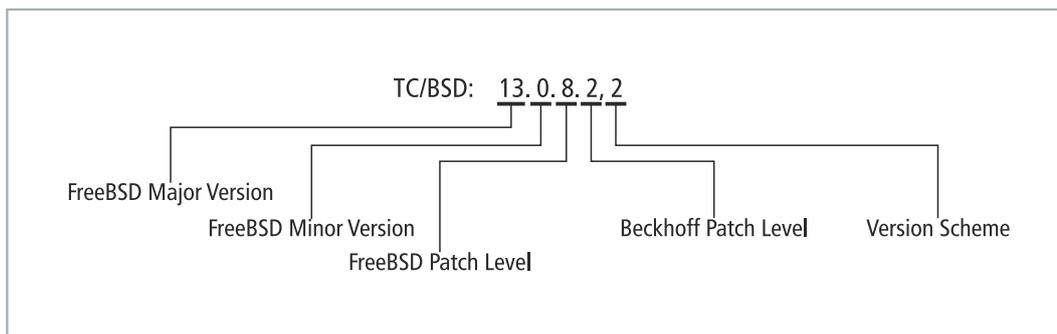


Abb. 15: Aufschlüsselung der TwinCAT/BSD-Version.

Beckhoff-Repositorys-Version aufrufen

Mit dem Befehl `pkg info os-generic-userland-conf | grep Version` wird die Pipeline-Nummer für das entsprechende interne Beckhoff-Repository angezeigt. In diesem Beispiel wird die Pipeline-ID 55702 hinter der TwinCAT/BSD-Version angezeigt:

```
Administrator@CX-3AE2C6:~ $ pkg info os-release-bhf | grep Version
Version : 13.0.11.3_55702
Administrator@CX-3AE2C6:~ $
```

Aktualisierung durchführen

Es gibt zwei Wege das System zu aktualisieren. Der erste Weg ist der reguläre für Minor-Versionen und TwinCAT-Updates. Der zweite Weg ist nur für die Aktualisierung der FreeBSD-Major-Versionen erforderlich, die meist neue FreeBSD-Features mitbringen (siehe: [FreeBSD-Release-Notes](#)).

1. [TwinCAT/BSD aktualisieren](#) [► 46]
2. [Major-Version aktualisieren](#) [► 46]

Konfigurationsdateien wie beispielsweise die `rc.conf` und `TcRegistry.xml` sind in der Regel von einer Systemaktualisierung und Installation neuer Pakete nicht betroffen und bleiben unverändert. Dadurch wird sichergestellt, dass alle Änderungen, die der Benutzer an den Konfigurationsdateien vornimmt, erhalten bleiben und nicht überschrieben werden.

Bei der Installation neuer Pakete müssen Konfigurationsdateien ggf. manuell angepasst werden. Da bei der Aktualisierung keine Benutzerkonfigurationen vorgenommen werden, kann sich ein System nicht nur in seiner Konfiguration, sondern auch in seinen installierten Paketen von einem neu installierten System unterscheiden, trotz gleicher Versionsstände.

1. TwinCAT/BSD aktualisieren

Der Befehl `pkg upgrade` wird verwendet, um Packages zu aktualisieren (siehe: [Packages aktualisieren](#) [► 52]). Dabei vergleicht `pkg upgrade` die Versionen aller installierter Pakete mit den Versionen, die in den konfigurierten Package-Repositorys verfügbar sind. Der Beckhoff Package-Server spiegelt einen Großteil der Packages aus dem normalen FreeBSD-Repository und beinhaltet darüber hinaus folgende spezifische Beckhoff-Packages, die aktualisiert werden können:

- TwinCAT/BSD-Updates
- TwinCAT 3 Updates
- TwinCAT 3 Functions

Zusätzlich versucht `pkg upgrade` auch die Abhängigkeiten der Packages zu aktualisieren. Es werden aber keine neuen Packages installiert, außer wenn es erforderlich ist, um die Abhängigkeiten der Packages zu erfüllen.

Es können auch einzelne Packages aktualisiert werden, es wird aber empfohlen, das gesamte System auf den neusten Stand zu bringen, um Inkompatibilitäten zu vermeiden. Das liegt daran, dass die Packages im Beckhoff-Repository in jedem Release als Gesamtsystem getestet werden.

Upgrade in einer neuen Boot-Umgebung durchgeführt, so dass das aktuelle System während des Upgrade-Prozesses weitgehend unberührt bleibt. Tritt während des Upgrades ein Fehler auf, wird die Boot-Umgebung einfach entfernt und das System in seinem ursprünglichen Zustand belassen. Auch der alte EFI-Loader wird wiederhergestellt.

Neben der Möglichkeit, TwinCAT/BSD mit Hilfe von `pkg upgrade` zu aktualisieren, steht mit dem Tool `tcbsd-upgrade` eine noch einfachere und von Beckhoff empfohlene Möglichkeit zur Verfügung, TwinCAT/BSD zu aktualisieren (siehe: [TwinCAT/BSD aktualisieren](#) [► 46]). Das Tool erstellt automatisch einen Wiederherstellungspunkt und führt das Upgrade in einer neuen Boot-Umgebung durch, sodass das aktuelle System während des Upgrade-Prozesses weitgehend unberührt bleibt. Tritt während des Upgrades ein Fehler auf, wird die Boot-Umgebung einfach entfernt und das System in seinem ursprünglichen Zustand belassen. Der alte EFI-Loader wird ebenfalls wiederhergestellt. Auch nach einer erfolgreichen Aktualisierung steht die alte Boot-Umgebung als Klon zur Verfügung, auf die jederzeit zurückgegriffen werden kann, bis sie manuell gelöscht wird.

2. Major-Version aktualisieren

Die aktuelle Major-Version ist erforderlich, weil nach einer Umstellung auf die nächsthöhere Major-Version alle Sicherheitsupdates nur für die aktuelle Version bereitgestellt werden. Ältere Versionen werden nicht mehr gepflegt.

Zusätzlich dazu können in Zukunft in der neusten Major-Version neue Features implementiert und zur Verfügung gestellt werden, die für TwinCAT/BSD erforderlich werden.

6.1 TwinCAT/BSD aktualisieren

Neben der Möglichkeit, TwinCAT/BSD mit Hilfe von `pkg upgrade` zu aktualisieren, steht mit dem Tool `tcbsd-upgrade` eine noch einfachere und von Beckhoff empfohlene Möglichkeit zur Verfügung, TwinCAT/BSD zu aktualisieren. Das Ziel ist es, das System auf den neusten Stand zu bringen. Das Tool erstellt automatisch einen Wiederherstellungspunkt mit dem aktuellen Zeitstempel. Sie können Wiederherstellungspunkte mit `restorepoint status` auflisten.

Darüber hinaus wird das Upgrade in einer neuen Boot-Umgebung durchgeführt, so dass das aktuelle System während des Upgrade-Prozesses weitgehend unberührt bleibt. Tritt während des Upgrades ein Fehler auf, wird die Boot-Umgebung einfach entfernt und das System in seinem ursprünglichen Zustand belassen. Auch der alte EFI-Loader wird wiederhergestellt.

Wenn nach dem Upgrade und dem Neustart etwas schief läuft, können Sie den Wiederherstellungspunkt verwenden, um das Upgrade rückgängig zu machen. Dies kann über SSH oder das Systemterminal erfolgen, wenn das System zugänglich ist:

```
bectl list
doas bectl activate upgrade-<timestamp>
reboot
```

Aktualisieren Sie das System wie folgt:

1. Installieren Sie das Tool mit dem Befehl `doas pkg install tcbsd-upgrade`
2. Geben Sie den Befehl `doas tcbsd-upgrade minor` in der Konsole ein und starten Sie das System nach erfolgreicher Aktualisierung neu.
 - ⇒ Ab diesem Zeitpunkt existieren mindestens zwei Boot-Umgebungen auf dem System und Sie können jederzeit mit `bectl` zur alten Boot-Umgebung zurückkehren oder diese während des Boot-Vorgangs über das Boot-Menü aufrufen (Leertaste drücken).
3. Wenn alles gut gelaufen ist und Sie sicher sind, dass Sie nichts rückgängig machen wollen, können Sie den Wiederherstellungspunkt bereinigen:

```
restorepoint status
doas restorepoint destroy upgrade-backup-<timestamp>
```

4. Ersetzen Sie die alte Boot-Umgebung (default) durch die neue Boot-Umgebung (`upgrade-<timestamp>`) und benennen Sie die neue Boot-Umgebung wieder in default um:

```
bectl list
doas bectl destroy default
doas bectl rename upgrade-<timestamp> default
```

5. Starten Sie TwinCAT/BSD mit `shutdown -r now` neu.
 - ⇒ Es ist wichtig, den alten Namen (default) für die Boot-Umgebung beizubehalten, um zu verhindern, dass alte Wiederherstellungspunkte (z.B. `factoryreset`) beschädigt werden. Das Tool `restorepoint` wird versuchen, die alte Boot-Umgebung (z.B. "zroot/ROOT/default") während der Wiederherstellung zu aktivieren und wird fehlschlagen, wenn die alte Boot-Umgebung nicht mehr existiert. Das Tool `tcbsd-upgrade` erstellt während des Upgrades Klone der aktuellen Boot-Umgebung, um die Historie oder Snapshots zu erhalten, so dass die alte Boot-Umgebung durch die neue ersetzt werden kann, um eine Beschädigung der Wiederherstellungspunkte zu vermeiden.

Sehen Sie dazu auch

- 📖 Wiederherstellungsoptionen [▶ 119]
- 📖 Sperren [▶ 53]

6.2 Major-Version aktualisieren

In diesem Kapitel wird beschrieben, wie die Aktualisierung einer Major-Version von beispielsweise TwinCAT/BSD 12 auf TwinCAT/BSD 13 durchgeführt werden kann. Die aktuelle Major-Version wird unter anderem für Sicherheitsupdates benötigt.

Die Aktualisierung erfolgt mit Hilfe eines Skripts, weil das gesamte Basissystem sowie der durch Beckhoff angepasste Kernel aktualisiert wird. Das Skript legt auch automatisch einen Wiederherstellungspunkt an, zu dem man zurückspringen kann (siehe: [Auf Wiederherstellungspunkt zurücksetzen](#) [▶ 121]).

Gehen Sie wie folgt vor:

1. Bringen Sie die letzte Major-Version mit `doas pkg update -f && doas pkg upgrade` auf den neusten Stand.
2. Installieren Sie das Skript für die Aktualisierung mit dem Befehl `doas pkg install tcbsd-upgrade`
3. Führen Sie das Skript mit dem Befehl `doas tcbsd-upgrade major` aus. Am Ende des Prozesses wird eine Rückmeldung über eine erfolgreiche Aktualisierung auf die nächsthöhere Major-Version angezeigt.

```
Successfully upgraded to TC/BSD 13 and activated the new BE "upgrade-2022-02-17T15:02:01Z"
Reboot is required.
```

4. Starten Sie nach erfolgreicher Aktualisierung TwinCAT/BSD mit `shutdown -r now neu`.

⇒ Nach dem Neustart steht die neue Major-Version zur Verfügung und wird nach der Anmeldung angezeigt.

```
Last login: Thu Feb 17 15:07:47 on pts/0
FreeBSD 13.0-RELEASE-p7 n244930-e4e6bcfbb68- BHF

The software licenses can be found in this folder: /usr/local/etc/TwinCAT/3.1/System/Legal/
TcOsSys.dll: TcOsSys_Rel131_4024_20211129.2
TwinCAT Build: 3.1.4024.22
AMS Net Id: 5.61.105.18.1.1
TC/BSD: 13.0.7.2,2
```

Anpassung der Boot-Umgebung

Das Upgrade wird in einer neuen Boot-Umgebung installiert. Eine Boot-Umgebung ist ein ZFS-Dateisystem, in das gebootet werden kann. Das alte ZFS-Dateisystem ist also weiterhin verfügbar und kann im Notfall als Backup verwendet werden. Zu diesem Zweck kann die Boot-Umgebung, in die das System booten soll, immer über das Bootloader-Menü und den Menüpunkt „Boot Environments“ ausgewählt werden (Leertaste beim Booten drücken).

Um die alte Boot-Umgebung zu entfernen und das System von Altlasten zu befreien, ist folgendes Vorgehen nach einem erfolgreichen Upgrade sinnvoll:

1. Wiederherstellungspunkt löschen, der vor dem Upgrade auf die neue Major-Version automatisch erstellt wird. Dieser dient ebenfalls als weiteres Fallback. Geben Sie den Befehl `doas restorepoint destroy` ein.
2. Wählen Sie den Wiederherstellungspunkt `upgrade-backup-<your timestamp>` aus dem Menü, damit dieser gelöscht wird.
3. Alte Boot-Umgebung (`default`) löschen mit `bectl destroy default`
4. Die neue Boot-Umgebung in `default` umbenennen mit `bectl rename upgrade-<timestamp> default`. Es muss immer eine "default" Boot-Umgebung geben, damit der Wiederherstellungspunkt `factoryreset` funktionieren kann.

Hinweis : Die Boot-Umgebung `restore` darf nicht gelöscht werden.

6.3 CPU-Mikrocode aktualisieren

TwinCAT/BSD bietet die Möglichkeit, den Mikrocode einer CPU automatisch beim Starten zu aktualisieren. Dadurch können beispielsweise die neuesten Security-Updates auf einem System installiert werden.

Diese Funktion ist standardmäßig deaktiviert. Testen Sie jedes Update, bevor Sie es installieren, da es das System beeinträchtigen kann.

Gehen Sie wie folgt vor:

1. Installieren Sie das Paket `cpu-microcode-amd` oder `cpu-microcode-intel` abhängig von der CPU mit dem Befehl `doas pkg install cpu-microcode-amd` oder `doas pkg install cpu-microcode-intel`.
2. Geben Sie in der Konsole `ee /boot/loader.conf` ein.
Die Datei `loader.conf` wird im Editor geöffnet

```
kern.geom.label.disk_ident.enable="0"  
kern.geom.label.gptid.enable="0"  
cryptodev_load="YES"  
zfs_load="YES"  
hint.attimer.0.clock="0"  
vmm_load="YES"  
pptdevs="0/30/3"
```

3. Ergänzen Sie folgende Zeilen in der Datei `loader.conf`:

```
cpu_microcode_load="YES"  
cpu_microcode_name="/boot/firmware/intel-ucode.bin"
```

4. Starten Sie TwinCAT/BSD neu mit dem Befehl `shutdown -r now`.

- ⇒ Mit diesen Einstellungen wird bei jedem Systemstart überprüft, ob Pakete mit aktualisiertem CPU-Mikrocode vorhanden sind, und installieren diese bei Bedarf automatisch. Entfernen Sie die beiden Zeilen aus der `loader.conf`, wenn diese Funktion nicht mehr gewünscht ist.

7 Package-Server

Der Beckhoff Package-Server ist ein von Beckhoff gehosteter Server, der eine Sammlung vorkompilierter Software enthält, die sogenannten Packages. Dies ist die einfachste Methode, um zusätzliche Software unter TwinCAT/BSD zu installieren oder bereits vorhandene Software zu aktualisieren.

Bei der Installation greift TwinCAT/BSD auf das voreingestellte Beckhoff-Repository zu:

<https://tcbsd.beckhoff.com/TCBSD/14/stable/packages/All/>

Der Beckhoff Package-Server spiegelt einen Großteil des normalen FreeBSD-Repositorys und beinhaltet darüber hinaus folgende spezifische Beckhoff-Packages:

- TwinCAT/BSD-Updates
- TwinCAT 3 Updates
- TwinCAT 3 Functions

● Unterstützte Packages

I Im Gegensatz zu Beckhoff-Packages, werden Packages von Drittanbietern nicht geprüft und nicht supportet.

Repositorys

Sie können auf weitere Repositorys zurückgreifen, wenn Sie andere Packages verwenden möchten, die nicht von Beckhoff bereitgestellt werden. Neben dem standardmäßig eingestellten Beckhoff-Repository können Sie weitere Repositorys hinzufügen, aktivieren, deaktivieren oder entfernen. Schalten Sie im Anschluss wieder auf das Beckhoff Repository zurück.

Achten Sie darauf, weitere Repositorys in einer eigenen Datei unter `/etc/pkg` zu konfigurieren. TwinCAT/BSD verfügt bei Auslieferung über zwei Repositorys:

- `TCBSD.conf` ist das Standard Beckhoff-Repository

```
TCBSD: {
  url: "https://tcbsd.beckhoff.com/TCBSD/14/stable/packages"
  enabled: true,
  signature_type: "fingerprints",
  fingerprints: "/usr/share/keys/bhf-pkg"
}
```

- `FreeBSD.conf` ist das offizielle FreeBSD-Repository und standardmäßig deaktiviert

```
FreeBSD: {
  url: "pkg+http://pkg.FreeBSD.org/${ABI}/quarterly",
  mirror_type: "srv",
  signature_type: "fingerprints",
  fingerprints: "/usr/share/keys/pkg",
  enabled: yes
}
```

7.1 Auf chinesischen Server wechseln

Das Beckhoff-Repository ist aus China nicht zugänglich und muss auf den chinesischen Server umgestellt werden. Führen Sie das Skript `pkgrepo-set` aus und wechseln Sie damit vom Standard-Server auf den chinesischen Server.

Wechseln Sie wie folgt auf den chinesischen Server:

1. Geben Sie den Befehl `doas sh /usr/local/share/examples/bhf/pkgrepo-set.sh china` in der Konsole ein.
 2. Die URL in der Datei `TCBSD.conf` wird von `https://tcbsd.beckhoff.com/TCBSD/14/stable/packages` auf `https://tcbsd.beckhoff.com.cn/TCBSD/14/stable/packages` umgestellt.
- ⇒ Sie haben den chinesischen Server erfolgreich eingestellt. Mit dem Befehl `doas sh /usr/local/share/examples/bhf/pkgrepo-set.sh release` können Sie die Standardeinstellungen wiederherstellen.

7.2 Auf FreeBSD-Repository umschalten

i Inkompatibilitäten mit bereits installierten Paketen

Das FreeBSD-Repository kann für Testzwecke genutzt werden, um bestimmte Pakete zu testen, die nicht auf dem Beckhoff Package-Server bereitgestellt werden. Aktualisieren Sie in der Zwischenzeit nicht das TwinCAT/BSD-System (`doas pkg upgrade`) über das FreeBSD-Repository, da dies zu Inkompatibilitäten mit bereits installierten Paketen führen kann und wechseln Sie nach den Tests wieder zurück auf den Beckhoff Package-Server.

In diesem Schritt wird gezeigt, wie Sie vom standardmäßig eingestellten Beckhoff-Repository auf das offizielle FreeBSD-Repository umschalten können, um Pakete zu testen, die nur auf dem FreeBSD-Repository bereitgestellt werden. Wenden Sie sich an den Beckhoff-Support, wenn bestimmte Pakete benötigt werden, damit diese in das Standard Beckhoff-Repository aufgenommen werden.

Achten Sie darauf, dass Packages möglicherweise nicht kompatibel mit TwinCAT/BSD sein können und nicht einwandfrei funktionieren, die nicht von einem Beckhoff-Repository installiert wurden. Grund dafür ist, dass das FreeBSD Basissystem für TwinCAT modifiziert wurde. Wechseln Sie nach den Tests wieder zurück auf den Beckhoff Package-Server.

Schalten Sie wie folgt auf das FreeBSD-Repository um:

1. Geben Sie den Befehl `doas ee /usr/local/etc/pkg/repos/FreeBSD.conf` in der Konsole ein.
2. Stellen Sie Variable `FreeBSD: {enabled: no}` auf "yes".

Sie haben erfolgreich den Package-Server gewechselt. Ab sofort werden alle Packages vom offiziellen FreeBSD-Repository geladen. Stellen Sie die Variable auf "no", um wieder das Standard Beckhoff-Repository zu verwenden.

7.3 Package-Verwaltung

Eine TwinCAT/BSD-Installation enthält die erforderliche Software für das Betriebssystem und die TwinCAT 3 Runtime. Sie können zusätzliche Software oder TwinCAT Functions installieren.

Sie müssen entscheiden, welche Funktionen Sie benötigen und eine Software auswählen, die diese Funktionen bereitstellt. In diesem Kapitel wird gezeigt wie Sie Packages, also vorkompilierte Software:

- suchen,
- installieren,
- aktualisieren,
- deinstallieren
- und sperren können.

Der Befehl `pkg info` listet alle Packages mit entsprechender Version auf, die auf dem System installiert sind. Mit `pkg info <packagename>` werden Informationen zu einem bestimmten Package angezeigt.

```
---snipped---
Administrator@CX-3B151A:~ % pkg info IPC-Diagnostics
IPC-Diagnostics-3.1.4024.5_2019110615523410164
Name           : IPC-Diagnostics
Version        : 3.1.4024.5_2019110615523410164
Installed on   : Fri Nov 8 10:55:37 2019 UTC
---snipped---
```

7.3.1 Suchen

Bevor Sie Software installieren, können Sie feststellen, ob die Software auf dem Package-Server zur Verfügung steht. Beachten Sie, dass die Suche nicht zwischen Groß- und Kleinschreibung unterscheidet. Erst mit dem Zusatz `-C` wird zwischen Groß- und Kleinschreibung unterschieden.

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `pkg search <packagename>` in der Konsole ein. Beispiel:

```
Administrator@CX-3B151A:~ % pkg search docbook
docbook-1.5                Meta-port for the different versions of the DocBook DTD
docbook-sgml-4.5_1        DocBook SGML DTD
docbook-xml-5.0_3         DocBook XML DTD
docbook-xsl-1.79.1_1,1    XSL DocBook stylesheets
sdocbook-xml-1.1_2,2      "Simplified" DocBook XML DTD
Administrator@CX-3B151A:~ %
```

2. Es werden mehrere Ergebnisse angezeigt.
3. Mit dem Befehl `pkg search -R docbook` können Sie sich zusätzliche Informationen zum Package anzeigen lassen,

```
---snippet---
name: "docbook"
origin: "textproc/docbook"
version: "1.5"
comment: "Meta-port for the different versions of the DocBook DTD"
maintainer: doceng@FreeBSD.org
www: http://www.oasis-open.org/docbook/
abi: "FreeBSD:12:*"
arch: "freebsd:12:*"
---snippet---
```

4. Nutzen Sie die zusätzliche Information, um die richtige Software auszusuchen.

⇒ Im nächsten Schritt können Sie die Software installieren.

7.3.2 Installieren



Wiederherstellungspunkt erstellen

Erstellen Sie einen Wiederherstellungspunkt, bevor Sie eine größere Systemänderung vornehmen oder Programme installieren (siehe: [Wiederherstellungsoptionen \[► 119\]](#)).

In diesem Schritt wird gezeigt, wie Sie neue Software unter TwinCAT/BSD installieren können. Die Software muss auf dem Package-Server zur Verfügung stehen (Siehe: [Suchen \[► 51\]](#)). Sie können zusätzliche Software oder TwinCAT Functions installieren.

Bei jeder Installation prüft das Programm `pkg`, ob der lokale Datenbestand mit dem auf dem Package-Server übereinstimmt und wird bei Bedarf aktualisiert.

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `doas pkg install <packagename>` in der Konsole ein. Beispiel:

```
---snippet---
Administrator@CX-3B151A:~ % doas pkg install docbook
Password:
Updating FreeBSD12-pkgbase repository catalogue...
FreeBSD12-pkgbase repository is up to date.
All repositories are up to date.
---snippet---
```

2. Das Programm `pkg` sucht automatisch nach weiteren Packages, die für die Installation erforderlich sind.
 3. Bestätigen Sie die Installation mit **[y]**.
- ⇒ Das Package wird aus dem Repository abgerufen und auf dem System installiert. Einige Packages enthalten Installationsmeldungen, die Anweisungen, Warnungen und hilfreiche Hinweise enthalten.

7.3.3 Aktualisieren

● Wiederherstellungspunkt erstellen



Erstellen Sie einen Wiederherstellungspunkt, bevor Sie eine größere Systemänderung vornehmen oder Programme aktualisieren (siehe: [Wiederherstellungsoptionen \[► 119\]](#)).

In diesem Schritt wird gezeigt, wie Sie Packages unter TwinCAT/BSD aktualisieren können. Erstellen Sie eine Sicherung von Ihrem System und starten Sie einen Probelauf mit dem Zusatz `-n`, bevor Sie Packages aktualisieren. Im Probelauf werden alle Packages aufgelistet, die aktualisiert werden können, ohne die Installation auszuführen.

Beta-Packages werden nicht mehr über `pkg upgrade` aktualisiert, sobald die Packages veröffentlicht wurden und nicht mehr im Beckhoff-Repository gelistet sind. Von diesem Zeitpunkt an müssen die Beta-Packages deinstalliert und stattdessen die veröffentlichten Packages installiert werden.

Aktualisieren Sie Packages wie folgt:

1. Geben Sie den Befehl `doas pkg upgrade -n` in der Konsole ein.

Die zu aktualisierenden Packages werden angezeigt.

```
Checking for upgrades (27 candidates): 100%
Processing candidates (27 candidates): 100%
The following 1 package(s) will be affected (of 0 checked):

Installed packages to be UPGRADED:
  ca_root_nss: 3.47_1 -> 3.47.1

Number of packages to be upgraded: 1

287 KiB to be downloaded.
```

2. Geben Sie den Befehl `doas pkg upgrade` in der Konsole ein, um alle Packages zu aktualisieren oder `doas pkg upgrade <packagename>`, um ein bestimmtes Package zu aktualisieren.

⇒ Schauen Sie sich die zu aktualisierenden Packages genau an. Lesen Sie bei Unklarheiten die Release-Informationen zum Package und starten Sie erst dann die Aktualisierung.

Definieren Sie Ausnahmen und sperren Sie Packages, die nicht aktualisiert werden sollen (Siehe: [Sperren \[► 53\]](#)). Gesperrte Packages werden nicht aktualisiert, deinstalliert oder neu installiert.

7.3.4 Deinstallieren

In diesem Schritt wird gezeigt, wie Sie Software unter TwinCAT/BSD deinstallieren können. Das Programm `pkg` stellt sicher, dass eine Deinstallation keine negativen Folgen für das System hat und achtet auf Abhängigkeiten unter den Packages.

Wenn Sie Software deinstallieren, von der eine andere Software abhängt, wird auch diese Software automatisch entfernt.

```
docbook: 1.5
sdocbook-xml: 1.1_2,2
xmlcatmgr: 2.2_2
docbook-xml: 5.0_3
xmlcharent: 0.3_2
docbook-sgml: 4.5_1
iso8879: 1986_3
```

Das Package `docbook` hängt von dem Package `iso8879` ab. Wenn Sie das Package `iso8879` deinstallieren, wird auch `docbook` entfernt. Sie können dieses Verhalten mit dem Zusatz `-f` unterdrücken und nur das ausgewählte Package deinstallieren, ohne dass das System die Abhängigkeiten beachtet.

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `doas pkg delete <packagename>` in der Konsole ein. Beispiel: `doas pkg delete iso8879`
2. TwinCAT/BSD listet Packages auf, die gelöscht werden können und berücksichtigt die Abhängigkeiten.

```
---snipped---
Administrator@CX-3B151A:~ % doas pkg delete iso8879
Password:
Checking integrity... done (0 conflicting)
```

```
Deinstallation has been requested for the following 3 packages (of 0 packages in the universe):
Installed packages to be REMOVED:
 iso8879-1986_3
 docbook-sgml-4.5_1
 docbook-1.5
---snipped---
```

3. Bestätigen Sie mit **[y]**, um die aufgelisteten Packages zu deinstallieren.

⇒ Die deinstallierten Packages werden abschließend zusammengefasst. Achten Sie darauf, dass sich im Laufe der Zeit unerwünschte Packages ansammeln können, wenn Sie beispielsweise Software mit dem Zusatz `-f` deinstallieren oder neue Softwareversionen andere Abhängigkeiten haben.

Mit dem Befehl `pkg autoremove` werden nicht benötigte Packages und Abhängigkeiten identifiziert, aufgelistet und zur Deinstallation vorgeschlagen. Lesen Sie die Liste vorsichtig. Wichtige Packages können auch gesperrt werden, damit diese nicht ausversehen deinstalliert werden (Siehe: [Sperrn](#) [► 53]).

7.3.5 Sperren

Damit Packages nicht ausversehen deinstalliert oder bei Updates aktualisiert werden, können Packages gesperrt werden. Gesperrte Packages werden nicht aktualisiert, deinstalliert oder neu installiert.

Diese Funktion kann besonders bei bestimmten TwinCAT Functions sinnvoll sein, um unerwünschte Updates zu verhindern. Die Sperrung verhindert nicht, dass jemand mit Root-Rechten die im Package enthaltenen Dateien manipuliert.

Sperren Sie Packages wie folgt:

1. Geben Sie den Befehl `doas pkg lock <packagename>` in der Konsole ein.

```
docbook-1.5: lock this package? [y/N]: y
Locking docbook-1.5
```

2. Bestätigen Sie die Abfrage mit **[y]**, um das Package zu sperren.

⇒ Das Package wird solange gesperrt, bis Sie das Package mit dem Befehl `doas pkg unlock <packagename>` entsperren. Mit dem Befehl `pkg lock -l`, können Sie sich alle gesperrten Packages anzeigen lassen.

```
Currently locked packages:
docbook-1.5
```

7.4 Lokales Repository einrichten

Um Software und Updates offline zu installieren, empfiehlt sich die Verwendung eines lokalen Repositorys. Das lokale Repository kann dann über einen USB-Stick oder einen Server im lokalen Netzwerk zur Verfügung gestellt werden. Dazu laden Sie zunächst das TwinCAT/BSD-Repository herunter. Dieses Repository kann dann entweder auf die FAT-Partition eines USB-Sticks kopiert oder über einen FTP- oder Webserver im Netzwerk zur Verfügung gestellt werden.

- [Repository auf USB-Stick bereitstellen](#) [► 53]
- [Eigenen Package-Server einrichten](#) [► 55]

Durch die Spiegelung des gesamten Inhalts bleibt auch die Paketverifizierung gleich. Für Ihr TwinCAT/BSD-System ist es so, als würden die Pakete weiterhin vom Beckhoff-Repository heruntergeladen werden.

In dieser Beschreibung werden alle Konfigurationsschritte lokal auf einem TwinCAT/BSD-System durchgeführt. Sollte dies nicht gewünscht sein, kann das TwinCAT/BSD-Repository alternativ auf ein Windows-System heruntergeladen werden. In diesem Fall wird das offizielle Beckhoff Powershell-Modul unter <https://github.com/Beckhoff/twinatbsd-tools> zum Download bereitgestellt.

7.4.1 Repository auf USB-Stick bereitstellen

In diesem Kapitel wird beschrieben, wie ein Repository auf einem USB-Stick bereitgestellt wird. Für die Arbeitsschritte wird TwinCAT/BSD als Host-System verwendet.

Voraussetzungen:

- Programm zum rekursiven Herunterladen von Dateien aus dem Internet. Ein Beispiel dafür ist das Programm `wget` welches für Linux und TwinCAT/BSD zur Verfügung steht.

Gehen Sie wie folgt vor:

1. Laden Sie das TwinCAT/BSD-Repository vom Beckhoff-Server herunter. Wenn Sie Linux oder TwinCAT/BSD nutzen, verwenden Sie das Kommando `wget --recursive --timestamping --level=inf --no-cache --no-parent --no-cookies --no-host-directories --relative --directory-prefix /tmp/mirror https://tcbsd.beckhoff.com/TCBSD/14/stable/packages/`
 2. Stecken Sie den USB-Stick in ihr TwinCAT/BSD-Gerät. Beachten Sie, dass das Gerät gemäß Ihrer BIOS-Einstellung möglicherweise direkt von dem USB-Stick bootet. Dann stecken Sie den USB-Stick erst nach dem Booten an.
 3. Binden Sie den USB-Stick in ihr System ein (siehe: [USB-Stick einbinden \[► 62\]](#)). Automount wurde aus Sicherheitsgründen ab Werk deaktiviert.
 4. Kopieren Sie das Repository aus dem Verzeichnis `/tmp/mirror` auf die FAT-Partition eines USB-Sticks mit dem Befehl `cp -r /tmp/mirror /mnt/usb`. Der Pfad `/mnt/usb` ist in diesem Beispiel der Mountpoint des USB-Sticks.
 5. Als Nächstes muss der Repository-Pfad geändert werden, der standardmäßig auf diesen Beckhoff Package-Server zeigt: <https://tcbsd.beckhoff.com/TCBSD/14/stable/packages/>
 6. In diesem Beispiel muss der Repository-Pfad auf den USB-Stick zeigen, um das lokale Repository auf dem USB-Stick verwenden zu können. Geben Sie folgenden Befehl ein: `doas sh /usr/local/share/examples/bhf/pkgrepo-set.sh file:///mnt/mirror/TCBSD/14/stable/packages`
- ⇒ Nutzen Sie das pkg-Tool wie gewohnt. Mit dem Befehl `doas pkg upgrade` können jetzt Packages vom USB-Stick aktualisiert und installiert werden. Statt des Beckhoff Package-Servers wird das lokale Repository auf dem USB-Stick verwendet. Beachten Sie, dass nach einem Neustart der USB-Stick wieder manuell eingebunden werden muss.

7.4.2 Eigenen Package-Server einrichten

Die folgenden Schritte können lokal auf einem TwinCAT/BSD-System durchgeführt werden.

1. Schlüssel für RSA-Verschlüsselung erstellen

Zunächst muss ein RSA-Schlüsselpaar erstellt werden. Ein RSA-Schlüsselpaar besteht aus einem privaten und einem öffentlichen Schlüssel. Der private RSA-Schlüssel wird zur Erzeugung digitaler Signaturen verwendet, und der öffentliche RSA-Schlüssel wird zur Überprüfung digitaler Signaturen verwendet.

Erstellen Sie einen privaten RSA-Schlüssel. Sie haben die Wahl zwischen RSA-Schlüsselgrößen von 2048 oder 4096 Bit:

```
openssl genrsa -out myRSAPrivate.key 2048
```

Erstellen Sie einen öffentlichen RSA-Schlüssel:

```
openssl rsa -in myRSAPrivate.key -out myRSAPublic.key -pubout
```

Beschränken Sie den Zugriff nur auf `root` oder speichern Sie den privaten Schlüssel an einem anderen Ort:

```
chmod 0400 myRSAPrivate.key
```

2. Pakete vom Beckhoff Package-Server abrufen

In diesem Schritt können entweder alle Pakete vom Beckhoff Package-Server abgerufen werden oder nur die Pakete, die auf dem System installiert sind.

Alle Pakete vom Server abrufen:

```
doas pkg fetch --yes --output /var/db/myRepository --all
```

Nur die installierten Pakete abrufen:

```
doas sh -c "pkg info | awk '{print \$1}' | xargs -I {} pkg fetch --yes --output /var/db/myRepository {}"
```

3. Repository modifizieren und erstellen

Die heruntergeladenen Pakete können mit benutzerdefinierten Paketen angereichert und auf diese Weise ein eigenes Repository zusammengestellt werden.

Benutzerdefinierten Pakete in das Repository verschieben:

```
mv my-package /var/db/myRepository/All/
```

Repository erstellen und mit dem zuvor erstellen privatem Schlüssel versehen:

```
doas pkg repo /var/db/myRepository/ myRSAPrivate.key
```

4. Repository-Verzeichnis auf den Webserver verschieben

Wenn Sie HTTPS verwenden wollen, benötigen Sie entweder einen Webserver mit einem gültigen Zertifikat (z. B. über letsencrypt beziehen) oder Sie können HTTP verwenden, da die Pakete sowieso schon signiert sind.

HTTPS

Wenn Sie eine eigene Zertifizierungsstelle (CA) verwenden, fügen Sie das Zertifikat ihrer CA zur Zertifikatsliste hinzu

```
/usr/local/etc/ssl/cert.pem
```

Bei Verwendung des mit TwinCAT/BSD ausgelieferten nginx-Servers, fügen Sie die folgenden Zeilen weiter unten in der Datei `/usr/local/etc/nginx/IPCdiagnostics.conf` unter den Bereich `"Server {}"` hinzu:

```
location /pkg {
    alias /var/db/myRepository/;
    autoindex on;
}
```

Danach muss der Webserver mit `doas service nginx restart` einmal neu gestartet werden, damit die Konfiguration aktiv wird. Hier liegen auch andere Seiten, die über den Webserver aufgerufen werden können.

HTTP

Falls Sie das Repository nur über HTTP bereitstellen wollen, lassen Sie den Webbrowser auf Port 80 lauschen und öffnen Sie den Port in der Firewall unter `/etc/pf.conf`. Ergänzen Sie dafür folgende Zeilen in der Datei `pf.conf`:

```
# allow port 80 for pkg repository
pass in quick proto tcp to port 80
```

Fügen Sie die folgenden Zeilen am Ende der Datei `/usr/local/etc/nginx/IPCDiagnostics.conf` unter den Bereich `"http {"` hinzu:

```
server {
    listen 80;
    location /pkg {
        alias /var/db/myRepository/;
        autoindex on;
    }
}
```

Danach muss der Webserver mit `doas service nginx restart` einmal neu gestartet werden, damit die Konfiguration aktiv wird. Achten Sie darauf, dass dieser Eintrag noch von der äußersten Klammer der `http-`Funktion umschlossen ist. Mit diesem Eintrag sind weiterhin nur HTTPS-Zugriffe für alle von Beckhoff vorkonfigurierten Dienste zulässig, erlaubt aber als Ausnahme den Zugriff auf das eigene Repository über HTTP.

5. Öffentlichen Schlüssel an Zielrechner verteilen

Kopieren Sie den öffentlichen Schlüssel `myRSAPublic.key` auf die Zielrechner, beispielsweise in das Verzeichnis `/usr/share/keys` mit Hilfe von `scp`.

6. Repository auf Zielrechnern verwenden

Das benutzerdefinierte Repository bzw. der interne Webserver kann jetzt auf den Zielrechnern als Ziel hinzugefügt und aktiviert werden. `TCBSD.conf` ist das Standard Beckhoff-Repository und befindet sich im Verzeichnis unter `/etc/pkg`. In der Datei befinden sich folgende Einträge.

```
TCBSD: {
    url: https://tcbbsd.beckhoff.com/TCBSD/14/stable/packages
    enabled: true,
    signature_type: "fingerprints",
    fingerprints: "/usr/share/keys/bhf-pkg"
}
```

Kopieren Sie im ersten Schritt die Datei `TCBSD.conf` und benennen Sie die Datei um, beispielsweise in `TCBSD_original`, damit die alle Änderungen schnell rückgängig gemacht werden können und wieder das Standard Beckhoff-Repository verwendet werden kann. Dieser Schritt ist nicht zwingend erforderlich und ist nur eine Sicherungsmaßnahme.

Passen Sie im nächsten Schritt die Datei `TCBSD.conf` unter `/etc/pkg` an, damit die Zielrechner zukünftig auf ihren eigenen Webserver zugreifen:

```
TCBSD: {
    url: "http://my-webserver/pkg",
    enabled: true,
    signature_type: "pubkey",
    pubkey: "/usr/share/keys/myRSAPublic.key"
}
```

Beachten Sie die letzte Zeile, die den Pfad zum öffentlichen Schlüssel auf dem Zielrechner enthält, den Sie in Schritt 5 auf den Zielrechner kopiert haben. Passen Sie den Pfad gegebenenfalls an, wenn Sie einen anderen Speicherort verwenden.

8 Konfiguration

8.1 Systeminformationen

TwinCAT/BSD stellt unterschiedliche Systeminformationen bereit. Die wichtigsten Systeminformationen, die für die tägliche Arbeit mit TwinCAT/BSD und TwinCAT erforderlich sind, können mit dem Tool `TcSysExe.exe` und der TwinCAT-Registry abgerufen werden

TcSysExe.exe

Mit `TcSysExe.exe` ist es beispielsweise möglich, den TwinCAT-Modus aus der Konsole zu steuern und TwinCAT in den Run- oder Config-Modus zu versetzen. Rufen Sie alle verfügbaren Parameter mit `TcSysExe.exe -help` auf. Folgende Systeminformationen sind besonders wichtig:

- Der Befehl `TcSysExe.exe` oder `TcSysExe.exe -version` listet Information zum verwendeten TwinCAT-Build, der AMS Net Id und der TwinCAT/BSD-Version auf:

```
The software licenses can be found in this folder: /usr/local/etc/TwinCAT/3.1/System/Legal/  
TcOsSys.dll: TcOsSys_Rel131_4024_20220407.2  
TwinCAT Build: 3.1.4024.29  
AMS Net Id: 5.66.247.12.1.1  
TC/BSD: 13.0.11.1,2
```

- Der Befehl `TcSysExe.exe --osImageVersion` zeigt die TwinCAT/BSD-Version an:

```
Administrator@CX-42F70C:~ $ TcSysExe.exe -osImageVersion  
TC/BSD: 13.0.11.1,2
```

- Der Befehl `TcSysExe.exe --platformid` zeigt das TwinCAT-3-Plattform-Level des verwendeten Industrie-PCs an:

```
Administrator@CX-42F70C:~ $ TcSysExe.exe -platformid  
HW Platform: 70
```

- Der Befehl `TcSysExe.exe --netid` zeigt die AMS Net Id des Industrie-PCs an:

```
Administrator@CX-42F70C:~ $ TcSysExe.exe -netid  
AMS Net Id: 5.66.247.12.1.1
```

TcRegistry.xml

Über die TwinCAT-Registry sind weitgreifende Systemeinstellungen möglich. Die Datei befindet sich im Verzeichnis `/usr/local/etc/TwinCAT/3.1/TcRegistry.xml` und kann mit `doas ee /usr/local/etc/TwinCAT/3.1/TcRegistry.xml` geöffnet und bearbeitet werden.

Bevor die `TcRegistry.xml` bearbeitet werden kann, muss der `TcSystemService` mit dem Befehl `doas service TcSystemService stop` gestoppt und nach Bearbeitung wieder mit `doas service TcSystemService start` gestartet werden.

Folgende Systeminformationen sind besonders wichtig und können in der XML-Datei bearbeitet werden:

- `AmsNetID`: [AMS NetID ändern \[► 114\]](#)
- `HeapMemSize`: [Heap-Speicher erhöhen \[► 116\]](#)
- `LockedMemSize`: [Router-Speicher anpassen \[► 117\]](#)

8.2 Benutzer und Rechteverwaltung

Es gibt drei Account-Typen, die jeweils unterschiedlichen Einschränkungen unterliegen und grundlegend für die Account-Verwaltung unter TwinCAT/BSD sind. Folgende Account-Typen gibt es unter TwinCAT/BSD:

- Superuser-Account
- Benutzer-Accounts
- Systembenutzer

Der **Superuser-Account**, auch `root` genannt, kann ohne Einschränkungen operieren. Anders als normale Benutzer-Accounts hat `root` die absolute Kontrolle über TwinCAT/BSD. Um die Systemintegrität und Sicherheit zu gewährleisten ist `root` standardmäßig deaktiviert. Dadurch ist es nicht möglich sich direkt als `root` anzumelden.

