



Application Note
Funktionen des integrierten WebServers

Hilscher Gesellschaft für Systemautomation mbH

www.hilscher.com

DOC091203AN05DE | Revision 5 | Deutsch | 2013-10 | Freigegeben | Öffentlich

Inhaltsverzeichnis

Inhaltsverzeichnis.....	2
1 Einleitung	3
1.1 Über dieses Dokument.....	3
1.1.1 Änderungsübersicht	3
1.1.2 Abkürzungen	3
1.1.3 Konventionen in diesem Dokument.....	4
1.2 Kurzbeschreibung WebServer	5
1.3 Geräte und Firmware mit integriertem WebServer	5
2 Zugang zum WebServer	6
2.1 Voraussetzungen	6
2.2 Seiten des WebServers aufrufen	7
3 Funktionen über HTTP	8
3.1 Geräte-Parameter anzeigen.....	8
3.2 Firmware-Version anzeigen und Firmware aktualisieren.....	9
3.3 File Upload	11
3.4 Reset.....	14
4 Zugangsverwaltung	15
4.1 Default-Zugangsverwaltung	15
4.2 Eigene Zugangsverwaltung.....	15
4.2.1 Gruppen und Rechte	16
4.2.2 Zugangsverwaltungsdatei <code>security.cfg</code>	17
4.2.3 Generierung eines Passwort-Hashs mit MD5.....	18
4.2.4 Zugangsverwaltungsdatei hochladen	19
4.2.5 Zugangsverwaltungsdatei löschen	21
5 Eigene Inhalte einbinden	22
5.1 Übersicht	22
5.2 Beispiele für das Einbinden eigener Inhalte.....	23
5.2.1 Beispiel 1: Firmenlogo in der Navigationsleiste austauschen.....	23
5.2.2 Beispiel 2: Design der Navigationsleiste ändern	24
5.2.3 Beispiel 3: Neue Webseite einbinden.....	25
6 Zugriff auf Verzeichnisse.....	28
7 Anhang	29
7.1 Abbildungsverzeichnis	29
7.2 Tabellenverzeichnis	29
7.3 Kontakte	30

1 Einleitung

1.1 Über dieses Dokument

Dieses Dokument beschreibt die HTTP-Funktionen des WebServers für Flash-basierte Real-Time-Ethernet-Kommunikationsmodule von Hilscher. Hier erfahren Sie, wie Sie mit einem Browser funktionale Webseiten aufrufen können, z. B. um eine Firmware zu aktualisieren. Außerdem finden Sie hier Informationen, wie Sie eigene Inhalte in den WebServer einbinden können.

1.1.1 Änderungsübersicht

Index	Datum	Kapitel	Änderungen
1	2009-12-21	alle	erstellt
2	2010-07-19	alle	Beschreibung der Funktionen erweitert und aktualisiert
3	2012-02-06	alle	komplett überarbeitet
4	2012-02-28	5.2	Abschnitt <i>Beispiele für das Einbinden eigener Inhalte</i> ergänzt
5	2013-10-15	1.3	Abschnitt <i>Geräte und Firmware mit integriertem WebServer</i> aktualisiert

Tabelle 1: Änderungsübersicht

1.1.2 Abkürzungen

Abkürzung	Langform
HTTP	Hypertext Transfer Protocol
TCP	Transmission Control Protocol
IP	Internet Protocol
SSI	Server Side Includes
iframe	Inline Frame

Tabelle 2: Abkürzungen

1.1.3 Konventionen in diesem Dokument

Hinweise, Handlungsanweisungen und Ergebnisse von Handlungen sind wie folgt gekennzeichnet:

Hinweise



Wichtig: <Wichtiger Hinweis>



Hinweis: <Hinweis>



<Hinweis, wo Sie weitere Informationen finden können>

Handlungsanweisungen

1. <Anweisung>

2. <Anweisung>

oder

➤ <Anweisung>

Ergebnisse

↪ <Ergebnis>

1.2 Kurzbeschreibung WebServer

Der in die Firmware von Hilscher-Kommunikationsmodulen für Real-Time-Ethernet-Systeme integrierte WebServer ermöglicht es, Statusparameter abzurufen sowie ein Firmware-Update oder ein Reset des Geräts über HTTP durchzuführen. Somit können Sie auf diese Funktionen mittels Standard-Webbrowser und Ethernet-Schnittstelle zugreifen.

Außerdem können Sie mittels File-Upload eigene Webseiten und Grafiken (z. B. Ihr Firmenlogo) auf dem WebServer hinterlegen und dadurch das Design der vom WebServer angezeigten Seiten nach Ihren Wünschen gestalten. Die HTTP-Funktionen des WebServers bleiben davon unberührt.

Der WebServer unterstützt ferner eine Benutzer- und Passwort-Verwaltung mit MD5-Kodierung. Eine Konfigurationsdatei (`security.cfg`), welche die Benutzer, Gruppen und Passwort-Definitionen enthält, kann mit der cifX Test Applikation auf den WebServer geladen werden.

1.3 Geräte und Firmware mit integriertem WebServer

Der WebServer steht in folgenden Hilscher-Geräten für Real-Time-Ethernet-Systeme und folgender Firmware zur Verfügung:

Produktfamilie	Artikel-bezeichnung	Protokoll	Firmware	Unterstützt ab Firmware-Version
comX	COMX 100CA-RE COMX 100CN-RE	EtherNet/IP Scanner	comXeim.nxf	2.4.9.2
		EtherNet/IP Adapter	comXeis.nxf	2.5.16.3
		Open Modbus/TCP	comXomb.nxf	2.5.4.0
		PROFINET IO Device	comXpns.nxf	3.4.33.0
		sercos Slave	comXs3s.nxf	3.0.8.0
	COMX 51CA-RE COMX 51CN-RE	EtherNet/IP Adapter	M060H000.nxf	2.7.12.0
		Open Modbus/TCP	M060L000.nxf	2.5.10.0
		PROFINET IO Device	cx51pns.nxf	3.5.22.0
		sercos Slave	M060J000.nxf	3.1.18.0
netIC	wird zur Zeit nicht unterstützt	–	–	–
netJACK	NJ 50D-RE	EtherNet/IP Adapter	J030H000.nxf	2.5.16.3
		Open Modbus/TCP	J030L000.nxf	2.5.4.0
		PROFINET IO Device	J030D000.nxf	3.4.33.0
		sercos Slave	J030J000.nxf	3.0.32.0
	NJ 51D-RE	EtherNet/IP Adapter	J060H000.nxf	2.7.12.0
		Open Modbus/TCP	J060L000.nxf	2.5.10.0
		PROFINET IO Device	J060D000.nxf	3.5.22.0
		sercos Slave	J060J000.nxf	3.1.18.0
	NJ 100EN-RE NJ 100DN-RE	EtherNet/IP Scanner	J020G000.nxf	2.4.9.2
		EtherNet/IP Adapter	J020H000.nxf	2.5.16.3
		Open Modbus/TCP	J020L000.nxf	2.5.4.0
		PROFINET IO Device	J020D000.nxf	3.4.33.0
		sercos Slave	J020J000.nxf	3.0.32.0

Tabelle 3: Liste der Geräte und Firmware mit integriertem WebServer

2 Zugang zum WebServer

2.1 Voraussetzungen

- Die Firmware des Kommunikationsmoduls muss mit der WebServer-Funktionalität ausgestattet sein. Die entsprechenden Module und Firmware finden Sie in der *Liste der Geräte und Firmware mit integriertem WebServer* auf Seite 5.
- Das Kommunikationsmodul ist betriebsbereit.
- Das Kommunikationsmodul ist über seine Ethernet-Schnittstelle mit einem Netzwerk verbunden.
- Sie verfügen über einen PC mit Verbindung zum Netzwerk und einen Webbrowser. Der WebServer wurde mit folgenden Browser-Versionen getestet:

Internet Explorer	8.0 (Windows XP)
	9.0 (Windows 7)
Firefox	10.0
Chrome	17.0
Opera	11.61
Safari	5.1.2

- Sie müssen die Adresse Ihres Kommunikationsmoduls sowie einen gültigen Benutzernamen mit Passwort kennen. Informationen zu Benutzernamen und Passwörtern finden Sie im Kapitel *Zugangsverwaltung* auf Seite 15.
- Falls Sie eine eigene Zugangsverwaltung betreiben möchten, benötigen Sie zum Hochladen der Zugangsverwaltungsdatei einen PC mit installierter cifX Test Applikation sowie ein passendes Evaluation Board, mit dem Sie Ihr Kommunikationsmodul mit dem PC verbinden können. Weitere Informationen hierzu finden Sie im Abschnitt *Eigene Zugangsverwaltung* auf Seite 15.

2.2 Seiten des WebServers aufrufen

Sie rufen den WebServer auf, indem Sie die IP-Adresse des Kommunikationsmoduls in die Adresszeile Ihres Webbrowsers eingeben.



Hinweis: Die IP-Adresse wird dem Kommunikationsmodul i. d. R. bei seiner Konfiguration mittels SYCON.net oder netX Configuration Tool zugewiesen. Nähere Informationen hierzu finden Sie im Bediener Manual des DTM für das entsprechende Protokoll.

Nach Eingabe der IP-Adresse gelangen Sie zunächst auf die Startseite (Homepage) des WebServers. Von dort können Sie über Links die anderen Seiten aufrufen.

Sie können die Webseiten auch aufrufen, indem Sie deren URL in der Adresszeile Ihres Browsers eingeben:

Webseite	Funktion	URL in Browser
Home	Geräte-Parameter anzeigen	http://<IP-Adresse>
Firmware Update	Firmwareversion anzeigen / Firmware aktualisieren	http://<IP-Adresse>/fwupdate.sht
File Upload	Datei hochladen oder löschen	http://<IP-Adresse>/upload.sht
Reset	Geräte-Reset	http://<IP-Adresse>/reset.sht

Tabelle 4: Übersicht der Webseiten und deren URLs

Alternativ können Sie die rein funktionalen Webseiten des WebServers, d. h. diejenigen HTML-Seiten, die lediglich die HTTP-Funktionen und keine Navigationsleiste oder Grafiken enthalten, direkt aufrufen, indem Sie folgende URL in der Adresszeile Ihres Browsers eingeben:

Funktion	URL in Browser
Firmwareversion anzeigen / Firmware aktualisieren	http://<IP-Adresse>/fwupdate
Datei hochladen oder löschen	http://<IP-Adresse>/upload
Geräte-Reset	http://<IP-Adresse>/reset

Tabelle 5: HTTP-Funktionen direkt aufrufen

3 Funktionen über HTTP

3.1 Geräte-Parameter anzeigen

Die Startseite des WebServers zeigt Ihnen Parameter zur Identifikation Ihres Gerätes.

Sie gelangen auf die Startseite, indem Sie die URL `http://<IP-Adresse>` in die Adresszeile Ihres Browsers eingeben. Nach dem Wechsel auf andere Seiten des WebServers gelangen Sie in der Navigationsleiste durch Anklicken der Schaltfläche **Home** wieder auf die Startseite zurück.



netX50/100 Configuration

Welcome to the administration interface of your netX device.

Here you can set different operating parameters and execute remote functions.

Device Information

Property	Value
Product Name:	netJACK 100
Device Number:	1625100
Serial Number:	20008
MAC Address:	00:02:a2:23:6c:81

Abbildung 1: Startseite WebServer (Darstellung im Internet Explorer, kann in anderen Browsern abweichen)

3.2 Firmware-Version anzeigen und Firmware aktualisieren

Auf der Seite **Firmware Update** sehen Sie die aktuell geladene Firmware-Version und können eine neue Firmware-Datei in Ihr Gerät laden.

Sie gelangen auf die Firmware-Seite, indem Sie die Schaltfläche **Firmware Update** in der Navigationsleiste anklicken oder die URL `http://<IP-Adresse>/fwupdate.sht` in die Adresszeile Ihres Browsers eingeben.



Hinweis: Diese Seite wird standardmäßig durch eine Passwort-Abfrage geschützt. Näheres hierzu finden Sie im Abschnitt *Zugangsverwaltung* auf Seite 15.