Benutzer-Accounts stehen für normale Benutzer zur Verfügung, die Zugriff auf TwinCAT/BSD erhalten sollen. Sie erhalten einen eindeutigen Benutzernamen, ein Home-Verzeichnis und können die eigene Benutzerumgebung anpassen. Der Benutzer `Administrator` ist standardmäßig angelegt. Er besitzt keine klassischen Administrator-Rechte wie unter Windows-Systemen, hat jedoch die Berechtigung, sich für bestimmte Zwecke Root-Rechte zu beschaffen.

Die **Systembenutzer** starten Dienste und Programme wie z.B. Mail- oder Webserver. Dadurch ist es möglich Programme bzw. Dienste einzuschränken oder Zugriffsrechte für bestimmte Aufgaben freizuschalten.

Root-Rechte

Weil es nicht möglich ist, sich als `root` anzumelden, haben Benutzer die Möglichkeit Root-Rechte zu erhalten, um ohne Beschränkungen unter TwinCAT/BSD operieren zu können. Verwenden Sie den Befehl `doas`, um Root-Rechte zu erhalten. Dabei entspricht `doas` dem Befehl `sudo`, einem Befehl der aus anderen unixartigen Betriebssystemen bekannt ist.

Gruppen

Unter TwinCAT/BSD können Benutzer-Accounts in Gruppen zusammengefasst werden, um ihre Berechtigungen zur Nutzung einzelner Funktionen oder Software zentral zu verwalten. Statt vielen Benutzer-Accounts dieselben einzelnen Rechte zuzuweisen, wird eine Benutzerrolle definiert, welche die zuzuweisenden Rechte enthält. Die Gruppen werden durch den Gruppennamen und die Gruppen-ID (`gid`) identifiziert. Der TwinCAT/BSD-Kernel entscheidet anhand der User-ID (`uid`) und der Gruppenmitgliedschaft eines Prozesses, ob er dem Prozess etwas erlaubt oder nicht.

Die Datei `group` enthält alle Gruppeninformationen, wie Gruppename, Gruppenpasswort, Gruppen-ID und eine Mitgliederliste der jeweiligen Gruppe. Rufen Sie die Datei mit `cat /etc/group` auf:

```
wheel:*:0:root,Administrator
```

Dieser Auszug zeigt die erste Zeile aus der Datei `group`. Die Datei ist in vier Felder unterteilt, die durch einen Doppelpunkt getrennt sind. Im ersten Feld steht der Gruppename (`wheel`), das zweite enthält ein verschlüsseltes Passwort (`*`), das dritte enthält die Gruppen-ID (`0`) und das vierte eine Liste mit den dazugehörigen Mitgliedern (`root, Administrator`).

Jeder Benutzer kann seine Zugehörigkeit zu einer Gruppe mit `id` bestimmen. Hier ein Beispiel mit dem Benutzer `Administrator`, der der Gruppe `1001 Administrator` und `0 wheel` angehört:

```
uid=1001(Administrator) gid=1001(Administrator) groups=1001(Administrator),0(wheel)
```

Mit `doas pw groupadd <groupname>` können Sie eine neue Gruppe erstellen. Benutzen Sie `pw groupshow <groupname>`, um sich eine Gruppe anzeigen zu lassen. Mit dem Befehl `doas pw groupmod <groupname> -M <username>`, können Sie einen Benutzer zu einer Gruppe hinzufügen.

```
Administrator@CX-3B151A:~ % pw groupshow AI
AI:*:1007:Skynet,DeepThought,Ava,HAL
```

8.2.1 Neuen Benutzer anlegen

Legen Sie mit Hilfe des Befehls `adduser` neue Benutzer unter TwinCAT/BSD an. Dabei werden Sie interaktiv durch den Prozess geleitet. Nur der Superuser (`root`) kann neue Benutzer anlegen. Deshalb müssen Sie den Befehl `adduser` als Administrator und mit Root-Rechten ausführen.

Diese Einstellungen sind alternativ über das Webinterface des Beckhoff Device Managers möglich (siehe: [Beckhoff Device Manager: Webinterface](#) [► 69]).

Voraussetzungen:

- Zugang zum Administrator-Account

Lege Sie neue Benutzer wie folgt an:

1. Geben Sie den Befehl `doas adduser` in der Konsole ein.
Bestätigen Sie den Befehl mit dem Passwort des Administrators.
2. Legen Sie einen Benutzernamen fest und tragen Sie den vollen Namen ein.

```
Username: NewUser
Full name: John Doe
```

3. Im nächsten Schritt können Sie die `Uid`, `Login group`, die sekundäre `Login group` und die `Login class` festlegen. Drücken Sie **[Enter]**, um Standardeinstellungen zu übernehmen.

```
Uid [Leave empty for defaults]:
Login group [NewUser]:
Login group is NewUser. Invite NewUser into other groups? []:
Login class [default]:
```

4. Wählen Sie unter `Shell (sh csh tcsh nologin) [sh]`: eine Shell aus, mit der sich der Benutzer einloggt. Standardmäßig wird für Skripte und die Kommandozeile die Bourne-Shell (`sh`) verwendet. Für die direkte Interaktion über die Kommandozeile bietet sich wegen einer besseren Übersichtlichkeit und eines größeren Funktionsumfangs jedoch vor allem `tcsh` als Shell an.

```
Shell (sh csh tcsh nologin) [sh]: tcsh
```

5. Drücken Sie bei den folgenden Parametern **[Enter]**, um Standardeinstellungen zu übernehmen.

```
Home directory [/home/NewUser]:
Home directory permissions (Leave empty for default):
Use password-based authentication? [yes]:
Use an empty password? (yes/no) [no]:
```

6. In diesem Schritt können Sie entscheiden, ob ein Passwort für den Benutzer zufällig generiert werden soll oder ob Sie selber ein Passwort vergeben wollen.

```
Use a random password? (yes/no) [no]:
```

7. Drücken Sie im Anschluss **[Enter]**, um die Standardeinstellungen unter `Lock out the account after creation? [no]`: zu übernehmen.

⇒ Im Anschluss wird eine Zusammenfassung ausgegeben. Sie können Ihre Angaben überprüfen und bei Bedarf einen weiteren Benutzer anlegen. Zusätzlich wird das generierte Benutzerpasswort angezeigt.

```
adduser: INFO: Successfully added (NewUser) to the user database.
adduser: INFO: Password for (NewUser) is: Luq39oGIwPhjT
Add another user? (yes/no): no
Goodbye!
```

8.2.2 Benutzerinformationen editieren

Mit dem Programm `chpass` können Sie weitere Benutzerinformationen editieren. Ein Superuser (`root`) hat erweiterte Rechte und kann mehr Felder editieren als andere Benutzer.

Ein Superuser (`root`) kann neben den normalen persönlichen Einstellungen, das Homeverzeichnis, die `Uid`, `Gid`, das Homeverzeichnis und den Login-Namen ändern. Zusätzlich sind Sicherheitseinstellungen möglich, indem Sie mit `Change` den Zeitpunkt für Passwortänderungen festlegen oder mit `Expire` festlegen wann der Benutzer-Account abläuft.

```
#Changing user information for NewUser.
Login: NewUser
Password: $6$q1X1/ZB/NGu9ulrF$.JYhoCPsGT6hk0GD34oJYWwOKGxY67ka8181py/0HY.7XvXK69
JdeYotMkNjNqVqBTTfblYBQ3SZ.MYxChPeQ1
Uid [#]: 1002
Gid [# or name]: 1002
Change [month day year]:
Expire [month day year]:
Class:
Home directory: /home/NewUser
```

Ein normaler Benutzer-Account kann den Vor- und Nachnamen, die Shell und die Kontaktinformationen bearbeiten.

```
#Changing user information for NewUser.
Shell: /bin/tcsh
Full Name: John Doe
Office Location:
Office Phone:
Home Phone:
Other information:
```

Editieren Sie Benutzerinformationen wie folgt:

1. Geben Sie den Befehl `chpass NewUser` in der Konsole ein. Oder `doas chpass NewUser`, wenn Sie die Informationen als Superuser (`root`) editieren wollen.
 2. Navigieren Sie mit den Pfeiltasten in die Zeile, die Sie editieren wollen.
 3. Drücken Sie **[Esc]**, um den Editor in den Kommandomodus zu schalten.
 4. Löschen Sie voreingestellte Werte mit **[x]**.
 5. Drücken Sie **[i]**, um neuen Text am Cursor einzufügen.
 6. Drücken Sie **[Esc]** und geben `:wq` in der Konsole ein, um die Änderungen zu speichern und den Editor zu verlassen. Oder geben Sie `q!` ein, um den Editor ohne Speichern zu verlassen.
- ⇒ Im Anschluss wird eine Rückmeldung ausgegeben, dass alle Änderungen erfolgreich gespeichert wurden. Bei fehlerhaften Eingaben wird eine Fehlermeldung mit einem Verweis auf die Stelle angezeigt.

```
/etc/pw.6RnflE: 15 lines, 412 characters.
chpass: upper-case letters are dangerous in a login name
chpass: user information updated
Administrator@CX-3B151A:~ %
```

8.2.3 Benutzer löschen

Mit dem Programm `rmuser` können Sie Benutzer-Accounts vollständig aus dem System entfernen. Benutzer-Accounts können nur vom Superuser (`root`) gelöscht werden.

Diese Einstellungen sind alternativ über das Webinterface des Beckhoff Device Managers möglich (siehe: [Beckhoff Device Manager: Webinterface \[► 69\]](#)).

Voraussetzungen:

- Zugang zum Administrator-Account

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `doas rmuser NewUser` in der Konsole ein. Bestätigen Sie den Befehl mit dem Passwort des Administrators.
2. Der Benutzer-Account wird angezeigt. Überprüfen Sie die Daten, bevor Sie weiter fortfahren.

```
Administrator@CX-3B151A:~ % doas rmuser NewUser
Password:
Matching password entry:

NewUser:$6$q1X1/ZB/NGu9ulrF$.JYhoCPsGT6hk0GD34oJYWwOKGxY67ka8181py/0HY.7XvXK69Jd
eY0tMkNjNqVqBTTfblyBQ3SZ.MYxChPeQ1:1002:1002::0:0:John Doe,,555 433423:/home/Ne wUser:/bin/tcsh

Is this the entry you wish to remove? Yes
```

3. Entfernen Sie den Benutzer-Account mit `yes`.

```
Remove user's home directory (/home/NewUser)? Yes
Removing user (NewUser): mailspool home passwd.
Administrator@CX-3B151A:~ %
```

4. Entfernen Sie das Homeverzeichnis mit `yes`.

⇒ Der Benutzer-Account wird zusammen mit dem Homeverzeichnis gelöscht. Einträge aus Gruppen, temporären Dateispeicherbereichen und E-Mails werden entfernt. Alle Prozesse des Benutzers werden beendet.

8.3 USB-Stick einbinden

In diesem Abschnitt wird gezeigt, wie Sie einen USB-Stick in TwinCAT/BSD einbinden können. Überprüfen Sie vorher die USB-Konfiguration. Verwenden Sie dazu den Befehl `dmesg`, um zu überprüfen, ob der USB-Stick in den Systemmeldungen erscheint:

```
umass0: <Generic Mass Storage, class 0/0, rev 2.00/1.01, addr 2> on usb0
umass0: SCSI over Bulk-Only; quirks = 0x4101
umass0:1:0: Attached to scbus1
da0 at umass-sim0 bus 0 scbus1 target 0 lun 0
da0: <Generic Flash Disk 8.07> Removable Direct Access SPC-2 SCSI device
da0: Serial Number 2EFBC899
da0: 40.000MB/s transfers
da0: 3900MB (7987200 512 byte sectors)
da0: quirks=0x2<NO_6_BYTE>
```

Die Angaben zu Fabrikat, Gerätedatei (`da0`), Geschwindigkeit und Kapazität können sich je nach Gerät unterscheiden.

Voraussetzungen:

- Der USB-Stick ist mit FAT32 formatiert.
- Schließen Sie den USB-Stick an den Industrie-PC an.

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `gpart show` ein, um nach einer FAT-Partition auf dem USB-Stick zu suchen. Der USB-Stick in diesem Beispiel hat eine FAT32-Partition und eine Größe von 3,8 GB. Siehe Eintrag: 1 fat32 (3.8G)

```
Administrator@CX-3B151A$ gpart show
=>      40  7728256  ada0  GPT  (3.7G)
        40    409600    1  efi  (200M)
        409640    2008    -  free - (1.0M)
        411648  7315456    2  freebsd-zfs (3.5G)
        7727104    1192    -  free - (596K)

=>      63  7987137  da0  MBR  (3.8G)
        63     737    -  free - (369K)
        800  7986400    1  fat32  (3.8G)
Administrator@CX-3B151A$
```

2. Geben Sie den Befehl `ls /dev/da0*` ein, um zu ermitteln wie die FAT32-Partition heißt. `da0s1` oder `da0p1`.

```
ls /dev/da0s1
/dev/da0 /dev/da0s1
```

3. Geben Sie den Befehl `doas mkdir /mnt/usb` ein, um das Verzeichnis `/mnt/usb` zu erstellen.
 4. Geben Sie den Befehl `doas mount -t msdosfs /dev/da0s1 /mnt/usb` ein, um den USB-Stick unter `/mnt/usb` einzubinden.
 5. Navigieren Sie mit dem Befehl `cd /mnt/usb` zum Mointpoint des USB-Sticks.
 6. Benutzen Sie den Befehl `ls`, um sich alle Ordner im Verzeichnis anzeigen zu lassen.
- ⇒ Sie haben erfolgreich einen USB-Stick in TwinCAT/BSD eingebunden. Die Einstellungen werden nicht dauerhaft gespeichert. Nach einem Neustart muss der USB-Stick erneut eingebunden werden.

USB-Geräte können auch automatisch eingebunden werden. Diese Funktion wurde ab Werk ausgeschaltet, um die Sicherheit von TwinCAT/BSD zu erhöhen. Weitere Informationen zum Automount-Service finden Sie unter: <https://www.freebsd.org/doc/handbook/usb-disks.html>

8.4 Automount für externe Datenträger aktivieren

Externe Datenträger werden unter TwinCAT/BSD nicht automatisch eingebunden, um die Sicherheit des Systems zu erhöhen. Die Automount-Funktion ist ab Werk deaktiviert. Im Normalfall müssen externe Datenträger aktiv und manuell in TwinCAT/BSD eingebunden werden, die Einstellungen werden aber nicht dauerhaft gespeichert und müssen nach einem Neustart erneut eingebunden werden.

In diesem Kapitel wird beschrieben, wie Sie externe Datenträger z. B. USB-Sticks, optische Laufwerke oder externe Festplatten, mit `devd-mount` automatisch und dauerhaft einbinden können. Der Datenträger muss ein Dateisystem verwenden, welches von FreeBSD erkannt wird, wie beispielsweise EXFAT, FAT32, FAT16, NTFS, UFS, ISO 9660 (CDs), UDF (DVDs).

Nützliche Befehle:

- `gpart show`: Gefundene Partitionen anzeigen.
- `mount`: Anzeigen, welcher Datenträger mit welchem Dateisystem an welcher Stelle eingebunden wurde.

Die Zugriffsberechtigungen können in der Konfigurationsdatei `/usr/local/etc/devd-mount.conf` angepasst werden. Standardmäßig sind Schreib-/Lesezugriff und Ausführen für den Benutzer `root` und für die Gruppe `operator` erlaubt. Für alle anderen Benutzer ist nur Lesen und Ausführen erlaubt.

Voraussetzungen:

- TwinCAT/BSD-Version: 14.x.xx.x, x

Gehen Sie wie folgt vor:

1. Installieren Sie das Skript `devd-mount` auf dem System mit `doas pkg install devd-mount`
 2. Starten Sie den Service `devd` nach der Installation mit `doas service devd restart neu`.
 3. Schließen Sie den externen Datenträger an den Industrie-PC an.
 4. Der Datenträger wird standardmäßig mit seiner Geräteknotenbezeichnung (device node), d. h. mit dem Namen, mit dem der Datenträger unter `/dev` gelistet wird, unter `/media` eingebunden.
- ⇒ Zieht man den Datenträger ab, bleiben die Mountpoints unter `/media` erhalten. Steckt man den Datenträger zwischenzeitlich oder nach einem Neustart wieder ein, wird er an gleicher Stelle wieder eingebunden.

Wenn in der Zwischenzeit ein zusätzlicher Datenträger eingebunden wird und der ursprüngliche Datenträger wieder eingesteckt wird, kann sich die Geräteknotenbezeichnung (device node), ändern und ein Datenträger wird beispielsweise unter `/media/da1` statt `/media/da0` eingebunden.

8.5 USV-Software konfigurieren

In diesem Kapitel wird beschrieben, wie die Beckhoff USV CU81x0-0xx0 für eine Kommunikation über die USB-Schnittstelle konfiguriert werden kann. Die dafür notwendige USV-Software bzw. das Paket `TcUpsSoftware` ist bereits in der aktuellen TwinCAT/BSD-Version enthalten. Bei älteren Versionen kann das Paket mit `doas pkg install TcUpsSoftware` nachinstalliert werden.

Beachten Sie, dass die USV-Software vorinstalliert ist, aber der USV-Service nicht automatisch bei Systemstart gestartet wird. Das Verhalten der USV bei einem Spannungsausfall erfolgt in der Konfigurationsdatei `TcUpsSoftware.conf` unter `/usr/local/etc/TcUpsSoftware.conf`

Tab. 6: USV-Software: Einstellungen in der Konfigurationsdatei.

Option	Wert	Beschreibung
<code>ShutdownOnBatteryEnable</code>	[0 oder 1]	Die Option ist standardmäßig eingeschaltet [=1]. Bei einem Spannungsausfall wird der Industrie-PC ordnungsmäßig heruntergefahren.
<code>ShutdownOnBatteryWait</code>	[0 ... 43200 Sekunden]	Wenn <code>ShutdownOnBatteryEnable</code> eingeschaltet ist, wird der Industrie-PC nach der eingestellten Zeit in Sekunden heruntergefahren.
<code>TurnUpsOffEnable</code>	[0 oder 1]	Wenn diese Option eingeschaltet ist [=1], wird die USV heruntergefahren, nachdem der Industrie-PC heruntergefahren wurde.
<code>TurnUpsOffWait</code>	[0 ... 600 Sekunden]	Wenn <code>TurnUpsOffEnable</code> eingeschaltet ist, wird die USV abgeschaltet, nachdem der Industrie-PC heruntergefahren wurde und die in dieser Option eingestellte Zeit abgelaufen ist.

Gehen Sie wie folgt vor:

1. Öffnen Sie die Konfigurationsdatei `rc.conf` mit dem Befehl `doas ee /etc/rc.conf`
 2. Ergänzen Sie Zeile `TcUpsSoftware_enable="YES"` in der Konfigurationsdatei, damit der Service automatisch bei jedem Systemstart gestartet wird.
 3. Öffnen Sie die Konfigurationsdatei `TcUpsSoftware.conf` mit dem Befehl `doas ee /usr/local/etc/TcUpsSoftware.conf` und tragen Sie die erforderlichen Werte für die Haltezeit der USV ein.
 4. Starten Sie den USV-Service mit dem Befehl `doas service TcUpsSoftware start`
- ⇒ Die USV-Software steuert die Beckhoff USV CU81x0-0xx0 bei einem Spannungsausfall entsprechend den Einstellungen in der Konfigurationsdatei `TcUpsSoftware.conf` und kann mit dem Befehl `doas service TcUpsSoftware stop` für die aktuelle Session wieder deaktiviert werden.

Soll der USV-Service dauerhaft deaktiviert werden, muss den Eintrag `TcUpsSoftware_enable="YES"` wieder aus der `rc.conf` entfernt werden.

8.6 Realtime-Ethernet deaktivieren

In diesem Kapitel wird gezeigt, wie Sie Realtime-Ethernet deaktivieren können, wenn Sie die Echtzeitkommunikation nicht benötigen und die Schnittstellen stattdessen für die herkömmliche Ethernetkommunikation mit voller Bandbreite verwenden wollen.

Realtime-Ethernet ist standardmäßig aktiv. Mit dem Befehl `TcRteConfig show` können Sie die aktuelle Konfiguration für die Schnittstellen aufrufen:

```
Administrator@CX-3B151A:~ % TcRteConfig show
sysctl:
dev.igb.1.iflib.tc_rte.mode: 0
dev.igb.1.iflib.support_tc_rte: 1
dev.igb.1.iflib.disable_tc_rte: 0
dev.igb.0.iflib.tc_rte.mode: 0
dev.igb.0.iflib.support_tc_rte: 1
dev.igb.0.iflib.disable_tc_rte: 0
```

Je nach Gerät können unterschiedliche Netzwerkadapter angezeigt werden. Im hier aufgeführten Beispiel heißen die Netzwerkadapter `igb0` und `igb1`.

Deaktivieren Sie Realtime-Ethernet wie folgt:

1. Geben Sie den Befehl `doas TcRteConfig disable igb.1` in der Konsole ein. Realtime-Ethernet wird für die Schnittstelle `igb.1` deaktiviert.

```
/boot/device.hints:  
dev.igb.1.iflib.disable_tc_rte="1"  
Administrator@CX-3B151A:~ %
```

2. Starten Sie den Industrie-PC mit dem Befehl `shutdown -r now neu`, damit die Einstellungen übernommen werden.

⇒ Nach dem Neustart wird Realtime-Ethernet für die Schnittstelle `igb.1` deaktiviert. Mit dem Befehl `doas TcRteConfig enable igb.1` können Sie Realtime-Ethernet wieder aktivieren. Auch hier werden die Einstellungen erst nach einem Neustart übernommen.

8.7 Dienste automatisch starten (Autostart)

In diesem Abschnitt wird gezeigt, wie Sie Anwendungen und Dienste automatisch nach dem Booten starten können. Unter TwinCAT/BSD ist dazu ein passender Eintrag in der Datei `/etc/rc.conf` erforderlich und wird beispielhaft anhand des Mosquitto-MQTT-Brokers gezeigt.

Generell enthält die Datei `/etc/rc.conf` Informationen zur Systemkonfiguration, also beispielsweise Informationen über den lokalen Hostnamen, Konfigurationsdetails für mögliche Netzwerkschnittstellen und welche Dienste bei einem Systemstart gestartet werden sollten.

Dieser Arbeitsschritt funktioniert nur mit Anwendungen und Diensten, die entsprechende rc-Skripte mitbringen, um als Dienst bzw. Daemon gestartet zu werden. Die Skripte werden unter `/etc/rc.d` abgelegt. Für eigene Anwendungen ohne solche rc-Skripte gibt es unter <https://docs.freebsd.org/en/articles/rc-scripting/> weiterführende Informationen, wie diese rc-Skripte erstellt werden können.

Voraussetzungen:

- Mosquitto MQTT-Broker.

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `doas ee /etc/rc.conf` in der Konsole ein.
Die Datei `rc.conf` wird geöffnet.
2. Navigieren Sie im Editor an das Ende der Datei und erstellen Sie folgenden Eintrag:
`mosquitto_enable="YES"`
3. Drücken Sie **[Esc]** und speichern Sie die Änderungen.
⇒ Der Mosquitto MQTT-Broker wird beim nächsten Systemstart automatisch gestartet.

8.8 Shell ändern

Eine Shell ist eine Kommandozeilen-Schnittstelle, mit der der Anwender mit TwinCAT/BSD interagieren und Befehle ausführen kann. TwinCAT/BSD enthält bereits bei Auslieferung einige Shells, darunter die als Standard eingestellte `sh`-Shell. Der Anwender kann jederzeit auf eine andere Shell, beispielsweise die `tcsh`-Shell ausweichen oder weitere Shells nachinstallieren.

Die Shells unterscheiden sich in den eingebauten Funktionen oder werden von Anwendern bevorzugt, wenn diese die tägliche Arbeit erleichtern, beispielsweise durch die Autovervollständigung von Dateinamen. Welche Shell vom Anwender eingesetzt wird, ist letztendlich eine Frage der persönlichen Vorliebe.

Alle im System vorhandenen Shells werden unter `/etc/shells` aufgelistet.

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `chsh -s tcsh` in der Konsole ein, um auf die `tcsh`-Shell zu wechseln.
2. Melden Sie sich mit dem Befehl `login <Benutzername>` erneut an.
⇒ Die `tcsh`-Shell ist jetzt als Standard-Shell für den eingeloggten Benutzer ausgewählt. Sie können die Shell jederzeit mit `chsh -s` wieder wechseln.

8.9 Tastatursprache umstellen

Wenn Sie die Tastatur auf eine andere Tastatursprache umstellen möchten, geht dies am schnellsten mit dem Befehl `kbdmap` und gilt für die aktuelle Session. Erstellen Sie einen Eintrag in der Datei `rc.conf`, damit die Spracheinstellungen auch nach einem Neustart bestehen bleiben.

Gehen Sie wie folgt vor:

1. Öffnen Sie die Datei `rc.conf` mit dem Befehl `doas ee /etc/rc.conf`
2. Navigieren Sie mit den Pfeiltasten nach unten und ergänzen Sie die folgende Zeile:
`keymap="de.kbd".`
3. Verwendet Sie ein entsprechendes Länderkürzel. In diesem Beispiel wird `de` als Länderkürzel für Deutsch verwendet.

⇒ Die Spracheinstellungen in der Datei `rc.conf` werden dauerhaft übernommen. Starten Sie TwinCAT/BSD mit `shutdown -r now` neu, damit die Änderungen wirksam werden. Entfernen Sie den Eintrag, um die Standardeinstellungen wiederherzustellen.

8.10 Uhrzeit mit NTP synchronisieren

Die interne Uhrzeit eines Industrie-PCs ist nie ganz exakt, weshalb es mit dem Network Time Protocol (NTP) eine Möglichkeit gibt, die exakte Uhrzeit zu ermitteln und festzulegen. Um die aktuelle Zeit zu erhalten, wird ein NTP-Client verwendet, um die lokale Systemzeit mit einem Zeitserver zu synchronisieren. Dazu bietet Beckhoff einen globalen NTP-Server-Pool an, über den die aktuelle Zeit zur Verfügung gestellt wird:

```
ntp.beckhoff-cloud.com
```

TwinCAT/BSD ist so vorkonfiguriert, dass es diesen NTP-Server-Pool verwendet, um die aktuelle Zeit zu ermitteln. Die Konfiguration des NTP-Clients erfolgt über die Konfigurationsdatei:

```
/etc/ntp.conf
```

Dort finden Sie bereits den Eintrag für den Beckhoff-NTP-Server-Pool `ntp.beckhoff-cloud.com`. Falls Sie einen eigenen NTP-Server verwenden möchten, ersetzen Sie den Eintrag durch die Adresse Ihres NTP-Servers.

Hinweis Wenn es sich dabei um einen Windows-NTP-Server handelt, ist zusätzlich der Eintrag `tos maxdist 30` in der Konfigurationsdatei `/etc/ntp.conf` erforderlich. Mit „*tos maxdist*“ wird die Entfernung angegeben, die ein NTP-Server entfernt sein darf bzw. wie lange ein Paket für eine Übertragung benötigt. Der Windows-Zeitserver funktioniert nur dann, wenn der Maximalwert angegeben wird, in diesem Fall der Wert „30“.

Diese Einstellungen sind alternativ über das Webinterface des Beckhoff Device Managers möglich (siehe: Beckhoff Device Manager: Webinterface [► 69]).

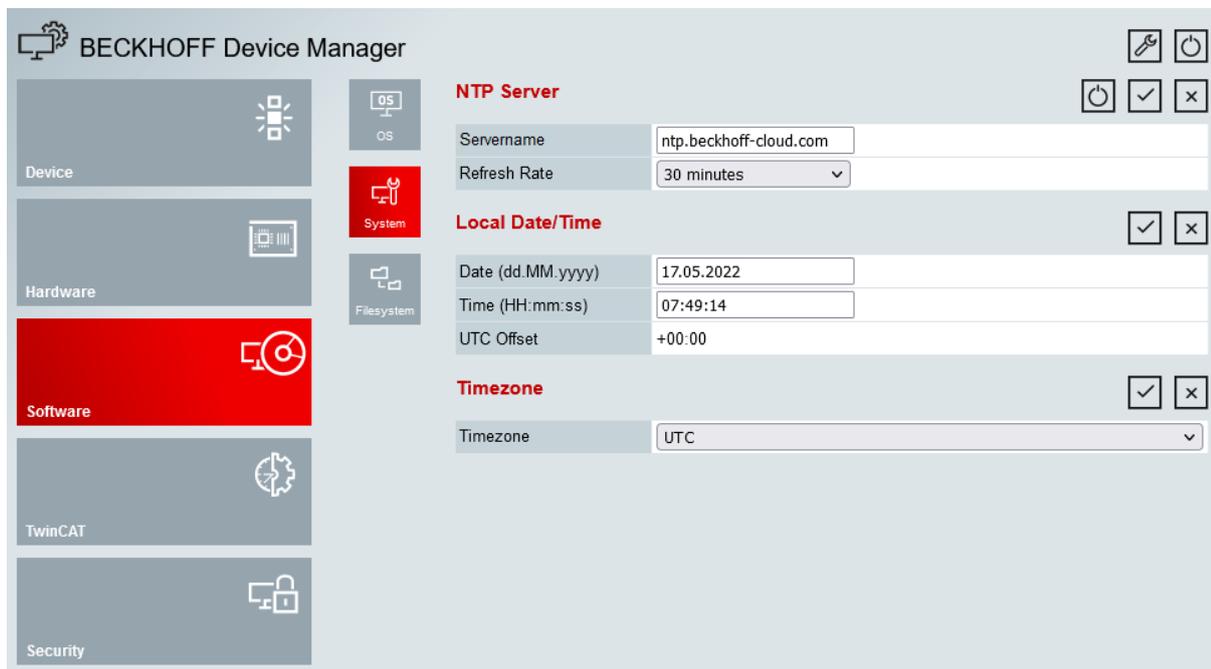


Abb. 16: NTP-Server-Einstellungen im Beckhoff Device Manager.

Beckhoff-NTP-Server-Pool

Der Beckhoff-NTP-Server-Pool ist ein globaler Server-Pool mit mehreren Zeitservern pro geografischer Region. Um nur die besten verfügbaren Server für Ihre Region zu nutzen, verwenden Sie einfach die globale Adresse `ntp.beckhoff-cloud.com` und es werden automatisch die richtigen Server für Ihre Region bereitgestellt.

Dieser Dienst ist ausschließlich für Beckhoff Industrie-PCs verfügbar und darf nur mit ausdrücklicher Genehmigung von Beckhoff anderweitig genutzt werden. Beckhoff übernimmt keine Garantie für die ständige Verfügbarkeit der Zeitserver. Dementsprechend übernimmt Beckhoff keine Haftung für einen Ausfall der Zeitserver.

<https://www.beckhoff.com/ntp-pool>

9 Remote-Zugriff

9.1 Beckhoff Device Manager: Webinterface

Mit dem Beckhoff Device Manager können Beckhoff Industrie-PCs diagnostiziert auf diese Weise wichtige Systemwerte überwacht werden, um Ausfall- und Stillstandszeiten zu vermeiden. Mit einer ausgefeilten Systemdiagnose ist es so möglich, kritische Zustände wie beispielsweise einen drohenden Hitzekollaps durch den Ausfall eines Lüfters oder eine unzureichende Kühlung im Schaltschrank frühzeitig zu erkennen. Der Beckhoff Device Manager steht nur für Beckhoff Industrie-PCs zur Verfügung, da ein für diesen Zweck modifiziertes BIOS vorausgesetzt wird.

Es wird sowohl der Remote-Zugriff von einem anderen PC als auch der Zugriff aus einer SPS heraus auf den Beckhoff Device Manager unterstützt. Dadurch kann der Device Manager einfach und intuitiv konfiguriert werden.

Webinterface

Das Webinterface kann über einen Standard-Webbrowser aufgerufen werden. Geben Sie dazu in die Suchleiste die IP-Adresse oder den Hostnamen des Industrie-PCs ein.

- Beispiel mit IP-Adresse: <https://169.254.136.237>
- Beispiel mit Hostnamen: <https://CX-16C2B8> oder mit BTN-Nummer bei neuen Geräten: <https://BTN-000zf650>

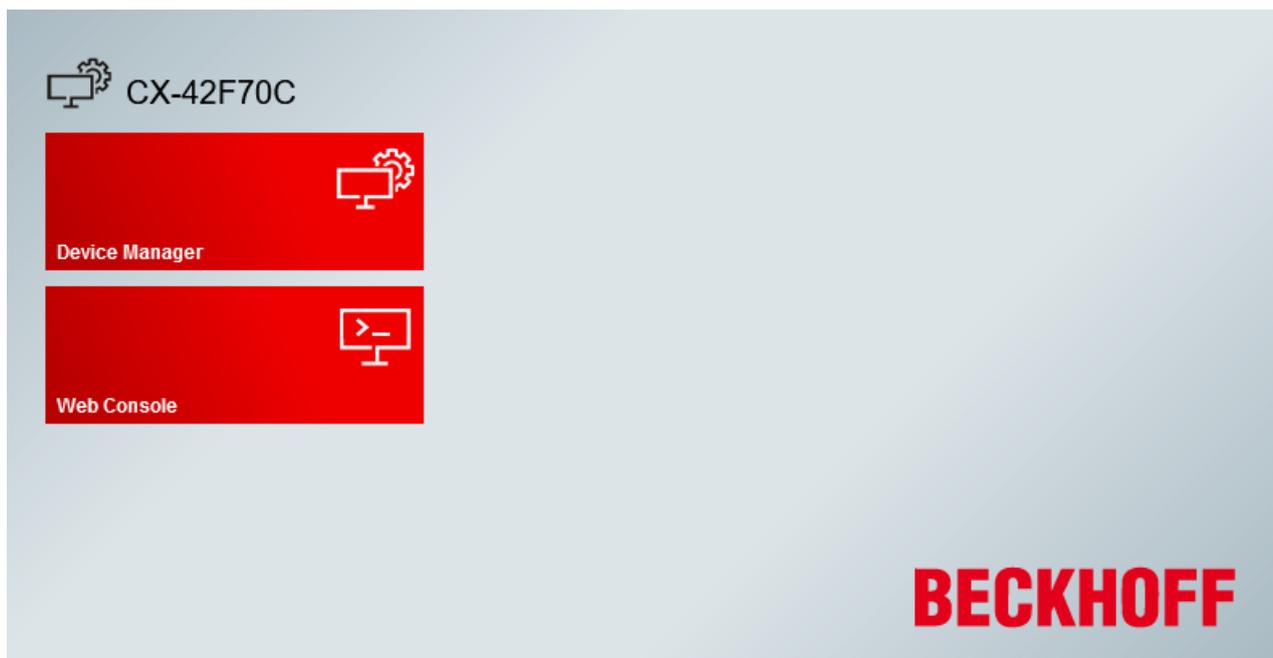


Abb. 17: Startseite des Beckhoff Device Managers.

Auf der Startseite des Beckhoff Device Managers können Sie entweder den Device Manager oder die Web-Konsole von TwinCAT/BSD starten. Mit der Web-Konsole erhalten Sie Zugriff auf die Konsole von TwinCAT/BSD und können damit den Industrie-PC ohne Monitor betreiben.

Der Zugriff auf das Webinterface ist durch die Login-Daten und das Standardpasswort des Administrators geschützt. Dieses sollten Sie unbedingt ändern, um unbefugten Zugriff auf das System zu verhindern. Zugangsdaten bei Auslieferung:

- Benutzername: `Administrator`
- Passwort: `1`

Der Host-PC und der Industrie-PC müssen sich im gleichen Netzwerk befinden und die Firewall den Zugriff über Port 443 (HTTPS) zulassen. Port 443 ist ab Werk freigeschaltet. Abhängig von der Struktur und Konfiguration Ihres Netzwerks (Proxy-Server etc.) kann der Hostname unter Umständen nicht aufgelöst werden. Wir empfehlen daher die Nutzung der IP-Adresse des Industrie-PCs.

Device Manager: Erste Seite

Der Beckhoff Device Manager wird nach dem Login gestartet. Die erste Seite liefert Ihnen zunächst einen grundlegenden Überblick über das Gerät. Von da aus gelangen Sie direkt in den Hardware-, Software-, TwinCAT und Sicherheitsbereich. Dadurch können Sie Hardware und Software gezielt überprüfen.

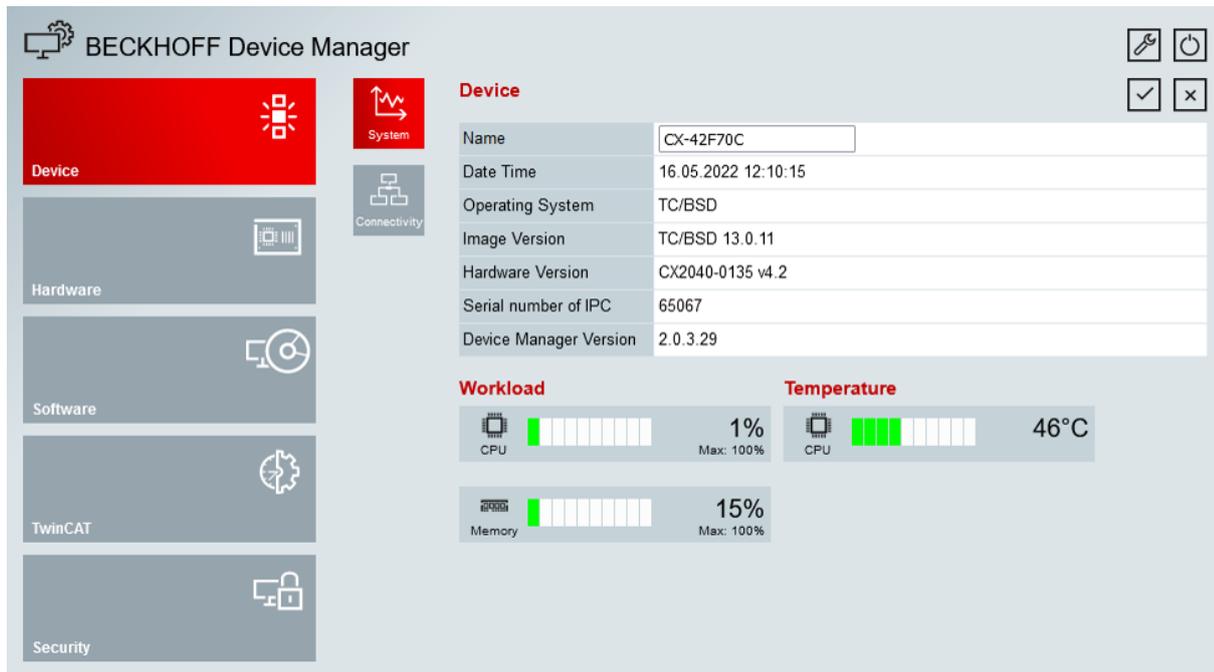


Abb. 18: Erste Seite des Beckhoff Device Managers.

Navigieren Sie von der Startseite aus weiter im Menü und konfigurieren Sie den Industrie-PC. Beachten Sie, dass Änderungen erst nach einer Bestätigung wirksam werden. Gegebenenfalls muss der Industrie-PC neu gestartet werden.

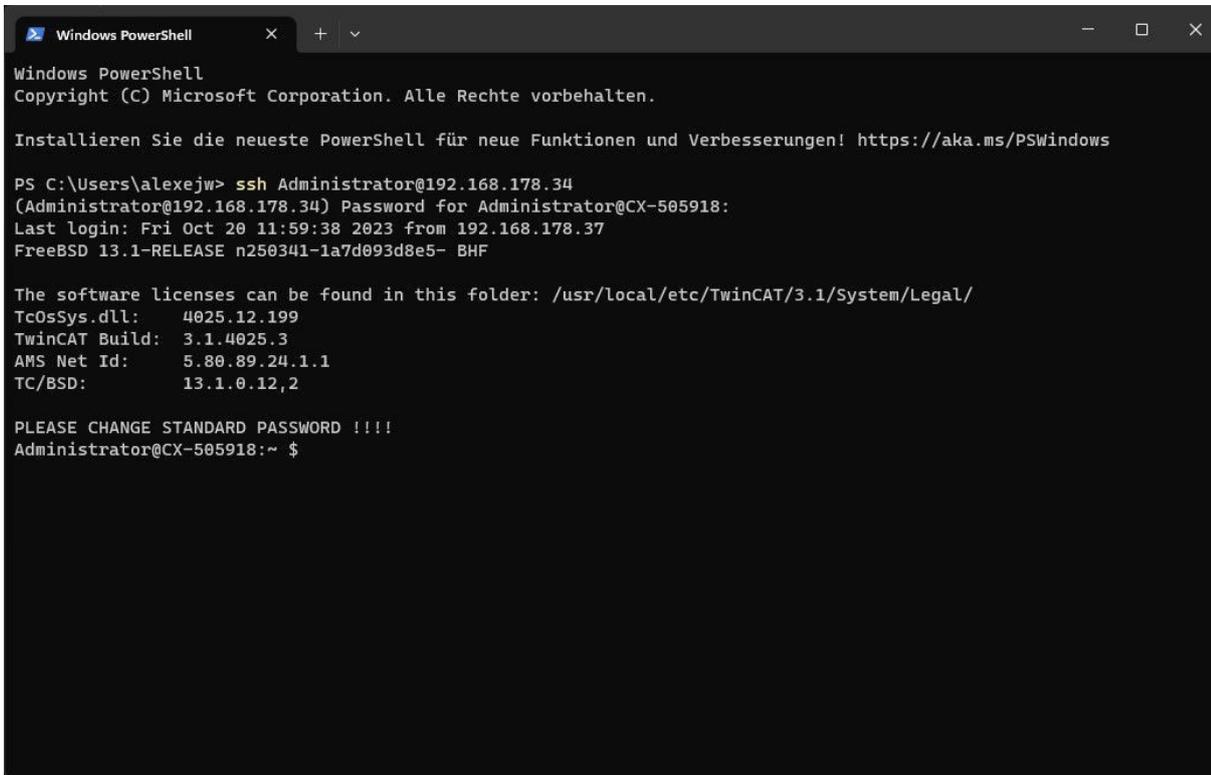
Einstellmöglichkeiten

Folgende Informationen und Einstellungen sind für TwinCAT/BSD verfügbar:

- Allgemeine Geräteinformationen: Auflistung der TwinCAT/BSD- und der TwinCAT-Version. Zusätzlich dazu werden Angaben zur Auslastung der CPU und des Arbeitsspeichers angezeigt.
- Netzwerkeinstellungen: Die Netzwerkeinstellungen können unabhängig von der Konsole geändert und beispielsweise die IP-Adressen der Ethernet-Schnittstellen geändert oder DHCP aktiviert oder deaktiviert werden.
- Speichermedien und Dateisystem: Sowohl der freie Speicherplatz als auch die Lebensdauer der Speichermedien werden angezeigt.
- TwinCAT/BSD-Packages: Auflistung der installierten Beckhoff-Packages mit Versionsangabe, die entweder relevant für TwinCAT oder das Betriebssystem TwinCAT/BSD sind.
- TwinCAT: Im Menü TwinCAT können ADS-Routen verwaltet und neue ADS-Routen angelegt werden.
- Benutzerverwaltung: Es können neue Benutzer oder Benutzergruppen angelegt werden.