Channel	Name	Version	Date
0	EtherNet/IP Scanner	2.4.9.1	13.10.2011

Firmware Update

Choose the new firmware file (.nxf) you want to install:

Submit your file by clicking on "transfer". The transfer will take a few seconds.

WARNING: Do not interrupt power or disconnect cable from the system while the transfer is in progress!

Abbildung 2: Firmware Update (Darstellung im Internet Explorer, kann in anderen Browsern abweichen)



Hinweis: Bei einem Firmware-Update müssen die gewählte Firmware und das Gerät zueinander passen; d. h. Sie können z. B. keine EtherNet/IP Scanner (Master) Firmware auf einen netJACK 50 mit netX 50 Chip laden. Vor einem Update findet eine automatische Kompatibilitätsprüfung statt. Dabei werden z. B. Geräteklasse und Hardware-Eigenschaften geprüft.

Firmware Identification

Im Bereich **Firmware Identification** werden die folgenden Parameter angezeigt:

- Kanalnummer (Channel bzw. Port)
- Name der geladenen Firmware
- Firmware-Version
- Datum der Firmware

Firmware Update

Im Bereich **Firmware Update** können Sie eine Firmware-Datei zum Upload in das Gerät auswählen und den Upload starten.

Klicken Sie die Schaltfläche **Durchsuchen**, um einen Dialog zur Auswahl der Datei zu öffnen. Pfad und Name der gewählten Datei werden im nebenstehenden Feld angezeigt.



Hinweis: Firmware-Dateien haben immer die Dateinamenserweiterung **.nxf**.

Bedienelement	Funktion
Anzeigefeld	Zeigt ausgewählte Datei mit Pfad.
Durchsuchen	Öffnet den Dateiauswahl-Dialog.
Transfer	Überträgt die ausgewählte Firmware-Datei zum Gerät.
Cancel	Bricht das Firmware-Update ab und löscht Inhalt des Anzeigefelds.

Tabelle 6: Bedienelemente Firmware-Update



VORSICHT!

Geräteschaden durch Unterbrechung des Datei-Transfers.

Unterbrechen Sie keinesfalls die Spannungsversorgung und ziehen Sie nicht das Netzkabel während des Transfers der Firmware-Datei. Wenn der Strom zum Zeitpunkt des Umschaltens von der alten zur schon gespeicherten neuen Firmware ausfällt, kann dies schwere Fehlfunktionen des Geräts zur Folge haben.

Nach dem Start des Uploads mit der Schaltfläche **Transfer** wird die Validität der Datei geprüft. Wird die Datei abgelehnt, erscheint eine Fehlermeldung, wird die Datei akzeptiert, erscheint die Meldung **Transfer succeeded**.

Nach erfolgreichem Transfer müssen Sie einen Reset ausführen, um die neue Firmware zu starten. Sehen Sie hierzu den Abschnitt *Reset* auf Seite 14.

3.3 File Upload

Auf der Seite **File Upload** können Sie Dateien in das per HTTP zugängliche Verzeichnis des WebServers laden sowie Dateien löschen. Außerdem können Sie hier sehen, welche Ordner und Dateien sich in dem Verzeichnis befinden.

Sie gelangen auf die Upload-Seite, indem Sie die Schaltfläche **File Upload** in der Navigationsleiste anklicken oder die URL `http://<IP-Adresse>/upload.sht` in die Adresszeile Ihres Browsers eingeben.



Hinweis: Diese Seite wird standardmäßig durch eine Passwort-Abfrage geschützt. Näheres hierzu finden Sie im Abschnitt *Zugangsverwaltung* auf Seite 15.

File Upload

With the upload interface you are able to transfer files to the server via HTTP.
If no target path is defined, the files are stored in server root. Use your document root path to store public content.
Upload module is ready.

Store

Chose the file you want to upload:

Define the path where the file should be stored:

Delete

Define the file or directory to be deleted:

File Overview

The following files are currently stored in the Filesystem.

PUB

- | COMMON.JS
- | DEVICE.JPG
- | FWUPDATE.SHT
- | HOME.SHT
- | RESET.SHT
- | UPLOAD.SHT
- | INDEX.HTM
- | LOGO.PNG
- | MENU.PRT
- | MENUBG.JPG
- | STYLE.CSS
- NOTES.TXT

Abbildung 3: File Upload (Darstellung im Internet Explorer, kann in anderen Browsern abweichen)

Store

Im Bereich **Store** können Sie eine Datei zum Upload auf den WebServer auswählen und den Upload starten. Beachten Sie dabei folgendes:

- Es kann immer nur eine Datei, nicht mehrere gleichzeitig übertragen werden.
- Der Name der Datei darf nicht länger als acht Zeichen sein (8.3 Namenskonvention), ansonsten wird die Datei nicht gespeichert.
- Die Gesamtgröße des Uploads sollte ein Megabyte nicht überschreiten.
- Wenn eine Datei gleichen Namens auf dem WebServer bereits vorhanden ist, wird diese ohne Warnhinweis überschrieben.

Klicken Sie die Schaltfläche **Durchsuchen**, um einen Dialog zur Auswahl der Datei zu öffnen. Pfad und Name der gewählten Datei werden im nebenstehenden Feld angezeigt.

Geben Sie in das Feld **Define the path...** das Verzeichnis des öffentlichen Ordners `pub` ein und klicken Sie anschließend die Schaltfläche **Upload**. Sie können einen neuen Unterordner anlegen, indem Sie ihn als Teil des Zielpfades eingeben, z. B. `pub/myfolder`.



Hinweis: Der File Upload kann nur auf das Verzeichnis `Port_1/sx` und die darunter liegenden Ordner zugreifen. Der Pfad `Port_1/sx` ist im File Upload bereits voreingestellt. Die Webseiten und Grafiken, die der WebServer anzeigen kann, liegen in diesem Verzeichnis im „öffentlichen“ Ordner `pub` (Pfad: `Port_1/sx/pub`). Wenn Sie eigene Webseiten oder Grafiken in den WebServer einbinden und anzeigen lassen möchten, müssen Sie diese in diesem öffentlichen Ordner ablegen. Da der Pfad `Port_1/sx` im File Upload bereits voreingestellt ist, brauchen Sie hierzu im Feld **Define the path...** nur den Namen des öffentlichen Ordners `pub` einzugeben. Wenn Sie den öffentlichen Ordner `pub` nicht angeben und das Feld leer lassen, werden die hochgeladenen Dateien eine Ebene höher im Verzeichnis `Port_1/sx` abgelegt und können somit später auch nicht im Browser angezeigt werden.

Wenn Sie dies wünschen, können Sie Dateien auf dem WebServer also quasi „verstecken“, indem Sie diese im Verzeichnis `Port_1/sx` ablegen.

Eine grafische Darstellung der benutzerrelevanten Verzeichnisse und der Zugriffsmöglichkeiten auf diese Verzeichnisse finden Sie im Kapitel *Zugriff auf Verzeichnisse* auf Seite 28.

Bedienelement	Funktion
Anzeigefeld	Zeigt ausgewählte Datei mit Pfad.
Durchsuchen	Öffnet den Dateiauswahl-Dialog.
Eingabefeld	Manuelle Eingabe des Ziel-Verzeichnisses.
Upload	Überträgt die ausgewählte Datei zum WebServer.
Cancel	Bricht den Transfer ab und löscht Inhalt des Anzeige-Felds.

Tabelle 7: Bedienelemente Datei-Upload



Hinweis: Sie können den File Upload nicht für ein Firmware Update verwenden, da der File Upload nur auf das Verzeichnis `Port_1/sx` und die darunter liegenden Ordner zugreifen kann, Firmware aber im `Port_0` gespeichert wird. Zum Upload einer Firmware-Datei müssen Sie die Funktion **Firmware Update** verwenden, wie im Abschnitt *Firmware-Version anzeigen und Firmware aktualisieren* auf Seite 9 beschrieben.

Ebenso wenig können Sie den File Upload zum Upload der Benutzer- und Passwort-Datei `security.cfg` verwenden, da diese Datei direkt im Root-Verzeichnis von `Port_1` gespeichert werden muss, auf das der File Upload keinen Zugriff hat. Zum Upload der Datei `security.cfg` müssen Sie die cifX Test Applikation verwenden. Sehen Sie hierzu den Abschnitt *Zugangsverwaltungsdatei hochladen* auf Seite 19.

Delete

Im Bereich **Delete** können Sie eine Datei oder einen Ordner vom WebServer löschen.

Geben Sie in das Feld den Pfad der Datei oder des Ordners ein, den Sie löschen möchten. Sie können nur Elemente löschen, die sich im Verzeichnis `Port_1/sx/` oder darunter befinden.

Bedienelement	Funktion
Eingabefeld	Manuelle Eingabe des Pfads der zu löschenden Elemente.
Delete	Löscht die ausgewählten Elemente vom WebServer.
Cancel	Bricht die Aktion ab und löscht Inhalt des Eingabefelds.

Tabelle 8: Bedienelemente Dateien löschen

File Overview

Im Bereich **File Overview** sehen Sie die Ordner und Dateien, die sich im Verzeichnis `Port_1/sx` (also im für den **File Upload** zugänglichen Verzeichnis des WebServers) befinden.



Hinweis: Alle Buchstaben werden als Großbuchstaben angezeigt. Falls ein Dateiname ein Leerzeichen enthält, wird nur der Teil des Dateinamens angezeigt, der sich **vor** dem Leerzeichen befindet.
Beispiel: Die Datei `my file.txt` wird als `MY.TXT` angezeigt.

3.4 Reset

Auf der Seite **Reset** können Sie ein Reset für Ihr Kommunikationsmodul durchführen.

Sie gelangen auf die Reset-Seite, indem Sie die Schaltfläche **Reset** in der Navigationsleiste anklicken oder die URL

`http://<IP-Adresse>/reset.sht` in die Adresszeile des Browsers eingeben.



Hinweis: Diese Seite wird standardmäßig durch eine Passwort-Abfrage geschützt. Näheres hierzu finden Sie im Abschnitt *Zugangsverwaltung* auf Seite 15.

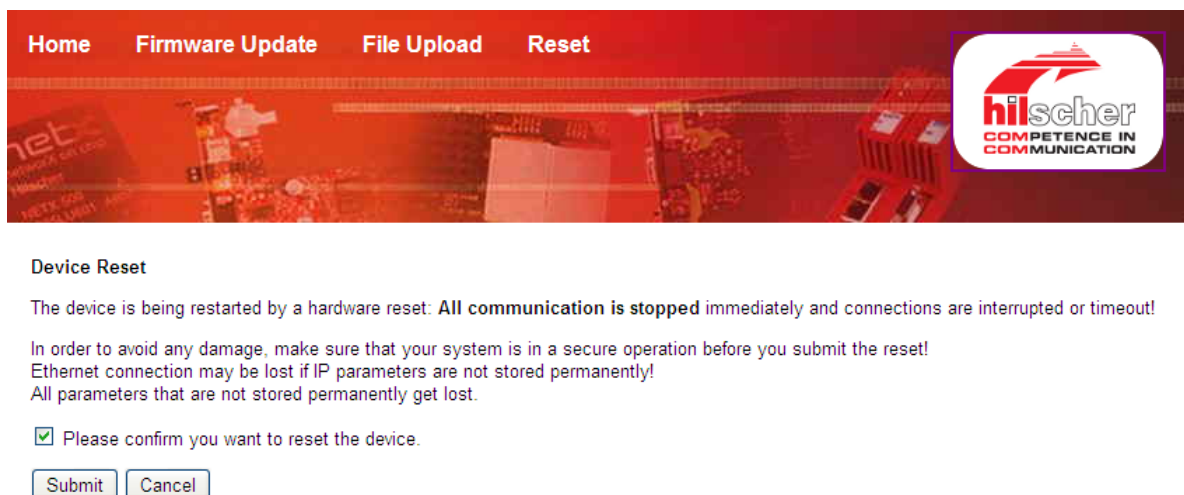


Abbildung 4: Reset (Darstellung im Internet Explorer, kann in anderen Browsern abweichen)

Ein Reset muss nach einem Firmware-Update oder einer Neukonfigurierung des Geräts durchgeführt werden und hat folgende Auswirkungen:

- Die Firmware wird neu gestartet und alle bestehenden Verbindungen werden unterbrochen oder führen zu einem Time-out.
- Die E/A-Kommunikation am Bus wird unterbrochen.
- Die IP-Verbindung kann verloren gehen, wenn die IP-Parameter nicht mittels SYCON.net oder dem netX Configuration Tool definiert und permanent im Gerät abgespeichert wurden.