9.2 Remote-Zugriff mit SSH

Wenn Sie einen SSH-Client auf Ihrem Host-PC haben, können Sie diesen für die Verbindung verwenden, da OpenSSH mittlerweile standardmäßig auf allen neueren Betriebssystemen vorhanden ist. Bei den aktuellen Windows 10-Versionen ist dies beispielsweise eine Windows-Funktion, die über PowerShell verwendet werden kann. Benutzen Sie dafür den Befehl `ssh Administrator@<bsd-ip>`.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

Installieren Sie die neueste PowerShell für neue Funktionen und Verbesserungen! https://aka.ms/PSWindows

PS C:\Users\alexejw> ssh Administrator@192.168.178.34
(Administrator@192.168.178.34) Password for Administrator@CX-505918:
Last login: Fri Oct 20 11:59:38 2023 from 192.168.178.37
FreeBSD 13.1-RELEASE n250341-1a7d093d8e5- BHF

The software licenses can be found in this folder: /usr/local/etc/TwinCAT/3.1/System/Legal/
TcOsSys.dll: 4025.12.199
TwinCAT Build: 3.1.4025.3
AMS Net Id: 5.80.89.24.1.1
TC/BSD: 13.1.0.12,2

PLEASE CHANGE STANDARD PASSWORD !!!!
Administrator@CX-505918:~ $
```

Abb. 19: Remote-Zugriff über SSH mit Hilfe der Windows PowerShell.

Sollten Sie Probleme mit dem Aufbau einer Verbindung über SSH haben, können Sie die SSH-Einstellungen bearbeiten und restriktive SSH-Einstellungen auskommentieren (siehe: [SSH-Einstellungen bearbeiten](#) [► 76]).

Zugriff via PuTTY

PuTTY ist eine Open-Source-Software, mit der eine Verbindung über Secure Shell (SSH), Telnet, Remote login oder eine serielle Schnittstelle hergestellt werden kann.

Benutzen Sie PuTTY, um eine SSH-Verbindung unter Windows zu einem Industrie-PC mit TwinCAT/BSD herzustellen. Nach erfolgreicher Verbindung wird eine Konsole gestartet, mit der per Remote-Zugriff Befehle abgesetzt werden können, die anschließend auf dem Industrie-PC ausgeführt werden.

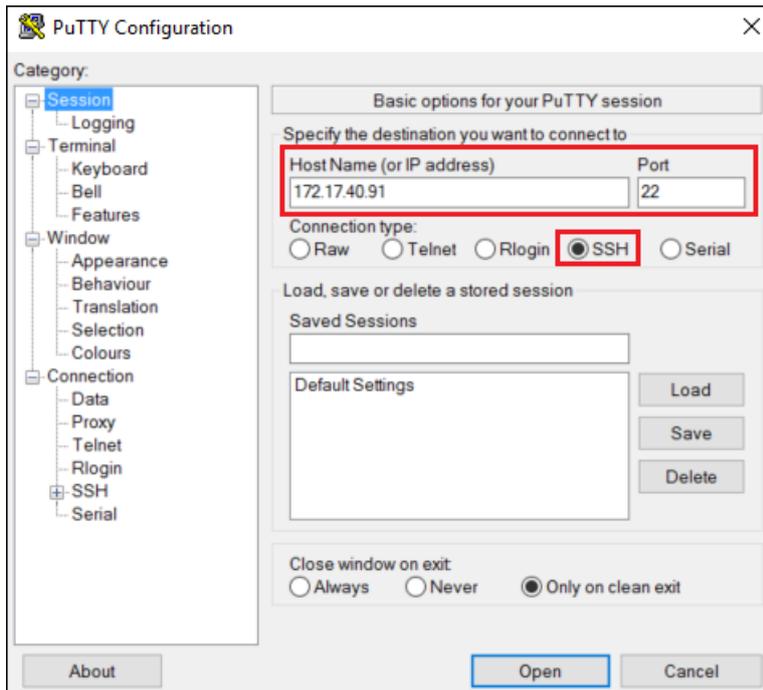
Voraussetzungen:

- PuTTY-Client herunterladen unter: <https://www.putty.org/>
Erforderliche Mindestversion: 0.70
- Der lokale PC (Entwicklungsrechner) und der Industrie-PC (TwinCAT/BSD) müssen mit dem gleichen Netzwerk oder direkt über ein Ethernet-Kabel miteinander verbunden werden.

Starten Sie eine SSH-Verbindung wie folgt:

1. Starten Sie den PuTTY-Client.

2. Geben Sie unter **Host Name (or IP adress)** den Hostnamen oder die IP-Adresse des Industrie-PCs ein.



3. Geben Sie unter **Port** den passenden Port ein. Für SSH ist dies in der Regel der Port 22.
4. Aktivieren Sie unter **Connection type** die Option **SSH** und klicken Sie auf **Open**. Die Konsole wird gestartet.

login as:

5. Geben Sie die Anmeldedaten für TwinCAT/BSD ein. Standard:
Login: Administrator
Passwort: 1

⇒ Sie haben erfolgreich eine SSH-Verbindung mit dem PuTTY-Client zu einem Industrie-PC mit TwinCAT/BSD hergestellt.

9.3 Dateien mit dem WinSCP-Client verwalten

9.3.1 WinSCP-Client starten und einsetzen

WinSCP (Windows Secure Copy) ist eine Open-Source-Software, mit der eine Verbindung über FTP, FTPS, SCP, SFTP, WebDAV oder S3h hergestellt werden kann.

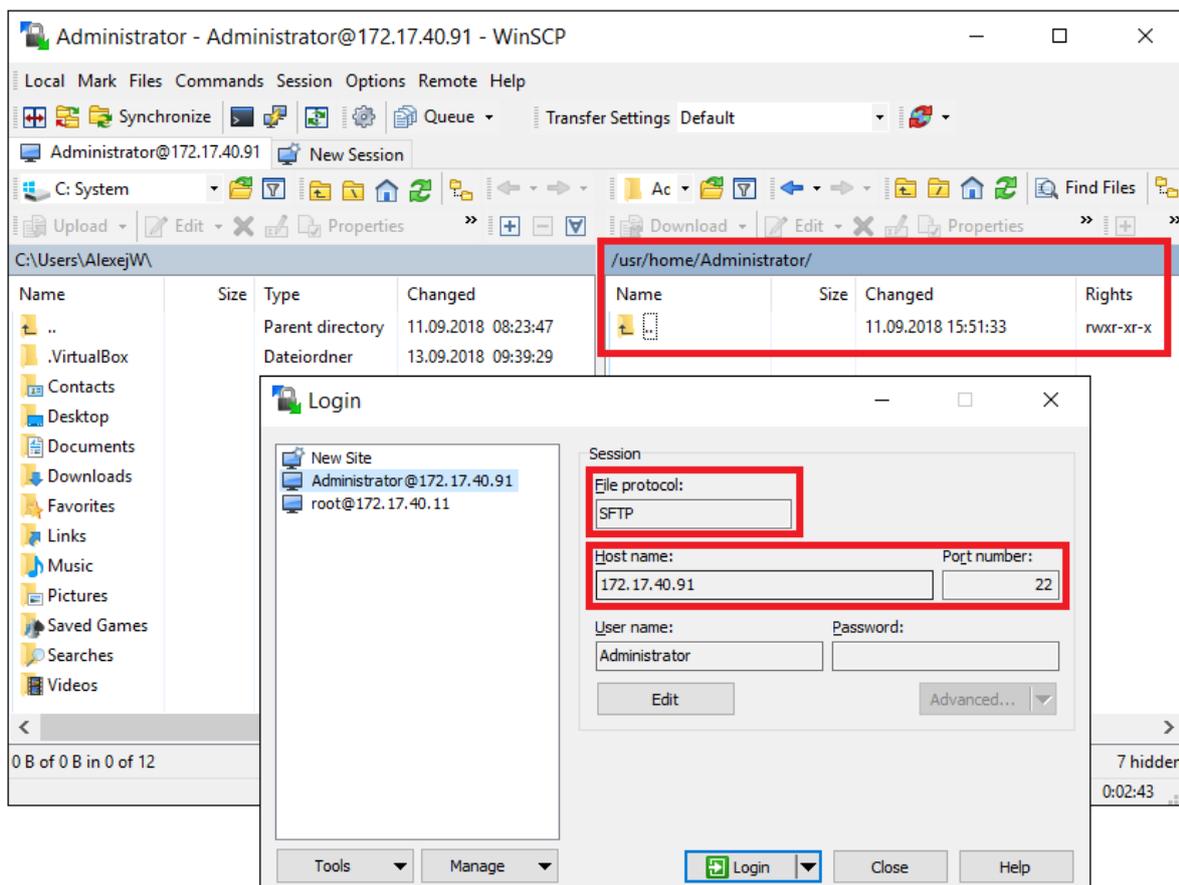
Benutzen Sie WinSCP, um eine SFTP-Verbindung unter Windows zu einem Industrie-PC mit TwinCAT/BSD herzustellen. Nach erfolgreicher Verbindung wird eine grafische Benutzeroberfläche gestartet, mit der ein geschützter Daten- und Dateitransfer zum Industrie-PC mit TwinCAT/BSD möglich ist. Mit WinSCP können Dateien in TwinCAT/BSD–Verzeichnisse kopiert, neue Verzeichnisse erstellt und Dateien editiert werden.

Voraussetzungen:

- WinSCP herunterladen unter: <https://winscp.net/>
Erforderliche Mindestversion: 5.13.2
- Der lokale PC (Entwicklungsrechner) und der Industrie-PC (TwinCAT/BSD) müssen mit dem gleichen Netzwerk oder direkt über ein Ethernet-Kabel miteinander verbunden werden.

Starten Sie eine Verbindung wie folgt:

1. Starten Sie den WinSCP-Client.
Das Login-Fenster erscheint.



2. Wählen Sie unter **File protocol** das SFTP-Protokoll aus.
3. Geben Sie unter **Host Name** und **Port number** die IP-Adresse und die Port-Nummer des Industrie-PCs ein.
4. Geben Sie die Anmeldedaten für TwinCAT/BSD ein und klicken Sie auf **Login**.
⇒ Sie haben erfolgreich eine SFTP-Verbindung zu einem Industrie-PC mit TwinCAT/BSD hergestellt und können geschützt Daten und Dateien zum Industrie-PC übertragen. Auf der rechten Seite der grafischen Benutzeroberfläche werden die TwinCAT/BSD–Verzeichnisse angezeigt.

9.3.2 WinSCP als root

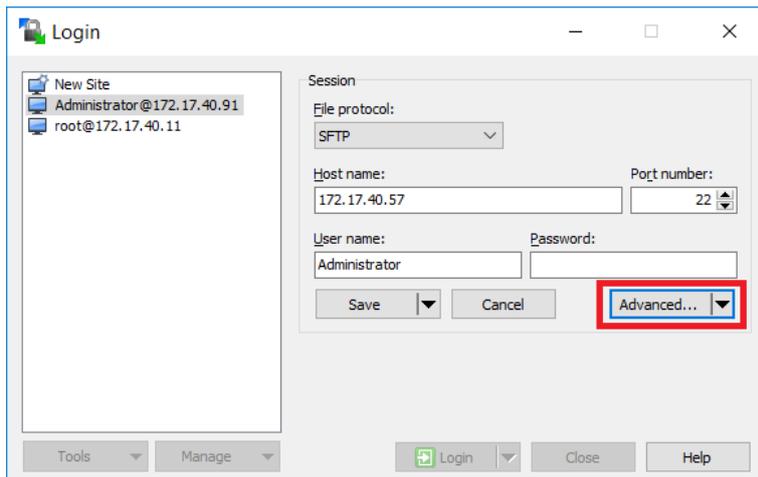
Mit dem Eintrag `doas /usr/libexec/sftp-server` startet WinSCP den SFTP-Server mit Root-Rechten. Dadurch können Sie zusätzliche Einstellungen vornehmen und Konfigurationsdateien anpassen.

Voraussetzungen:

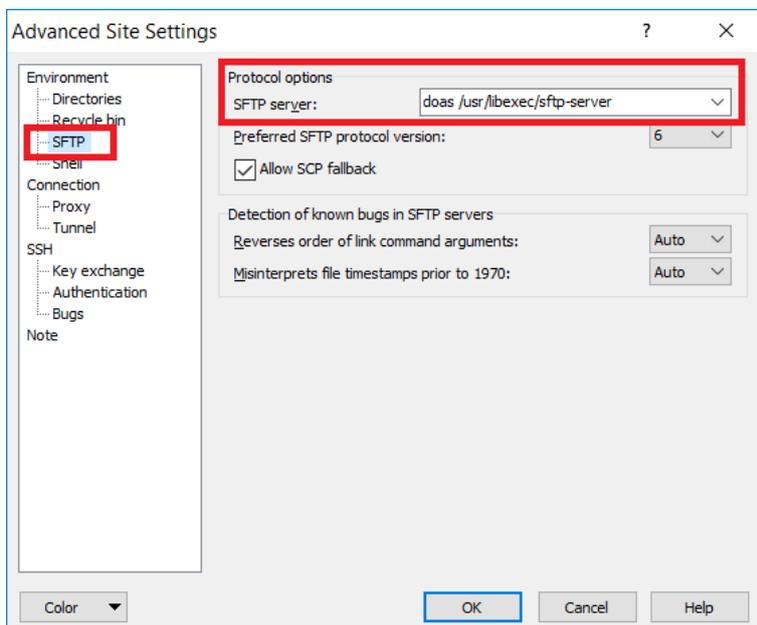
- Installierter WinSCP-Client.

Gehen Sie wie folgt vor:

1. Starten Sie den WinSCP-Client.
Das Login-Fenster erscheint.
2. Klicken Sie auf **Advanced**, um weitere Einstellungen zu öffnen.



3. Klicken Sie links in der Strukturansicht auf **SFTP** und geben unter **SFTP server** den Wert `doas /usr/libexec/sftp-server` ein.



4. Speichern Sie die Einstellungen für das Administrator-Konto.

⇒ Melden Sie sich anschließend mit dem Administrator-Konto an. Sie erhalten nun über WinSCP Zugriff mit Root-Rechten.

9.3.3 Dateien öffnen und editieren

Mit dem WinSCP-Client können Sie mit Hilfe einer grafischen Oberfläche Dateien öffnen und editieren. Beachten Sie, dass nur Dateien editiert werden können, für die Sie die nötigen Zugriffsrechte haben.

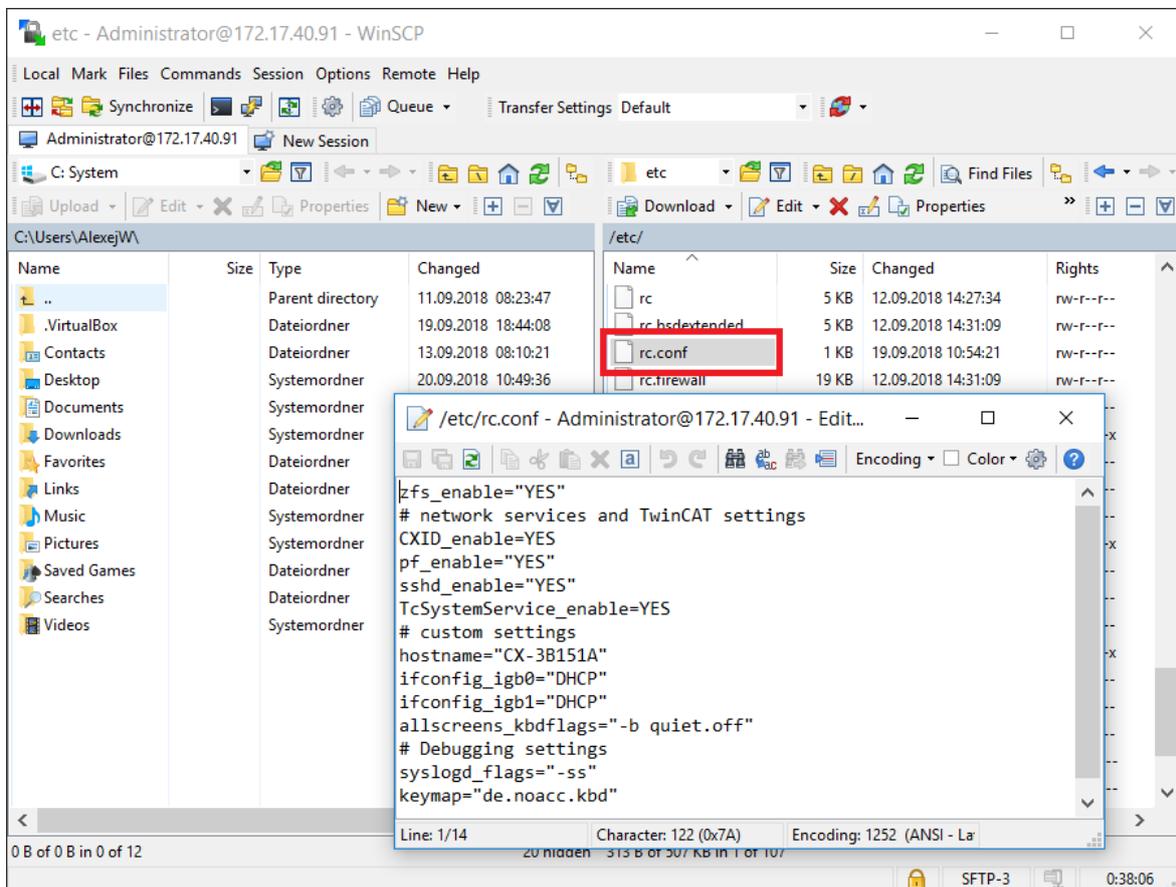
In diesem Arbeitsschritt wird an der Konfigurationsdatei `rc.conf` beispielhaft gezeigt, wie Dateien mit dem WinSCP-Client geöffnet und editiert werden können.

Voraussetzungen:

- WinSCP-Client (siehe: [WinSCP-Client starten und einsetzen \[▶ 73\]](#)).
- Root-Rechte für WinSCP aktivieren (siehe: [WinSCP als root \[▶ 74\]](#)).

Gehen Sie wie folgt vor:

1. Starten Sie den WinSCP-Client.
Das Login-Fenster erscheint.
2. Geben Sie die Anmeldedaten für TwinCAT/BSD ein und klicken Sie auf **Login**.
3. Navigieren Sie in das Verzeichnis `/etc` und klicken Sie doppelt auf die Datei `rc.conf`.
Die Datei wird im WinSCP-Editor geöffnet.



4. Alternativ können Sie auf die Datei rechtsklicken und die Datei mit einem Editor Ihrer Wahl öffnen.
5. Sobald Sie die Änderungen speichern, werden die Änderungen an TwinCAT/BSD übertragen.

⇒ Sie haben erfolgreich eine Datei geöffnet und editiert. Auf diese Weise können Sie alle Dateien mit dem WinSCP-Client verwalten.

9.4 SSH-Einstellungen bearbeiten

SSH ist unter TwinCAT/BSD restriktiv konfiguriert. Es werden aktuelle Verschlüsselungsmethoden verwendet. Sollten Sie Probleme mit dem Aufbau einer Verbindung über SSH haben, können Sie die SSH-Einstellungen bearbeiten und restriktive SSH-Einstellungen auskommentieren.

Beachten Sie, dass damit die restriktiven Einstellungen von Beckhoff für eine sichere Netzwerkverbindung aufgehoben werden. Beckhoff empfiehlt eine andere Software für eine SSH-Verbindung zum TwinCAT/BSD einzusetzen oder die bestehende Software zu aktualisieren.

Voraussetzungen:

- Zugriffsrechte auf die Datei `sshd_config`

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `doas ee /etc/ssh/sshd_config` in der Konsole ein.
Die Datei `sshd_config` wird geöffnet.

2. Kommentieren Sie die folgenden vier Zeilen aus, um restriktive SSH-Einstellungen aufzuheben.

```
#Ciphers chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-  
gcm@openssh.com,aes256-gcm@openssh.com  
#HostKeyAlgorithms ssh-rsa,rsa-sha2-256,rsa-sha2-512,ssh-ed25519  
#KexAlgorithms diffie-hellman-group14-sha256,diffie-hellman-group16-  
group18-sha512,curve25519-sha256,curve25519-sha256@libssh.org  
#MACs hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,umac-128-etm@openssh.com
```

3. Starten Sie den SSH-Server mit dem Befehl `doas service sshd restart` neu, damit die Einstellungen übernommen werden.

⇒ Sie können die restriktiven SSH-Einstellungen jederzeit wiederherstellen, indem Sie die Kommentierung wieder entfernen.

10 TwinCAT/BSD Hypervisor

Der TwinCAT/BSD Hypervisor ermöglicht das Ausführen von virtuellen Maschinen unter TwinCAT/BSD.

Der TwinCAT/BSD Hypervisor basiert auf dem FreeBSD Hypervisor `bhyve(4)`. Durch die Integration von `bhyve` in TwinCAT/BSD wird eine gleichzeitige und effiziente Ausführung von virtuellen Maschinen und TwinCAT SPS- und Motion-Anwendungen auf demselben Industrie-PC ermöglicht.

Diese Dokumentation bietet einen Überblick über verschiedene Features des TwinCAT/BSD Hypervisors.

10.1 Geräte- und Funktionsunterstützung

Die Ausführung von virtuellen Maschinen mit `bhyve(8)` erfordert einen Industrie-PC mit aktueller Intel®- oder AMD™-CPU, die die hardwaregestützte Virtualisierung unterstützen.

Die Tabelle [Geräteunterstützung für TwinCAT/BSD Hypervisor, Device- und GPU-Passthrough](#). [► 77] gibt einen Überblick über aktuelle Industrie-PCs, die die Ausführung von virtuellen Maschinen mit dem TwinCAT/BSD Hypervisor ermöglichen und ob die Features Device-Passthrough oder GPU-Passthrough unterstützt werden. Diese Übersicht ist eine technische Information. Sie lässt keine Rückschlüsse darauf zu, ob es für das jeweilige Gerät Bestelloptionen für vorinstallierte virtuelle Maschinen gibt. Die verfügbaren Bestelloptionen finden Sie in der Preisliste oder auf der Beckhoff-Homepage.

Tab. 7: Geräteunterstützung für TwinCAT/BSD Hypervisor, Device- und GPU-Passthrough.

TwinCAT/BSD Geräte	Hypervisor	Device-Passthrough	GPU-Passthrough
CX51x0	Ja	Nein	Nein
CX52x0	Ja	Ja	Nein
CX20x2	Ja	Ja	Nein
CX20x3	Ja	Ja	Nein
C601x-0010	Ja	Nein	Nein
C601x-0020	Ja	Ja	Nein
C601x-0030	Ja	Ja	Nein
C602x-0000	Ja	Ja	Nein
C602x-0010	Yes	Yes	Yes
C603x-0060	Ja	Ja	Nein
C603x-0070	Ja	Ja	Ja*
C603x-0080	Yes	Yes	Yes
C6040-0090	Yes	Yes	Yes

* BIOS-Version ≥ 0.37 und Aktivierung von Powermanagement (PM-Support) im BIOS erforderlich.

10.2 Virtuelle Maschinen starten und verwalten

Virtuelle Maschinen werden mit den Programmen `bhyve` und `bhyvectl` gestartet und verwaltet. Bevor eine virtuelle Maschine mit `bhyve` gestartet werden kann, muss das Kernelmodul `vmm.ko` geladen werden:

```
doas kldload -n vmm.ko
```

Damit dieser Schritt nicht nach jedem Neustart wiederholt werden muss, kann das Kernelmodul bereits beim Systemstart von TwinCAT/BSD geladen werden, indem `vmm_load="YES"` in der `/boot/loader.conf` gesetzt wird:

```
doas sysrc -f /boot/loader.conf vmm_load="YES"
```

Wenn das Kernelmodul geladen ist, kann eine virtuelle Maschine durch den Aufruf von `bhyve` gestartet werden:

```
bhyve [OPTIONS] <vm_instance>
```

Die Parameter [OPTIONS] bestimmen dabei die Konfiguration der virtuellen Maschine, über die beispielsweise die Anzahl der verwendeten virtuellen CPUs, die Größe des Arbeitsspeichers oder der Speicherort von lokalen Dateien festgelegt werden kann. Der letzte Parameter <vm_instance> des Aufrufs legt den Instanznamen der virtuellen Maschine fest.

VM-Instanz mit einfacher Basiskonfiguration starten

Eine UEFI-basierte virtuelle Maschine mit zwei virtuellen CPUs und 2 GB Arbeitsspeicher kann mit folgendem Befehl gestartet werden:

```
doas bhyve \  
-c sockets=1,cores=2,threads=1 \  
-m 2G \  
-s 0,hostbridge \  
-s 31,lpc \  
-l bootrom,/usr/local/share/uefi-firmware/BHYVE_BHF_UEFI.fd \  
-l com1,stdio \  
-A -H -P \  
samplevm
```

Vereinfacht dargestellt sieht die Basiskonfiguration der VM-Instanz wie folgt aus:

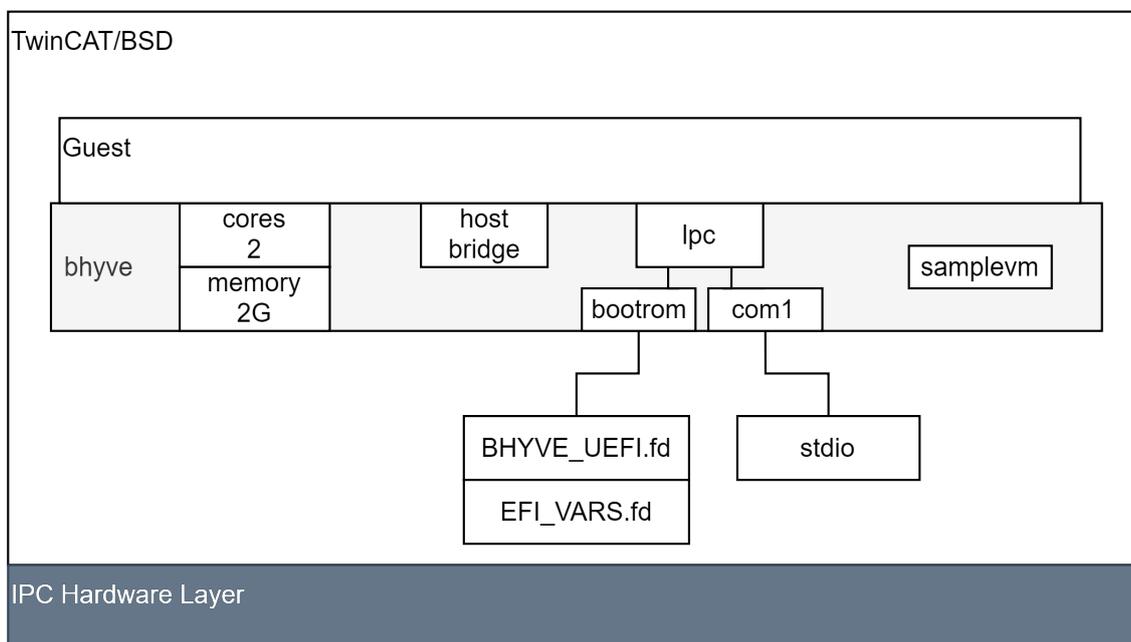


Abb. 20: Basiskonfiguration einer VM-Instanz.

Sobald der Bhyve-Prozess mit den Parametern gestartet wird, steht die virtuelle Maschine mit dem Instanznamen `samplevm` zur Verfügung. Bhyve startet die als `bootrom` hinterlegte UEFI-Firmware. Anschließend wird die UEFI-Shell über die virtuelle Schnittstelle `com1` ausgegeben und durch den Parameter `stdio` an die Standard-Streams des TwinCAT/BSD-Hosts umgeleitet, sodass die UEFI-Shell auf der Kommandozeile angezeigt wird:

```
UEFI Interactive Shell v2.2  
EDK II  
UEFI v2.70 (BHYVE, 0x00010000)  
map: No mapping found.  
Press ESC in 1 seconds to skip startup.nsh or any other key to continue.  
Shell>
```

Durch die Eingabe von `reset -s` in der UEFI-Shell kann die virtuelle Maschine wieder heruntergefahren werden. Der Bhyve-Prozess wird dann mit dem Rückgabewert 1 beendet. Um die virtuelle Maschine erneut zu starten, muss das komplette Bhyve-Kommando mit den gleichen Parametern aufgerufen werden.

Erläuterung der Parameter

Die Bedeutung der einzelnen Parameter kann mit `bhyve -h` abgerufen werden. Detaillierte Beschreibungen der Parameter finden sich im Handbuch zu [bhyve](#). Alternativ kann das Handbuch über die Kommandozeile mit dem Befehl `man bhyve` aufgerufen werden.

Im Folgenden werden die im obigen Beispiel verwendeten Parameter kurz erläutert.

Parameter	Beschreibung
-c sockets=1,cores=2,threads=1	Konfiguration der virtuellen CPU-Topologie. In diesem Beispiel ein CPU-Socket mit zwei Kernen und einem Thread pro Kern.
-m 2G	Der virtuellen Maschine zur Verfügung stehende Arbeitsspeicher. In diesem Beispiel 2 GB.
-s 0,hostbridge	Eine virtuelle Hostbridge, um die virtuelle CPU mit dem virtuellen PCI-Bus zu verbinden. Die Hostbridge sollte per Konvention stets an der PCI-Adresse -s 0:0:0 (kurz -s 0) konfiguriert werden.
-s 31,lcp	LPC/PCI-ISA-Bridge zur Anbindung von emulierten LPC-Geräten. Die LPC/PCI-ISA-Bridge sollte per Konvention stets an der PCI-Adresse -s 0:31:0 konfiguriert werden (kurz -s 31).
-l bootrom,/usr/local/share/uefi-firmware/BHYVE_BHF_UEFI.fd	Ein emuliertes Bootrom am LPC-Bus. Als ROM wird die UEFI-Firmware in der Datei /usr/local/share/uefi-firmware/BHYVE_BHF_UEFI.fd übergeben.
-l com1,stdio	Eine serielle Schnittstelle am LPC-Bus deren Ein- und Ausgaben auf die Standard Input- und Output-Streams von bhyve umgeleitet werden.
-A	Legt bhyve ACPI-Tabellen für die virtuelle Maschine an.
-H	Gibt den virtuellen CPU-Thread frei, wenn eine HLT-Anweisung erkannt wird. Andernfalls werden die virtuellen CPUs 100 % der Host-CPU's nutzen.
-P	Erzwingt die Beendigung der virtuellen Gast-CPU, wenn eine PAUSE-Anweisung erkannt wird.

Parameter beginnend mit `-s` dienen der Konfiguration von virtuellen PCI-Slots denen wiederum emulierte PCI-Geräte zugewiesen werden können (Beispiele siehe: [Erweiterte VM-Konfiguration](#) [► 83]). Parameter beginnend mit `-l` dienen der Konfiguration von emulierten LPC-Geräten hinter der LPC/PCI-ISA-Bridge.

Virtuelle Maschinen verwalten

Gestartete virtuelle Maschinen werden als Bhyve-Prozesse auf dem TwinCAT/BSD-Host aufgelistet. Entsprechend können laufende virtuelle Maschinen mit `ps (1)` aufgelistet werden:

```
ps -a | grep bhyve
7048 0 SC 0:31.06 bhyve: samplevm (bhyve)
7642 0 SC 0:01.83 bhyve: debian11 (bhyve)
```

Laufende virtuelle Maschinen können über den TwinCAT/BSD-Host heruntergefahren oder beendet werden, indem Signale via `kill (1)` an den jeweiligen Bhyve-Prozess gesendet werden. Über das TERM-Signal kann eine ACPI-Shutdown-Anfrage an die virtuelle Maschine gesendet werden, um das Herunterfahren der virtuellen Maschine anzustoßen:

```
doas kill -s TERM $(pgrep -f "bhyve: samplevm")
```

Reagiert die virtuelle Maschine nicht auf ACPI-Shutdown-Anfragen, kann mit dem KILL-Signal der Bhyve-Prozess direkt beendet werden:

```
doas kill -s KILL $(pgrep -f "bhyve: samplevm")
```

Nachdem ein Bhyve-Prozess beendet wurde, kann dessen Rückgabewert (Exit-Code) durch die Shell-Variable `$?` abgefragt werden:

```
echo $?
```

Rückgabewerte größer 1 zeigen an, dass die virtuelle Maschine nicht ordnungsgemäß heruntergefahren werden konnte. Wenn die virtuelle Maschine neu gestartet werden soll oder die Konfiguration einer VM-Instanz zwischen den Aufrufen von `bhyve` geändert wurde, muss die VM-Instanz zunächst mit `bhyvectl` entfernt werden:

```
doas bhyvectl --vm=samplevm --destroy
```

Instanzen von virtuellen Maschinen werden als Gerätedateien unter `/dev/vmm` aufgelistet und können mit `bhyvectl` weiter verwaltet werden. Mit `ls -al /dev/vmm` kann zudem festgestellt werden, welche virtuellen Maschinen aktuell auf dem TwinCAT/BSD-Host angelegt sind:

```
ls /dev/vmm
samplevm
```

10.3 Shell-Skripte einsetzen

Virtuelle Maschinen können mit Hilfe von Shell-Skripten einfach gestartet und verwaltet werden. Durch geskriptete VM-Anwendungen lassen sich Konfigurationen persistent speichern und nach einem Neustart wiederverwendet werden. In Kombination mit weiteren Anweisungen und Shell-Skripten können so beliebige VM-Anwendungen unter TwinCAT/BSD einrichten werden.

Das folgende Beispielskript zeigt den Grundaufbau einer geskripteten VM-Anwendung:

```
# root permissions are required to run VMs
if test "$(id -u)" -ne 0; then
printf "%s must be run as root\n" "${0##*/}"
exit 1
fi

# Default values for VM configuration
vm_name="samplevm"

# Ensure that kernel modul vmm.ko is loaded
kldload -n vmm.ko

while true; do
# destroy former VM instance to ensure we start
# with a clean VM configuration
if test -e "/dev/vmm/${vm_name}"; then
bhyvectl --vm="${vm_name}" --destroy
fi

# start a simple UEFI based VM instance
_bhyve_rc=0
bhyve \
-A -H -P \
-c sockets=1,cores=1,threads=1 \
-m 1G \
-s 0:0,hostbridge \
-l bootrom,/usr/local/share/uefi-firmware/BHYVE_BHF_UEFI.fd \
-l com1,stdio \
-s 31:0,lpc \
"${vm_name}"
_bhyve_rc=$?

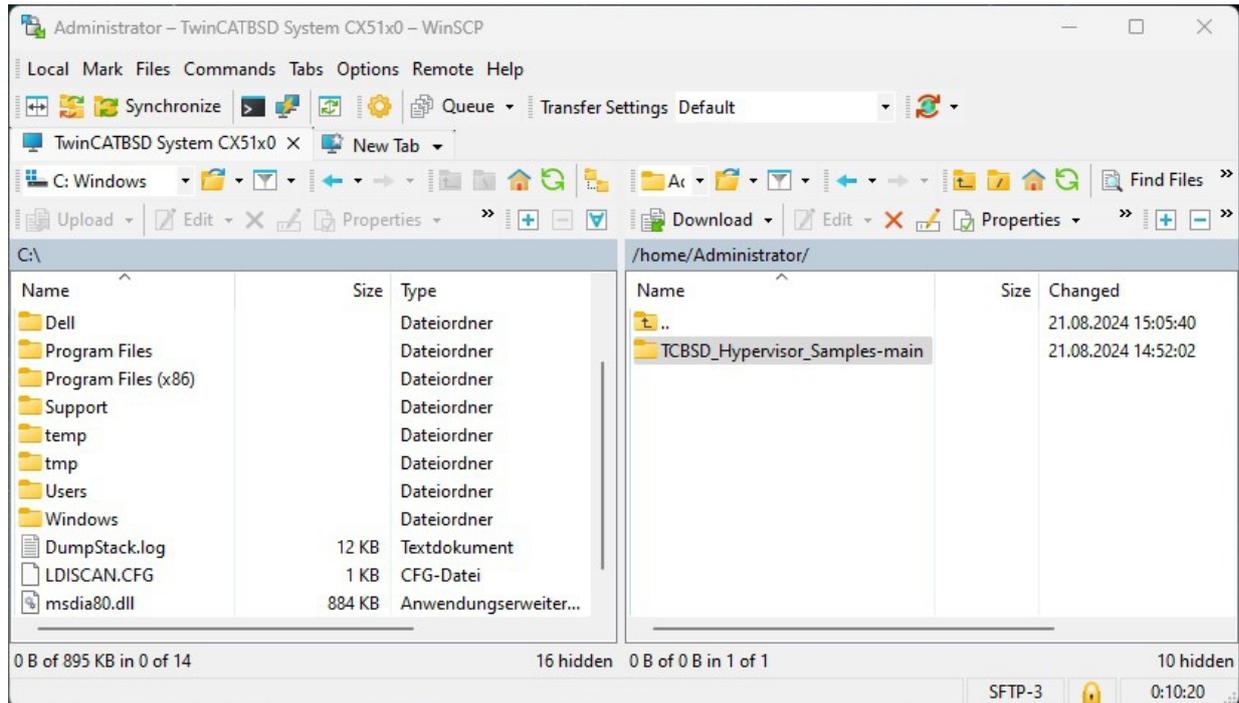
# according to bhyve man pages the return codes indicates
# how the VM was terminated:
# 0: rebooted
# 1: powered off
# ...
# 4: exited due to an error
if test "${_bhyve_rc}" -ne 0; then
printf "bhyve exited with return code: %s\n" "${_bhyve_rc}"
break
fi
printf "Restarting %s\n" "${vm_name}"
done
```

Das Beispielskript kann in einer Textdatei auf dem TwinCAT/BSD-Host gespeichert und ausgeführt werden. Alternativ kann das Beispielskript auf GitHub-Repository unter https://github.com/Beckhoff/TCBSD_Hypervisor_Samples heruntergeladen und auf den TwinCAT/BSD-Host kopiert werden.

Gehen Sie dafür wie folgt vor:

1. Laden Sie sich das Beispielskript unter https://github.com/Beckhoff/TCBSD_Hypervisor_Samples herunter.

- Kopieren Sie den gesamten Ordner auf den TwinCAT/BSD-Host in das Verzeichnis `/home/Administrator` indem Sie beispielsweise das Programm WinSCP verwenden.



- Alternativ können Sie mit dem folgenden Kommando das Beispielskript direkt unter TwinCAT/BSD laden und entpacken:

```
fetch -o /home/Administrator/main.zip \
https://github.com/Beckhoff/TCBSD_Hypervisor_Samples/archive/refs/heads/main.zip \
&& unzip -d /home/Administrator main.zip
```

- Navigieren Sie mit `cd /home/Administrator/TCBSD_Hypervisor_Samples-main/basic_vm_script` in das neue Verzeichnis.
 - Geben Sie den Befehl `doas make` ein, um das Beispielskript `samplevm` zu installieren. Zusätzlich zur Installation werden die Dateiberechtigungen eingestellt und damit das Beispielskript ausführbar gemacht. Ohne den Befehl `doas make` müssen die Dateiberechtigungen manuell eingestellt werden, um das Beispielskript ausführen zu können.
 - Geben Sie abschließend den Befehl `doas samplevm` ein, um das Beispielskript auszuführen.
- ⇒ Die virtuelle Maschine bootet in die UEFI-Shell, die auf der Kommandozeile ausgegeben wird.

```
UEFI Interactive Shell v2.2
EDK II
UEFI v2.70 (BHYVE, 0x00010000)
map: No mapping found.
Press ESC in 1 seconds to skip startup.nsh or any other key to continue.
Shell>
```

Sie können zur Kommandozeile zurückkehren, indem Sie die virtuelle Maschine mit dem Befehl `reset -s` herunterfahren. Um virtuelle Maschinen als Systemservice unter TwinCAT/BSD zu starten, können Shell-Skripte in Kombination mit dem rc-Framework eingesetzt werden und damit virtuelle Maschinen als Systemservice verwaltet oder beim Systemstart automatisch gestartet werden (siehe: [Autostart von Shell-Skripten](#) [▶ 82]).

10.4 Autostart von Shell-Skripten

Um eine virtuelle Maschine als Systemservice zu verwalten oder beim Systemstart automatisch zu starten, kann der Aufruf von `bhyve` oder ein Shell-Skript in das `rc`-Framework eingebunden werden.

Das GitHub-Repository: https://github.com/Beckhoff/TCBSD_Hypervisor_Samples/tree/main/vm_autostart umfasst Beispieldateien, die aufzeigen, wie eine einfache VM-Konfiguration mit Hilfe von Shell-Skripten in das `rc`-Framework eingebunden werden kann. Das Beispiel im Verzeichnis `vm_autostart` enthält dafür die entsprechenden Dateien.

Wenn das Beispielskript wie in Kapitel [Shell-Skripte einsetzen \[► 80\]](#) beschrieben, auf den TwinCAT/BSD-Host geladen wurde, kann mit `cd /home/Administrator/TCBSD_Hypervisor_Samples-main/vm_autostart` in das Verzeichnis gewechselt werden.

```
vm_autostart
├── Makefile
├── rc.d
│   └── samplevm
└── samplevm
```

Das im Kapitel [Shell-Skripte einsetzen \[► 80\]](#) aufgezeigte Beispielskript `samplevm` ist um `start`, `stop` und `status` Parameter erweitert worden, um eine VM-Konfiguration mit VNC-Zugriff über die Kommandozeile starten und stoppen zu können.

Über das `vm_autostart/rc.d/samplevm` Shell-Skript wird das `vm_autostart/samplevm` Shell-Skript in das `rc`-Framework eingebunden.

Steuerung des VM-Systemservice mit dem Beispielskript:

1. Navigieren Sie in das Verzeichnis mit `cd /home/Administrator/TCBSD_Hypervisor_Samples-main/vm_autostart`
 2. Geben Sie den Befehl `doas make` ein, um beide Dateien aus dem `vm_autostart` Verzeichnis auf dem TwinCAT/BSD-Host zu installieren.
 3. Geben Sie anschließend `doas service samplevm enable` ein, um die VM-Instanz über `service(8)` als Systemservice für den Autostart zu aktivieren.
 4. Nach der Einbindung des Shell-Skripts als Systemservice, kann die virtuelle Maschine mit dem Befehl `doas service samplevm start` gestartet werden.
 5. Der Befehl `doas service samplevm status` gibt aus, ob die virtuelle Maschine wieder gestartet wurde und mit welcher Prozess ID sie ausgeführt wird.
- ⇒ In diesem Beispiel kann auf die virtuelle Maschine über einen VNC-Client via TCP-Port "5900" zugegriffen werden. Ab sofort wird die virtuelle Maschine auch nach einem Neustart des TwinCAT/BSD-Hosts wieder gestartet und ist für die Nutzung verfügbar.
1. Mit dem Befehl `doas service samplevm stop` kann die virtuelle Maschine wieder gestoppt werden.
 2. Mit dem Befehl `doas service samplevm disable` wird der Autostart der VM wieder deaktiviert.

Das Beispielskript ist eine erste Ausgangsbasis, auf der aufgebaut werden kann und veranschaulicht, wie virtuelle Maschinen unter TwinCAT/BSD gestartet, verwaltet und automatisiert werden können. Das Beispielskript `vm_autostart/samplevm` kann je nach Bedarf angepasst und erweitert werden, um eine gewünschte VM-Konfiguration zu erreichen. Das Kapitel [Erweiterte VM-Konfiguration \[► 83\]](#) erläutert weitere Parameter, die verwendet werden können, um die Konfiguration einer virtuellen Maschine auszuweiten.

Detaillierte Informationen zum Erstellen von `rc.d`-Skripten finden sich im FreeBSD-Handbuch im Kapitel [Practical rc.d scripting in BSD](#).

10.5 Erweiterte VM-Konfiguration

10.5.1 ZFS-Datasets als Speicherort für virtuelle Maschinen

Das Verwenden von ZFS-Datasets bieten die Möglichkeit, Funktionen und Eigenschaften von ZFS wie Quotas, Komprimierung, Blockgrößen oder Snapshots für VM-Anwendungen zu nutzen.

Der folgende Aufruf erstellt ein Dateisystem als Speicherort für die virtuelle Maschine `samplevm` und mounted das Dateisystem in der Verzeichnisstruktur unter `/vms/samplevm`:

```
doas zfs create -o mountpoint=/vms/samplevm zroot/samplevm
```

Das Dateisystem kann nun verwendet werden, um Dateien für virtuelle Laufwerke, EFI-Variablen oder andere VM-bezogene Daten zu sichern.

Sicherungspunkte von virtuellen Festplatten via ZFS-Snapshots

ZFS Snapshots können auf ZFS-Datasets angewendet werden, um Sicherungspunkte von virtuellen Maschinen zu erstellen (siehe auch: [ZFS-Volumes als Datenspeicher für virtuelle Festplatten \[► 87\]](#)). Der Zustand einer virtuellen Maschine kann so zu einem bestimmten Zeitpunkt gesichert und bei Bedarf wiederhergestellt werden.

Ein Snapshot des ZFS-Dataset `zroot/samplevm` kann via [zfs-snapshot\(8\)](#) angelegt werden:

```
doas zfs snapshot zroot/samplevm@latest
```

`@latest` definiert den Namen des Snapshots.

Um das ZFS-Dataset und die darin gespeicherten Dateien auf den Zustand des Snapshots `@latest` zurückzuspielen, kann folgender Befehl verwendet werden

```
doas zfs rollback zroot/samplevm@latest
```

Während des Erstellens und Zurückspielens sollte die VM-Instanz heruntergefahren sein.

Ausführlichere Informationen zum Z-Dateisystem und zur Verwendung von ZFS-Datasets und Snapshots finden sich im Kapitel [Das Z-Dateisystem der FreeBSD Dokumentation](#)

10.5.2 UEFI-basierte virtuelle Maschinen

UEFI-basierte virtuelle Maschinen können durch die Parameter `-l, bootrom, <efi-rom>[, <efi-vars>]` gestartet werden. Für `<efi-rom>` muss der Pfad zu einer EFI-ROM-Datei angegeben werden. Optional kann an der Stelle `<efi-vars>` der Pfad zu einer Datei angegeben werden, die wiederum als Speicherort für EFI-Variablen der virtuellen Maschine dient.

Dateien mit EFI-Variablen sollten pro VM-Instanz angelegt werden. Der folgende Befehl erstellt eine Kopie der Datei `BHYVE_BHF_UEFI_VARS.fd`, die für die VM-Instanz `samplevm` genutzt werden soll.

```
doas cp /usr/local/share/uefi-firmware/BHYVE_BHF_UEFI_VARS.fd /vms/samplevm/EFI_VARS.fd
```

Die Datei `EFI_VARS.fd` wird anschließend als `<efi-vars>` Parameter dem `bhyve` Aufruf übergeben.

Zusätzlich sollte der Parameter `fwcfg=qemu` angehängen werden. Dadurch wird es der Firmware ermöglicht, auf die dynamisch erzeugten ACPI-Tabellen von `bhyve` zuzugreifen.

```
doas bhyve \
-c sockets=1,cores=1,threads=1 \
-m 2G \
-l bootrom,/usr/local/share/uefi-firmware/BHYVE_BHF_UEFI.fd,/vms/samplevm/EFI_VARS.fd,fwcfg=qemu \
-l com1,stdio \
-s 0:0,hostbridge \
-s 31:0,lpc \
-A -H -P \
samplevm
```

10.5.3 VNC-basierte Interaktion mit virtuellen Maschinen

HINWEIS

Ungesicherter TCP-Port

Eingehende Verbindungen auf TCP-Port 5900 werden in diesem Beispiel nicht durch die Firewall blockiert. Richten Sie eine sichere und verschlüsselte Verbindung ein und sichern Sie den TCP-Port 5900 über SSH, sobald der Betrieb in einem ungesicherten Netzwerk stattfindet.

Mit Virtual Network Computing (VNC) besteht die Möglichkeit eine virtuelle Maschine auf einem TwinCAT/BSD-Host über eine Netzwerkverbindung zu steuern. Dafür stellt `bhyve` einen integrierten VNC-Server bereit, um mit VM-Instanzen zu interagieren.

Grafische Ausgaben der virtuellen Maschine und Benutzereingaben an die virtuelle Maschine können über den integrierten VNC-Server übertragen werden, indem die virtuelle Maschine mit einem Frame-Buffer-Gerät `fbuf` konfiguriert wird. Dem Frame-Buffer-Gerät `fbuf` können folgende Optionen übergeben werden, um den VNC-Server zu konfigurieren:

```
fbuf, [rfb=ip-and-port] [,w=width] [,h=height] [,vga=vgaconf] [,wait] [,password=password]
```

Der folgende Aufruf startet die virtuelle Maschine `samplevm` mit einem Frame-Buffer-Gerät an PCI-Slot 2. Über die Konfigurationsoptionen wird festgelegt, dass der VNC-Server auf TCP-Port 5900 des TwinCAT/BSD-Hosts auf Verbindungen lauscht. Zudem wird die Bildauflösung des Frame-Buffers auf 1024x768 Pixel festgelegt. Weitere Konfigurationsoptionen des `fbuf` Geräts finden sich in den [bhyve Manpages](#)

```
doas bhyve \
-c sockets=1,cores=1,threads=1 \
-m 2G \
-l bootrom,/usr/local/share/uefi-firmware/BHYVE_BHF_UEFI.fd,fwcfg=qemu \
-s 0,hostbridge \
-s 2,fbuf,rfb=0.0.0.0:5900,w=1024,h=768 \
-s 31,lpc \
-A -H -P \
samplevm
```

Abhängig vom VNC-Client kann es vorkommen, dass Mauszeigerpositionen nicht präzise übergeben werden. Der `bhyve`-Aufruf kann dann um eine `xhci,tablet` Gerätekonfiguration erweitert werden.

```
doas bhyve \
-c sockets=1,cores=1,threads=1 \
-m 2G \
-l bootrom,/usr/local/share/uefi-firmware/BHYVE_BHF_UEFI.fd,fwcfg=qemu \
-s 0,hostbridge \
-s 2,fbuf,rfb=0.0.0.0:5900,w=1024,h=768 \
-s 3,xhci,tablet \
-s 31,lpc \
-A -H -P \
samplevm
```

Der integrierte VNC-Server unterstützt keine Transportschichtssicherheit. Eingehende TCP-Verbindungen auf Port 5900 werden standardmäßig vom TwinCAT/BSD-Paket-Filter `pf(8)` blockiert. Eingehende Verbindungen können durch die Konfiguration des Paket-Filters erlaubt werden (siehe: [Firewall](#)).

10.5.4 Virtuelle Laufwerke

Virtuelle Maschinen können mit virtuellen Laufwerken (Block-Storage-Devices) konfiguriert werden. Diese können wiederum als virtuelle Festplatten (nvme, ahci-hd oder virtio-blk) oder als virtuelle CD-ROM-Laufwerk (ahci-cd) verwendet werden.

Der folgende Aufruf startet die virtuelle Maschine `samplevm` mit einem emulierten NVMe-Laufwerk und einem virtuellen AHCI-CD-ROM-Laufwerk:

```
doas bhyve \  
-c sockets=1,cores=2,threads=1 \  
-m 2G \  
-l bootrom,/vms/samplevm/BHYVE_BHF_UEFI.fd,/vms/samplevm/EFI_VARS.fd,fwcfg=qemu \  
-s 0,hostbridge \  
-s 2,fbuf,rfb=0.0.0.0:5900,w=1024,h=768 \  
-s 3,xhci,tablet \  
-s 10,nvme,/vms/samplevm/disk0.img \  
-s 15,ahci-cd,/vms/samplevm/os-installer.iso,ro \  
-s 31,lpc \  
-H -P -A \  
samplevm
```

Die resultierende VM-Konfiguration sieht wie folgt aus:

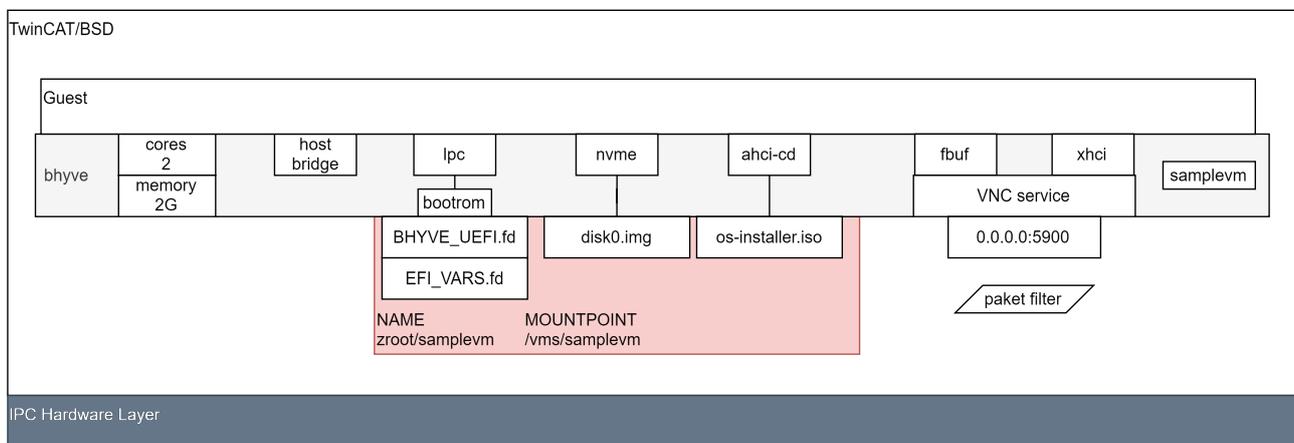


Abb. 21: VM-Instanz mit virtuellen Laufwerken.

Beide Laufwerke nutzen als Datenspeicher reguläre Dateien als Disk-Image bzw. ISO-CDROM auf dem TwinCAT/BSD-Host. Beide Dateien müssen vor dem Aufruf von `bhyve` existieren. Alternativ können auch Block-Geräte wie ZFS-Volumes als Datenspeicher übergeben werden (siehe: [ZFS-Volumes als Datenspeicher für virtuelle Festplatten](#) [► 87]).

Um Gastbetriebssystemen die konfigurierten Laufwerke über ACPI bekannt zu machen, muss zusätzlich der Parameter `-A` übergeben werden.

In dem Beispiel oben, wird die Disk-Image-Datei `/vms/samplevm/disk0.img` als Datenspeicher für die virtuelle Festplatte genutzt (siehe: [Disk-Image Dateien als Datenspeicher für virtuelle Festplatten](#) [► 86]).

Auf die Datei `/vms/samplevm/os-installer.iso` wird nur lesend zugegriffen. Entspricht das Speicherabbild von `os-installer.iso` einem bootfähigem ISO-Abbild kann so z.B. die Installation eines Betriebssystems innerhalb der virtuellen Maschine gestartet werden (siehe: [Debian Linux als Gastbetriebssystem installieren](#) [► 97]).

Beide Dateien sind in diesem Beispiel im Verzeichnis `/vms/samplevm` gespeichert, das zum zuvor erstellten ZFS-Datensatz `zroot/samplevm` gehört. Das ZFS-Datensatz dient somit als Speicherort für die persistenten Daten der virtuellen Maschine. Somit können ZFS-Snapshots zum Sichern und Wiederherstellen der Daten genutzt werden.

10.5.4.1 Disk-Image Dateien als Datenspeicher für virtuelle Festplatten

Disk-Image Dateien sind reguläre Dateien, in denen der Inhalt von virtuellen Festplatten abgespeichert werden kann. Eine leere Disk-Image Datei, die maximal 20 GB umfasst, kann mit Hilfe von `truncate(1)` wie folgt angelegt werden:

```
truncate -s 20G /vms/samplevm/disk0.img
```

Die erstellte `disk0.img` Datei kann anschließend als Backend für eine virtuelle Festplatte dem `bhyve` Aufruf übergeben werden:

```
doas bhyve \
-c sockets=1,cores=2,threads=1 \
-m 2G \
-l bootrom,/usr/local/share/uefi-firmware/BHYVE_BHF_UEFI.fd \
-s 0,hostbridge \
-s 10,nvme,/vms/samplevm/disk0.img \
-s 31,lpc \
-H -P -A \
samplevm
```

10.5.4.2 Verwendung von Installationsmedien (ISO-Images)

Installationsprogramme für Betriebssysteme werden oft als ISO-Abbilder über Webseiten zum Download bereitgestellt. Unter TwinCAT/BSD kann `fetch(8)` verwendet werden, um ein ISO-Abbild von einer Website herunter zu laden.

Der folgende Aufruf lädt das Debian-ISO-Abbild `debian-11.5.0-amd64-netinst.iso` von der Webseite cdimage.debian.org und speichert es lokal in der Datei `os-installer.iso`.

```
fetch -o os-installer.iso https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/debian-11.5.0-amd64-netinst.iso
```

Die heruntergeladene ISO-Datei kann dann wiederum als Medium in einem virtuellen CD-ROM Laufwerk (`ahci-cd`) einer virtuellen Maschine genutzt werden.

```
doas bhyve \
-c sockets=1,cores=1,threads=1 \
-m 2G \
-l bootrom,/usr/local/share/uefi-firmware/BHYVE_BHF_UEFI.fd \
-s 0,hostbridge \
-s 2,fbuf,rfb=0.0.0.0:5900,w=1024,h=768 \
-s 3,xhci,tablet \
-s 15,ahci-cd,/usr/home/Administrator/os-installer.iso,ro \
-s 31,lpc \
-A -H -P \
samplevm
```

10.5.4.3 ZFS-Volumes als Datenspeicher für virtuelle Festplatten

ZFS-Volumes sind ein Typ von ZFS-Datasets und werden als Block-Geräte unter `/dev/zvol/zroot` gelistet. Ein ZFS-Volume kann als Datenspeicher für virtuelle Laufwerke genutzt werden, um so die Vorteile von ZFS-Datasets wie Snapshots, Klone oder Komprimierung zu nutzen.

Über den folgenden Befehl wird das ZFS-Volume `zroot/vms/samplevm/disk0` im ZFS-Pool `zroot` mit 20GB angelegt

```
doas zfs create -V 20G zroot/vms/samplevm/disk0
```

Der folgende Aufruf startet die virtuelle Maschine `samplevm` mit einer emulierten NVME-Festplatte die als Datenspeicher das ZFS-Volume `zroot/vms/samplevm/disk0` nutzt, welches unter dem Verzeichnis `/dev/zvol/zroot/vms/samplevm/disk0` zur Verfügung steht.

```
doas bhyve \
-c sockets=1,cores=1,threads=1 \
-m 2G \
-l bootrom,/usr/local/share/uefi-firmware/BHYVE_BHF_UEFI.fd \
-s 0,hostbridge \
-s 2,fbuf,rfb=0.0.0.0:5900,w=1024,h=768 \
-s 3,xhci,tablet \
-s 10,nvme,/dev/zvol/zroot/vms/samplevm/disk0 \
-s 31,lpc \
-A -H -P \
samplevm
```

10.5.5 Netzwerkkonfiguration von virtuellen Maschinen

Virtuelle Maschinen können mit virtuellen Netzwerkcontrollern konfiguriert werden, um so die virtuelle Maschine mit einem Netzwerk zu verbinden. Virtuelle Maschinen nutzen dafür [tap\(4\)](#) oder [vmnet\(4\)](#) Netzwerkschnittstellen des TwinCAT/BSD-Hosts, die wiederum unter TwinCAT/BSD mit Hilfe von [ifconfig\(8\)](#) verwaltet werden.

Der folgende Befehl erstellt ein neue `vmnet(4)` Instanz:

```
doas ifconfig vmnet create
```

```
vmnet0
```

Auf ähnliche Weise können `tap(4)` Instanzen erstellt werden

```
doas ifconfig tap create
```

```
tap0
```

`tap(4)` und `vmnet(4)` Netzwerkschnittstellen können über `cloned_interfaces` bereits beim Systemstart angelegt werden. Dazu können die Instanzen der `cloned_interfaces` Auflistung in der `rc`-Konfiguration hinzugefügt werden:

```
doas sysrc cloned_interfaces+="vmnet0 tap0"
```

Die erstellten `vmnet(4)` oder `tap(4)` Instanzen (in diesem Fall `vmnet0` und `tap0`) können anschließend als Ethernet-Endpunkt für eine virtuelle Maschine verwendet werden, um zwischen TwinCAT/BSD-Host und der virtuellen Maschinenumgebung Ethernet-Pakete auszutauschen.

Dafür wird der `bhyve` Aufruf um ein oder mehrere emulierte `virtio-net` Gerät gestartet, welche als Endpunkt die zuvor erstellten Netzwerkschnittstellen nutzen. Für jede Netzwerkschnittstelle der virtuellen Maschine wird eine MAC-Adresse generiert. Optional kann jeder Netzwerkschnittstelle auch eine definierte MAC-Adresse mit `,mac=xx:xx:xx:xx:xx:xx` übergeben werden.

Der folgende Befehl startet eine virtuelle Maschine mit zwei virtuellen Netzwerkcontrollern, die als Endpunkte auf Host-Seite die oben genannten Instanzen `vmnet0` und `tap0` an PCI-Slot `-s 20` und `-s 21` nutzen und definierte MAC-Adressen erhalten:

```
doas bhyve \
-c sockets=1,cores=1,threads=1 \
-m 2G \
-l bootrom,/usr/local/share/uefi-firmware/BHYVE_BHF_UEFI.fd,fwcfg=qemu \
-s 0,hostbridge \
-s 2,fbuf,rfb=0.0.0.0:5900,w=1024,h=768 \
-s 3,xhci,tablet \
-s 20,virtio-net,vmnet0,mac=58:9c:fc:02:34:25 \
-s 21,virtio-net,tap0,mac=58:9c:fc:03:5e:ec \
```

```
-s 31,lpc \
-A -H -P \
samplevm
```

Die Anbindung von virtuellen Maschinen an externe Netzwerke erfolgt somit immer über `tap(4)` oder `vmnet(4)` Geräte.

Die Konfiguration mit virtuellen Netzwerkcontrollern sieht wie folgt aus:

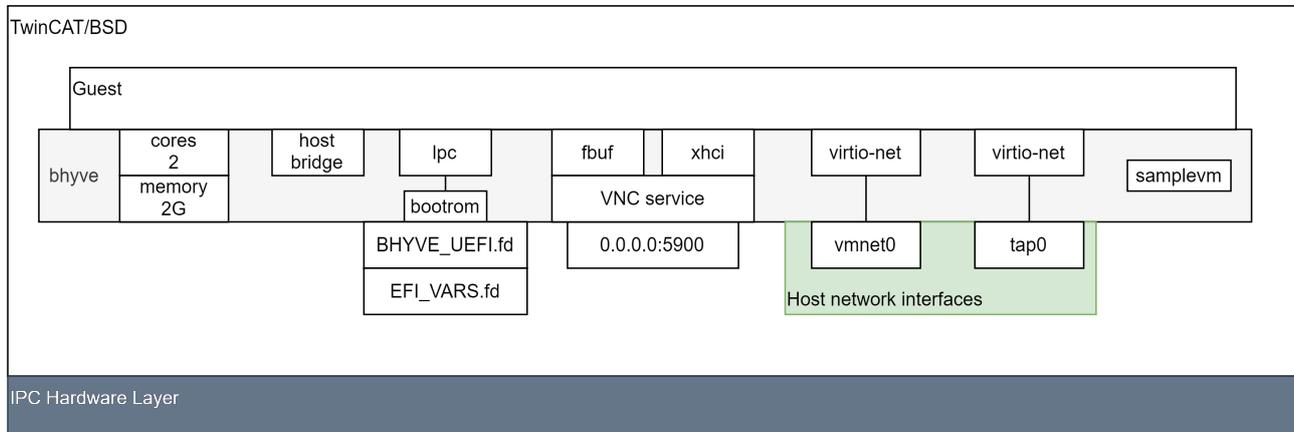


Abb. 22: Konfiguration einer VM-Instanz mit virtuellen Netzwerkcontrollern.

Je nach Anwendungsfall kann eine virtuelle Maschine auch mit weiteren Netzwerkcontrollern konfiguriert werden, um an unterschiedlichen Netzwerken angebunden zu werden. Die Anbindung einer virtuellen Maschine an ein Netzwerk wird anschließend über die Konfiguration der jeweiligen `tap(4)` oder `vmnet(4)` Geräte auf dem TwinCAT/BSD-Host bestimmt. Dadurch ergeben sich unterschiedliche Möglichkeiten die Kommunikation von virtuellen Maschinen in ein Netzwerk zu realisieren:

1. [Host-Only-Netzwerk \[► 89\]](#)
2. [NAT-Netzwerk \[► 92\]](#)
3. [Bridge-Netzwerk \[► 90\]](#)
4. [Ethernet-Device-Passthrough \[► 94\]](#)

10.5.5.1 Host-Only-Netzwerk

In einer Host-Only-Netzwerkkonfiguration werden Netzwerkpakete lediglich zwischen virtueller Maschine und TwinCAT/BSD-Host ausgetauscht. Hierfür wird auf dem TwinCAT/BSD-Host eine `vmnet(4)` Schnittstelle angelegt. Die `vmnet(4)` Instanz dient als Backend für einen emulierten Ethernet-Controller vom Typ `virtio-net` oder `e1000` der virtuellen Maschine. Innerhalb des Gastsystems wird der Ethernet-Controller als Netzwerkschnittstelle erkannt. Die IP-Adressen der Host- und Gast-Netzwerkschnittstellen werden anschließend so konfiguriert, dass sich ein Host-Only Netzwerk ergibt.

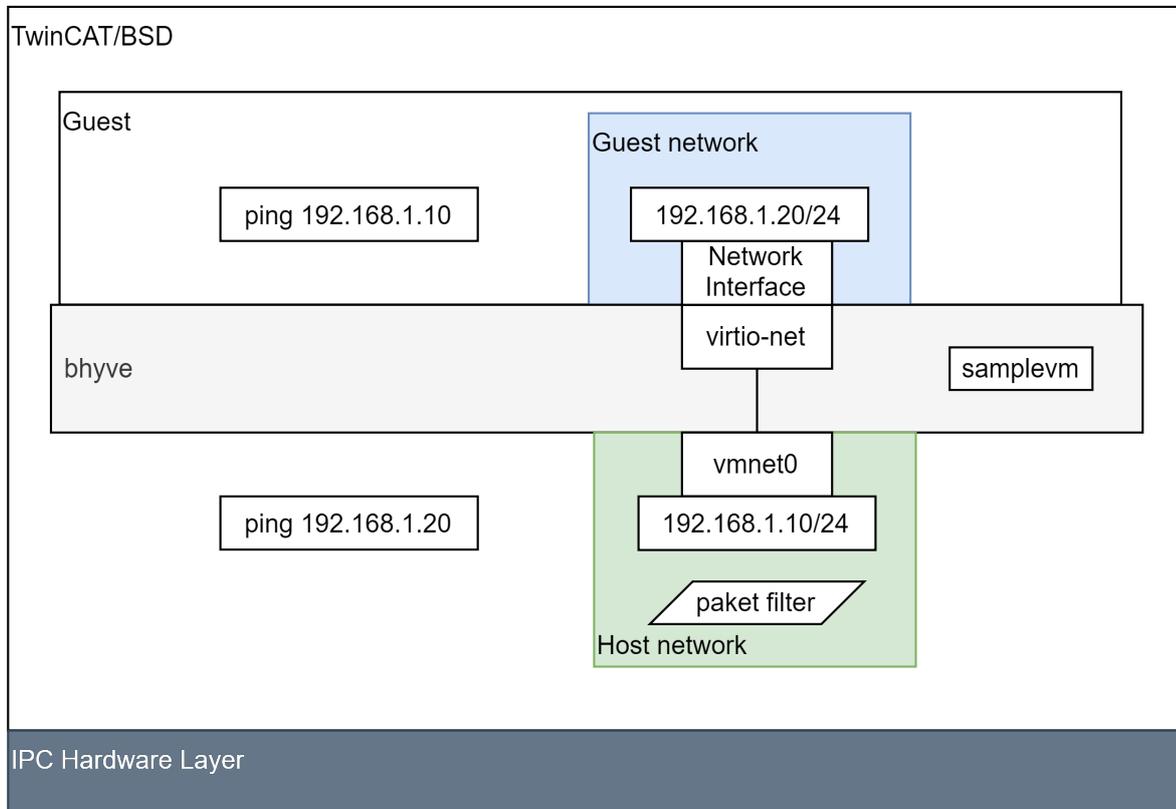


Abb. 23: VM-Instanz mit einer Host-Only-Netzwerkkonfiguration.

Zum Konfigurieren eines Host-Only-Netzwerks wird auf dem TwinCAT/BSD-Host mit `ifconfig` eine `vmnet(4)` Schnittstelle angelegt und dieser Netzwerkschnittstelle eine private IP-Adresse zugewiesen.

```
doas ifconfig vmnet create inet 192.168.1.10 netmask 255.255.255.0
```

Damit die `vmnet`-Instanz bereits beim Systemstart angelegt wird, kann diese in der `rc`-Konfiguration hinterlegt werden:

```
doas sysrc cloned_interfaces+="vmnet0"
doas sysrc ifconfig_vmnet0="inet 192.168.1.10 netmask 255.255.255.0"
```

Der virtuellen Maschine wird das `vmnet(4)`-Gerät anschließend als Backend für einen virtuellen Netzwerk-Controller vom Typ `virtio-net` übergeben (vgl. Abbildung oben).

Innerhalb des Gastsystems wird das virtuelle Netzwerkinterface so konfiguriert, dass es sich im gleichen IP-Netzwerk wie das `vmnet0` Interface des TwinCAT/BSD-Hosts befindet (Beispiel oben: 192.168.1.0/24). Anschließend kann die Host-Only-Kommunikation mit `ping`-Anfragen zwischen TwinCAT/BSD-Host und Gastsystem überprüft werden.

Der folgende Aufruf startet die virtuelle Maschine `samplevm` mit einem `virtio-net`-basierten Netzwerkcontroller an PCI-Adresse 20. Als Backend wird die zuvor konfigurierte `vmnet0` Instanz übergeben.

```
doas bhyve \
-c sockets=1,cores=1,threads=1 \
-m 2G \
-l bootrom,/usr/local/share/uefi-firmware/BHYVE_BHF_UEFI.fd,fwcfg=qemu \
-s 0,hostbridge \
-s 20,virtio-net,vmnet0 \
```

```
-s 31,lpc \
-A -H -P \
samplevm
```

10.5.5.2 Bridge-Netzwerk

HINWEIS

Verbindungsabbruch und eingeschränkte Verfügbarkeit im Netzwerk

Änderungen an den Filterregeln haben Einfluss auf die Verfügbarkeit des TwinCAT/BSD-Hosts, der virtuellen Maschine sowie deren Dienste im Netzwerk.

In einem Bridge-Netzwerk wird eine physische Netzwerkschnittstelle des TwinCAT/BSD-Hosts (z.B. `igb0`) über ein `bridge(4)` Gerät mit einem `tap(4)` Gerät verbunden. Das `tap(4)` Gerät dient wiederum als Backend für ein virtuelles Netzwerkinterface der virtuellen Maschine (siehe: [Netzwerkconfiguration von virtuellen Maschinen](#) [▶ 87]).

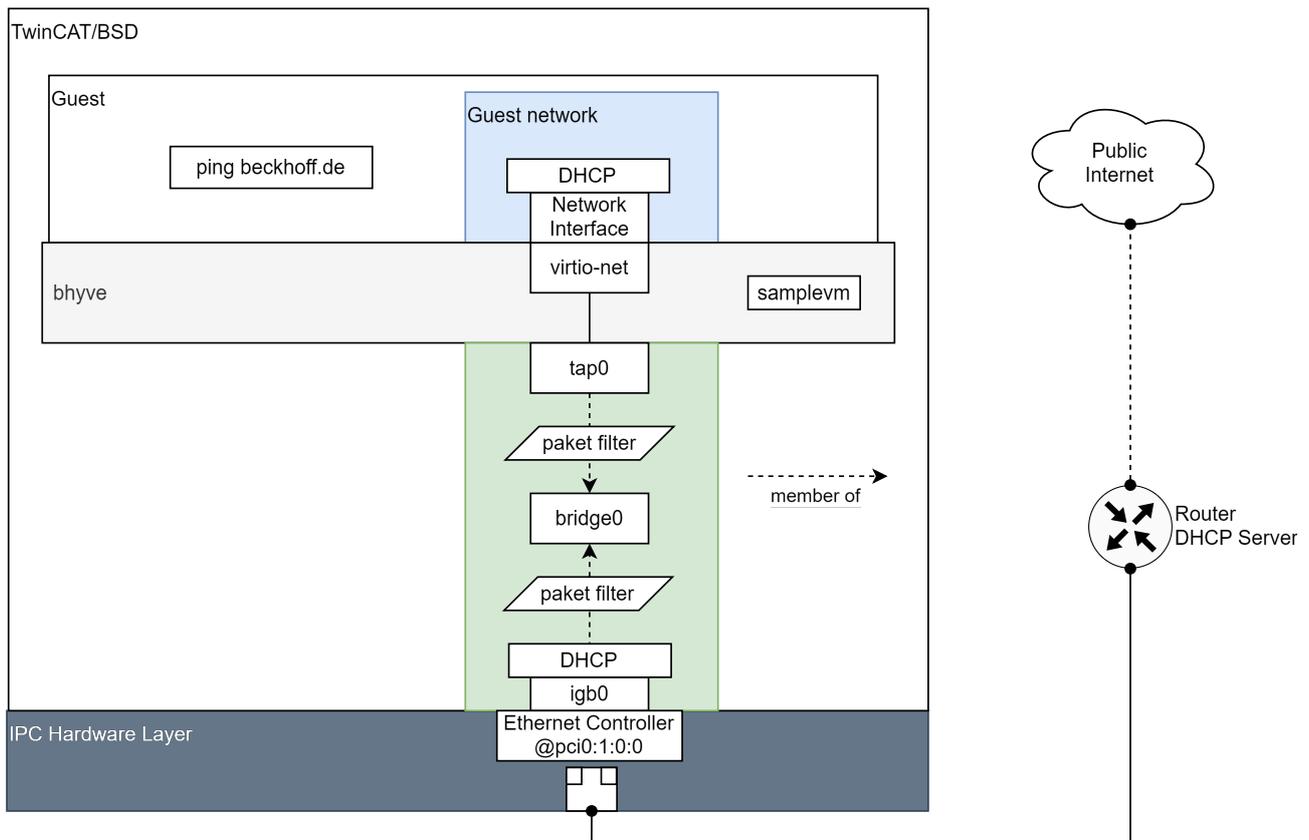


Abb. 24: VM-Instanz mit einer Bridge-Netzwerkconfiguration.

Die Netzwerkkommunikation der virtuellen Maschine wird so über das jeweilige `tap(4)` Gerät durch ein `bridge(4)` Gerät auf Ethernet-Ebene mit dem physischen Netzwerkinterface des TwinCAT/BSD-Hosts gebrückt.

Konfiguration der Netzwerkkomponenten

Auf dem TwinCAT/BSD-Host wird ein `bridge(4)` Gerät mit Hilfe von `ifconfig(8)` erstellt:

```
doas ifconfig bridge create
```

Die Ausgabe `bridge0` erscheint.

Ebenso wird ein `tap(4)` Geräte als Backend für das virtuelle Netzwerkinterface angelegt:

```
doas ifconfig tap create
```

Die Ausgabe `tap0` erscheint.

Um Netzwerkpakete zwischen einem physischen Netzwerkkarte des TwinCAT/BSD-Hosts und einem tap(4) Gerät über die bridge0 weiterzuleiten, müssen die entsprechenden Geräte Mitglieder der bridge0 werden.

Der folgende Aufruf macht das physische Netzwerkkarte igb0 des TwinCAT/BSD-Host und das tap0 Gerät zu Mitgliedern der bridge0 Instanz:

```
doas ifconfig bridge0 addm igb0 addm tap0 up
```

Abhängig vom eingesetzten Industrie-PC oder der verwendeten Ethernet-Schnittstelle kann die Benennung der Netzwerkschnittstelle unter TwinCAT/BSD variieren und beispielsweise als em0, em1 oder igb1 angezeigt werden.

Damit die bridge0 Konfiguration bereits beim Systemstart angelegt wird, kann diese in der rc-Konfiguration hinterlegt werden:

```
doas sysrc cloned_interfaces+="bridge0 tap0"
doas sysrc ifconfig_bridge0="addm igb0 addm tap0 up"
```

Über ifconfig bridge0 können die Mitglieder (members) der bridge0 überprüft werden:

```
ifconfig bridge0
bridge0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
ether 58:9c:fc:10:ff:e1
id 00:00:00:00:00:00 priority 32768 hellotime 2 fwddelay 15
maxage 20 holdcnt 6 proto rstp maxaddr 2000 timeout 1200
root id 00:00:00:00:00:00 priority 32768 ifcost 0 port 0
member: tap0 flags=143<LEARNING,DISCOVER,AUTOEDGE,AUTOPTP>
ifmaxaddr 0 port 5 priority 128 path cost 2000000
member: igb0 flags=143<LEARNING,DISCOVER,AUTOEDGE,AUTOPTP>
ifmaxaddr 0 port 1 priority 128 path cost 2000000
groups: bridge
nd6 options=9<PERFORMNUD,IFDISABLED>
```

Das entsprechende bhyve(8) Kommando nutzt lediglich die tap0 Instanz, um die virtuelle Maschine mit dem Bridge-Netzwerk zu verbinden:

```
doas bhyve \
-c sockets=1,cores=1,threads=1 \
-m 2G \
-l bootrom,/usr/local/share/uefi-firmware/BHYVE_BHF_UEFI.fd,fwcfg=qemu \
-s 0,hostbridge \
-s 2,fbuf,rfb=0.0.0.0:5900,w=1024,h=768 \
-s 3,xhci,tablet \
-s 20,virtio-net,tap0 \
-s 31,lpc \
-A -H -P \
samplevm
```

Filterregeln im Bridge-Netzwerk

Standardmäßig blockiert der Paketfilter pf(8) unter TwinCAT/BSD den Austausch von Netzwerkpaketen an einem bridge(4) Gerät.

Das Filterverhalten an bridge(4) Geräten kann über sysctl(8) deaktiviert werden. Indem die Variablen net.link.bridge.pfil_member und net.link.bridge.pfil_bridge auf 0 gesetzt werden:

```
doas sysctl net.link.bridge.pfil_member=0
doas sysctl net.link.bridge.pfil_bridge=0
```

Um die Einstellungen persistent zu setzen, müssen folgende Zeilen in der Datei /etc/sysctl.conf eingefügt werden:

```
net.link.bridge.pfil_member=0
net.link.bridge.pfil_bridge=0
```

Weitere Informationen finden sich in den man-pages zu bridge(4), sysctl(8) und sysctl.conf(5).

Alternativ können für die bridge(4) und deren Mitglieder pf(8) Filterregeln definiert werden, um den Paketaustausch im Bridge-Netzwerk zu regeln (siehe: [Firewall](#) [▶ 35]).

10.5.5.3 NAT-Netzwerk

Ein NAT-Netzwerk kann genutzt werden, um Anfragen aus einem privaten VM-Netzwerk (z. B. einem Host-Only-Netzwerk) an ein externes Netzwerk zu schicken.

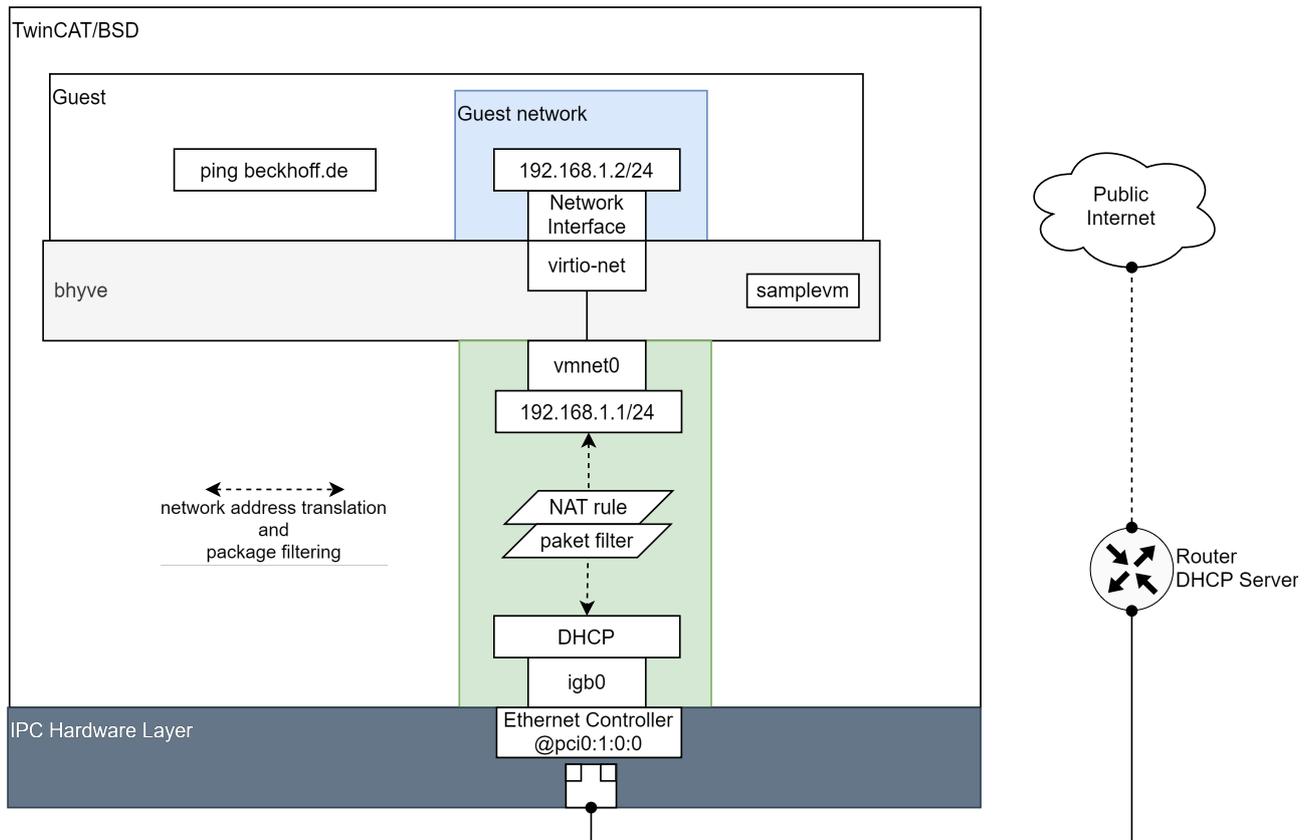


Abb. 25: VM-Instanz mit einer NAT-Netzwerkconfiguration.

Unter TwinCAT/BSD muss dafür das Weiterleiten von IP-Paketen zwischen Netzwerkschnittstellen aktiviert werden:

```
doas sysctl net.inet.ip.forwarding=1
```

Um diese Einstellung persistent zu speichern kann `net.inet.ip.forwarding=1` der Datei `/etc/sysctl.conf` hinzugefügt werden. Außerdem werden für die Übersetzung der privaten Netzwerkadressen in ein externes Netzwerk entsprechende NAT-Regeln (Network-Address-Translation-Regeln) im `pf(8)` benötigt.

Im folgenden Beispiel wird die `vmnet0` Konfiguration aus dem Kapitel [Host-Only-Netzwerk \[► 89\]](#) für das private Netzwerk zwischen virtueller Maschine und TwinCAT/BSD Host verwendet.