Hinweis: Wenn Sie einen Reset ausführen und die IP-Parameter nicht permanent gespeichert waren oder wenn Sie das Gerät auf ein anderes Ethernet-Protokoll umgestellt haben, müssen Sie dem Gerät seine IP-Adresse mit Hilfe eines geeigneten Tools neu zuordnen, bevor Sie wieder auf den WebServer zugreifen können.

Aktivieren Sie die Checkbox vor **Please confirm...**, um zu bestätigen, dass Sie ein Reset durchführen möchten. Um den Reset zu starten, klicken Sie anschließend die Schaltfläche **Submit**.

Die Schaltfläche **Cancel** entfernt das Häkchen aus der Checkbox vor **Please confirm...** wieder.

4 Zugangsverwaltung

4.1 Default-Zugangsverwaltung

Der Zugriff auf die Funktionen **Firmware Update**, **File Upload** und **Reset** ist standardmäßig durch eine Nutzer-Authentifizierung geschützt.

Wenn Sie eine der oben genannten Funktionen aufrufen, erscheint ein Passwort-Dialog. Die Default-Zugangsparameter für sämtliche Funktionen sind:

Benutzername: admin

Kennwort: admin

Diese Default-Zugangsparameter gelten solange, bis Sie eine Zugangsverwaltungsdatei `security.cfg` mit einem neuen Kennwort für den Benutzer `admin` auf dem WebServer im Root-Verzeichnis von `Port_1` hinterlegt haben.

4.2 Eigene Zugangsverwaltung

Sie können eine eigene Zugangsverwaltung für den WebServer einrichten. Hierzu können Sie Benutzer und deren Rechte-Gruppen sowie Passwörter in einer Textdatei definieren und als Zugangsverwaltungsdatei `security.cfg` im Root-Verzeichnis von `Port_1` auf dem WebServer hinterlegen. Dabei müssen Passwörter als MD5-Code/Hash eingetragen werden. Zur Erzeugung des MD5-Codes können Sie einen beliebigen, als Freeware oder Online-Tool erhältlichen, externen MD5 Generator verwenden.

Zum Hochladen oder Löschen der Zugangsverwaltungsdatei müssen Sie die cifX Test Applikation verwenden.

Sobald Sie eine Zugangsverwaltungsdatei `security.cfg` auf den WebServer geladen haben, gelten die darin enthaltenen Zugangsberechtigungen, und die Parameter der Default-Zugangsverwaltung sind außer Kraft gesetzt.



Wichtig: Achten Sie darauf, dass Sie in der Zugangsverwaltungsdatei einen Benutzer `admin` mit einem neuen Kennwort anlegen, um die alten Default-Zugangsparameter (`admin / admin`) außer Kraft zu setzen und den Zugang zum WebServer wirkungsvoll zu schützen. Ist kein Benutzer `admin` in der Zugangsverwaltungsdatei enthalten, gelten zusätzlich zu den anderen in der Zugangsverwaltungsdatei enthaltenen Zugangsberechtigungen weiterhin die alten Default-Zugangsparameter für den `admin`.

Das Löschen der `security.cfg` setzt die Zugangsverwaltung wieder auf die Default-Zugangsparameter zurück.

4.2.1 Gruppen und Rechte

Zugriffsrechte auf Funktionen des WebServers sind an Rechte-Gruppen gekoppelt.

Folgende Rechte-Gruppen sind zur Zeit auf dem WebServer eingerichtet:

Rechte-Gruppe	Funktion
reset	erlaubt ein Reset des Geräts
firmware	erlaubt die Aktualisierung der Firmware des Geräts
upload	erlaubt Speichern und Löschen von Dateien im Verzeichnis Port_1/sx

Tabelle 9. Gruppen und deren Rechte

Die Zuordnung der Rechte-Gruppe zu einem Benutzernamen erfolgt dadurch, dass in der Zugangsverwaltungsdatei die Rechte-Gruppen in der gleichen Zeile hinter dem Benutzernamen und dem MD5 Passwort-Hash aufgelistet werden. Einem Nutzer können mehrere Rechte-Gruppen zugewiesen sein.



Hinweis: Der User `admin` ist immer automatisch Mitglied in allen drei Rechte-Gruppen `reset`, `firmware` und `upload`; auch wenn dem `admin` diese Rechte-Gruppen nicht explizit zugewiesen wurden.

4.2.2 Zugangsverwaltungsdatei `security.cfg`

In der Zugangsverwaltungsdatei `security.cfg` können Sie mit Hilfe eines einfachen Text-Editors neue Benutzer eintragen, einem Benutzer Rechte-Gruppen zuweisen, sowie ein Passwort in Form eines MD5-Hash eintragen.

Die ASCII-Textdatei beginnt mit der Angabe des Realm, danach folgen die Zeilen mit den Parametern der Benutzer. Eine Zeile enthält jeweils die Parameter eines einzelnen Benutzers. Dabei ist folgende Syntax zu beachten:

```
<Benutzername>;<MD5-Hash aus  
Benutzername:Realm:Passwort>;<Rechte-Gruppe1>,<Rechte-  
Gruppe2>;
```

Auf der Hilscher Communication Solutions DVD finden Sie unter Examples & API > WebServer pages > Common > Port_1 die Beispieldatei `security.cfg`, die Sie als Vorlage für ihre eigene Zugangsverwaltungsdatei verwenden und abändern können. Die Datei enthält bereits die drei vordefinierten Benutzer `user`, `manager` und `admin` mit folgenden Passwörtern und Rechten:

Benutzername	Passwort	Rechte-Gruppe
user	user	reset
manager	manager	reset, firmware
admin	admin	firmware, reset, upload

Tabelle 10. Benutzer-Passwort-Rechte-Matrix der Beispieldatei `security.cfg`

Diese Zuordnungen werden in der `security.cfg` mit den folgenden Zeichenketten realisiert:

```
Realm
{
netX
user;22176e7c9cae6489e738723d8a2aaeaf;reset;
manager;8e6225ec4bcace3ebe45b9e40a9ae325;reset,firmware;
admin;4f1cb4bf1c6adef50e6278fb95cfd12d;firmware,reset,upload;
}
```

Benutzername MD5-Hash Rechte-Gruppe(n)

Abbildung 5: Zeichenketten in Beispieldatei `security.cfg`

4.2.3 Generierung eines Passwort-Hashs mit MD5

Passwörter müssen in der Zugangsverwaltungsdatei als MD5-Hash hinterlegt werden. Sie können den Passwort-Hash mit jedem beliebigen MD5-Generator erzeugen und anschließend die erzeugte Zeichenkette in die entsprechende Zeile der Zugangsverwaltungsdatei `security.cfg` hineinkopieren.