```
ifconfig vmnet0
```

```
vmnet0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=80000<LINKSTATE>
ether 58:9c:fc:10:56:5b
inet 192.168.1.1 netmask 0xfffff00 broadcast 192.168.1.255
groups: vmnet
media: Ethernet autoselect
status: no carrier
nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
```

Über das physische Netzwerkinterface `igb0` ist der IPC mit einem externen Netzwerk verbunden:

```
ifconfig igb0
```

```
igb0: flags=8863<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=4a004a9<RXCSUM,VLAN_MTU,JUMBO_MTU,VLAN_HWCSUM,LRO,RXCSUM_IPV6,NOMAP>
ether 00:01:05:62:3b:b0
inet 172.17.98.154 netmask 0xfffff00 broadcast 172.17.98.255
media: Ethernet autoselect (1000baseT <full-duplex>)
status: active
nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
```

Für die Übersetzung der privaten Adressen in das externe Netzwerk kann folgende pf-Regel zunächst in einer Textdatei (`samplevm.nat.conf`) gespeichert werden und anschließend über `pfctl(8)` geladen werden:

```
nat on igb0 from vmnet0:network to any -> (igb0)
doas pfctl -a "bhf-nat/samplevm-nat" -f samplevm.nat.conf
```

Zusätzlich soll eingehender Netzwerkverkehr in das private Netzwerk erlaubt werden:

```
pass from vmnet0:network to any keep state
```

Der Regelsatz kann wiederum in einer Textdatei gespeichert und über `pfctl(8)` geladen werden:

```
doas pfctl -a "bhf/bhyve/samplevm " -f samplevm.filters.conf
```

Sind beide Regelsätze geladen, kann die virtuelle Maschine mit `vmnet0` als Backend für den virtio-net basierten Netzwerkcontroller gestartet werden:

```
doas bhyve \
-c sockets=1,cores=1,threads=1 \
-m 2G \
-l bootrom,/usr/local/share/uefi-firmware/BHYVE_BHF_UEFI.fd,fwcfg=qemu \
-s 0,hostbridge \
-s 20,virtio-net,vmnet0 \
-s 31,lpc \
-A -H -P \
samplevm
```

Innerhalb des Gastbetriebssystems kann die Kommunikation in das externe Netzwerk mit ping-Anfragen überprüft werden:

```
ping beckhoff.com
PING beckhoff.com (18.195.44.45) from 192.168.1.2 : 56(84) bytes of data.
64 bytes from ec2-18-195-44-45.eu-central-1.compute.amazonaws.com (18.195.44.45): icmp_seq=1 ttl=245
time=7.44 ms
64 bytes from ec2-18-195-44-45.eu-central-1.compute.amazonaws.com (18.195.44.45): icmp_seq=2 ttl=245
time=7.27 ms
64 bytes from ec2-18-195-44-45.eu-central-1.compute.amazonaws.com (18.195.44.45): icmp_seq=3 ttl=245
time=7.36 ms
^C
```

Dabei ist zu beachten, dass der virtuellen Netzwerkschnittstelle im Gastbetriebssystem eine Netzwerkadresse im Bereich des `vmnet0` Netzwerks (`192.168.1.0/24` siehe oben) zugewiesen wird. Außerdem muss die `vmnet0` Adresse (`192.168.1.1`) als Default-Gateway eingetragen werden, sowie Adressen von Name-Servern hinterlegt werden, um öffentliche Domainnamen wie `beckhoff.com` aufzulösen.

10.5.5.4 Ethernet-Device-Passthrough

Industrie-PCs mit IOMMU-Unterstützung ermöglichen das explizite Zuweisen von physischen Ethernet-Geräten an eine virtuelle Maschine. Die virtuelle Maschine kann somit direkt über das physische Ethernet-Gerät mit einem Netzwerk verbunden werden, ohne dass Netzwerkpakete über den TwinCAT/BSD-Host vermittelt werden. Das allgemeine Vorgehen für die Zuweisung von PCI-Geräten ist im Kapitel [PCI-Device-Passthrough](#) [[94](#)] beschrieben.

Die folgende Abbildung stellt dar, wie das Ethernet-Gerät an PCI-Adresse 3:0:0 an die `samplevm` durchgereicht wird, um die virtuelle Maschine mit einem externen Netzwerk zu verbinden.

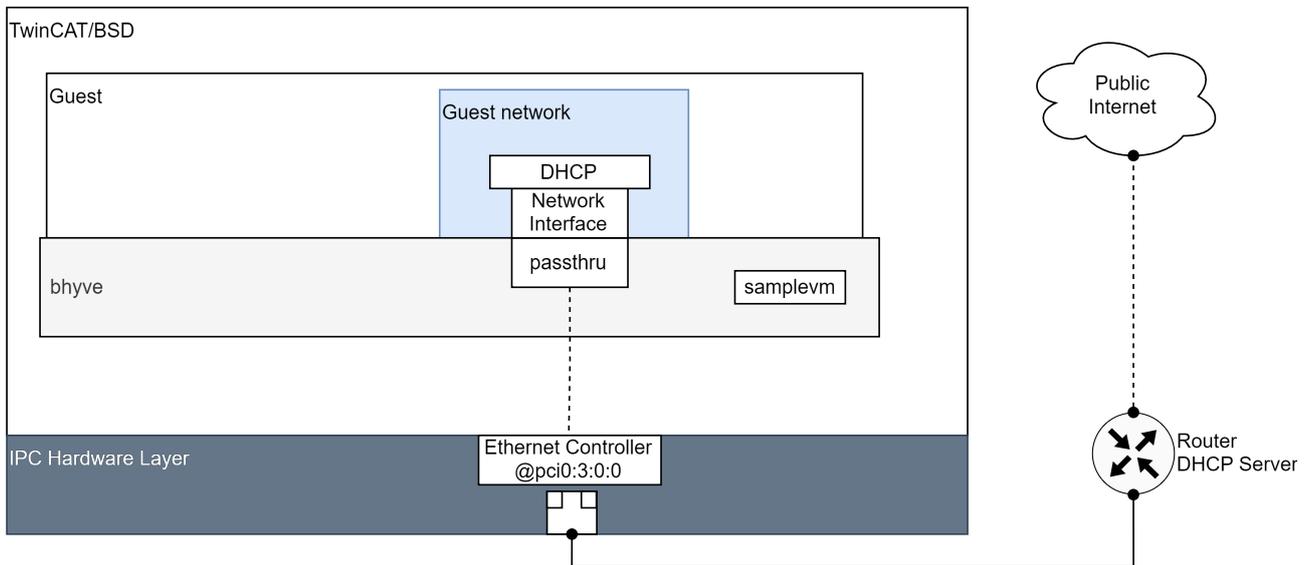


Abb. 26: VM-Instanz mit einer Ethernet-Device-Passthrough-Konfiguration.

Der folgende `bhyve` Aufruf weist das Ethernet-Gerät an der physischen PCI-Adresse **3:0:0** der virtuellen PCI-Adresse **20** der virtuellen Maschine zu:

```
doas bhyve \
-c sockets=1,cores=2,threads=1 \
-m 2G \
-l bootrom,/usr/local/share/uefi-firmware/BHYVE_BHF_UEFI.fd,fwcfg=qemu \
-s 0,hostbridge \
-s 20,passthru,3/0/0 \
-s 31,lpc \
-A -H -P -S\
samplevm
```

10.5.6 PCI-Device-Passthrough

Industrie-PCs mit IOMMU-Virtualisierungsfunktionen erlauben das explizite Zuweisen von physischen PCI-Geräten an eine virtuelle Maschine (siehe Tabelle: [Geräteunterstützung für TwinCAT/BSD Hypervisor, Device- und GPU-Passthrough](#). [[77](#)]). PCI-Geräte wie die GPU, Netzwerkschnittstellen oder USB-Controller können als `passthru` Geräte explizit einer virtuellen Maschine zugewiesen werden.

Um ein PCI-Gerät einer virtuellen Maschine zuzuweisen, wird zunächst dessen PCI-Adresse benötigt. Mit dem Kommando `pciconf -l` werden alle PCI-Geräte sowie ihre Adressen gelistet.

```
$ pciconf -l
...
vgapci0@pci0:0:2:0: class=0x030000 rev=0x00 hdr=0x00 vendor=0x8086 device=0x3e92 subvendor=0x8086
subdevice=0x2212
xhci0@pci0:0:20:0: class=0x0c0330 rev=0x10 hdr=0x00 vendor=0x8086 device=0xa36d subvendor=0x8086
subdevice=0x7270
igb0@pci0:1:0:0: class=0x020000 rev=0x03 hdr=0x00 vendor=0x8086 device=0x1533 subvendor=0x8086
subdevice=0x1533
...
```

Im folgenden Beispiel sollen die drei gelisteten Geräte einer virtuellen Maschine zugewiesen werden.

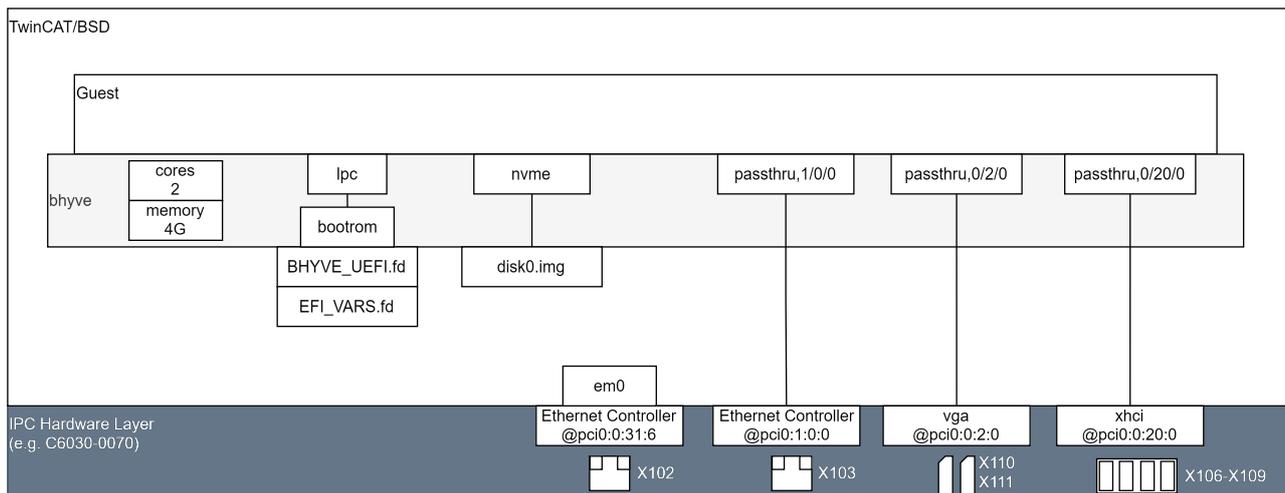


Abb. 27: Konfiguration einer VM-Instanz mit PCI-Device-Passthrough.

Gerät	Beschreibung	Adresse
vgapci0@pci0:0:2:0	GPU	pci0:0:2:0
igb2@pci1:0:0:0	Ethernet Controller	pci1:0:0:0
xhci1@pci0:20:0:0	USB-Controller	pci0:20:0:0

Um die Geräte vom TwinCAT/BSD-Host zu isolieren, werden Geräten mit devctl der ppt (PCI PassThrough) Treiber zugewiesen.

```
doas devctl set driver -f pci0:0:2:0 ppt
doas devctl set driver -f pci0:0:20:0 ppt
doas devctl set driver -f pci0:1:0:0 ppt
```

Um die Treiber bereits beim Systemboot zu setzen, können die PCI-Adressen als pptdevs der Datei /boot/loader.conf hinzugefügt werden:

```
pptdevs="1/0/0 0/2/0 0/20/0"
```

Eine erneute Ausgabe von pciconf -l zeigt nun, dass die ppt Treiber den Geräten zugewiesen wurden:

```
$ pciconf -l
...
ppt0@pci0:0:2:0: class=0x030000 rev=0x00 hdr=0x00 vendor=0x8086 device=0x3e92 subvendor=0x8086
subdevice=0x2212
ppt1@pci0:0:20:0: class=0x0c0330 rev=0x10 hdr=0x00 vendor=0x8086 device=0xa36d subvendor=0x8086
subdevice=0x7270
ppt2@pci0:1:0:0: class=0x020000 rev=0x03 hdr=0x00 vendor=0x8086 device=0x1533 subvendor=0x8086
subdevice=0x1533
...
```

Die PCI-Geräte können nun bhyve mit dem Parameter -s [slot],passthru,[slot/bus/function] übergeben werden. Die Werte für [slot/bus/function] beziehen sich dabei auf die PCI-Adressen der pciconf -l Ausgabe. Da Passthrough-Geräte fixe Speicheradressen verwenden, muss bhyve zusätzlich das Flag -s als Parameter übergeben werden, um Memory-Swapping für den Prozess zu deaktivieren.

Der bhyve Aufruf mit zugewiesener on-board GPU, Ethernet- und USB-Controller ergibt sich für das Beispiel wie folgt:

```
doas bhyve \
-c sockets=1,cores=2,threads=1 \
-m 4G \
-l bootrom,/usr/local/share/uefi-firmware/BHYVE_BHF_UEFI.fd,fwcfg=qemu \
-s 0:0,hostbridge \
-s 2:0,passthru,0/2/0 \
-s 3:0,passthru,0/20/0 \
-s 10:0,nvme,/vms/samplevm/disk0.img \
-s 20:0,passthru,1/0/0 \
-s 31:0,lpc \
-A -H -P -S \
samplevm
```

Erweiterte Parameter für das Durchreichen der integrierten GPU

Das Durchreichen der integrierten GPU auf unterstützten IPCs benötigt erweiterte bhyve-Parameter, damit die EFI-Firmware `BHYVE_BHF_UEFI.fd` die integrierte Grafikkarte während des Boot-Vorgangs der virtuellen Maschine korrekt initialisieren und dem Gast-Betriebssystem zur Verfügung stellen kann.

```
doas bhyve \
-c sockets=1,cores=2,threads=1 \
-m 4G \
-l bootrom,/usr/local/share/uefi-firmware/BHYVE_BHF_UEFI.fd,fwcfg=qemu \
-s 0:0,hostbridge \
-s 2:0,passthru,0/2/0,rom=/vms/samplevm/gop.rom \
-s 3:0,passthru,0/20/0 \
-s 10:0,nvme,/vms/samplevm/disk0.img \
-s 20:0,passthru,1/0/0 \
-s 31:0,lpc \
-o pci.0.31.0.pcireg.vendor=host \
-o pci.0.31.0.pcireg.device=host \
-o pci.0.31.0.pcireg.revid=host \
-o pci.0.31.0.pcireg.subvendor=host \
-o pci.0.31.0.pcireg.subdevice=host \
-A -H -P -S \
samplevm
```

Der `passthru` Parameter für die integrierte Grafikkarte (`-s 2:0,passthru,0/2/0`) wird um `,rom=/vms/samplevm/gop.rom` erweitert.

Die Datei `gop.rom` wird für die Initialisierung der Grafikkarte durch das EFI benötigt und kann mit folgendem Befehl erstellt werden:

```
doas gop-dump /vms/samplevm/gop.rom
```

Zusätzlich müssen, wie oben dargestellt, die PCI-Register der emulierten LPC-Bridge beim `bhyve` Aufruf auf den Wert `host` gesetzt werden:

```
-o pci.0.31.0.pcireg.vendor=host \
-o pci.0.31.0.pcireg.device=host \
-o pci.0.31.0.pcireg.revid=host \
-o pci.0.31.0.pcireg.subvendor=host \
-o pci.0.31.0.pcireg.subdevice=host \
```

10.5.7 Durchreichen von Eingabegeräten

Eingaben über Maus und Tastatur können über ein `virtio-input` Gerät an die virtuelle Maschine übergeben werden. In diesem Fall muss nicht der gesamte USB-Controller via PCI-Device-Passthrough durchgereicht werden sodass andere USB-Schnittstellen weiterhin dem TwinCAT/BSD Host zur Verfügung stehen.

Um Eingaben über `virtio-input` an die virtuelle Maschine weiterzuleiten, müssen dem `virtio-input` Gerät die Eingabe-Events des angeschlossenen Gerätes `/dev/input/eventN` übergeben werden.

Der folgende Beispielaufruf übergibt die integrierte GPU mit Hilfe von PCI-Device Passthrough und die Eingabe-Events `/dev/input/event4` und `/dev/input/event3` per `virtio-net`.

```
doas bhyve \
-c sockets=1,cores=2,threads=1 \
-m 4G \
-l bootrom,/vms/samplevm/UEFI.fd,/vms/samplevm/EFI_VARS.fd,fwcfg=qemu \
-s 0,hostbridge \
-s 2,passthru,0/2/0,rom=/vms/samplevm/gop.rom \
-s 3,virtio-input,/dev/input/event4 \
-s 4,virtio-input,/dev/input/event3 \
-s 10,nvme,/vms/samplevm/disk0.img \
-s 31,lpc \
-o pci.0.31.0.pcireg.vendor=host \
-o pci.0.31.0.pcireg.device=host \
-o pci.0.31.0.pcireg.revid=host \
-o pci.0.31.0.pcireg.subvendor=host \
-o pci.0.31.0.pcireg.subdevice=host \
-A -H -P samplevm
```

Identifizierung von Eingabe-Events angeschlossener USB-Geräte

Mit Hilfe des Kommandos `sysctl kern.evdev.input` können angeschlossene Eingabegeräte sowie ihre IDs gelistet werden, um so die Zuordnung zwischen Eingabegerät und `/dev/input/event<ID>` zu ermitteln.

Im folgenden Beispiel lässt sich eine USB Maus (`ums0`) mit Input ID 4 und eine USB-Tastatur (`ukbd0`) mit Input ID 3 erkennen.

```
kern.evdev.input.4.uniq: 2057366C5943
kern.evdev.input.4.phys: ukbd1
kern.evdev.input.4.id: { bustype = 0x0003, vendor = 0x046d, product = 0xc093, version = 0x0000 }
kern.evdev.input.4.name: Logitech Advanced Corded Mouse M500s, class 0/0, rev 2.00/53.00, addr 2
kern.evdev.input.3.uniq:
kern.evdev.input.3.phys: ukbd0
kern.evdev.input.3.id: { bustype = 0x0003, vendor = 0x046d, product = 0xc328, version = 0x0000 }
kern.evdev.input.3.name: Logitech USB Keyboard, class 0/0, rev 1.10/86.00, addr 1
kern.evdev.input.2.uniq:
kern.evdev.input.2.phys: acpi_button0
kern.evdev.input.2.id: { bustype = 0x0019, vendor = 0x0000, product = 0x0000, version = 0x0001 }
kern.evdev.input.2.name: Sleep Button
kern.evdev.input.1.uniq:
kern.evdev.input.1.phys: sysmouse
kern.evdev.input.1.id: { bustype = 0x0006, vendor = 0x0000, product = 0x0000, version = 0x0000 }
kern.evdev.input.1.name: System mouse
kern.evdev.input.0.uniq:
kern.evdev.input.0.phys: kbdmux0
kern.evdev.input.0.id: { bustype = 0x0006, vendor = 0x0000, product = 0x0000, version = 0x0000 }
kern.evdev.input.0.name: System keyboard multiplexer
```

Dementsprechend können wie im Beispiel oben die Eingabe-Events von Maus und Tastatur an die virtuelle Maschine übergeben werden.

10.6 Debian Linux als Gastbetriebssystem installieren

Im folgenden Beispiel soll **Debian** in einer virtuellen Maschine unter TwinCAT/BSD installiert werden. Als Vorlage können die Shell-Skripte aus dem GitHub-Repository https://github.com/Beckhoff/TCBSD_Hypervisor_Samples/tree/main/vm_autostart verwendet werden.

```
TCBSD_Hypervisor_Samples/vm_autostart
├── Makefile
├── rc.d
│   └── samplevm
└── samplevm
```

Anforderungen an das VM-Setup:

Für die Ausführung von Debian als Gastbetriebssystem ohne grafischen Desktop soll die VM zwei virtuelle Kerne und 2GB RAM zur Verfügung stellen. Die VM soll UEFI basiert sein, um Gastbetriebssysteme zu booten. Die Debian Installation soll über ein „net installer“ ISO-CDROM Image erfolgen. Für den Internetzugriff wird die VM über ein Bridge-Netzwerk mit dem Netzwerk des Hosts verbunden.

Um mit dem Debian-Installer zu interagieren, soll eine VNC-Verbindung zur VM ermöglicht werden. Die benötigten Skripte, die Dateien für das UEFI und virtuellen Datenträger (CDROM-ISO und Festplatte) sollen zudem auf einem ZFS-Dataset gespeichert werden, damit nach der Installation des Betriebssystems der Stand über ein ZFS-Snapshot gesichert und zu einem späteren Zeitpunkt wiederhergestellt werden kann.

Einen Überblick über die Konfiguration ist folgender Abbildung dargestellt:

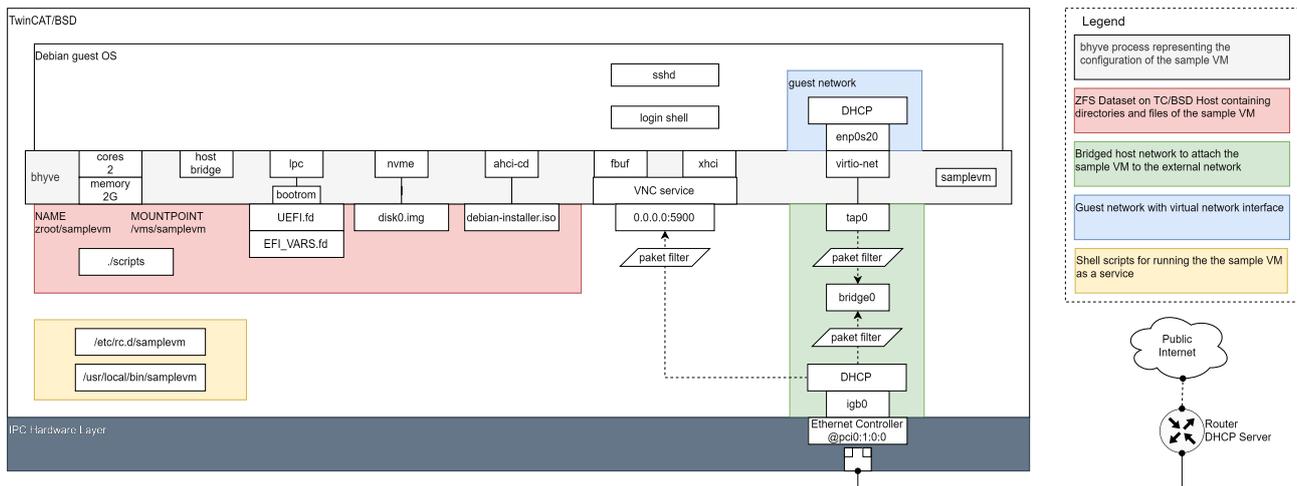


Abb. 28: Debian Linux sample VM

Voraussetzungen:

- Für alle folgenden Befehle werden root-Rechte angenommen. Wechseln Sie via `doas sh` in eine root-Shell.

Gehen Sie für die Einrichtung der Konfiguration wie folgt vor:

- Erstellen Sie ein ZFS-Datasets als Speicherort für virtuelle Maschinen [► 83] Konfiguration:

```
zfs create -p -o mountpoint=/vms/samplevm zroot/samplevm
```

- Laden und entpacken Sie die GitHub-Beispielskripte nach `/vms/samplevm/scripts`:

```
fetch -o /home/Administrator/main.zip \
https://github.com/Beckhoff/TCBSD_Hypervisor_Samples/archive/refs/heads/main.zip
unzip -d /vms/samplevm /home/Administrator/main.zip
mv /vms/samplevm/TCBSD_Hypervisor_Samples-main/vm_autostart /vms/samplevm/scripts
rm -rf /vms/samplevm/TCBSD_Hypervisor_Samples-main /home/Administrator/main.zip
```

- Im nächsten Schritt soll der `bhyve` Aufruf innerhalb des `/vms/samplevm/vm_autostart/sample` angepasst werden. Die Datei kann mit `ee` geöffnet und bearbeitet werden:

```
ee /vms/samplevm/scripts/samplevm
```

- Suchen Sie den `bhyve` Aufruf und passen Sie die Parameter wie folgt an:

```
bhyve \
-c sockets=1,cores=2,threads=1 \
-m 2G \
-l bootrom,/vms/samplevm/UEFI.fd,/vms/samplevm/EFI_VARS.fd,fwcfg=qemu \
-s 0,hostbridge \
-s 2,fbuf,rfb=0.0.0.0:5900,w=1280,h=1024 \
-s 3,xhci,tablet \
-s 10,nvme,/vms/samplevm/disk0.img \
-s 15,ahci-cd,/vms/samplevm/debian-installer.iso,ro \
-s 20,virtio-net,tap0 \
-s 31,lpc \
-A -H -P -w \
"${vm_name}"
```

- Schließen sie den Editor mit `ESC` und speichern Sie die Änderungen an der Datei.
- Der angepasste `bhyve` Aufruf referenziert in den Programm-Parametern Dateien, die noch nicht auf dem TwinCAT/BSD Host vorhanden sind. In den nächsten Schritten werden daher die nötigen Dateien angelegt.
- Für die Installation des Betriebssystems soll die Debian "network install" CD-ISO verwendet werden. Die ISO Datei kann mit `fetch` (8), wie im Kapitel Verwendung von Installationsmedien (ISO-Images) [► 86] beschrieben, heruntergeladen und später als Datenträger eines `ahci-hd` Geräts dem `bhyve` Aufruf übergeben werden:

```
fetch -o /vms/samplevm/debian-installer.iso https://cdimage.debian.org/mirror/cdimage/archive/12.0.0/amd64/iso-cd/debian-12.0.0-amd64-netinst.iso
```

- Um Debian auf einer virtuellen Festplatte installieren zu können, wird mit folgendem Kommando ein leeres Disk-Image angelegt, welches als Backend für das emulierte `nvme` Gerät im oberen `bhyve` Aufruf verwendet wird:

```
truncate -s 20G /vms/samplevm/disk0.img
```

9. Debian nutzt EFI-Variablen, um Informationen über bootfähige Datenträger abzuspeichern. Daher sollte für die virtuelle Maschine eine Kopie der Datei `/usr/local/share/uefi-firmware/BHYVE_BHF_UEFI_VARS.fd` als auch die UEFI-Firmware selbst in dem Verzeichnis des ZFS-Dataset abgelegt werden:

```
cp /usr/local/share/uefi-firmware/BHYVE_BHF_UEFI.fd /vms/samplevm/UEFI.fd
cp /usr/local/share/uefi-firmware/BHYVE_BHF_UEFI_VARS.fd /vms/samplevm/EFI_VARS.fd
```

10. Für die Debian-Installation benötigt die virtuelle Maschine eine Internetverbindung. Hierfür wird auf dem TwinCAT/BSD-Host entsprechend der Abbildung oben ein [Bridged-Netzwerk](#) [► 90] angelegt:

```
ifconfig bridge create name bridge0
ifconfig tap create name tap0
ifconfig bridge0 addm tap0 addm igb0 up

sysrc cloned_interfaces+="bridge0 tap0"
sysrc ifconfig_bridge0="addm tap0 addm igb0 up"

echo "net.link.bridge.pfil_bridge=0" >> /etc/sysctl.conf
echo "net.link.bridge.pfil_member=0" >> /etc/sysctl.conf
sysctl -f /etc/sysctl.conf
```

11. Jetzt liegen alle Dateien auf dem TwinCAT/BSD Host bereit, die in den Programm-Parametern des oben angepassten `bhyve` aufrufs referenziert sind. Dementsprechend kann das `samplevm` Skript im Verzeichnis `/vms/samplevm/scripts` gestartet werden:

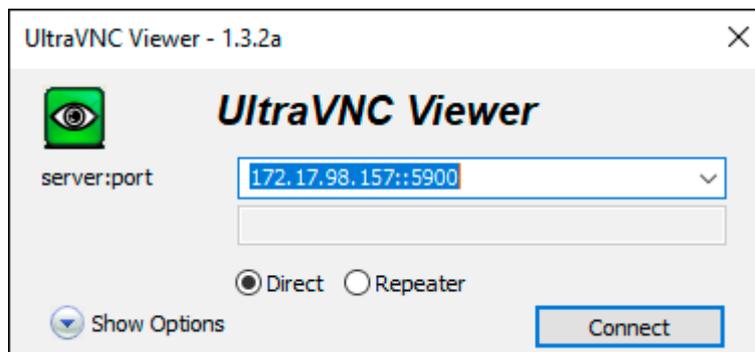
```
cd /vms/samplevm/scripts
sh -x samplevm start
```

12. Durch das `-x` Flag werden die ausgeführten Kommandos in dem Skript auf der Kommandozeile ausgegeben. Sobald der `bhyve` (8) Prozess ausgeführt wird, sollte folgende Ausgabe auf der Kommandozeile erscheinen:

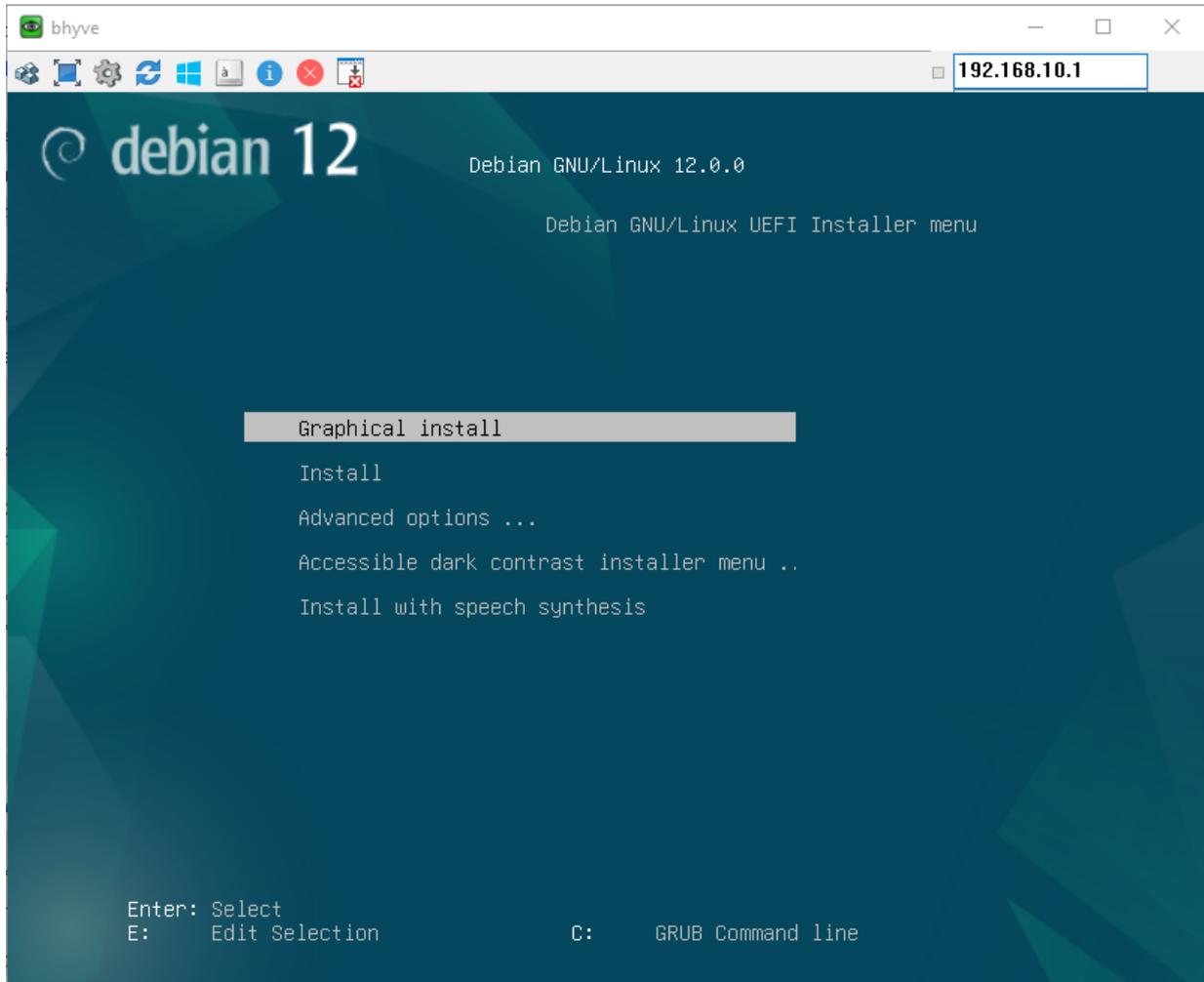
```
+ _bhyve_rc=0
+ bhyve -c 'sockets=1,cores=2,threads=1' -m 2G -l 'bootrom,/vms/samplevm/UEFI.fd,/vms/samplevm/EFI_VARS.fd,fwcfg=qemu' -s 0,hostbridge -s '2,fbuf,rfb=0.0.0.0:5900,w=1280,h=1024' -s 3,xhci,tablet -s 10,nvme,/vms/samplevm/disk0.img -s 15,ahci-cd,/vms/samplevm/debian-installer.iso,ro -s 20,virtio-net,tap0 -s 31,lpc -A -H -P -w samplevm

fbuf frame buffer base: 0x12ec16e00000 [sz 16777216]
```

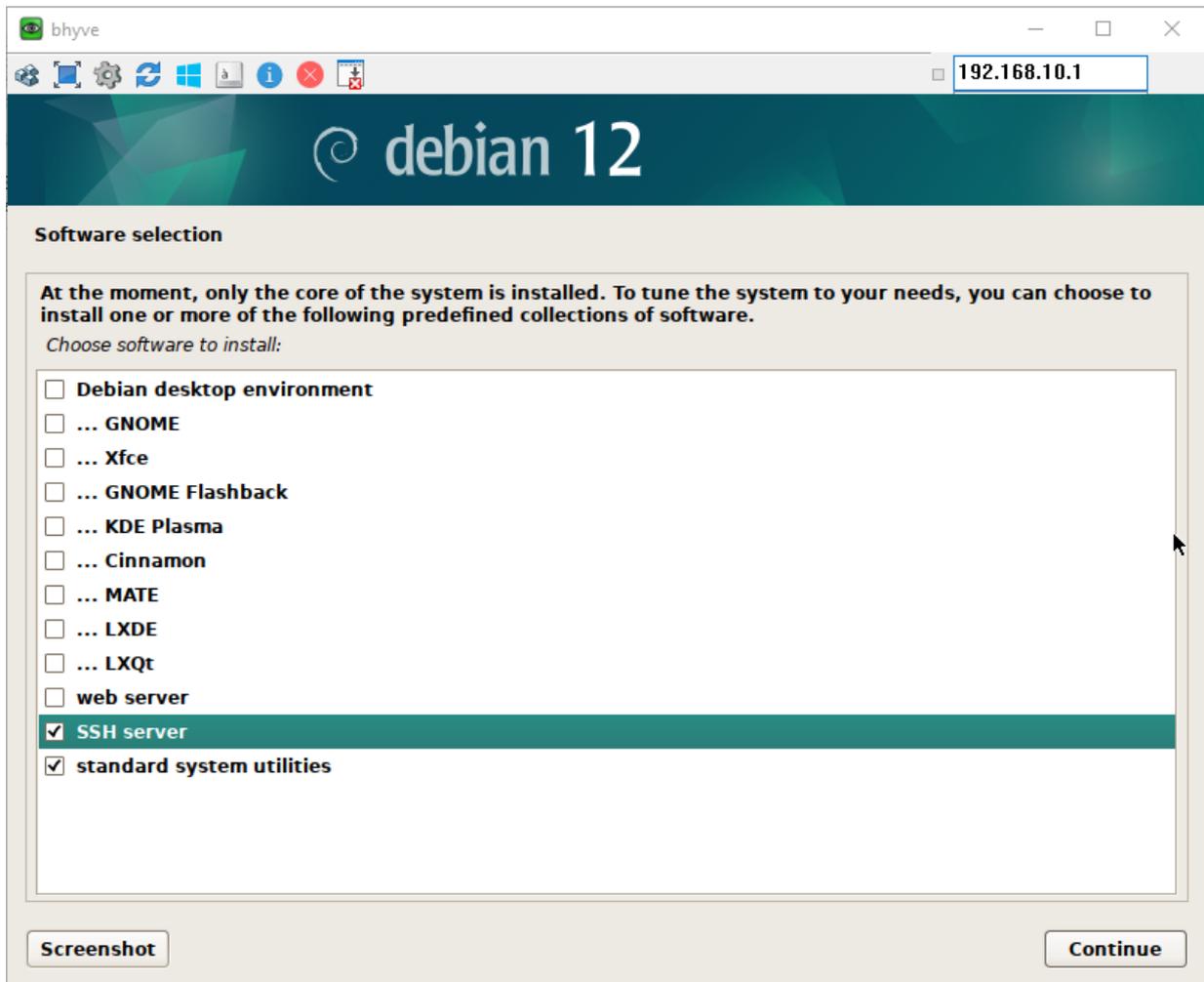
13. Nun kann ein VNC-Client, wie beispielsweise [Ultra-VNC](#) verwendet werden, um sich mit der virtuellen Maschine zu verbinden:



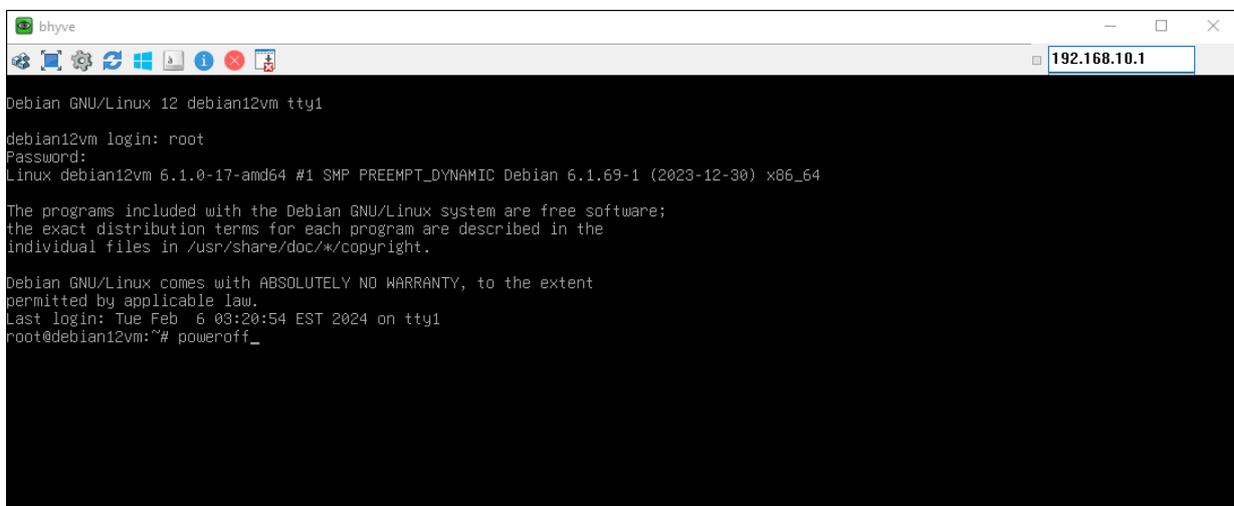
14. Nach erfolgreicher Verbindung über einen VNC-Client wird das Installationsmenü angezeigt. Starten Sie die Installation von Debian:



15. Da Debian ohne Grafischen Desktop installiert werden soll, können die Optionen „Debian Dektop Environment“ und „... GNOME“ abgewählt werden. Die Option „SSH-Server“ muss angewählt werden, damit später über einen SSH-Client auf die Debian Kommandozeile zugegriffen werden kann.



16. Sobald die Installation von Debian abgeschlossen ist, wird die virtuelle Maschine neu gestartet. Dadurch bricht die VNC-Verbindung ab. Nach einem erneuten Verbindungsaufbau kann das Betriebssystem Debian in der virtuellen Maschine über VNC bedient werden.
17. Mit dem Kommando `ip --brief address` kann die Netzwerkadresse der virtuellen Maschine im Netzwerk ausgegeben werden. Über die Netzwerkadresse kann so z.B. eine SSH Verbindung mit einem SSH-Client für den Fernzugriff auf das Debian Betriebssystem hergestellt werden.
18. Für die abschließenden Schritte sollte die VM heruntergefahren werden.



19. Wenn per SSH eine Verbindung zu der VM aufgebaut werden kann und das Betriebssystem installiert ist, kann der bhyve Aufruf angepasst werden, weil weder die VNC-Verbindung noch der Debian-Installer für die nächsten Bootvorgänge benötigt werden:

```
bhyve \
-c sockets=1,cores=2,threads=1 \
-m 2G \
-l bootrom,/vms/samplevm/UEFI.fd,/vms/samplevm/EFI_VARS.fd,fwcfg=gemu \
-s 0,hostbridge \
-s 10,nvme,/vms/samplevm/disk0.img \
-s 20,virtio-net,tap0 \
-s 31,lpc \
-A -H -P -w \
"${vm_name}"
```

20. Um den aktuellen Stand der Konfiguration zu sichern, kann mit folgendem Kommando ein ZFS Snapshot des Datasets erstellt werden. So werden die aktuellen Stände der Autostart-Skripte, als auch die Dateien für die virtuelle Festplatten und das UEFI der virtuellen Maschine gesichert und können so wieder auf den aktuellen Stand des wiederhergestellt werden:

```
zfs snapshot zroot/samplevm@os-installed
```

Über das Makefile lässt sich die VM-Konfiguration als Service registrieren. Dadurch kann das Skript im Autostart hinterlegt werden und über service(8) verwaltet werden:

```
cd /vms/samplevm/scripts
make install
service samplevm enable
service samplevm status
service samplevm start
service samplevm status
service samplevm stop
```

10.7 Windows als Gastbetriebssystem

Das Betriebssystem TwinCAT/BSD stellt mit dem integrierten Hypervisor die Möglichkeit bereit, Windows in einer virtuellen Maschine (kurz VM) zu betreiben.

Diese Funktionalität ist besonders für Kunden und Anwender interessant, die nicht auf Windows verzichten können, aber weiterhin TwinCAT/BSD mit allen TwinCAT-3-Runtime-Funktionen nutzen möchten. TwinCAT/BSD inklusive Windows VM kann entweder ab Werk bestellt oder nachträglich auf bestehenden Industrie-PCs nachinstalliert werden.

In beiden Fällen ist eine gültige Lizenz für den Betrieb von Windows in einer virtuellen Maschine notwendig.

Bestelloptionen für die Installation ab Werk

Die folgenden Bestelloptionen ermöglichen es, eine TwinCAT/BSD Industrie-PC ab Werk mit einer vorkonfigurierten und lizenzierten Windows VM zu bestellen:

- [C9900-S620: Windows 10 vorinstalliert mit Device-Passthrough \[► 103\]](#) für Industrie-PCs mit integrierter Grafikkarte und vorkonfigurierter Grafikausgabe.
- [C9900-S621: Windows 10 vorinstalliert ohne Device-Passthrough \[► 104\]](#) und ohne vorkonfigurierter Grafikausgabe.

Nachträgliche Installation auf bestehenden Industrie-PCs

Ausgelieferte Industrie-PCs können nachträglich auf TwinCAT/BSD (C9900-S60x) mit optionaler Windows VM (C9900-S62x) umgestellt werden. Der Upgrade-Prozess kann über den Beckhoff Service angestoßen werden. Alle dafür notwendigen Dateien werden vom Beckhoff Service bereitgestellt.

- [Windows VM mit vm-installer nachinstallieren \[► 105\]](#)

10.7.1 C9900-S620: Windows 10 vorinstalliert mit Device-Passthrough

Mit der Bestelloption C9900-S620 werden TwinCAT/BSD basierte Industrie-PCs mit einer vorkonfigurierten und lizenzierten Windows 10 VM ausgeliefert. Mit der Konfiguration werden die integrierte Grafikkarte, der USB-Controller und eine Ethernet-Schnittstelle per Device-Passthrough explizit an die Windows VM durchgereicht. Dadurch kann die Windows-Umgebung über ein Display angezeigt und über USB-Eingabegeräte (Maus, Tastatur, Multitouch) bedient werden.

Die folgende Abbildung zeigt die schematische Konfiguration der Bestelloption C9900-S620.

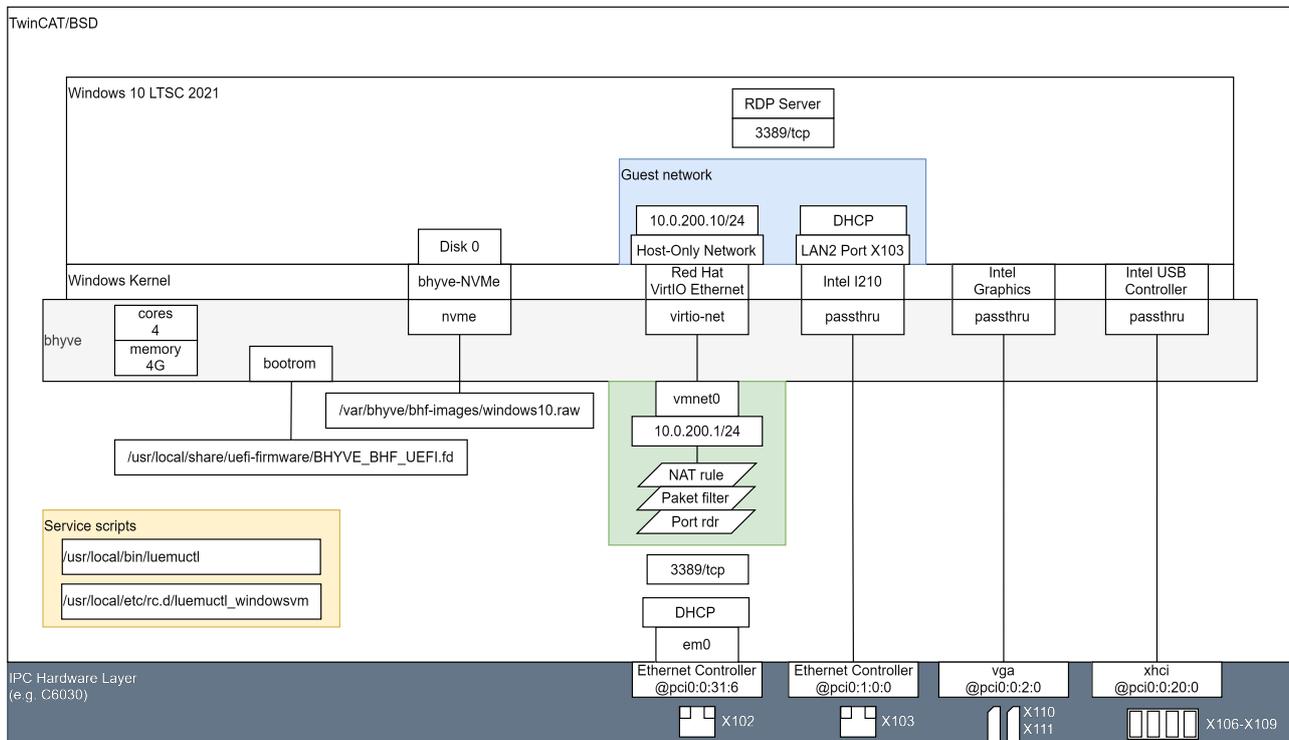


Abb. 29: C9900-S620 Bestelloption mit vorkonfigurierter Windows 10 VM mit Device-Passthrough.

Der Windows VM werden standardmäßig 4 CPU-Kerne und 4 GB Arbeitsspeicher zugewiesen. Die VM bootet im UEFI-Modus und lädt das installierte Windows Betriebssystem von Disk 0. Die virtuelle Disk 0 ist 30GB groß und beinhaltet neben der Boot-Partition auch die Windows C:\ Partition. Die zugehörige Disk-Datei befindet sich bei Auslieferung unter `/var/bhyve/bhf-images/windows10.raw`.

Ab Werk hat Windows zwei konfigurierte Netzwerkschnittstellen. Über das Host-Only Network kann auf die Dienste des TwinCAT/BSD Hosts zugegriffen werden (Web-Konsole, SSH, o.ä.). Gleichzeitig ermöglicht die Netzwerkkonfiguration eine ausgehende Netzwerkkommunikation über das Netzwerk des Hosts durch eine NAT-Regel zwischen dem Netzwerk von `vmnet0` und `em0`.

Im Auslieferungszustand ist zudem eine Port-Weiterleitung für das Remote-Desktop-Protokoll hinterlegt. Die Windows VM kann so per Remote-Desktop Client über die IP-Adresse des TwinCAT/BSD Hosts erreicht werden.

Die Netzwerkschnittstelle LAN2 Port X103 greift direkt auf den Ethernet-Controller am Port X103 des IPCs zu. Dementsprechend kann eine direkte Verbindung zwischen dem angeschlossenen Netzwerk und der Windows VM hergestellt werden.

Der Autostart der Windows VM wird ab Werk über das Programm `/usr/bin/luemuctl` und das entsprechend rc-Script `/usr/local/etc/rc.d/luemuctl_windowsvm` gesteuert. Dementsprechend stehen die Kommandos `service luemuctl_windowsvm [enable|disable|start|stop|status]` zum Verwalten des Dienstes zur Verfügung.

Weitere Informationen zu `luemuctl` können der man-Seiten `man luemuctl` und `man luemuctl-service` entnommen werden.

Für die Konfiguration der Windows VM mit Device-Passthrough muss der Industrie-PCs folgende Mindestausstattung erfüllen:

- Prozessoroptionen Intel® Core™ i3, i5 oder i7 der neunten oder elften Generation
- Speichererweiterung auf mindestens 8 GB DDR4-RAM
- Datenträgergröße mindestens 80 GB
- C9900-B617: Sonder-BIOS zur Unterstützung von GPU-Passthrough für Intel® Core™ der neunten Generation

10.7.2 C9900-S621: Windows 10 vorinstalliert ohne Device-Passthrough

Mit der Bestelloption C9900-S621 werden TwinCAT/BSD basierte Industrie-PCs mit einer vorkonfigurierten und lizenzierten Windows 10 VM ausgeliefert. Diese Bestelloption ist Anwendungsfälle vorgesehen, in denen per Remote-Desktop auf die Windows VM zugegriffen werden soll und somit kein Device-Passthrough von Geräten benötigen oder auf IPCs ausgeführt werden kann, die Device-Passthrough nicht unterstützen.

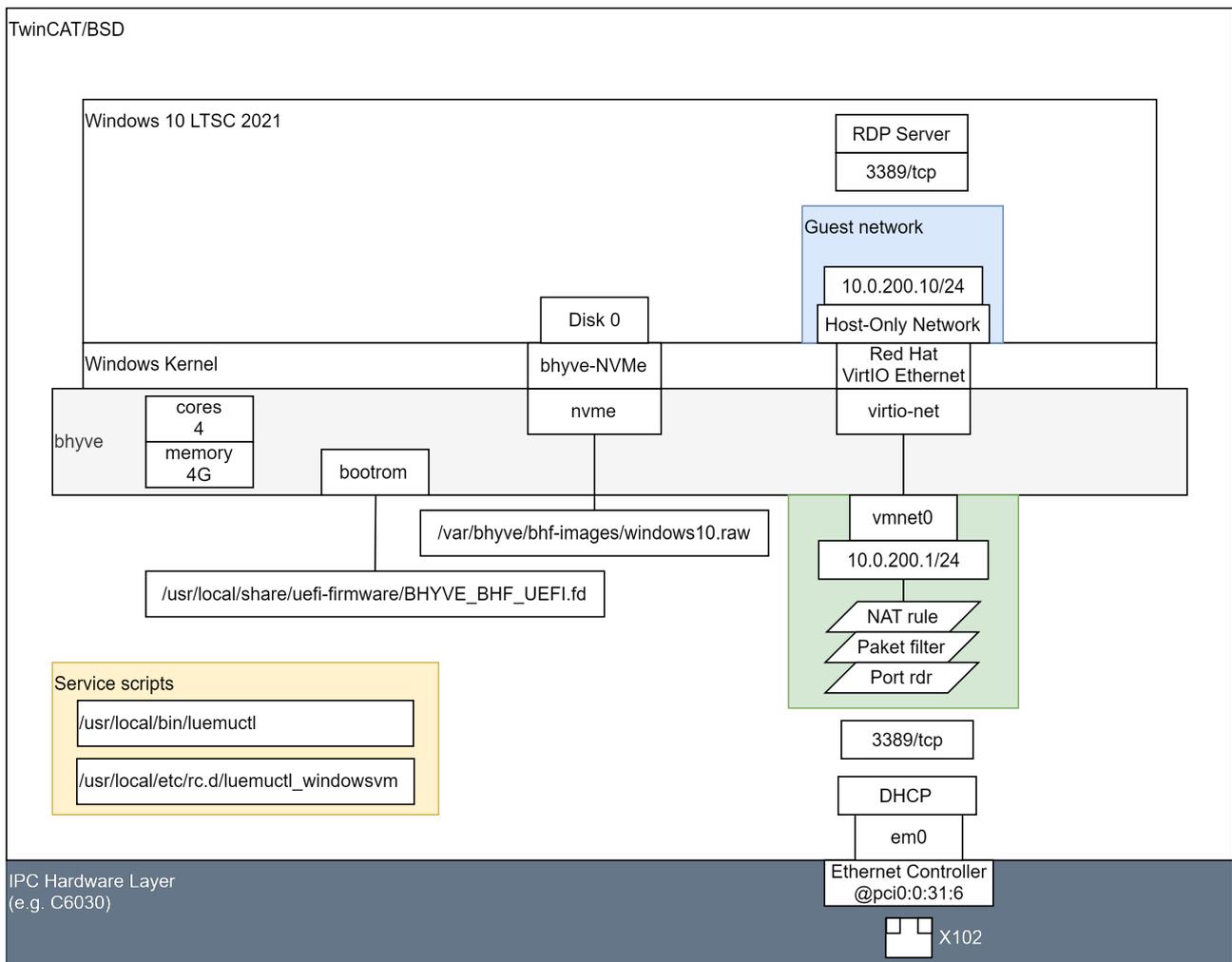


Abb. 30: C9900-S621 Bestelloption mit vorkonfigurierter Windows 10 VM.

Der Windows VM werden standardmäßig 4 CPU-Kerne und 4 GB Arbeitsspeicher zugewiesen. Die VM bootet im UEFI-Modus und lädt das installierte Windows Betriebssystem von Disk 0. Die virtuelle Disk 0 ist 30GB groß und beinhaltet neben der Boot-Partition auch die Windows C:\ Partition. Die zugehörige Disk-Datei befindet sich bei Auslieferung unter `/var/bhyve/bhf-images/windows10.raw`.

Ab Werk hat Windows eine konfigurierte Netzwerkschnittstelle. Über das Host-Only Network kann auf die Dienste des TwinCAT/BSD Hosts zugegriffen werden (z.B. Web-Konsole, SSH, o.ä.). Gleichzeitig ermöglicht die Netzwerkkonfiguration eine ausgehende Netzwerkkommunikation über das Netzwerk des Hosts durch eine NAT-Regel zwischen dem Netzwerk von `vmnet0` und `em0`.

Im Auslieferungszustand ist zudem eine Port-Weiterleitung für das Remote-Desktop-Protokoll hinterlegt (TCP-Port 3389). Die Windows VM kann so per Remote-Desktop Client über die IP-Adresse des TwinCAT/BSD Hosts erreicht werden.

Der Autostart der Windows VM wird ab Werk über das Programm `/usr/bin/luemuctl` und das entsprechend `rc-Script /usr/local/etc/rc.d/luemuctl_windowsvm` gesteuert. Dementsprechend stehen die Kommandos `service luemuctl_windowsvm [enable|disable|start|stop|status]` zum Verwalten des Dienstes zur Verfügung.

Weitere Informationen zu `luemuctl` können der man-Seiten `man luemuctl` und `man luemuctl-service` entnommen werden.

Für die Verwendung ohne GPU-Passthrough in Kombination mit einer Windows VM müssen die Industrie-PCs folgende Mindestausstattung erfüllen:

- Prozessoroptionen Intel® Core™ i3, Core™ i5 oder Core™ i7 der neunten oder elften Generation, CX20x2 mit Intel® Xeon®-D, CX20x3 und CX56xx mit AMD Ryzen™
- mindestens 8 GB DDR4-RAM
- mindestens 80 GB großen Speichermedium

10.7.3 Windows VM mit `vm-installer` nachinstallieren

Auf bestehenden TwinCAT/BSD Geräten können die Bestelloptionen -S620 und -S621 mit Hilfe des Programms `vm-installer` nachinstalliert werden.

Voraussetzung ist eine gültige TwinCAT/BSD und Windows VM Lizenz. Beide Lizenzen können durch als Lizenz-Upgrade beim Beckhoff Service (service@beckhoff.com) angefragt werden.

Mit der Bestellung der Windows VM wird Ihnen ein persönlicher Download-Link für das Windows Disk-Image bereitgestellt.

Das Image können Sie mit dem folgenden `fetch(8)` Kommando direkt auf den TwinCAT/BSD Host laden. Alternativ kann die geladene Datei auch mit WinSCP auf das TwinCAT/BSD System kopiert werden.

```
fetch https://fileexchange.beckhoff.com/fop/dMtKokIr/IN-0410-0612-08-1-154031.raw.zstd
```

Das komprimierte Disk-Image kann anschließend mit `unzstd(8)` entpackt und wie folgt in die Datei `windows.raw` geschrieben werden:

```
unzstd -o windows.raw IN-0410-0612-08-1-154031.raw.zstd
```

Das entpackte Disk-Image (`windows.raw`) wird vom Programm `vm-installer` verwendet, um eine virtuelle Maschine entsprechen der S620 oder S621 Option zu konfigurieren.

Das Programm `vm-installer` wird mit folgendem `pkg` Aufruf installiert:

```
doas pkg install -y vm-installer
```

Um eine Windows VM entsprechend der Bestelloption C9900-S620 mit `vm-installer` auf dem System zu installieren, kann folgender Aufruf verwendet werden:

```
doas vm-installer install \  
--logfolder="/var/log/windowsvm" \  
--nat-if=em0 \  
--passthru \  
windows.raw
```

Um eine Windows VM entsprechend der Bestelloption C9900-S621 zu installieren, kann folgender Aufruf verwendet werden:

```
doas vm-installer install \  
--logfolder="/var/log/windowsvm" \  
--nat-if=em0 \  
windows.raw
```

In beiden Fällen wird das Disk-Image `windows.raw` initialisiert und das Windows-Gastsystem entsprechend eingerichtet.

Nach der Installation kann der Status der VM über das Kommando `doas service luemuctl_windowsvm status` abgefragt werden.

Über die IP-Adresse des TwinCAT/BSD Host ist die laufende Windows VM via Remote Desktop für den Benutzer erreichbar.

10.7.4 Anpassen der Windows VM Konfiguration

Die Bestellung ab Werk oder die nachträgliche Installation von C9900-S620/-S621 mit `vm-installer` nutzen das rc-Script `/usr/local/etc/rc.d/luemuctl_windowsvm`, um die VM als Service mit dem Programm `/usr/bin/luemuctl` zu verwalten.

Weitere Informationen zu `luemuctl` können der man-Seite `man luemuctl` entnommen werden. Entsprechend den man-Seiten kann das Kommando `luemuctl run [OPTIONS] <vm_disk>` in der Datei `/usr/local/etc/rc.d/luemuctl_windowsvm` angepasst werden.

Alternativ kann das verwendete Disk-Image in eigenen Shell-Skripten als Disk-Image referenziert werden, wenn die initialisierte Windows-Umgebung in erweiterten VM-Konfigurationen genutzt werden soll.

11 C/C++ Projekte für TwinCAT/BSD

In diesem Kapitel wird gezeigt, wie Sie ausführbaren Code

- lokal auf dem Industrie-PC unter TwinCAT/BSD kompilieren können,
- oder remote auf TwinCAT/BSD-Zielsystemen kompilieren und debuggen können.

11.1 Unter TwinCAT/BSD kompilieren

In diesem Schritt wird gezeigt, wie Sie ausführbaren Code direkt unter TwinCAT/BSD mit dem Compiler LLVM generieren. Dazu wird beispielhaft ein C/C++ Projekt erstellt, welches die ADS-Schnittstelle nutzen soll. Um die Funktionen der TcAdsDll in Ihrem C/C++ Projekt zu nutzen, müssen Sie die Headerdatei TcAdsAPI.h in Ihr Projekt einbinden.

Die ADS-Headerdatei befindet sich im folgenden Verzeichnis:

`usr/local/include/TcAdsAPI.h`

Beispiel C/C++ Projekt `adstest.c`

```
#include <stdio.h>
#include <stdint.h>
#include "TcAdsAPI.h"

int main(){
    printf("ADS Test Sample\n");

    long nTemp;
    AdsVersion* pDLLVersion;
    nTemp = AdsGetDllVersion();
    pDLLVersion = (AdsVersion *)&nTemp;
    printf("Version: %d\n", (int)pDLLVersion->version);
    printf("Revision: %d\n", (int)pDLLVersion->revision);
    printf("Build: %d\n", (int)pDLLVersion->build);
    //printf("Ads DLL Version: %d\n", version);

    long l_port;
    l_port = AdsPortOpen();
    printf("Port opened: %ld\n", l_port);
    AdsPortClose();
    printf("Port closed\n");
    return 0;
}
```

Voraussetzungen:

- Installieren Sie das Developer-Package mit dem Befehl `doas pkg install os-generic-userland-devtools`

Generieren Sie ausführbaren Code wie folgt unter TwinCAT/BSD:

1. Kopieren Sie die Datei `adstest.c` in ein beliebiges TwinCAT/BSD-Verzeichnis. Zum Beispiel: `/usr/local/ADSinterface`
2. Navigieren Sie in das Verzeichnis mit der Beispieldatei `adstest.c`
3. Mit dem Befehl `doas cc -c -I /usr/local/include/ -D POSIX adstest.c -o adstest.o` wird die Datei `adstest.c` kompiliert.
4. Linken Sie die kompilierte Datei mit der ADS-Library mit dem Befehl `cc -lpthread adstest.o /usr/local/lib/libTcAdsDll.so -o adstest`
5. Führen Sie die Datei mit `./adstest` aus.

11.2 Remote-Debugging von Applikationen mit Visual Studio Code (VSC)

Dieser Abschnitt beschreibt, wie Sie Ihre auf Windows basierende Entwicklungsumgebung nutzen können, um Applikationen auf TwinCAT/BSD-Zielsystemen zu kompilieren und zu debuggen.

Die Grundidee ist, dass Sie Ihren gesamten Quellcode auf dem Windows-Entwicklungsrechner aufbewahren. Die Bearbeitung des Quellcodes erfolgt unter Windows und auch das Debugging-Frontend läuft auf Ihrem normalen Windows-Entwicklungsrechner. Zum Kompilieren und Debuggen auf TwinCAT/BSD wird eine SSH-Verbindung verwendet. Dieser Prozess kann in folgende Schritte aufgeteilt werden:

1. Synchronisieren Sie den Quellcode über SSH mit Hilfe von `rsync` vom Windows-Entwicklungsrechner zum TwinCAT/BSD-Zielsystem.
2. Kompilieren Sie die Applikation über eine SSH-Verbindung auf dem Zielsystem.
3. Debuggen Sie mit Hilfe von VSC über eine SSH-Verbindung zu `gdb`, das auf dem Zielsystem läuft.

Voraussetzungen:

- Stellen Sie sicher, dass folgende Pakete installiert sind:
 - `llvm`
 - `os-generic-userland-devtools`
 - `gdb`
 - `rsync`
- Installieren Sie OpenSSH für Windows: https://learn.microsoft.com/en-us/windows-server/administration/openssh/openssh_install_firstuse
- Erstellen Sie einen Benutzerschlüssel für den Entwicklungsrechner. Wir empfehlen den Algorithmus `ed25519` (`ssh-keygen -t ed25519`) https://learn.microsoft.com/en-us/windows-server/administration/openssh/openssh_keymanagement#user-key-generation
- Kopieren Sie den öffentlichen Schlüssel mit Hilfe der Powershell auf Ihr Zielsystem:


```
(Get-Content -Encoding UTF8 $home\.ssh\id_ed25519.pub).Replace("`r`n", "`n") | ssh Administrator@172.17.66.111 'cat >> ~/.ssh/authorized_keys'
```
- Installieren Sie die Remote-Debugging-Erweiterung VSC auf Ihrem Entwicklungsrechner:


```
(CTRL+p) ext install ms-vscode.cpptools
```
- Installieren Sie `cwrsync` unter `C:\Program Files\cwrsync` auf Ihrem Entwicklungsrechner. Diese Software ist eine `rsync`-Implementierung für Windows und ist beispielsweise erhältlich unter: <https://www.itefix.net/cwrsync>

VSC-Einstellungen:

Jetzt sind `cwrsync` und `ssh` verfügbar, und Sie können VSC weiter für das Remote-Debugging einrichten.

1. Beginnen Sie mit der Synchronisierung des Quellcodes. Vergewissern Sie sich, dass Sie einen Ordner `.vscode` in Ihrem Projektverzeichnis haben. Wählen Sie dann aus dem VSC-Menü:

```
Terminal->Configure Tasks...->Create tasks.json from template->Others
```

2. Passen Sie die folgende Vorlage entsprechend Ihrer Konfiguration an, um eine Task wie `sync-src-to-remote` zu erhalten.

```
{
  "version": "2.0.0",
  "windows": {
    "options": {
      "shell": {
        "executable": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
        "args": [
          "-NoProfile",
          "-ExecutionPolicy",
          "Bypass",
          "-Command"
        ]
      }
    }
  },
  "tasks": [
    {
      "label": "sync-src-to-remote",
      "type": "shell",
      "args": [
        "-aP",
        "--exclude",
        ".git",

```

```

    "--exclude",
    "This folder should be ignored",
    "-e", "c:''Program Files''/cwrsync/bin/ssh.exe -i ${userHome}/.ssh/id_ed25519 -o
'StrictHostKeyChecking no'",
    ".",
    "Administrator@172.17.66.111:~/${workspaceFolderBasename}/"
  ],
  "command": "c:/Program Files/cwrsync/bin/rsync.exe",
  "problemMatcher": []
}
]
}

```

3. Sie können die neue Task wie folgt testen:

Menu->Terminal->Run Task->sync-src-to-remote

4. Jetzt sollten Sie etwas im Terminal-Ausgabefenster sehen und die Quelldateien sollten auf Ihrem Zielsystem erscheinen. Wenn Sie "Permission denied"-Fehler sehen, versuchen Sie diese zusätzlichen rsync-Argumente:

```
--chmod=u=rwX --chmod=go=rX"
```

5. Wenn Sie einen anderen SSH-Port verwenden, fügen Sie ihn mit `-p <Port>` hinzu:

```
"c:''Program Files''/cwrsync/bin/ssh.exe -p 22222 -i ${userHome}/.ssh/id_ed25519 -o
'StrictHostKeyChecking no'"
```

6. Der nächste Schritt besteht darin, Ihre Applikation remote auf Ihrem Zielsystem zu erstellen. Fügen Sie eine weitere Task `build-on-remote` zu Ihrer `tasks.json` hinzu.

```

{
  "version": "2.0.0",
  "windows": {
    "options": {
      "shell": {
        "executable": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
        "args": [
          "-NoProfile",
          "-ExecutionPolicy",
          "Bypass",
          "-Command"
        ]
      }
    }
  },
  "tasks": [
    {
      "label": "sync-src-to-remote",
      "type": "shell",
      "args": [
        "-aP",
        "--exclude",
        ".git",
        "--exclude",
        "This folder should be ignored",
        "-e", "c:''Program Files''/cwrsync/bin/ssh.exe -i ${userHome}/.ssh/id_ed25519 -o
'StrictHostKeyChecking no'",
        ".",
        "Administrator@172.17.66.111:~/${workspaceFolderBasename}/"
      ],
      "command": "c:/Program Files/cwrsync/bin/rsync.exe",
      "problemMatcher": []
    },
    {
      "dependsOn": "sync-src-to-remote",
      "label": "build-on-remote",
      "group": "build",
      "type": "shell",
      "args": [
        "Administrator@172.17.66.111",
        "cd ${workspaceFolderBasename}; clang++ -g -Wall -pedantic main.cpp -o main. bin"
      ],
      "command": "ssh",
      "problemMatcher": []
    }
  ]
}

```

7. Dieses Mal können Sie `STRG+SHIFT+B` verwenden, um die neue `build-on-remote` Task auszuführen, da wir sie der Gruppe `build` hinzugefügt haben.

8. Fügen Sie eine Startkonfiguration hinzu, um Ihre Applikation remote zu debuggen. Wählen Sie im Menü:

Run->Add configuration

9. Bearbeiten Sie die launch.json Vorlage so, dass sie Ihren eigenen Anforderungen entspricht:

```
{
  "version": "0.2.0",
  "configurations": [
    {
      "name": "debug-on-remote",
      "type": "cppdbg",
      "request": "launch",
      "cwd": "/home/Administrator/${workspaceFolderBasename}",
      "preLaunchTask": "build-on-remote",
      "program": "main",
      "stopAtEntry": false,
      "externalConsole": false,
      "sourceFileMap": {
        "/home/Administrator/${workspaceFolderBasename}": "${workspaceFolder}"
      },
      "pipeTransport": {
        "debuggerPath": "/usr/bin/gdb",
        "pipeProgram": "ssh",
        "pipeArgs": [
          "Administrator@172.17.66.111"
        ]
      },
      "MIMode": "gdb",
      "setupCommands": [
        {
          "description": "Enable pretty-printing for gdb",
          "text": "-enable-pretty-printing",
          "ignoreFailures": true
        }
      ]
    }
  ]
}
```

10. Passen Sie ein paar Parameter an Ihre Anforderungen an:

program: should be the binary on your remote machine you want to debug
 pipeTransport->pipeArgs :username and ip address for your remote machine

Jetzt haben Sie eine launch.json Datei. Mit F5 wird ein Debugger ausgeführt, der mit Ihrem Programm auf dem Zielrechner verbunden ist.

Hinweis : Stellen Sie sicher, dass Sie mit aktivierten Debugsymbolen kompilieren ("-g").

12 TwinCAT 3

12.1 Zielsysteme suchen

Bevor Sie mit dem Industrie-PC arbeiten können, müssen Sie Ihren lokalen Rechner mit dem Industrie-PC verbinden. Danach können Sie den Industrie-PC mit Hilfe der IP-Adresse oder dem Host Namen suchen und anschließend als Zielsystem festlegen.

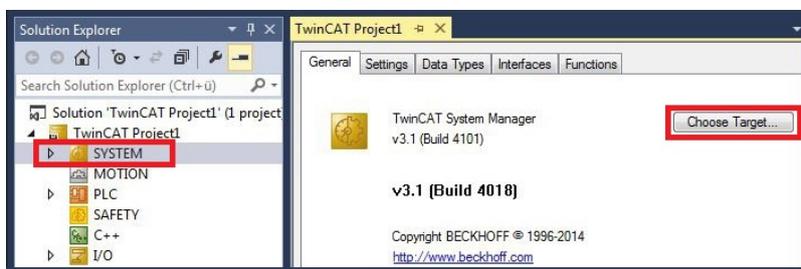
Dazu müssen der lokale PC und der Industrie-PC mit dem gleichen Netzwerk oder direkt über ein Ethernet-Kabel miteinander verbunden werden.

Voraussetzungen für diesen Arbeitsschritt:

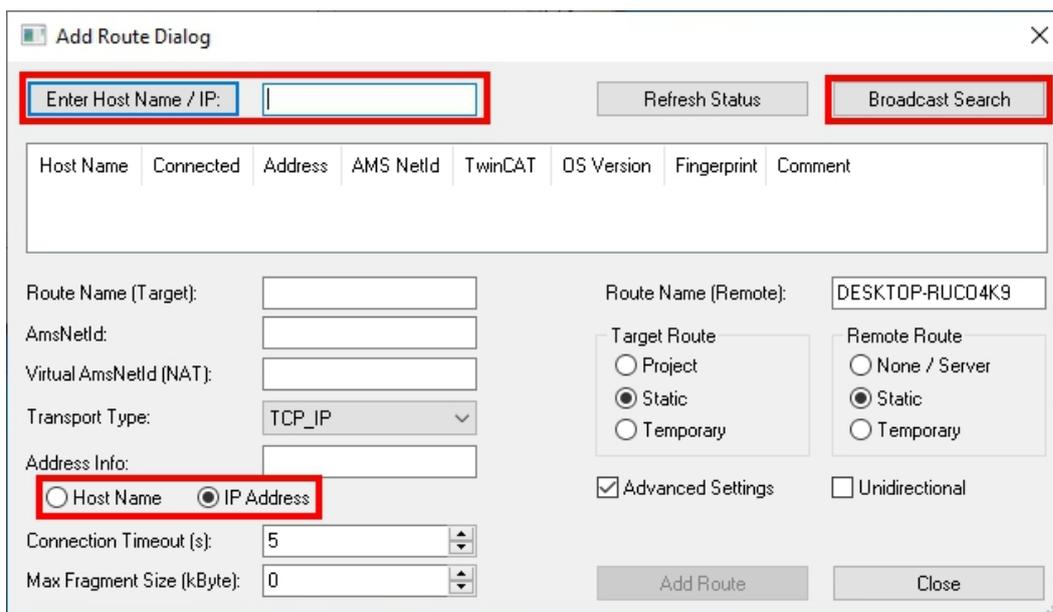
- TwinCAT 3 muss sich im Config Mode befinden.
- IP-Adresse oder Host Name des Industrie-PCs muss bekannt sein.

Suchen Sie wie folgt nach einem Zielsystem:

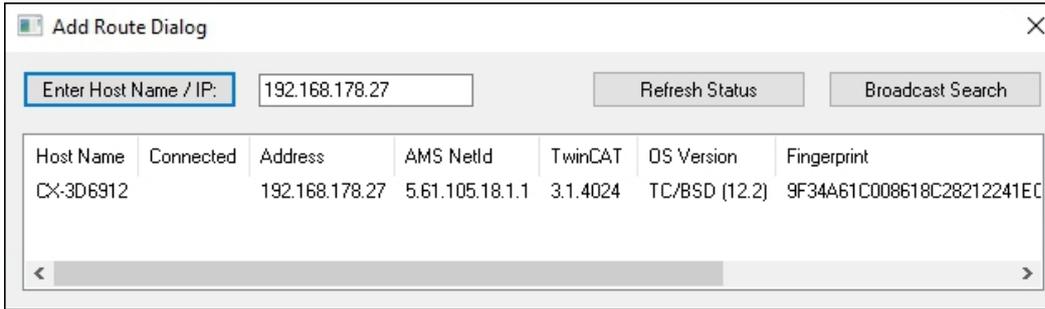
1. Klicken Sie oben im Menü auf **File > New > Project** und erstellen Sie ein neues TwinCAT XAE Projekt.
2. Klicken Sie links in der Strukturansicht auf **SYSTEM** und dann auf **Choose Target**.



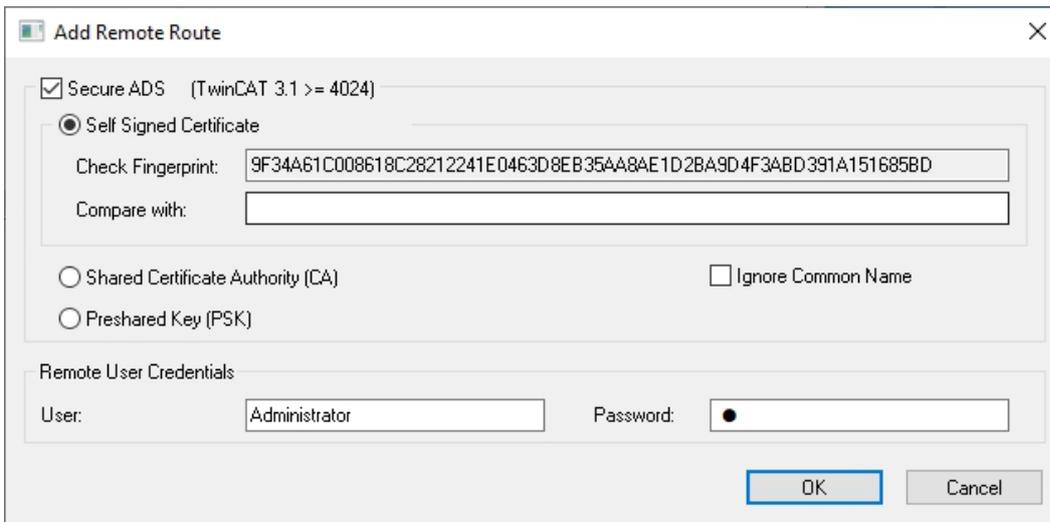
3. Klicken Sie auf **Search (Ethernet)**.
4. Benutzen Sie die Funktion **Broadcast Search**, um nach dem Industrie-PC zu suchen. Die Funktion **Broadcast Search** funktioniert nicht, wenn sich der lokale Rechner und der Industrie-PC nicht im selben Subnetz befinden. Geben Sie in dem Fall unter **Enter Host Name / IP** die IP-Adresse des Industrie-PCs ein und drücken Sie **[Enter]**.



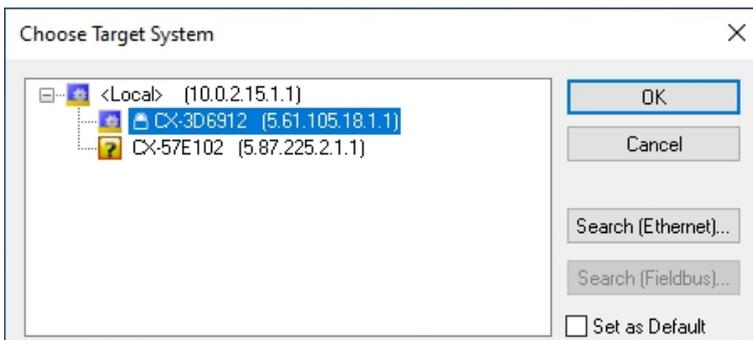
5. Markieren Sie den gewünschten Industrie-PC und klicken Sie auf **Add Route**.



6. Loggen Sie sich mit „Administrator“ und dem Passwort „1“ ein. Beachten Sie, dass standardmäßig nur Secure-ADS möglich ist. Für unverschlüsselte ADS-Verbindungen müssen Sie den entsprechenden ADS-Port in der Firewall öffnen (siehe: [Firewall](#) [▶ 35]).



7. Klicken Sie auf **Close**, wenn Sie keine weiteren Geräte suchen wollen und schließen damit das Add Route Fenster. Das neue Gerät wird im Fenster **Choose Target System** angezeigt.
8. Markieren Sie den Industrie-PC welchen Sie als Zielsystem festlegen wollen und klicken Sie auf **OK**.



- ⇒ Sie haben erfolgreich in TwinCAT nach einem Industrie-PC gesucht und als Zielsystem eingefügt. In der Menüleiste wird das neue Zielsystem mit dem Hostnamen angezeigt.



Mit dieser Vorgehensweise können Sie nach allen verfügbaren Geräten suchen und auch jederzeit zwischen den Zielsystemen wechseln. Als Nächstes können Sie den Industrie-PC scannen.

12.2 Geräte scannen

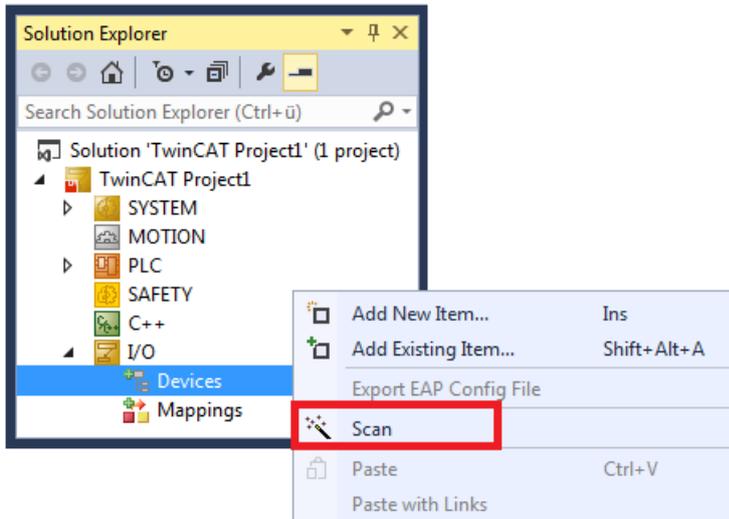
In diesem Arbeitsschritt wird gezeigt, wie Sie einen Industrie-PC in TwinCAT scannen und anschließend weiter konfigurieren.

Voraussetzungen für diesen Arbeitsschritt:

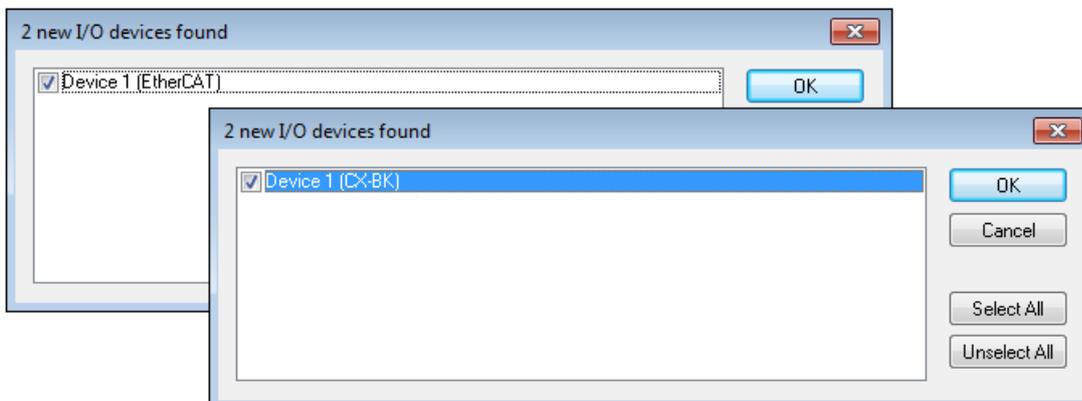
- Ein Industrie-PC wurde bereits als Zielsystem ausgewählt.

Fügen Sie den Embedded-PC wie folgt ein:

1. Starten Sie TwinCAT und öffnen Sie ein leeres Projekt.
2. Klicken Sie links in der Strukturansicht mit rechter Maustaste auf **I/O Devices**.
3. Klicken Sie im Kontextmenü auf **Scan**.



4. Wählen Sie Geräte, die Sie verwenden wollen und bestätigen die Auswahl mit **OK**. Es stehen immer Geräte zur Auswahl, die tatsächlich verfügbar sind.



Bei Embedded-PCs mit angeschlossenen Busklemmen (K-Bus) wird ein Buskoppler Device (CX-BK) angezeigt. Bei EtherCAT-Klemmen (E-Bus) wird der EtherCAT-Koppler angezeigt.

5. Bestätigen Sie die Anfrage mit **Ja**, um nach Boxen zu suchen.
 6. Klicken Sie bei der Anfrage, ob FreeRun aktiviert werden soll, auf **Ja**.
- ⇒ Der Industrie-PC wurde erfolgreich in TwinCAT gescannt und wird in der Strukturansicht mit den Ein- und Ausgängen angezeigt.

12.3 AMS NetID ändern

In diesem Arbeitsschritt wird gezeigt, wie Sie die AMS NetID des Industrie-PCs ändern können. Beachten Sie, dass Sie damit die Adresse des Industrie-PCs im TwinCAT-Netzwerk ändern. Die AMS NetID" besteht aus 6 Byte, wird in einer Punktnotation und im Hexadezimalsystem dargestellt.

Voraussetzungen:

- Zugriffsrechte auf die Datei *TcRegistry.xml*

Gehen Sie wie folgt vor:

1. Stoppen Sie den TcSystemService mit dem Befehl `doas service TcSystemService stop`
2. Geben Sie den Befehl `doas ee /usr/local/etc/TwinCAT/3.1/TcRegistry.xml` in der Konsole ein.

Die Datei *TcRegistry.xml* wird geöffnet.

```
<Value Name="CurrentVersion" Type="SZ">3.1</Value>
<Key Name="System">
  <Value Name="RunAsDevice" Type="DW">1</Value>
  <Value Name="AmsNetId" Type="BIN">053B151A0101</Value>
</Key>
```

3. Ändern Sie die AMS NetID unter dem Eintrag `<Value Name="AmsNetId" Type="BIN">053B151A0101</Value>`.
Der Eintrag `053B151A0101` entspricht folgender AMS NetID: 5.59.21.26.1.1
 4. Drücken Sie **[Esc]** und speichern Sie die Änderungen.
- ⇒ Sie haben die AMS NetID erfolgreich geändert. Starten Sie den TcSystemService erneut mit dem Befehl `doas service TcSystemService start`

12.4 TwinCAT in den Run- oder Config Modus versetzen

Sie können direkt aus TwinCAT/BSD heraus, also mit Hilfe der Konsole, TwinCAT in den Run- oder Config-Modus versetzen. Die Steuerung erfolgt über das Tool `TcSysExe.exe`, welches darüber hinaus Informationen zu Lizenzen, unterschiedlichen Versionen und System-IDs zur Verfügung stellt. Rufen Sie weitere Informationen mit `TcSysExe.exe --help` ab.

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `doas TcSysExe.exe --config` in der Konsole ein, um TwinCAT in den Config-Modus zu versetzen.
 2. Geben Sie den Befehl `doas TcSysExe.exe --run` in der Konsole ein, um TwinCAT in den Run-Modus zu versetzen.
- ⇒ Mit dem Befehl `TcSysExe.exe --mode` wird der aktuelle TwinCAT-Status in der Konsole angezeigt.

12.5 ADS-Routen manuell anlegen oder löschen

In diesem Schritt wird beschrieben, wie Sie direkt aus TwinCAT/BSD heraus eine ADS-Route manuell anlegen oder löschen können. Um ADS-Routen aus TwinCAT/BSD heraus zu konfigurieren, kann das Tool `ads` genutzt werden. Mit dem Befehl `ads` werden alle verfügbaren Parameter angezeigt. Bereits vorhandene ADS-Routen werden in der Datei `StaticRoutes.xml` aufgelistet.

Diese Einstellungen sind alternativ über das Webinterface des Beckhoff Device Managers möglich (siehe: [Beckhoff Device Manager: Webinterface](#) [► 69]).

Gehen Sie wie folgt vor:

1. Legen Sie die ADS-Route nach dem folgenden Muster an:

```
[<target[:port]>] [OPTIONS...] <command> [CMD_OPTIONS...] [<command_parameter>...]
```

2. Verwenden Sie unter `<target>` den Hostnamen, die IP-Adresse oder die Ams Net Id des Zielsystems, um eine neue ADS-Route anzulegen.

3. Verwenden Sie für `<command>` das Kommando `addroute` und folgende Optionen:

```
--addr=<hostname> or IP address of the routes destination
--netid=<AmsNetId> of the routes destination
--password=<password> for the user on the remote TwinCAT system
--username=<user> on the remote TwinCAT system (optional, defaults to Administrator)
--routename=<name> of the new route on the remote TwinCAT system (optional, defaults to --addr)
```

4. Geben Sie beispielsweise den Befehl `ads 192.168.0.231 addroute --addr=192.168.0.1 --netid=192.168.0.1.1.1 --password=1 --routename =example.beckhoff.com` in der Konsole ein.

- ⇒ Legen Sie neue ADS-Routen nach dem gezeigten Muster an oder löschen Sie die nicht benötigten ADS-Routen in der Datei `StaticRoutes.xml` unter den Einträgen `<Route>`.