Der MD5-Hash muss mit folgenden Parametern in folgender Syntax erzeugt werden:

`<Benutzername>:<Realm>:<Passwort>`

Für eine Nutzerin Hildegard Mustermann mit dem Passwort „Sommertag“ müssten Sie somit folgende Zeichenkette in den MD5-Generator eingeben:

`Hildegard Mustermann:netX:Sommertag`

Aus dieser Zeichenkette erzeugt der Generator den Hash `dc45c059135e49461f90bcc08bcb266d`.

Beachten Sie folgende Hinweise zu Benutzernamen und Passwörtern:

- Sie dürfen alle druckbaren ASCII-Zeichen und das Leerzeichen verwenden (ASCII-Zeichen 32 [dec] bis 126 [dec]), für den Benutzernamen jedoch kein Semikolon (;), da das Semikolon in der Zugangsverwaltungsdatei als Trennzeichen fungiert.
- Sie dürfen keine diakritischen Zeichen wie Umlaute (ä, ü, ö) oder Akzente (é, è, ê) und kein Eszett (ß) verwenden.
- Groß- und Kleinschreibung werden unterschieden.
- Die Schreibweise des Benutzernamens, die Sie im MD5-Generator und später im Anmelde-Dialog des WebServers verwenden, muss mit der Schreibweise in der Zugangsverwaltungsdatei übereinstimmen (z. B. in Hinblick auf Leerzeichen zwischen Vor- und Nachnamen).
- Die Schreibweise des Passworts, die Sie im MD5-Generator verwenden, muss mit der Schreibweise übereinstimmen, die Sie im Anmelde-Dialog des WebServers verwenden.

4.2.4 Zugangsverwaltungsdatei hochladen

Die Zugangsverwaltungsdatei `security.cfg` muss im Root-Verzeichnis von `Port_1` des Systems gespeichert werden.

Da der **File Upload** des WebServers nur auf das Verzeichnis `Port_1/sx` zugreifen kann, nicht aber auf das Root-Verzeichnis von `Port_1`, müssen Sie zum Hochladen der Zugangsverwaltungsdatei die Hilscher cifX Test Applikation verwenden.

Die cifX Test Applikation, die Bestandteil des cifX Device Drivers für Windows® ist, ermöglicht einen Zugriff auf das Kommunikationsmodul über dessen Host-Schnittstelle. Dazu müssen Sie das Kommunikationsmodul mit Hilfe eines Evaluation Boards in einen PC einbauen, bzw. mit einem PC verbinden, auf dem die cifX Test Applikation installiert ist. Nähere Informationen zum Einsatz von Evaluation Boards finden Sie in dem Benutzerhandbuch zu Ihrem Kommunikationsmodul.

Schrittanleitung Zugangsverwaltungsdatei hochladen

1. cifX Test Applikation starten.

➤ Doppelklicken Sie im Startmenü von Windows® den Eintrag **Systemsteuerung > cifX Test**.

➤ Die cifX Test Applikation öffnet sich.

2. Channel1 des Geräts in der cifX Test Applikation öffnen.

➤ Wählen Sie in der Menüleiste **Device > Open**

➤ Der Dialog **Channel Selection** öffnet sich.

➤ Markieren Sie im linken Fenster den Eintrag **Channel1** und klicken Sie anschließend die Schaltfläche **Open**.

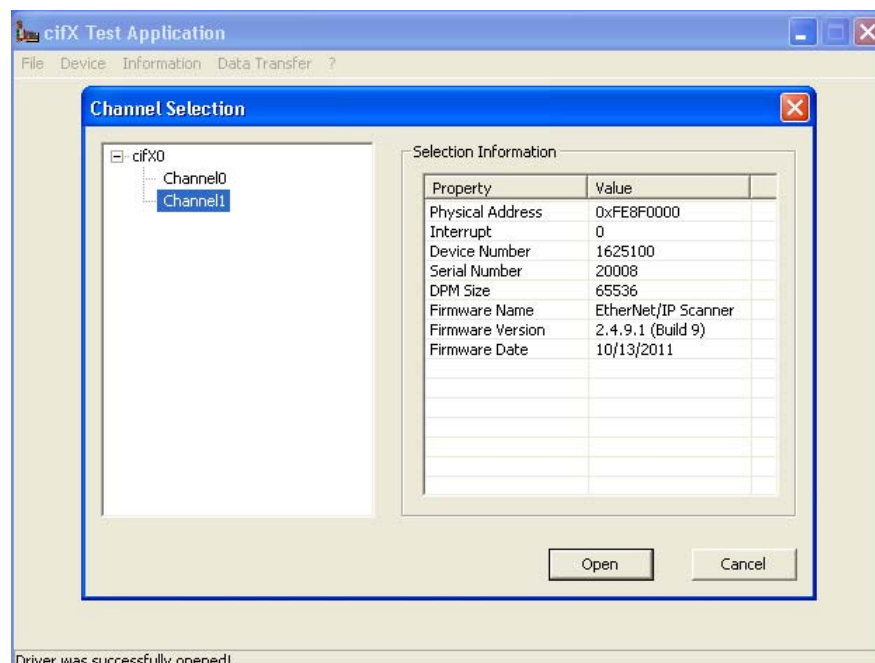



Abbildung 6: Auswahl des Channel in cifX Test Applikation

➤ Der Port ist geöffnet und der Dialog **Channel Selection** schließt sich wieder.

3. Zugangsverwaltungsdatei in das Gerät laden.

- Wählen Sie in der Menüleiste **Device > Download**.
- Das Fenster **Download Test** öffnet sich.
- Wählen Sie in der Dropdown-Liste **Download Mode** den Eintrag **File Download**.
- Klicken Sie in der Zeile **Filename** auf die Schaltfläche , um den Dateiauswahl-Dialog zu öffnen.
- Wählen Sie im Dateiauswahl-Dialog die Datei `security.cfg` auf Ihrem Dateisystem und klicken Sie anschließend die Schaltfläche **Öffnen**.
- Der Dateiauswahl-Dialog schließt sich wieder.
- Klicken Sie die Schaltfläche **Download**, um die Zugangsverwaltungsdatei in das Gerät zu übertragen.



Hinweis: Beachten Sie, dass eine bereits auf dem Gerät vorhandene `security.cfg` beim Download überschrieben wird, ohne dass Sie eine Warnmeldung erhalten.

Die in den Root-Verzeichnissen des Geräts gespeicherten Dateien können Sie sich in der cifX Test Applikation unter **Device > File Explorer** anzeigen lassen und gegebenenfalls auf Ihr lokales System herunterladen (öffnen Sie vorher den entsprechenden Port bzw. Channel).

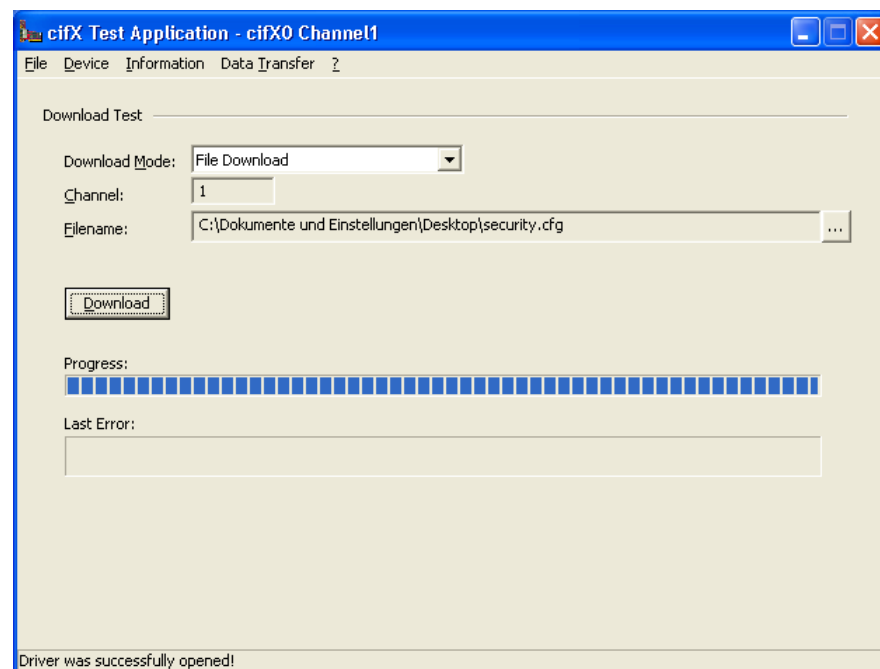


Abbildung 7: Zugangsverwaltungsdatei übertragen

- Sie haben die Zugangsverwaltungsdatei in das Gerät übertragen.



Hinweis: Um die neue Zugangsverwaltungsdatei zu aktivieren, müssen Sie ein Reset auf dem Gerät ausführen.

In der cifX Test Applikation können Sie dies unter **Device > Reset** tun.

4.2.5 Zugangsverwaltungsdatei löschen

Sie können die Zugangsverwaltungsdatei `security.cfg` mit der cifX Test Applikation vom WebServer löschen und somit die Default-Zugangsparameter wieder in Kraft setzen.

Schrittanleitung Zugangsverwaltungsdatei löschen

- Starten Sie die cifX Test Applikation und öffnen Sie Channel1 wie in den Schritten 1 und 2 im Abschnitt *Zugangsverwaltungsdatei hochladen* beschrieben.
- Wählen Sie **Device > File Explorer** und markieren Sie die unter **Filename** aufgeführte `security.cfg`.

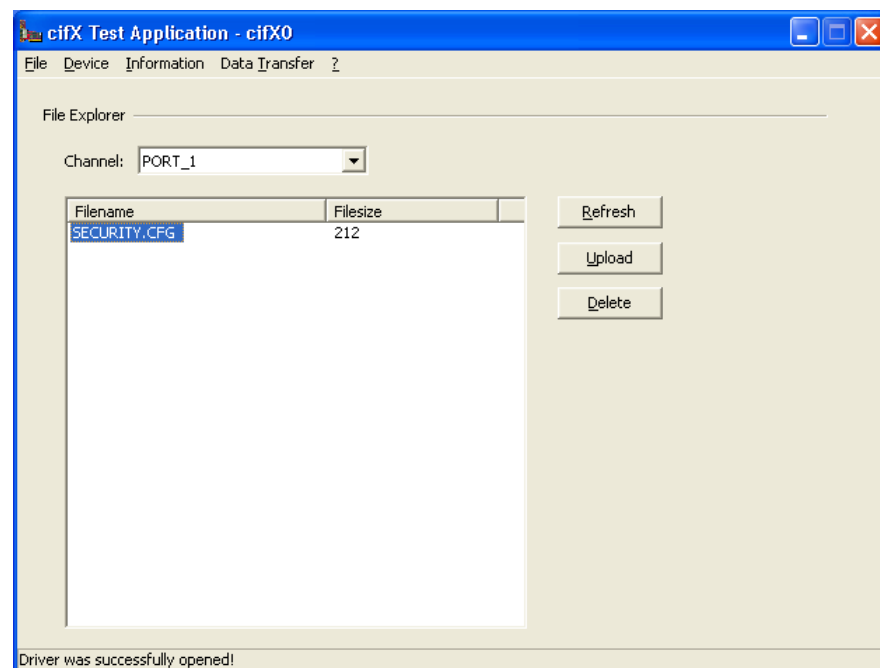


Abbildung 8: Dateien in File Explorer anzeigen und löschen



Hinweis: Sie können die Datei bei Bedarf vor dem Löschen sichern, indem Sie sie mit der Schaltfläche **Upload** vom WebServer auf Ihren PC hochladen und dort speichern.

- Klicken Sie die Schaltfläche **Delete**, um die Datei zu löschen.
- Führen Sie unter **Device > Reset** ein Reset aus.
- Sie haben die Zugangsverwaltungsdatei `security.cfg` gelöscht. Es gelten wieder die Default-Zugangsparameter (siehe Abschnitt *Default-Zugangsverwaltung* auf Seite 15).

5 Eigene Inhalte einbinden

5.1 Übersicht

Sie können eigene Webseiten und Grafiken (z. B. Ihr Firmenlogo) auf dem WebServer hinterlegen oder die vorhandenen Webseiten ändern, um das Design der vom WebServer angezeigten Seiten nach Ihren Wünschen zu gestalten.

Neue Dateien können Sie mit dem **File Upload** in das öffentliche Verzeichnis des WebServers `Port_1/sx/pub` hochladen, wie im Abschnitt *File Upload* auf Seite 11 beschrieben.

Beachten Sie dabei folgendes:

- Es werden nur 8.3 Namen unterstützt, d. h. ein Dateiname darf nicht mehr als acht Zeichen umfassen, die Namensweiterung nicht mehr als drei Zeichen.
- Der Speicherbedarf der Dateien im öffentlichen Verzeichnis sollte insgesamt zwei Megabyte nicht überschreiten.

Die HTTP-Funktionen **Firmware Update**, **File Upload** und **Reset** bleiben von Änderungen, die Sie im öffentlichen Verzeichnis vornehmen, unberührt, da die eigentlichen HTML-Seiten, die den Code für diese Funktionen enthalten, für den Nutzer unzugänglich abgelegt sind. Selbst wenn Sie sämtliche Seiten, die Links auf diese Funktionen enthalten, im öffentlichen Ordner löschen, können Sie diese Funktionen immer noch direkt über deren URL aufrufen. Die entsprechenden URLs finden Sie in der Tabelle *HTTP-Funktionen direkt aufrufen* auf Seite 7.

Beispieldateien auf Communication Solutions DVD

Auf der Hilscher Communication Solutions DVD finden Sie unter `Examples & API > WebServer pages > Common > Port_1 > sx > pub` die gleichen Dateien, die sich nach Auslieferung Ihres Gerätes auch im öffentlichen Verzeichnis des WebServers befinden und die bei Aufruf des WebServers angezeigt werden. Diese Dateien können Sie lokal als Templates verwenden und nach Ihren Wünschen abändern – indem Sie z. B. neuen HTML-Code einfügen, das Stylesheet ändern oder Grafiken durch eigene Logos ersetzen – und anschließend auf den WebServer hochladen.



Hinweis: Bei der Bilddatei `device.jpg` im Verzeichnis `Examples & API > WebServer pages > Common > Port_1 > sx > pub` auf der DVD handelt es sich um eine Platzhalter-Datei. Sie finden ein Bild von Ihrem Gerät auf der DVD im Verzeichnis `Examples & API > WebServer pages > Product` in einem Unterordner, der nach Ihrem Gerät benannt ist (zur Zeit `comX` oder `netJACK`).

Server Side Includes und Inlineframes

Die meisten Seiten des WebServers arbeiten mit Server Side Includes (SSI) und Inlineframes (iframe), mit deren Hilfe man HTML-Code oder andere Webseiten dynamisch einbinden kann. Eine HTML-Datei, die SSI-Anweisungen enthält, muss die Dateieindung `.sht` oder `.stm` aufweisen, um vom WebServer verarbeitet werden zu können.

In den Dateien `fwupdate.sht`, `reset.sht` und `upload.sht` beispielsweise ist die Menüleiste als SSI Anweisung `<!--#include file="menu.prt" -->` eingebunden, und die HTML-Seiten, die den eigentlichen Code für die Funktionen **Firmware Update**, **File Upload** und **Reset** enthalten, sind als iframes (z. B. `<iframe src="fwupdate"...">`) eingebettet.

5.2 Beispiele für das Einbinden eigener Inhalte

Nachfolgend finden Sie Schrittanleitungen für typische Anpassungen, die Sie als Nutzer an den Webseiten des WebServers vornehmen können. Beachten Sie, dass dies beispielhafte Beschreibungen sind, und – abhängig von Ihren Kenntnissen in Webdesign – auch andere Vorgehensweisen möglich sind.

5.2.1 Beispiel 1: Firmenlogo in der Navigationsleiste austauschen

In der Navigationsleiste der WebServer-Seiten befindet sich oben rechts das Hilscher-Logo. Weil hinter diesem Logo ein Hyperlink hinterlegt ist, gelangen Sie durch Anklicken des Logos mit Ihrem Browser auf die Firmenwebseite der Hilscher GmbH. Wenn Sie das Hilscher-Logo durch Ihr eigenes Firmenlogo ersetzen möchten, und der Hyperlink auf Ihre eigene Firmenwebseite führen soll, gehen Sie folgendermaßen vor:

1. Bilddatei austauschen. Hierfür müssen Sie keinen HTML-Code ändern.
 - Überschreiben Sie einfach die auf dem WebServer vorhandene Bilddatei `logo.png`, die das Hilscher-Logo enthält. Dazu müssen Sie lediglich eine PNG-Datei gleichen Namens mit Ihrem Firmenlogo per File Upload auf den WebServer in den Ordner `pub` hochladen. (Siehe Abschnitt *File Upload* auf Seite 11.)
Für das Logo sind Abmessungen von etwa 150 (Breite) x 100 (Höhe) in Pixeln empfehlenswert.
 - Sobald Sie eine Seite des WebServers erneut aufrufen, wird statt des Hilscher-Logos die neue Bilddatei mit Ihrem Firmenlogo angezeigt.
2. Hyperlink anpassen. Hierfür müssen Sie in der Datei `menu.prt` den HTML-Code ändern, der die