```
---snipped---
<?xml version="1.0"?>
<TcConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <RemoteConnections>
    <Route>
      <Name>example.beckhoff.com</Name>
      <Address>192.168.0.1</Address>
      <NetId>192.168.0.1.1.1</NetId>
      <Type>TCP_IP</Type>
      <Flags>64</Flags>
    </Route>
    <Route>
      <Name>DESKTOP-RUCO4K9</Name>
      <Address>192.168.40.88</Address>
      <NetId>192.168.2.15.1.1</NetId>
      <Type>TCP_IP</Type>
      <Flags>64</Flags>
    </Route>
  </RemoteConnections>
</TcConfig>
---snipped---
```

12.6 Heap-Speicher erhöhen

HINWEIS

Überdimensionierter Heap-Speicher

Bei einem zu großen Heap-Speicher wird der gesamte Arbeitsspeicher allokiert, was das zu führt, dass das System nicht mehr richtig arbeitet. Achten Sie darauf, dass der Heap-Speicher im Verhältnis zum verfügbaren Arbeitsspeicher nicht zu groß gewählt wird.

Wenn der Heap-Speicher für den Download eines SPS-Projekts zu klein ist, wird ein entsprechender Fehler ausgegeben und der Vorgang abgebrochen.

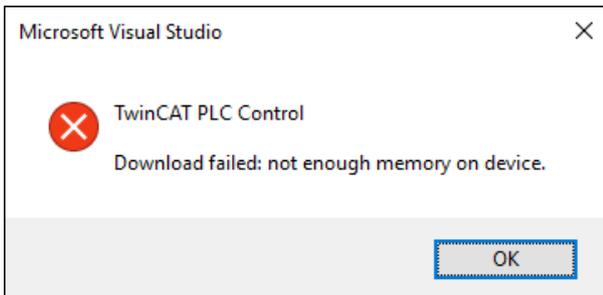


Abb. 31: Fehlermeldung bei einem zu kleinen Heap-Speicher.

Beim Aktivieren des TwinCAT-Projekts, bei dem sich das SPS-Projekt im AutoStart befindet, schaltet TwinCAT einfach zurück in den Config-Modus und es gibt keine Fehlermeldung oder Ähnliches.

Die Größe des Heap-Speichers wird nicht automatisch angepasst, kann aber unter TwinCAT/BSD für umfangreiche SPS-Projekte in der Datei `/usr/local/etc/TwinCAT/3.1/TcRegistry.xml` erhöht werden. Dazu muss die XML-Datei wie folgt erweitert werden:

```
Path: HKEY_LOCAL_MACHINE\SOFTWARE\BECKHOFF\TWINCAT3\SYSTEM
Entry: <Value Name="HeapMemSizeMB" Type="DW">{size in MB}</Value>
```

Gehen Sie wie folgt vor:

1. Stoppen Sie den TcSystemService mit dem Befehl `doas service TcSystemService stop`
2. Geben Sie den Befehl `doas ee /usr/local/etc/TwinCAT/3.1/TcRegistry.xml` in der Konsole ein. Die Datei `TcRegistry.xml` wird geöffnet.
3. Fügen Sie den Eintrag `<Value Name="HeapMemSizeMB" Type="DW">{size in MB}</Value>` unter `<Key Name="System">` in die XML-Datei ein.

```
---snipped---
<Key Name="System">
  <Value Name="RunAsDevice" Type="DW">1</Value>
  <Value Name="RTimeMode" Type="DW">0</Value>
  <Value Name="AmsNetId" Type="BIN">0542F70C0101</Value>
  <Value Name="LockedMemSize" Type="DW">33554432</Value>
  <Value Name="SysStartupState" Type="DW">5</Value>
  <Value Name="HeapMemSizeMB" Type="DW">1024</Value>
---snipped---
```

4. Die Größe wird in Megabyte festgelegt. In diesem Beispiel sind es 1024 MB.
 - ⇒ Starten Sie den TcSystemService erneut mit dem Befehl `doas service TcSystemService start`. Nachdem der Heap-Speicher auf 1024 MB erhöht wurde, startet das SPS-Projekt und der Download wird nicht mit einem Fehler abgebrochen.

12.7 Router-Speicher anpassen

Der Arbeitsspeicher wird von TwinCAT/BSD und von TwinCAT (TwinCAT-Speicher) verwendet. Der TwinCAT-Speicher unterteilt sich weiter in den Router-Speicher und den SPS-Speicher. Der Router-Speicher wird für die ADS-Kommunikation und der SPS-Speicher für das eigentliche SPS-Programm inklusive TcConfiguration, Mapping und Daten verwendet.

Eine Anpassung des Router-Speicher ist nur erforderlich, wenn eine große Menge an ADS-Kommunikation stattfindet und es aus diesem Grund notwendig wird, die Größe des Router-Speichers entsprechend auszuliegen. Standardmäßig wird der Router-Speicher in TwinCAT eingestellt. Der maximale Wert für den Router-Speicher beträgt 1024 MB.

Vergewissern Sie sich, dass der Heap-Speicher größer ist als der Router-Speicher und erhöhen Sie andernfalls den Heap-Speicher, bevor Sie den Router-Speicher anpassen (siehe: [Heap-Speicher erhöhen](#) [► 116]). In diesem Kapitel wird gezeigt, wie der Router-Speicher auch unter TwinCAT/BSD angepasst werden kann.

Dazu muss die XML-Datei unter `/usr/local/etc/TwinCAT/3.1/TcRegistry.xml` wie folgt angepasst werden:

```
Path: HKEY_LOCAL_MACHINE\SOFTWARE\BECKHOFF\TWINCAT3\SYSTEM
Entry: <Value Name="LockedMemSize" Type="DW">{size in Byte}</Value>
```

Gehen Sie wie folgt vor:

1. Stoppen Sie den TcSystemService mit dem Befehl `doas service TcSystemService stop`
2. Geben Sie den Befehl `doas ee /usr/local/etc/TwinCAT/3.1/TcRegistry.xml` in der Konsole ein. Die Datei `TcRegistry.xml` wird geöffnet.
3. Passen Sie den Eintrag `<Value Name="LockedMemSize" Type="DW">{size in Byte}</Value>` in der XML-Datei an.

```
---snipped---
<Key Name="System">
  <Value Name="RunAsDevice" Type="DW">1</Value>
  <Value Name="RTimeMode" Type="DW">0</Value>
  <Value Name="AmsNetId" Type="BIN">0542F70C0101</Value>
  <Value Name="LockedMemSize" Type="DW">33554432</Value>
  <Value Name="SysStartupState" Type="DW">5</Value>
  <Value Name="HeapMemSizeMB" Type="DW">1024</Value>
---snipped---
```

4. In in diesem Beispiel ist ein Wert von 33554432 Byte = 32 MB eingestellt. Ändern Sie den Wert beispielsweise auf 67108864 Byte, damit der Router-Speicher auf 64 MB erhöht wird.
- ⇒ Starten Sie den TcSystemService erneut mit dem Befehl `doas service TcSystemService start`.

12.8 Isolierte Kerne zuweisen

Bei Multicore-Systemen bietet TwinCAT 3 die Möglichkeit, einzelne Kerne zu isolieren. Damit können verschiedene TwinCAT-Tasks einem für die Echtzeitnutzung isolierten Kern zugewiesen werden. In diesem Abschnitt wird gezeigt, wie isolierte Kerne in der TwinCAT/BSD-Konsole eingestellt werden.

Voraussetzungen:

- Ein Multicore-Industrie-PC. Ein CPU-Kern (Shared) für TwinCAT/BSD und drei CPU-Kerne (Isolated) sollen für unterschiedliche TwinCAT-Tasks zur Verfügung stehen.

Gehen Sie wie folgt vor:

1. Mit dem Befehl `TcCoreConf` lässt sich eine Übersicht der verfügbaren Kerne und ihrer Festlegung Shared/Isolated ausgeben.
 2. Geben Sie den Befehl `doas TcCoreConf -s 1` in der Konsole ein. Damit wird ein CPU-Kern (Shared) für TwinCAT/BSD festgelegt. Die restlichen drei CPU-Kerne werden isoliert.
 3. Starten Sie den Industrie-PC mit dem Befehl `shutdown -r now neu`, damit die Einstellungen übernommen werden.
 4. Anschließend können Sie sich mit dem Befehl `sysctl hw.ncpu` die Anzahl der CPU-Kerne (Shared) anzeigen lassen.
- ⇒ Sie haben erfolgreich einen CPU-Kern (Shared) und drei CPU-Kerne (Isolated) konfiguriert. Mit dem Befehl `TcCoreConf` können die Einstellungen kontrolliert werden. Die aktuellen Einstellungen können Sie auch in TwinCAT 3 (XAE) vom Industrie-PC auslesen. Klicken Sie dafür unter **Real-Time** auf die Schaltfläche **Read from Target**.

CPU	RT-CPU	Base Time	CPU Limit	Latency Warning
0 (Windows)	✓ Default	1 ms	80 %	(none)
1 (Isolated)	✓	1 ms	100 %	(none)
2 (Isolated)	✓	1 ms	100 %	20 µs
3 (Isolated)	✓	1 ms	100 %	20 µs

Object	RT-CPU	Base Time (ms)	Cycle Time (ms)	Cycle Ticks	Priority
PlcTask	Default (0)	1 ms	10 ms	10	1
I/O Idle Task	Default (0)	1 ms	1 ms	1	11
PlcTask1	Default (0)	1 ms	10 ms	10	20
PlcAuxTask	Default (0)	1 ms	(none)	0	50

Mit `TcCoreConf --help` werden alle verfügbaren Befehle angezeigt. Mit `doas TcCoreConf -d` können z.B. alle CPU-Kerne wieder auf „Shared“ zurückgesetzt werden.

```
Administrator@CX-3B151A:~ % TcCoreConf -help
TcCoreConf:
-s --set CPUs
    set number of shared cores
-d --delete
    set all cores as shared core
-f NAME, --file NAME
    set name of configuration file to change
--rsdp ADDR
    set pointer for RSDP
--show
    show active settings of shared/isolated cores
--strip
    remove hints of unknown apic-ids
--noflat
    don't add flat cpu topology setting
```

13 Wiederherstellungsoptionen

Definieren Sie eine Backup- und Wiederherstellungsstrategie für Ihr TwinCAT/BSD-System, um im Falle eines Datenverlustes oder bei defekten Speichermedien TwinCAT/BSD in sehr kurzer Zeit wiederherstellen zu können. Backups tragen dazu bei, Ausfallzeiten zu minimieren und auf diese Weise die Arbeit ohne große Produktionsverluste fortzusetzen. Es sollte sowohl ein Prozess für die Erstellung einer Sicherheitskopie als auch ein Prozess für deren Wiederherstellung definiert werden. Dabei sollten auch Security-Aspekte berücksichtigt werden und beispielsweise definiert werden, wo das Backup gespeichert werden soll.

Beckhoff bietet mit dem TwinCAT/BSD-Installer-Stick eine einfache Backup-Lösung an. Zusätzlich dazu sind mit dem Programm `restorepoint` Wiederherstellungspunkte unter TwinCAT/BSD möglich, welche den aktuellen Zustand des Systems speichern und bei Bedarf wiederherstellen. Eine Vielzahl von Implementierungen ist somit verfügbar, wobei die genaue Definition einer Backup- und Wiederherstellungsstrategie dem Anwender überlassen ist.

Folgende Szenarien sind möglich und sollen dazu dienen, die unterschiedlichen Funktionsweisen zu verstehen. Die vorgestellten Szenarien sollten jedoch nicht als der von Beckhoff empfohlene und einzige Weg betrachtet werden.

Szenario 1: Werkseinstellungen

Ein Industrie-PC mit TwinCAT/BSD soll bei einem Problem auf Werkseinstellungen zurückgesetzt werden.

- Der Anwender testet und entwickelt auf einem Industrie-PC mit TwinCAT/BSD.
- In der Test- und Entwicklungsphase gibt es ein Problem, weil beispielsweise grundlegende Einstellungen verändert wurden.
- Der Anwender löst das Problem, indem TwinCAT/BSD auf Werkseinstellungen zurückgesetzt wird (siehe: [Auf Werkseinstellungen zurücksetzen \[► 120\]](#)).

Szenario 2: Serienproduktion

Die Test- und Entwicklungsphase wurde erfolgreich abgeschlossen. Der Maschinenbauer will in die Serienproduktion gehen:

- Der Maschinenbauer erstellt einen Wiederherstellungspunkt (Auslieferungszustand OEM), um das System bei einem Fehler wiederherstellen zu können (siehe: [Wiederherstellungspunkt erstellen \[► 121\]](#)). Der Endkunde des Maschinenbauers kann diesen Wiederherstellungspunkt seinerseits bei Problemen nutzen.
- Anschließend aktiviert der Maschinenbauer den Write Filter, um TwinCAT/BSD im vorkonfigurierten Zustand zu sichern und um eine Fehlkonfiguration beim Endkunden zu verhindern (siehe: [Write Filter \[► 29\]](#)).
- Im letzten Schritt erstellt der Maschinenbauer ein Backup, welches er als Masterimage ablegt und für die Serienproduktion nutzt (siehe: [Backup erstellen \[► 123\]](#)).

Szenario 3: Inbetriebnahme beim Endkunden

Die Maschine kommt beim Endkunden an und soll nach der Inbetriebnahme abgesichert werden:

- Nach der Parametrierung der Maschine erstellt der Endkunde einen Wiederherstellungspunkt „Inbetriebnahme“ (siehe: [Wiederherstellungspunkt erstellen \[► 121\]](#)).
- Anschließend aktiviert der Endkunde den Write Filter, um eine versehentliche Fehlkonfiguration zu vermeiden (siehe: [Write Filter \[► 29\]](#)).
- Der Endkunde erstellt ein eigenes Backup (siehe: [Backup erstellen \[► 123\]](#)), um beispielsweise im Fall eines defekten Datenträgers das System wiederherstellen zu können (siehe: [Backup wiederherstellen \[► 124\]](#)).

13.1 Wiederherstellungspunkt

Wiederherstellungspunkte dienen dazu, einen alten Systemstand wiederherzustellen, wenn TwinCAT/BSD nach einer größeren Systemänderung oder einer Fehlkonfiguration ein unerwünschtes Verhalten aufweist und sich dieses Verhalten nicht leicht beheben lässt. Der Vorteil von Wiederherstellungspunkten ist, dass auf diese Weise Konfigurationsfehler einfach und schnell rückgängig gemacht werden, ohne TwinCAT/BSD neu zu installieren.

Den Zeitpunkt für die Erstellung eines Wiederherstellungspunktes legen Sie fest, wenn Sie beispielsweise eine größere Systemänderung vornehmen oder Programme von Drittanbietern installieren. Wiederherstellungspunkte ersetzen jedoch kein vollständiges Backup und schützen nicht vor Datenverlust. Regelmäßige Backups sind eine weitere Schutzmaßnahme, mit der Sie sich beispielsweise vor Datenverlust durch defekte Speichermedien schützen können (siehe: [Backup erstellen \[► 123\]](#)).

Die Wiederherstellungspunkte werden in der Konsole mit dem Programm `restorepoint` erstellt und verwaltet. Folgende Modi werden vom Programm unterstützt:

- `status`: Listet alle verfügbaren Wiederherstellungspunkte auf. Bei Auslieferung ist ein Wiederherstellungspunkt mit dem Namen `factoryreset`, die Beckhoff Werkseinstellungen, verfügbar.
- `create`: Erstellt einen neuen Wiederherstellungspunkt. Der Name des Wiederherstellungspunktes kann als Argument festgelegt werden. Wenn kein Name angegeben wird, wird ein automatisch generierter Name verwendet.
- `rollback`: Rückkehr zu einem bestimmten Wiederherstellungspunkt. Beachten Sie, dass alle Daten, die nach dem Wiederherstellungspunkt erstellt wurden, zerstört werden. Wenn kein Wiederherstellungspunkt als Argument angegeben wird, wird der Benutzer mit einem interaktiven Dialog gefragt.
- `destroy`: Der angegebene Wiederherstellungspunkt wird zerstört. In diesem Modus bleiben alle vorhandenen Daten erhalten, der Wiederherstellungspunkt selbst wird aber gelöscht.

Wiederherstellungspunkte unter TwinCAT/BSD basieren auf ZFS-Snapshots. Dadurch verbrauchen sie bei ihrer Erstellung kaum Speicherplatz. Jede Änderung des gespeicherten Wiederherstellungspunktes zum aktuellen Live-System, mit dem der Anwender arbeitet, spiegelt sich im verbrauchten Speicherplatz des Wiederherstellungspunktes wieder. Lassen sie sich mit `zfs list -t snap` alle Snapshots des Systems anzeigen.

Die Spalte `USED` zeigt den real verbrauchten Speicherplatz des Snapshots, die Spalte `REFER` zeigt den Speicherplatz, auf den der Snapshot verweist, der aber real in anderen Datensets gespeichert ist. Es empfiehlt sich also immer vor einer Änderung im System einen Wiederherstellungspunkt zu erstellen, da dies kaum Systemressourcen kostet. Nach einiger Zeit und vielen Änderungen zwischen Wiederherstellungspunkt und Live-System empfiehlt es sich nicht mehr benötigte Wiederherstellungspunkten zu löschen, um den anwachsenden Speicherplatz der Wiederherstellungspunkte wieder freizugeben.

13.1.1 Auf Werkseinstellungen zurücksetzen

Sie können TwinCAT/BSD jederzeit auf Werkseinstellungen zurücksetzen und den Auslieferungsstand wiederherstellen, wenn das System beispielsweise nach einer Fehlkonfiguration nicht mehr richtig funktioniert.

Die Wiederherstellungspunkte werden in der Konsole mit dem Programm `restorepoint` erstellt und verwaltet. In diesem Abschnitt wird gezeigt, wie Sie TwinCAT/BSD auf Werkseinstellungen zurücksetzen.

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `doas restorepoint rollback factoryreset` in der Konsole ein.
 2. Es werden alle Snapshots angezeigt, auf die das System zurückgesetzt wird.
 3. Bestätigen Sie die Wiederherstellung mit `[y]`.
- ⇒ Das System wird auf Werkseinstellungen zurückgesetzt. Nach einem Neustart befindet sich TwinCAT/BSD wieder im Auslieferungszustand.

13.1.2 Wiederherstellungspunkt erstellen

● Speicherplatzverbrauch durch Wiederherstellungspunkte

i Ein Wiederherstellungspunkt verbraucht Speicherplatz, weil das komplette System gesichert wird, darunter auch Kernel-Dumps unter `/var/crash`. Räumen Sie das System vor der Erstellung eines Wiederherstellungspunktes auf oder löschen Sie alte Wiederherstellungspunkte.

Wiederherstellungspunkte dienen dazu, einen alten Systemstand wiederherzustellen, wenn TwinCAT/BSD nach einer größeren Systemänderung oder einer Fehlkonfiguration nicht mehr richtig funktioniert. Erstellen Sie Wiederherstellungspunkte, wenn Sie größere Systemänderungen vornehmen, Programme installieren oder Tests durchführen wollen.

Die Wiederherstellungspunkte werden in der Konsole mit dem Programm `restorepoint` erstellt und verwaltet. In diesem Abschnitt wird gezeigt, wie Sie Wiederherstellungspunkte unter TwinCAT/BSD erstellen.

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `doas restorepoint create` in der Konsole ein.
2. Der Wiederherstellungspunkt wird mit einem automatisch generierten Namen erstellt.
3. Überprüfen Sie die Erstellung des Wiederherstellungspunktes mit dem Befehl `restorepoint status` und lassen Sie sich alle Wiederherstellungspunkte anzeigen.

```
Administrator@CX-4FAA38$ restorepoint status
last BE: zroot/ROOT/default
factoryreset
2020-08-28T08:56:14Z
2020-08-28T09:03:05Z
```

4. Benutzen Sie alternativ den Befehl `doas restorepoint create your-restorepoint` um einen eigenen Namen für den Wiederherstellungspunkt festzulegen.

⇒ Der Wiederherstellungspunkt wird erstellt und kann jederzeit genutzt werden, um das System zurückzusetzen (siehe: [Auf Wiederherstellungspunkt zurücksetzen \[► 121\]](#)).

```
Administrator@CX-4FAA38$ restorepoint status
last BE: zroot/ROOT/default
factoryreset
2020-08-28T08:56:14Z
2020-08-28T09:03:05Z
your-restorepoint
```

13.1.3 Auf Wiederherstellungspunkt zurücksetzen

HINWEIS

Datenverlust

Daten und Wiederherstellungspunkte, die nach einem bestimmten Wiederherstellungspunkt erstellt wurden, werden beim Zurücksetzen eines davor liegenden Wiederherstellungspunktes gelöscht.

Sollte TwinCAT/BSD nach einer Fehlkonfiguration nicht mehr richtig funktionieren, dann können Sie diese Konfigurationsfehler mit Hilfe von Wiederherstellungspunkten einfach und schnell rückgängig machen, ohne TwinCAT/BSD neu zu installieren.

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `restorepoint status` in der Konsole ein, um sich alle verfügbaren Wiederherstellungspunkte anzuzeigen.

```
Administrator@CX-4FAA38$ restorepoint status
last BE: zroot/ROOT/default
factoryreset
2020-08-28T08:56:14Z
2020-08-28T09:03:05Z
your-restorepoint
```

2. Geben Sie den Befehl `doas restorepoint rollback` in der Konsole ein, um alle vorhandenen Wiederherstellungspunkte zu sehen.
3. Wählen Sie einen Menüpunkt, um das System auf einen bestimmten Wiederherstellungspunkt zurückzusetzen.

```
Administrator@CX-4FAA38~ $ doas restorepoint rollback
Password:
 1 factoryreset
 2 2020-08-28T08:56:14Z
 3 2020-08-28T09:03:05Z
 4 your-restorepoint
```

4. Es werden alle Snapshots angezeigt, auf die das System zurückgesetzt wird.
5. Bestätigen Sie die Wiederherstellung mit **[y]**.
⇒ TwinCAT/BSD wird auf den Wiederherstellungspunkt zurückgesetzt und neu gestartet. Beachten Sie, dass Daten und Wiederherstellungspunkte, die nach dem gewählten Wiederherstellungspunkt erstellt wurden, beim Zurücksetzen gelöscht werden.

13.1.4 Restore-Bootumgebung einsetzen

Sie haben die Möglichkeit einen Wiederherstellungspunkt aus der Restore-Bootumgebung wiederherzustellen, wenn TwinCAT/BSD nicht mehr bootet und dadurch die Konsole unzugänglich ist. Starten Sie dazu das Bootmenü während des Bootvorgangs, um in die Restore-Bootumgebung zu wechseln.

Gehen Sie wie folgt vor:

1. Starten Sie den Industrie-PC.
2. Halten Sie beim Booten die **[Leertaste]** gedrückt. Das Bootmenü erscheint.

```
REHPOT SIRHCCR AMMAIT SI RH CN AI LUJSNE JOKIEHL PGSLINO
IR AM KN AR FN EF FE TS SN AH LE AF
ARLEIN ADKCI RT APGNI NNEHDRA HC IR ETLAM NOMAR
EI NO EL OR IM AR XA MN IT RA MR UH
TRAERD NASUALK OKZTIE RA WT FU SN EGALDN UR G#
New Automation Technology

Welcome to TC/BSD

1. Boot Multi user [Enter]
2. Boot Single user
3. Escape to loader prompt
4. Reboot
5. Cons: Video

Options:
6. Kernel: default/kernel (1 of 1)
7. Boot Options
8. Boot Environments
9. Rollback restorepoint
```

3. Wählen Sie die Option **Rollback restorepoint**.
⇒ TwinCAT/BSD wird in der Restore-Bootumgebung gestartet. Jetzt können Sie die Werkseinstellungen mit dem Befehl `restorepoint rollback factoryreset` wiederherstellen oder einen eigens erstellten Wiederherstellungspunkt nutzen (siehe: [Auf Wiederherstellungspunkt zurücksetzen](#) ► [121](#))).

13.2 Backup und Restore

Im Gegensatz zu einem Wiederherstellungspunkt kann bei einem Backup TwinCAT/BSD als Sicherheitskopie auf einem externen Speichermedium gespeichert und verwaltet werden.

Diese Sicherheitskopie kann dazu benutzt werden, um das System im Fall eines Systemausfalls bzw. eines Datenverlustes wiederherzustellen. Erstellen Sie regelmäßig Backups von Ihrem System, um Ihren Industrie-PC wieder auf den Stand zurücksetzen zu können, den er zum Zeitpunkt des Backups hatte.

13.2.1 Backup erstellen

Sie können ein Backup mit Hilfe des TwinCAT/BSD-Installer-Sticks erstellen und wiederherstellen. Alle Backups werden auf einer FAT32-Partition auf dem USB-Stick gespeichert. FAT32 ist interoperabel mit Windows und FreeBSD®. Dadurch können die erstellten Backups sowohl mit einem TwinCAT/BSD-System als auch mit einem Windows-System verwaltet werden.

Voraussetzungen:

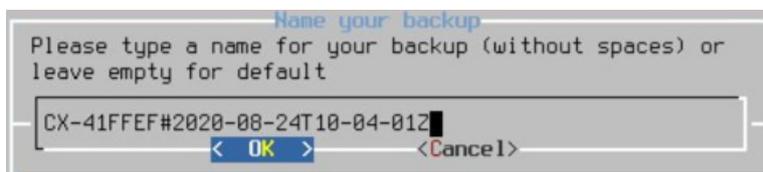
- TwinCAT/BSD-Installer-Stick (siehe: [Bootfähigen USB-Stick erstellen](#) [► 19]).

Erstellen Sie ein Backup wie folgt:

1. Schließen Sie den TwinCAT/BSD-Installer-Stick an den Industrie-PC an.
2. Booten Sie den Industrie-PC vom TwinCAT/BSD-Installer-Stick.
3. Öffnen Sie das Bootmenü mit **[F7]**. Wenn der Industrie-PC nicht automatisch vom USB-Stick booten sollte.
4. Wählen Sie den UEFI-Eintrag für den USB-Stick aus und bestätigen mit **[Enter]**. Der Industrie-PC bootet vom USB-Stick und der Beckhoff TwinCAT/BSD-Installer wird ausgeführt.
5. Wählen Sie die Option **Backup**.



6. Vergeben Sie einen Dateinamen für das Backup oder übernehmen Sie den Standardnamen aus Hostnamen und Zeitstempel.



7. Wählen Sie die Option **Reboot** für einen Neustart, sobald das Backup fertiggestellt wurde.
 - ⇒ Die Backups werden mit dem jeweiligen Dateinamen auf dem USB-Stick gespeichert. Archivieren Sie die Backups auf dem USB-Stick. Sie können die Backups auch auf ein externes Speichermedium kopieren oder im Netzwerk archivieren.

13.2.2 Backup wiederherstellen

● Geeignete Backups für die Wiederherstellung verwenden

i Ein Backup darf nur auf einem Gerät innerhalb einer Serie, z.B. CX51x0, CX20x3, C6015 usw., wiederhergestellt werden, da sonst Inkompatibilitäten auftreten können, wenn das Backup auf einem Gerät einer anderen Serie wiederhergestellt wird.

Sie können ein Backup mit Hilfe des TwinCAT/BSD-Installer-Sticks wiederherstellen. Dazu muss der Industrie-PC vom TwinCAT/BSD-Installer-Stick gebootet werden.

Voraussetzungen:

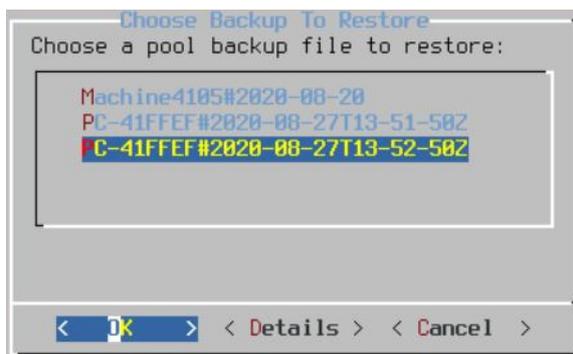
- TwinCAT/BSD-Installer-Stick (siehe: [Bootfähigen USB-Stick erstellen \[► 19\]](#)).

Gehen Sie wie folgt vor:

1. Schließen Sie den TwinCAT/BSD-Installer-Stick an den Industrie-PC an.
2. Booten Sie den Industrie-PC vom TwinCAT/BSD-Installer-Stick.

Öffnen Sie das Bootmenü mit [F7], wenn der Industrie-PC nicht automatisch vom USB-Stick booten sollte.

3. Wählen Sie den UEFI-Eintrag für den USB-Stick aus und bestätigen mit **[Enter]**. Der Industrie-PC bootet vom USB-Stick und der Beckhoff TwinCAT/BSD-Installer wird ausgeführt. Wählen Sie die Option **Restore**.
4. Wählen Sie das Backup, welches auf dem Industrie-PC wiederhergestellt werden soll.



⇒ Starten Sie den Industrie-PC nach der Wiederherstellung neu. Der Industrie-PC ist wieder auf dem Stand, den er zum Zeitpunkt des Backups hatte.

13.2.3 Backup aus Live-System erstellen und wiederherstellen

Wenn es ihre Applikation erfordert, können Backups auch aus dem Live-System heraus und ohne TwinCAT/BSD-Installer-Stick erstellt und wiederhergestellt werden. Benutzen Sie dazu die Skripte TcBackup und TcRestore.

Erstellen Sie ein Backup aus dem laufenden System nur dann, wenn das System zum Zeitpunkt des Backups nicht auf den Datenträger schreibt. Ein Backup kann beschädigt werden, wenn das System während des Backups schreibend auf den Datenträger zugreift. Stellen Sie also sicher, dass keine Prozesse laufen, die persistent Daten sichern und dass die Datenträger, auf der Sie ihr Backup wiederherstellen wollen, groß genug ist.

Das Ausführen von TcBackup und TcRestore sowie das Schreiben in und aus der Datei, in der das Backup gesichert wird, muss mit Root-Rechten geschehen. Führen Sie also vorher eine Shell mit Root-Rechten aus, in der Sie dann arbeiten, oder führen Sie den einzelnen Befehl als einen String mit einer Shell mit Root-Rechten aus. Letzteres wird in den nachfolgenden Beispielen gezeigt.

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `doas sh -c "TcBackup.sh --disk /dev/ada0 > backup.tcbkp00"` ein, um ein Backup vom Datenträger ada0 in die Datei Backup.tcbkp00 zu erstellen.
2. Geben Sie den Befehl `doas sh -c "TcRestore.sh --disk /dev/ada1 < backup.tcbkp00"` ein, um ein Backup aus der Datei Backup.tcbkp00 auf dem Datenträger ada1 wiederherzustellen.

- ⇒ Sie können beide Befehle kombinieren. Mit dem Befehl `doas sh -c "TcBackup.sh --disk /dev/ada0 | TcRestore.sh --disk /dev/ada1"` wird ein Backup vom Datenträger `ada0` erstellt und sofort auf dem Datenträger `ada1` wiederhergestellt.

14 Fehlerbehandlung und Diagnose

14.1 Kernelmeldungen für Diagnose nutzen

Sie können Kernelmeldungen für eigene Diagnosezwecke oder für den Beckhoff Support einschalten. Die Kernelmeldungen werden beim Booten von TwinCAT/BSD angezeigt und bleiben an der Fehlerstelle stehen. Dadurch können Sie oder der Beckhoff Support Fehler lokalisieren.

Voraussetzungen:

- Neustart erforderlich. Die Kernelmeldungen können immer nur beim Booten eingeschaltet werden.

Gehen Sie wie folgt vor:

1. Starten Sie den Industrie-PC.
 2. Drücken Sie während des Bootvorgangs die **[Leertaste]**.
Der Bootvorgang wird angehalten.
 3. Drücken Sie die Taste **[6]** und wählen damit die Option **6. Boot Options**.
Das Menü **Boot Options** erscheint.
 4. Drücken Sie die Taste **[5]** und aktivieren damit die Option **5. Verbose: on**.
 5. Drücken Sie **[Enter]**, um den Vorgang abzuschließen.
- ⇒ TwinCAT/BSD wird weiter gebootet und die Kernelmeldungen werden angezeigt. Diese Einstellungen werden nicht gespeichert. Wiederholen Sie die gezeigten Arbeitsschritte, wenn Sie die Kernelmeldungen beim nächsten Start wieder benötigen.

14.2 Logdateien

Kernel-, Security- und TwinCAT-Logs können für Diagnosezwecke genutzt werden und befinden sich in folgenden Verzeichnissen.

Allgemeiner Kernel-Log

`/var/log/messages`

Öffnen Sie den Kernel-Log mit folgendem Befehl:

```
cat /var/log/messages
```

Security-Log

`/var/log/security`

Öffnen Sie den Security-Log mit folgendem Befehl:

```
doas cat /var/log/security
```

Filtern Sie die Ausgabe von `cat` mit dem Pipe-Operator und dem Programm `grep`. Der Pipe-Operator übergibt die Ausgabe von `cat` an das Programm `grep`, welches seinen Input nach einem Ausdruck filtern kann. Verwenden Sie den Ausdruck `cat /var/log/messages | grep -i tc` um nach allen TwinCAT relevanten Daten zu filtern. Durch die Option `-i` wird die Groß- und Kleinschreibung nicht beachtet.

Mit dem Programm `less` können Textdateien ausgegeben und durchsucht werden. Mit **[&]** lässt sich beispielsweise die Suchfunktion starten. Mit **[h]** werden Infos zu weiteren Funktionen zu angezeigt. Mit **[q]** beendet sich das Programm.

Ein weiteres nützliches Programm im Hinblick auf Logdateien ist `tail`. Hier werden nur die letzten Einträge ausgegeben. Dies ist es vor allem dann sinnvoll, wenn nur die aktuellsten Log-Einträge von Interesse sind. Mit dem Befehl `tail -5 /var/log/messages` werden die letzten fünf Einträge der Logdatei ausgegeben.

14.3 Dumps

Kernel-Dump

Der Kernel-Dump befindet sich unter:

`/var/crash`

14.3.1 Automatischen Prozess-Dump nutzen

Sobald ein Prozess abstürzt, wird automatisch ein Memory-Dump erzeugt und in der Datei `progname.core` gespeichert. Die Datei enthält den vollständigen Zustand des Prozesses beim Absturz. Die Datei wird meistens dort abgelegt, wo der User-Mode Prozess liegt: `/usr/local/bin`

Die Datei kann anschließend mit einem Debugger, beispielsweise `gdb`, analysiert werden. Im Folgenden wird die lokale Analyse des Dumps direkt auf dem TwinCAT/BSD-System beschrieben. Die Analyse kann natürlich auch mit entsprechenden Programmen auf dem Windows-Entwicklungsrechner erfolgen. Kopieren Sie hierfür den Dump beispielsweise mit WinSCP auf ihren Windows Rechner.

Voraussetzungen:

- Installieren Sie den Debugger `gdb` mit `pkg install gdb`.

Gehen Sie wie folgt vor:

1. Navigieren Sie zum passenden Verzeichnis, wenn Sie sich nicht im gleichen Verzeichnis wie die Datei mit dem Prozess-Dump befinden.
 2. Geben Sie den Befehl `gdb -c <filename>` in die Konsole ein, um einen Prozess-Dump zu untersuchen.
- ⇒ Geben Sie `help` ein, um sich weitere Informationen über den Namen des GDB-Befehls oder allgemeine Informationen über GDB anzuzeigen.

14.3.2 Prozess-Dump manuell erzeugen

Benutzen Sie das Programm `gcore`, wenn Sie beispielsweise störanfällige Programme untersuchen wollen oder sich Ihr Industrie-PC in einer Endlosschleife oder Ähnliches befindet. Der Prozess-Dump ist besonders nützlich, um einen Snapshot eines laufenden Prozesses zu erstellen und Prozesse unter TwinCAT/BSD zu analysieren.

Standardmäßig wird der Prozess-Dump in die Datei `core.pid` geschrieben. Die Datei kann anschließend mit einem Debugger, beispielsweise `gdb`, analysiert werden.

Gehen Sie wie folgt vor:

1. Ermitteln Sie die Prozess-ID (`pid`) des gewünschten Prozesses mit dem Befehl `pgrep -l <processname>`. Mit `ps -A` können Sie alle Prozesse auflisten.
2. Geben Sie den Befehl `gcore <pid>` in der Konsole ein. Beispiel: `gcore 6674`
3. Der Befehl `gcore 6674` generiert eine Datei mit dem Namen `core.6674`

⇒ Die Datei wird im aktuellen Verzeichnis angelegt. Diese Datei kann anschließend mit einem Debugger gelesen und analysiert werden. Mit der Option `-c` können Sie einen eigenen Dateinamen festlegen.
Beispiel: `gcore -c testfile 6674`

14.3.3 Systeminformationen zur Analyse bereitstellen

Mit dem Tool `bhinfo` können verschiedene Systeminformationen gesammelt und beispielsweise als ZIP-Datei zur Auswertung an den Beckhoff Support geschickt werden. Die ZIP-Datei enthält unter anderem verschiedene Versionsinformationen sowohl zu TwinCAT/BSD als auch zu TwinCAT. Es werden Informationen über installierte Pakete, laufende Prozesse, Netzwerkkonfiguration, Konfigurationsdateien und vieles mehr geliefert.

1. Geben Sie den Befehl `doas bhinfo /home/Administrator/FileOutput` in der Konsole ein.

- ⇒ Die Datei `FileOutput` wird im Verzeichnis `/home/Administrator/` gespeichert.
- 2. Verwenden Sie beispielsweise [WinSCP \[► 73\]](#), um die ZIP-Datei auf Ihren Windows-Entwicklungsrechner zu kopieren.
- ⇒ Die ZIP-Datei stellt wichtige Systeminformationen gebündelt zur Verfügung und kann zur Auswertung an den Beckhoff Support geschickt werden.

14.4 ADS-Monitor einsetzen

Der TwinCAT ADS-Monitor ist in zwei Applikationen aufgeteilt. Der AMS-Logger zeichnet die AMS-Kommandos auf, der AMS-Viewer zeigt die aufgezeichneten Daten an oder kann den AMS-Logger fernsteuern.

Der AMS-Logger wird mit dem Programm `tcamslog` aufgerufen und konfiguriert. Zusätzliche Parameter legen beispielsweise fest, wie groß die Logdatei maximal werden kann oder ob ein Ringbuffer verwendet werden soll.

Tab. 8: ADS-Monitor, Parameter der `tcamslog` Applikation.

Parameter	Beschreibung
-l	<code>listen</code> Wartet auf eine Verbindung des AMS-Viewers.
-p	<code>port</code> Port für die Verbindung des AMS-Viewers. Standard: 0xbf12/48914
-c	<code>capture</code> Startet die Aufzeichnung von AMS-Kommandos.
-f	<code>file</code> Dateiname der Logdatei. Standard: <code>ams.cap</code>
-d	<code>dir</code> Verzeichnis in dem die Logdatei gespeichert wird. Standard ist das aktuelle Verzeichnis.
-s	<code>size</code> Maximale Größe der Logdatei. Standard: 15MB
-r	<code>ringbuffer</code> Standardmäßig eingeschaltet. Dazu wird die Aufzeichnung auf zwei oder mehrere Dateien verteilt.

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `tcamslog -c -r -s 20 -f testlog` in der Konsole ein, um AMS-Kommandos aufzuzeichnen.
 2. Die verwendeten Parameter legen in dem Beispiel die Größe `[-s]`, den Dateinamen `[-f]` und die Verwendung des Ringbuffers `[-r]` fest.
- ⇒ Laden Sie die aufgezeichneten AMS-Kommandos im nächsten Schritt in den AMS-Viewer, um die Logdatei zu analysieren.

14.5 Netzwerkverkehr mit Wireshark analysieren

TwinCAT/BSD verfügt standardmäßig über einen Paket-Sniffer. Das Programm `tcpdump` überwacht die Ethernet-Schnittstellen, zeichnet den Netzwerkverkehr auf und speichert die Daten in einer Datei auf dem Industrie-PC ab.

Die gespeicherte Datei kann anschließend auf einen Entwicklungsrechner kopiert, mit Wireshark geöffnet und analysiert werden.

Voraussetzungen:

- Wireshark installiert auf dem Entwicklungsrechner: <https://www.wireshark.org/download.html>
Wireshark User's Guide: https://www.wireshark.org/docs/wsug.html_chunked/

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `doas tcpdump -i igb1 -s 0 -w DHCP.pcap` in der Konsole ein. In diesem Beispiel entspricht `igb1` der Ethernet-Schnittstelle X000.
-i Ethernet-Schnittstelle.
-s Länge des Snapshots. Der Wert „0“ setzt die Länge auf den Standardwert von 262144 Bytes.
-w Datei in welcher die Ausgabe gespeichert werden soll.

2. Bestätigen Sie die den Befehl mit dem Passwort des Administrators.

```
tcpdump: listening on igb1, link-type EN10MB (Ethernet), capture size 262144 bytes
```

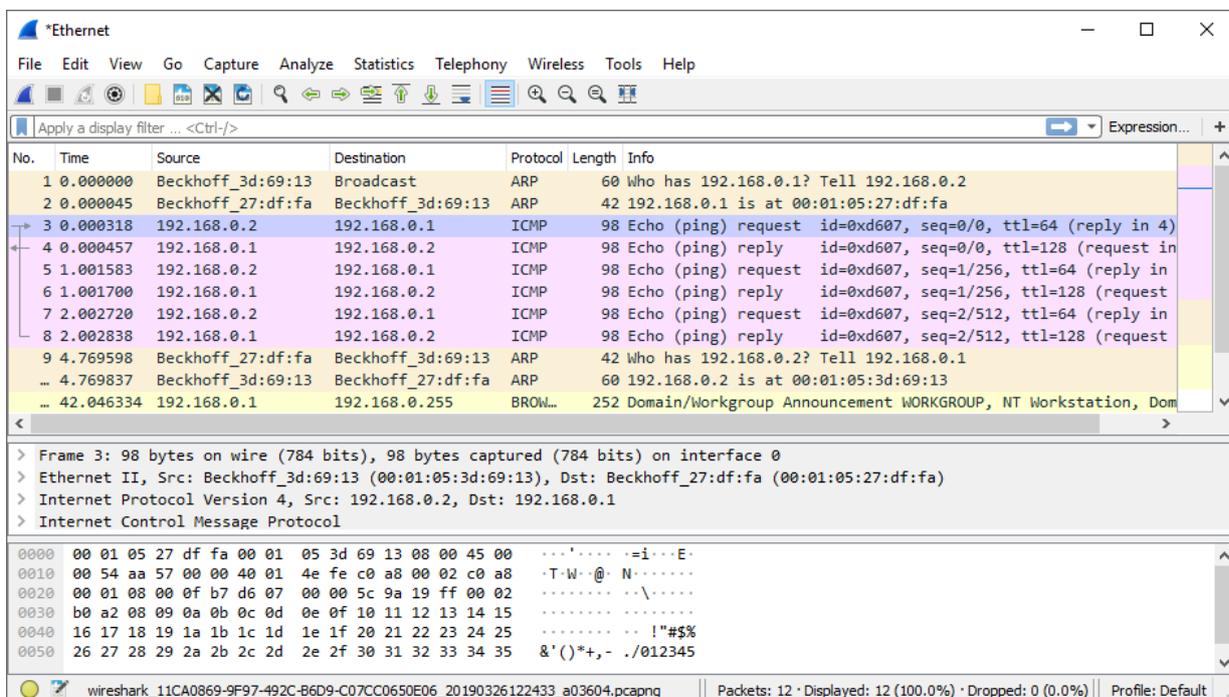
3. Sie können die Aufzeichnung jederzeit mit **[Strg] + [c]** beenden.

```
33523 packets captured
33531 packets received by filter
0 packets dropped by kernel
Administrator@CX-3B151A:~ %
```

4. In diesem Beispiel wird die Datei **DHCP.pcap** im Homeverzeichnis unter `/home/Administrator` gespeichert.

5. Kopieren Sie die Datei **DHCP.pcap** mit Hilfe des WinSCP-Clients auf einen Entwicklungsrechner (siehe: [Dateien mit dem WinSCP-Client verwalten \[▶ 73\]](#)).

⇒ Sie haben den Netzwerkverkehr erfolgreich auf der Ethernet-Schnittstelle `igb1` aufgezeichnet. Anschließend können Sie die Datei **DHCP.pcap** mit Wireshark öffnen und analysieren.



14.6 Systemreparatur

Wenn TwinCAT/BSD aufgrund eines inkonsistenten Dateisystems oder Fehlers in einer Konfigurationsdatei nicht bootet, gibt es zwei Möglichkeiten die TwinCAT/BSD-Installation zu reparieren oder Daten zu retten.

Nutzen Sie für die Reparatur oder Datenrettung entweder den

- TwinCAT/BSD-Installer-Stick, den Sie für die Installation verwendet haben
- oder den Single-User Modus, den Sie während des Systemstarts ausführen können.

14.6.1 Vom USB-Installer Stick booten

HINWEIS

Sicherheitsrisiko

In der Voreinstellung hat jeder Benutzer, der physischen Zugang zum Industrie-PC hat, Root-Rechte und damit volle Kontrolle über das System. Beschränken Sie den Zugang zum Industrie-PC auf vertrauenswürdige Personen.

Der TwinCAT/BSD-Installer-Stick kann zur Reparatur oder Datenrettung verwendet werden, wenn beispielsweise ein fehlerhafter Prozess einen Systemstart verhindert oder ein fehlerhaftes TwinCAT-Projekt eine Bootschleife verursacht.

Sobald Sie vom TwinCAT/BSD-Installer-Stick booten, haben Sie Zugriff auf ein vollwertiges TwinCAT/BSD-System, welches auf dem USB-Stick installiert ist. Dadurch können Sie im Gegensatz zum Single-User Modus wichtige Daten direkt auf den USB-Stick kopieren oder nach einer Reparatur ein Backup erstellen.

Gehen Sie wie folgt vor:

1. Booten Sie vom TwinCAT/BSD-Installer-Stick und wählen Sie die Option **shell**.



2. Importieren Sie den Speicher-Pool (zpool) ihres TwinCAT/BSD-Systems mit dem Befehl `zpool import -fR /tmp/zpool zroot`.
 3. Mounten Sie zunächst das Standard-Dataset mit dem Befehl `zfs mount zroot/ROOT/default`. Alle anderen Datasets werden automatisch gemountet.
- ⇒ Auf die Dateisysteme des kaputten Systems kann nun über `/tmp/zpool` zugegriffen werden.

14.6.2 Single-User Modus starten

HINWEIS

Sicherheitsrisiko

In der Voreinstellung hat jeder Benutzer, der physischen Zugang zum Industrie-PC hat, Root-Rechte und damit volle Kontrolle über das System. Beschränken Sie den Zugang zum Industrie-PC auf vertrauenswürdige Personen.

Der Single-User Modus gewährt vollen Zugriff auf das lokale System, die Konfigurationsdateien und kann während des Systemstarts ausgeführt werden. Der Single-User Modus ist mit dem Abgesicherten Modus unter Windows vergleichbar und kann zur Reparatur oder Datenrettung verwendet werden, wenn beispielsweise ein fehlerhafter Prozess einen Systemstart verhindert oder ein fehlerhaftes TwinCAT-Projekt eine Bootschleife verursacht.

Im Single-User Modus haben Sie keinen Zugriff auf das Netzwerk und es laufen keine Prozesse. Die Prozesse und das Netzwerk können bei Bedarf gestartet werden.

Gehen Sie wie folgt vor:

1. Halten Sie beim Booten die **[Leertaste]** gedrückt. Das Bootmenü erscheint.
2. Wählen Sie den Single-User Modus mit **[2]**.

```

REHPOT SIRHCCR AMNAIT SI RH CN AI LUJSNE JOKIEHL PGSLINO
IR AM KN AR FN EF FE TS SN AH LE AF
ARLEIN ADKCI RT APGNI NNEHDRA HC IR ETLAM NOMAR
EI NO EL OR IM AR XA MN IT RA MR UH
TRAERD NASUALK OKZTIE RA WT FO SN EGALDN UR G#
New Automation Technology

Welcome to TC/BSD

1. Boot Multi user [Enter]
2. Boot Single user
3. Escape to loader prompt
4. Reboot
5. Cons: Video

Options:
6. Kernel: default/kernel (1 of 1)
7. Boot Options
8. Boot Environments
9. Rollback restorepoint

```

3. Das Dataset `zroot/ROOT/default` wird automatisch gemountet. Sie können mit dem Befehl `zfs mount -a` alle Datasets mounten oder auch die Datasets einzeln mounten.
 4. Aktivieren Sie die Schreibrechte für das Dataset `zroot/ROOT/default` mit dem Befehl `zfs set readonly=off zroot/ROOT/default` um Änderungen am System vornehmen zu können.
- ⇒ Sie können den Single-User Modus mit `exit` wieder verlassen.

15 Anhang

15.1 Wichtige Befehle

In diesem Kapitel werden wichtige und häufig verwendete Befehle zusammengefasst und erklärt. Die Zusammenfassung ist eine Hilfe, soll eine erste Anlaufstelle sein und hat keinen Anspruch auf Vollständigkeit.

15.1.1 TwinCAT

Tab. 9: Wichtige Befehle und Tools, TwinCAT.

Befehl	Beschreibung
ads	Mit dem Tool können ADS-Routen verwaltet werden. Darüber hinaus können Variablen gelesen, geschrieben oder Lizenzinformationen, wie beispielsweise die System-ID) gelesen werden. Geben Sie den Befehl <code>ads</code> in der Konsole ein, um sich alle Parameter zu dem Tool anzuzeigen. Beispiel ADS-Route anlegen: <code>ads 192.168.0.231 addroute --addr=192.168.0.1 --netid=192.168.0.1.1.1 --password=1</code>
TcSysExe.exe	Mit TcSysExe.exe ist es beispielsweise möglich, den TwinCAT-Modus aus der Konsole zu steuern und TwinCAT in den Run- oder Config-Modus zu versetzen. Darüber hinaus können Informationen zu Lizenzen, unterschiedlichen Versionen und System-IDs abgerufen werden. Mit dem Befehl <code>TcSysExe.exe --help</code> werden alle verfügbaren Parameter angezeigt.
TcRegistry.xml	In der Datei <code>TcRegistry.xml</code> kann die Ams Net Id, die HeapMemSize und LockedMemSize eingestellt werden.
StaticRoutes.xml	Die Datei <code>StaticRoutes.xml</code> wird verwendet, um ADS-Routen aus TwinCAT/BSD heraus zu konfigurieren.
TcCoreConf	Mit dem Tool ist es möglich CPU-Kerne zu verwalten und beispielsweise CPU-Kerne zu isolieren. Geben Sie den Befehl <code>TcCoreConf --help</code> in der Konsole ein, um sich alle Parameter anzuzeigen.
TcRteConfig	Mit diesem Tool kann Realtime-Ethernet deaktivieren werden, wenn Sie die Echtzeitkommunikation nicht benötigen. Geben Sie den Befehl <code>TcRteConfig --help</code> in der Konsole ein, um sich alle Parameter anzuzeigen.

15.1.2 Shell

Tab. 10: Wichtige Befehle, Shell allgemein.

Befehl	Beschreibung
<code>script</code>	Erstellt ein Typescript von der Terminalsitzung.
<code>which <command></code>	Suchen Sie nach dem Befehl <code><command></code> im aktuellen Verzeichnis und zeigen Sie an, wo er gefunden wurde.
<code>history 20</code>	20 zuletzt eingegebenen Befehle anzeigen.
<code>!<num>< code=""></num><></code>	Befehl <code><num></code> aus der Historie erneut ausführen.
<code><command1>; <command2></code>	Befehl 1 gefolgt von Befehl 2 ausführen.
<code><command1> && <command2></code>	Führen Sie <code><command1></code> aus, dann <code><command2></code> aber nur wenn <code><command1></code> erfolgreich war (<code>\$? = 0</code>).
<code><command1> <command2></code>	Ausgang von <code><command1></code> auf Eingang von <code><command2></code> weiterleiten.
<code><command> >&out.txt</code>	Sowohl Standardausgang und Fehlerausgang eines Befehls in die Datei <code>out.txt</code> senden.
<code>printenv</code>	Alle Umgebungsvariablen anzeigen.
<code>echo \$PATH</code>	Einzelne Umgebungsvariable "PFAD" anzeigen.

Befehl	Beschreibung
setenv <variable> "value" [csh]	Setzt Umgebungsvariable <variable>.
unsetenv <variable> [csh]	Entfernt Umgebungsvariable <variable>.
^C (Ctrl-C)	Aktuellen Befehl beenden.
^U (Ctrl-U)	Löschen bis zum Zeilenanfang.
reset	Terminaleinstellungen zurücksetzen.
exit logout	Shell verlassen.

Tab. 11: Wichtige Befehle, Job-Steuerung.

Befehl	Beschreibung
^C (Ctrl-C)	Aktuellen Vordergrundprozesses beenden.
^Z (Ctrl-Z)	Aktuellen Vordergrundprozess aussetzen. Erzeugt einen ausgesetzten Job.
jobs	Jobs unter dieser Shell auflisten.
kill %<num>	Job mit der Nummer <num> beenden.
fg fg %<num>	Ausgesetzten Prozess im Vordergrund neu starten.
bg bg %<num>	Ausgesetzten Prozesses im Hintergrund neu starten.
<command> &	Befehl als Hintergrund-Job starten.

15.1.3 Datei- und Verzeichnisverwaltung

Tab. 12: Wichtige Befehle, Dateiverwaltung.

Befehl	Beschreibung
less <file>	Inhalt der Datei wird ausgelesen Leertaste = nächste Seite, b = vorherige Seite, q = verlassen / = Vorwärtssuche, ? = Rückwärtssuche, n = Suche wiederholen
grep -i <string> <file>	Zeigt alle Zeilen, die die angegebene Zeichenkette enthalten; -i= achtet auf Groß- und Kleinschreibung.
wc -l <file>	Zählt die Zeilen in der Datei.
tail -f <file>	Besonders nützlich für Logdateien. Die letzten 10 Zeilen der Datei werden angezeigt. Durch den Parameter -f werden auch neu hinzugefügte Zeilen angezeigt. Mit ^C verlassen.
Tail -n <file>	Hiermit kann die Anzahl der ausgegebenen Zeilen angepasst werden. Bsp.: tail -n <file> zeigt nur die letzte Zeile der Datei an.
strings <file> less	Extrahiert Strings aus einer Binärdatei.
touch <file>	Erstellt eine Datei, wenn nicht bereits vorhanden oder aktualisiert den Zeitstempel.
rm <file>	Datei löschen.
cp <file> <user>	Datei kopieren.
cp <file1> <file2> ... <path>/	Kopieren Sie eine oder mehrere Dateien in ein anderes Verzeichnis. Der nachgestellte Schrägstrich nach <path> ist nicht unbedingt erforderlich, verhindert aber Fehler beim Kopieren einer Datei wenn der Pfad nicht existiert.
mv <oldname> <user>	Datei oder Verzeichnis umbenennen.
mv <file1> <file2> ... <path>/	Eine oder mehrere Dateien in ein Verzeichnis verschieben.
ln <file> <user>	Erstellen Sie einen Hardlink von <file> zu <user> (beide Namen zeigen auf die gleiche Inode des Dateisystems). Beide Namen müssen sich auf demselben Dateisystem befinden.
ln -s <path> <user>	Machen Sie <user> zu einem symbolischen- oder Soft-Link, der auf den Pfad verweist, der eine Datei oder ein Verzeichnis sein kann und überall im Dateisystem liegen kann.

Tab. 13: Wichtige Befehle, Dateiberechtigungen.

Befehl	Beschreibung
ls -l <file>	Zeigt Berechtigungen für Dateien oder Verzeichnisse an. -rwxrwxrwx Für eine Datei: r erlaubt Lesen; w erlaubt Schreiben/Anhängen; x erlaubt Ausführen. Für ein Verzeichnis: r erlaubt das Auflisten von Inhalten; w erlaubt das Erstellen oder Löschen von Dateien innerhalb des Verzeichnisses; x erlaubt die Eingabe des Verzeichnisses.
ls -ld <path>	Verzeichnisse werden wie files angezeigt. Ohne -d wird bei der Eingabe von Verzeichnissen rekursiv alles in dem Verzeichnis aufgelistet.
chown <user> <path> chgrp <group> <path> chown <user>:<group> <path>	Ändern Sie den Besitzer, die Gruppe oder beides bei einer Datei oder einem Verzeichnis.
chmod [ugoa]+[rwx] <path> chmod [ugoa]-[rwx] <path>	Hinzufügen oder Entfernen von Berechtigungen. u = Benutzer (Besitzer), g = Gruppe, o = Andere, a = Alle (ugo) z.B. "chmod go+r file" fügt die Berechtigung 'r' zu 'Gruppe' und 'Anderen' hinzu.
chmod <nnn> <path>	Ändern Sie alle Bits auf einmal auf den Oktalwert nnn. z.B. "chmod 640 file" setzt rw- für Benutzer, r-- für Gruppe, --- für Andere. 0 --- 1 --x 2 -w- 3 -wx 4 r-- 5 r-x 6 rw- 7 rwx
umask umask <nnn>	Zeigen oder setzen Sie die Dateierstellungsmaske für diese Sitzung; dies sind die Berechtigungsbits, die bei neu erstellten Dateien nicht gesetzt werden. Beispielsweise bedeutet "umask 022", dass neu erstellte Dateien nicht mehr als rwxr-xr-x Berechtigungen haben.

Tab. 14: Wichtige Befehle, Dateisuche.

Befehl	Beschreibung
<code>find <path> -type f</code>	Findet alle Dateien unter dem angegebenen Pfad. Verwenden Sie "." für das aktuelle Verzeichnis. Mit der Option <code>-type f</code> werden nur Dateien angezeigt.
<code>find <path> -type f -name 'placeholder*'</code>	Findet alle Dateien unter dem angegebenen Pfad, deren Name mit "placeholder" beginnt.
<code>find <path> -type f xargs <command></code>	Finden Sie alle Dateien unter dem Pfad und wenden <code><command></code> auf jede von ihnen an.
<code>find <path> -type f -print0 xargs -0 <command></code>	Sichere Version des oberen Befehls und funktioniert mit Dateinamen, die Leerzeichen enthalten.

Tab. 15: Wichtige Befehle, Komprimierte Dateien und Archive.

Befehl	Beschreibung
<code>gzip -dc <file>.gz less</code> <code>bzip2 -dc <file>.bz2 less</code>	Komprimierte Textdatei lesen, ohne sie auf der Festplatte zu entpacken.
<code>tar -tzf <file>.tgz</code> or <code>.tar.gz</code> <code>tar -tjf <file>.tbz2</code> or <code>.tar.bz2</code>	Zeigt den Inhalt des komprimierten tar-Archivs. Option <code>-v</code> für mehr Details hinzufügen.
<code>tar -xvzf -C <path> <file>.tgz</code> <code>tar -xvjf -C <path> <file>.tbz2</code>	Extrahieren Sie den Inhalt des komprimierten Archivs in das angegebene Verzeichnis, ansonsten in das aktuelle Verzeichnis.

Tab. 16: Wichtige Befehle, Verzeichnisse.

Befehl	Beschreibung
<code>pwd</code>	Aktuelles Verzeichnis anzeigen.
<code>cd <path></code>	In ein Unterverzeichnis des aktuellen Verzeichnisses wechseln.
<code>cd ..</code>	Eine Ebene nach oben, in das übergeordnete Verzeichnis wechseln.
<code>cd /</code> <code>cd /<absolute path></code> <code>cd ~<user></code> <code>cd</code>	Aktuelles Verzeichnis wechseln: zum Root-Verzeichnis, zu einem absoluten Pfad, zum Heimverzeichnis eines bestimmten Benutzers oder zu Ihrem eigenen Heimverzeichnis.
<code>ls</code> <code>ls <path></code>	Listet den Inhalt des aktuellen Verzeichnisses oder des angegebenen Verzeichnisses auf.
<code>ls -l</code>	Verzeichnis in Langform auflisten.
<code>ls -a</code>	Auflistung aller Dateien, einschließlich versteckter Dateien.
<code>ls -d</code>	Listet das Verzeichnis selbst, stattdessen Inhalt.
<code>ls -ld <path></code>	Beispiel für die Kombination von Flags.
<code>mkdir <path></code>	Ein Verzeichnis erstellen.
<code>rmdir <path></code>	Ein leeres Verzeichnis löschen.
<code>rm -rf <path></code>	Rekursiv ein Verzeichnis und seinen gesamten Inhalt löschen.

15.1.4 Systemadministration

Tab. 17: Wichtige Befehle, Benutzer-Accounts.

Befehl	Beschreibung
id	Aktuelle uid-, gid- und zusätzliche Gruppen anzeigen.
whoami	Nur aktuellen Benutzernamen anzeigen.
cat /etc/passwd	Alle Benutzer-Accounts anzeigen.
cat /etc/group	Alle Gruppen anzeigen.
pw useradd <user> -m	Benutzer anlegen; -m = Heimverzeichnis erstellen.
passwd passwd <user>	Passwort für sich selbst oder für ein anderes Konto festlegen oder ändern (nur Administrator).
pw usermod <user> -G wheel	Benutzer zur Gruppe "wheel" hinzufügen oder einfach /etc/group direkt bearbeiten.
pw userdel <user> -r	Benutzer löschen; -r = Homeverzeichnis und alle Inhalte entfernen.
cat /etc/master.passwd	Alle Konten anzeigen, einschließlich verschlüsselter Passwörter.
vipw	Sperren Sie master.passwd Bearbeiten Sie es und bauen Sie Passwortdatenbanken neu auf.

Tab. 18: Wichtige Befehle, Dateisystem.

Befehl	Beschreibung
mount	Gemountete Dateisysteme anzeigen.
df df -h	Zeigt belegten und freien Speicherplatz in allen gemounteten Dateisystemen an. Zusatz -h = zeigt 1G statt 1048576.
du -c <path>	Fügt Speicherplatz hinzu der von Dateien oder Verzeichnissen im angegebenen Pfad oder im aktuellen Verzeichnis belegt wird.
mount -r -t cd9660 /dev/acd0 /cdrom	Gerät /dev/acd0 [IDE CD] im Verzeichnis /cdrom mounten; Dateisystemtyp ist cd9660; -r =nur lesend.
umount /cdrom	Gerät auswerfen. Gerät darf nicht verwendet werden.
fstab	Prozesse mit offenen Dateien auflisten.
cat /etc/fstab	Dateisystemtabelle anzeigen.
mount /cdrom	Mounten Sie /cdrom mit Parametern aus /etc/fstab
mount -a	Mounten Sie alle Dateisysteme in /etc/fstab mit Ausnahme derjenigen, die mit "noauto" gekennzeichnet sind (dies geschieht beim normalen Booten, ist aber nützlich beim Booten im Single-User-Modus).

Tab. 19: Wichtige Befehle, Packages.

Befehl	Beschreibung
pkg info	Übersichtsliste der installierten Packages anzeigen.
pkg info <package>	Detaillierte Beschreibung des Packages anzeigen.
pkg info -l <package>*	Liste aller im Package enthaltenen Dateien anzeigen.
pkg add <file>-1.2.3.tbz	Package aus Datei installieren.
pkg add -r <package>	Package vom Standard-FTP-Server installieren.
PACKAGEROOT="ftp://ftp.uk.freebsd.org" pkg add -r <package>	Package von einem alternativen FTP-Server installieren.
pkg install <package>	Installiert Package aus entferntem Repository oder lokalem Archiv.
pkg delete <package>	Package deinstallieren.

Tab. 20: Wichtige Befehle, Kernelmodule.

Befehl	Beschreibung
kldstat	Geladene Module anzeigen.
kldload <module>	Laden Sie das benannte Modul und alle Module, von denen es abhängt.
kldunload <module>	Modul entladen.

Tab. 21: Wichtige Befehle, Netzwerk.

Befehl	Beschreibung
ifconfig	Alle Schnittstellen anzeigen.
ifconfig igb0 192.168.0.1/24	Schnittstelle konfigurieren.
netstat -r -n	Tabelle mit Weiterleitungen anzeigen.
route add default 192.168.0.254	Eine statische Standardroute hinzufügen.
ping <IP-Adress>	Testpakete senden. Mit ^C beenden.
tracert -n <IP-Adress>	Testpakete senden und zwischengeschaltete Router anzeigen.
tcpdump -i igb0 -n -s1500 -X	Zeigt komplette Pakete an, die über eine bestimmte Schnittstelle gesendet und empfangen wurden. Die zweite Form zeigt nur Paketheader zum/vom TCP-Port 80.
tcpdump -i igb0 -n tcp port 80 -w <file>	Mit der Option -w <file> wird der Netzwerk-Dump in die Datei <file> gespeichert.
/etc/rc.d/netif start	Netzwerkschnittstellen über die Einstellungen in /etc/rc.conf initialisieren.
/etc/rc.d/routing start	Statische Routen aus den Einstellungen in /etc/rc.conf initialisieren.
/etc/rc.d/dhclient start	Konfigurieren Sie Schnittstellen, die in /etc/rc.conf mit "DHCP" gekennzeichnet sind.
netstat -finet -n	Aktive Netzwerkverbindungen anzeigen. Mit -a lauschende Sockets hinzufügen.
sockstat -4 -l	Zeigt Prozesse an, die auf IPv4- und IPv6-Sockets hören.

Tab. 22: Wichtige Befehle, Prozesse.

Befehl	Beschreibung
ps aux	Alle Prozesse anzeigen.
ps aux grep <processname>	Zeigt alle Prozesse an, die dem Muster <prozessname> entsprechen. Beachten Sie, dass grep <prozessname> selbst angezeigt werden kann.
top	Kontinuierliche Anzeige der aktivsten Prozesse. Mit q beenden.
kill <pid>	Prozess mit der angegebenen Prozess-ID wird schnell bereinigt und beendet.

Tab. 23: Wichtige Befehle, Systemstatus.

Befehl	Beschreibung
Alt-F1 ... Alt-F8	Zwischen virtuellen Konsolen wechseln.
date	Aktuelles Datum und Uhrzeit anzeigen.
ntpdate -b <server1> <server1> ...	Uhr mit den angegebenen NTP-Servern synchronisieren.
uptime	Zeit seit letztem Neustart und durchschnittliche Last anzeigen.
w	Zeigt an, wer gerade eingeloggt ist.
last -10	Die letzten 10 Anmeldungen anzeigen.
Shutdown -r now	Neustart.
doas shutdown -p now	Abschaltung.

15.1.5 Wichtige Dateien und Verzeichnisse.

Tab. 24: Wichtige Dateien und Verzeichnisse.

Pfad	Beschreibung
/boot/kernel/kernel	Der Kernel selbst.
/boot/kernel/	
/boot/loader.conf	Kernelmodule beim Start. Siehe /boot/defaults/loader.conf <pre>hint.acpi.0.disabled=1 # disable ACPI if_wi_load="YES" # load the 'wi' network driver snd_driver_load="YES" # load all sound drivers</pre>
/dev/null	Der "Bit-Eimer". Um alle Ausgaben eines Befehls (stdout und stderr) zu verwerfen: <pre># somecommand >/dev/null 2>&1 [sh]</pre>
/etc/crontab	Regelmäßig geplante Aufgaben.
/etc/group	Bindet zusätzliche Gruppen an Benutzer (wird erst nach der nächsten Anmeldung wirksam).
/etc/hosts	Lokale Zuordnungen zwischen IP-Adressen und Hostnamen.
/etc/inetd.conf	Steuert Dienste, die von inet gestartet wurden, aber keine eigenen Daemonprozesse haben, z.B. ftpd.
/etc/localtime	Binärdatei, nicht editierbar. Beschreibt die aktuelle Zeitzone. <pre># cp /usr/share/zoneinfo/Africa/Maputo /etc/localtime</pre>
/etc/mail/mailler.conf	Konfiguriert, welcher MTA verwendet wird, wenn lokale Prozesse E-Mails generieren.
/etc/make.conf	Standardwerte für die Erstellung von Softwareanwendungen/Ports. Nur vorhanden, wenn von Benutzer erstellt. Wenn nicht vorhanden, werden die Standwerte der Ports verwendet.
/etc/motd	"Nachricht des Tages" wird beim Login angezeigt.
/etc/newsyslog.conf	Konfiguriert die automatische Rotation von Protokolldateien.
/etc/periodic/...	Verschiedene Skripte, die zu geplanten Zeiten ausgeführt werden.
/etc/rc.conf	Master-Konfigurationsdatei. Siehe /etc/defaults/rc.conf für zulässige Einstellungen. <pre># Netzwerkeinstellungen hostname="foo.example.com" ifconfig_igb0="192.168.0.1/24" # oder "DHCP" defaultrouter="192.168.0.254". # Uhr beim Hochfahren einstellen ntpdate_enable="YES". ntpdate_flags="-b ntp-1.example.net ntp-2.example.net". # Dienste aktivieren inetd_enable="YES" sshd_enable="YES".</pre>
/etc/rc.d/...	Startup-Skripte. Ausführen als /etc/rc.d/<script> start or /etc/rc.d/<script> stop Funktioniert nur, wenn der entsprechende Service existiert. <pre>service_enable="YES" in /etc/rc.conf</pre>
/etc/rc.local	Erstellen Sie dieses Skript, um zusätzliche Befehle beim Systemstart auszuführen.
/etc/resolv.conf	DNS-Client konfigurieren <pre>example.com nameserver 192.0.2.1 nameserver 192.0.2.2.2</pre>
/etc/ssh/sshd_config	ssh-Daemon konfigurieren, um z.B. root-Logins zu erlauben oder abzulehnen.

Pfad	Beschreibung
/etc/sysctl.conf	Setzt Laufzeit-Kernelvariablen beim Hochfahren: net.inet.ip.forwarding=1 # wenn dieses System ein Router ist.
/etc/syslog.conf	Konfigurieren Sie die Ziele von Protokollmeldungen. Nach der Änderung: # killall -1 syslogd
/etc/ttys	Konfigurieren von Logins auf seriellen Leitungen oder Modems.
/rescue/...	Statisch verknüpfte Binärdateien für den Einsatz in Notfällen.
/root	Homeverzeichnis für 'root'-Benutzer (also ist es immer noch verfügbar, wenn andere Dateisysteme nicht eingebunden sind).
/usr/local/etc/...	Konfigurationsdateien für Drittanbieterprogramme (Ports/Package).
/usr/share/skel/...	Platzhalter, die das Homeverzeichnis eines neuen Benutzers füllen.
/var/db/pkg/...	Pfad unter dem pkg installierte Packages hinterlegt (nicht ändern!).
/var/log/maillog	Mail-Protokolldatei.
/var/log/messages	Allgemeine Systemprotokolldatei.
/var/mail/<user>	Standardspeicherort für das Postfach des Benutzers.
/var/run/<inetd>.pid	Datei mit Prozess-ID des laufenden 'inetd'-Daemons.
/var/spool/mqueue/...	Sendmail Warteschlange.
/var/tmp	Temporäre Dateien; Anwendungen sollten hier große Dateien schreiben und nicht in /tmp, wie es normalerweise auf einem größeren Dateisystem der Fall ist.
~/.ssh/authorized_keys	Öffentliche Schlüssel, die den privaten Schlüsseln entsprechen, die sich über die SSH RSA/DAS-Authentifizierung an diesem Konto anmelden dürfen.

15.1.6 Texteditoren

Tab. 25: Wichtige Befehle, vi-Editor.

Befehl	Beschreibung
:q! [Enter]	Beenden ohne zu speichern.
:wq [Enter]	Schreiben und beenden.
:wq! [Enter]	Schreiben und Beenden, erzwingt das Überschreiben der schreibgeschützten Datei.
:w filename [Enter]	Schreiben in eine andere Datei.
^L (Ctrl-L)	Bildschirm neu zeichnen.
^	An den Anfang der Zeile bewegen.
\$	An das Ende der Zeile verschieben.
h j k l	Cursor nach links / unten / oben / rechts / oben / unten bewegen (alternativ zu den Pfeiltasten).
:num [Enter]	Gehe zu Zeilennummer.
G	Zur letzten Zeile gehen.
/pattern [Enter]	Suche nach Muster vorwärts.
?pattern [Enter]	Suche rückwärts nach Muster.
n	Letzte Suche wiederholen.
i text ESC	Text vor der Cursorposition einfügen.
A text ESC	Text nach Zeilenende anhängen.
o text ESC	Neue Zeile nach der aktuellen öffnen und Text einfügen.
x	Zeichen unter dem Cursor löschen.
r char	Ersetzt das Zeichen unter dem Cursor durch ein anderes einzelnes Zeichen.
dd	Gesamte Zeile löschen.
yy	Aktuelle Zeile kopieren ("ziehen").
num yy	Kopieren von Zahlenzeilen, beginnend mit der aktuellen Zeile.
p	Kopierpuffer nach der aktuellen Zeile einfügen.

Tab. 26: Wichtige Befehle, Easy-Editor (ee).

Befehl	Beschreibung
ESC	Popup-Menü.
^C	Eingabeaufforderung.
^C quit [Enter]	Beenden ohne zu speichern.
^C exit [Enter]	Schreiben und beenden.
^C write [Enter]	Schreiben in eine andere Datei.
^A	An den Anfang der Zeile bewegen.
^E	An das Ende der Zeile verschieben.
^C num [Enter]	Gehe zu Zeilennummer nummerieren.
^Y string [Enter]	Suche nach Zeichenkette vorwärts.
^X	Letzte Suche wiederholen.
^K	Gesamte Zeile löschen.

15.1.7 Dokumentation

Tab. 27: Wichtige Befehle, Dokumentation.

Befehl	Beschreibung
man <command> man 5 <command> man -a <command>	Zeigt die Handbuchseite für den Befehl <command> an. Wenn eine Seite mit dem gleichen Namen in mehreren Abschnitten existiert, können Sie die Abschnittsnummer angeben oder -a, um Seiten aus allen Abschnitten anzuzeigen.
man -k <string>	Suche nach Zeichenkette <string> im Handbuch.
man hier	Beschreibung der Verzeichnisstruktur
cd /usr/share/doc; ls cd /usr/share/examples; ls	Durchsuchen Sie die Systemdokumentation und Beispiele. Beachten Sie insbesondere /usr/share/doc/de/books/handbook/index.html
cd /usr/local/share/doc; ls cd /usr/local/share/ examples	Durchsuchen Sie die Package-Dokumentation und Beispiele.

15.2 Literaturverzeichnis

Lucas, Michael W., Absolute FreeBSD: The Complete Guide to FreeBSD, San Francisco 2019.

Lucas, Michael W., Jude, Allan, FreeBSD Mastery: ZFS, Tilted Windmill Press 2015.

The FreeBSD German Documentation Project, FreeBSD Handbuch, unter: https://www.freebsd.org/doc/de_DE.ISO8859-1/books/handbook/ (abgerufen am: 08.07.2019).

Schneider, Wolfram, FreeBSD Manual Pages, unter: <https://www.freebsd.org/cgi/man.cgi> (abgerufen am: 08.07.2019).

15.3 FreeBSD Copyright

Copyright 1992-2023 The FreeBSD Project.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the FreeBSD Project.

15.4 Support und Service

Beckhoff und seine weltweiten Partnerfirmen bieten einen umfassenden Support und Service, der eine schnelle und kompetente Unterstützung bei allen Fragen zu Beckhoff Produkten und Systemlösungen zur Verfügung stellt.

Downloadfinder

Unser Downloadfinder beinhaltet alle Dateien, die wir Ihnen zum Herunterladen anbieten. Sie finden dort Applikationsberichte, technische Dokumentationen, technische Zeichnungen, Konfigurationsdateien und vieles mehr.

Die Downloads sind in verschiedenen Formaten erhältlich.

Beckhoff Niederlassungen und Vertretungen

Wenden Sie sich bitte an Ihre Beckhoff Niederlassung oder Ihre Vertretung für den lokalen Support und Service zu Beckhoff Produkten!

Die Adressen der weltweiten Beckhoff Niederlassungen und Vertretungen entnehmen Sie bitte unserer Internetseite: www.beckhoff.com

Dort finden Sie auch weitere Dokumentationen zu Beckhoff Komponenten.

Beckhoff Support

Der Support bietet Ihnen einen umfangreichen technischen Support, der Sie nicht nur bei dem Einsatz einzelner Beckhoff Produkte, sondern auch bei weiteren umfassenden Dienstleistungen unterstützt:

- Support
- Planung, Programmierung und Inbetriebnahme komplexer Automatisierungssysteme
- umfangreiches Schulungsprogramm für Beckhoff Systemkomponenten

Hotline: +49 5246 963-157

E-Mail: support@beckhoff.com

Beckhoff Service

Das Beckhoff Service-Center unterstützt Sie rund um den After-Sales-Service:

- Vor-Ort-Service
- Reparaturservice
- Ersatzteilservice
- Hotline-Service

Hotline: +49 5246 963-460

E-Mail: service@beckhoff.com

Beckhoff Unternehmenszentrale

Beckhoff Automation GmbH & Co. KG

Hülshorstweg 20
33415 Verl
Deutschland

Telefon: +49 5246 963-0

E-Mail: info@beckhoff.com

Internet: www.beckhoff.com

Tabellenverzeichnis

Tab. 1	Änderungshinweise für die Dokumentation.....	8
Tab. 2	Änderungshinweise für das Betriebssystem.....	9
Tab. 3	Beschreibung der Verzeichnisse im Installer-Ordner.....	18
Tab. 4	Überblick über wichtige TwinCAT/BSD-Verzeichnisse.....	28
Tab. 5	Firewall-Regel für unverschlüsselte ADS-Kommunikation.....	36
Tab. 6	USV-Software: Einstellungen in der Konfigurationsdatei.....	64
Tab. 7	Geräteunterstützung für TwinCAT/BSD Hypervisor, Device- und GPU-Passthrough.....	77
Tab. 8	ADS-Monitor, Parameter der tcamslog Applikation.....	128
Tab. 9	Wichtige Befehle und Tools, TwinCAT.....	132
Tab. 10	Wichtige Befehle, Shell allgemein.....	132
Tab. 11	Wichtige Befehle, Job-Steuerung.....	133
Tab. 12	Wichtige Befehle, Dateiverwaltung.....	134
Tab. 13	Wichtige Befehle, Dateiberechtigungen.....	134
Tab. 14	Wichtige Befehle, Dateisuche.....	135
Tab. 15	Wichtige Befehle, Komprimierte Dateien und Archive.....	135
Tab. 16	Wichtige Befehle, Verzeichnisse.....	135
Tab. 17	Wichtige Befehle, Benutzer-Accounts.....	136
Tab. 18	Wichtige Befehle, Dateisystem.....	136
Tab. 19	Wichtige Befehle, Packages.....	136
Tab. 20	Wichtige Befehle, Kernelmodule.....	136
Tab. 21	Wichtige Befehle, Netzwerk.....	137
Tab. 22	Wichtige Befehle, Prozesse.....	137
Tab. 23	Wichtige Befehle, Systemstatus.....	137
Tab. 24	Wichtige Dateien und Verzeichnisse.....	138
Tab. 25	Wichtige Befehle, vi-Editor.....	139
Tab. 26	Wichtige Befehle, Easy-Editor (ee).....	140
Tab. 27	Wichtige Befehle, Dokumentation.....	140

Abbildungsverzeichnis

Abb. 1	TwinCAT/BSD-Bootloader während des Starts.	10
Abb. 2	Add-Route-Dialog mit einem TwinCAT/BSD-Zielsystem und dazugehöriger IP-Adresse.....	11
Abb. 3	Remote-Zugriff über SSH mit Hilfe der Windows PowerShell.....	12
Abb. 4	Zugriff über die webbasierte Konsole eines TwinCAT/BSD-Systems.....	13
Abb. 5	Zugriff auf den Gerätemanager eines TwinCAT/BSD-Systems.....	13
Abb. 6	Passwort ändern im Webinterface des Beckhoff Device Managers.	14
Abb. 7	Beckhoff TwinCAT/BSD-Installer: Startseite mit interaktivem Menü.....	15
Abb. 8	FAT-Partition und Ordnerstruktur des TwinCAT/BSD-Installer-Sticks unter Windows.	16
Abb. 9	Ordnerstruktur des TwinCAT/BSD-Installer-Sticks mit zwei Backup-Ordern.	16
Abb. 10	Aufbau der TwinCAT 3 Runtime unter TwinCAT/BSD.....	24
Abb. 11	Übersicht zum Aufbau des Speicher-Pools inklusive Speichermedien und Datasets.....	26
Abb. 12	Datasets des TwinCAT/BSD-Betriebssystems.	27
Abb. 13	TwinCAT/BSD-Verzeichnisstruktur.	28
Abb. 14	Beispiel für die Verwendung des SMS-Funktionsbausteins in TwinCAT 3.....	41
Abb. 15	Aufschlüsselung der TwinCAT/BSD-Version.	44
Abb. 16	NTP-Server-Einstellungen im Beckhoff Device Manager.	67
Abb. 17	Startseite des Beckhoff Device Managers.	69
Abb. 18	Erste Seite des Beckhoff Device Managers.....	70
Abb. 19	Remote-Zugriff über SSH mit Hilfe der Windows PowerShell.....	71
Abb. 20	Basiskonfiguration einer VM-Instanz.....	78
Abb. 21	VM-Instanz mit virtuellen Laufwerken.	85
Abb. 22	Konfiguration einer VM-Instanz mit virtuellen Netzwerkcontrollern.....	88
Abb. 23	VM-Instanz mit einer Host-Only-Netzwerkconfiguration.	89
Abb. 24	VM-Instanz mit einer Bridge-Netzwerkconfiguration.	90
Abb. 25	VM-Instanz mit einer NAT-Netzwerkconfiguration.	92
Abb. 26	VM-Instanz mit einer Ethernet-Device-Passthrough-Konfiguration.....	94
Abb. 27	Konfiguration einer VM-Instanz mit PCI-Device-Passthrough.	95
Abb. 28	Debian Linux sample VM	98
Abb. 29	C9900-S620 Bestelloption mit vorkonfigurierter Windows 10 VM mit Device-Passthrough.	103
Abb. 30	C9900-S621 Bestelloption mit vorkonfigurierter Windows 10 VM.....	104
Abb. 31	Fehlermeldung bei einem zu kleinen Heap-Speicher.	116

Trademark statements

Beckhoff®, TwinCAT®, TwinCAT/BSD®, TC/BSD®, EtherCAT®, EtherCAT G®, EtherCAT G10®, EtherCAT P®, Safety over EtherCAT®, TwinSAFE®, XFC®, XTS® and XPlanar® are registered trademarks of and licensed by Beckhoff Automation GmbH.

Third-party trademark statements

AMD is a trademark of Advanced Micro Devices, Inc.

Debian is a registered trademark owned by Software in the Public Interest, Inc.

FreeBSD is a registered trademark of The FreeBSD Foundation and is used by Beckhoff with the permission of The FreeBSD Foundation.

Intel, the Intel logo, Intel Core, Xeon, Intel Atom, Celeron and Pentium are trademarks of Intel Corporation or its subsidiaries.

itec is a registered trademark of TE Connectivity Industrial GmbH.

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft, Microsoft Azure, Microsoft Edge, PowerShell, Visual Studio, Windows and Xbox are trademarks of the Microsoft group of companies.

VNC® is a trademark of RealVNC Limited and is protected by trademark registrations and/or pending trademark applications in the European Union, United States of America and other jurisdictions.

Wireshark is a registered trademark of Sysdig, Inc.

Mehr Informationen:
www.beckhoff.de/twincat-bsd

Beckhoff Automation GmbH & Co. KG
Hülshorstweg 20
33415 Verl
Deutschland
Telefon: +49 5246 9630
info@beckhoff.com
www.beckhoff.com

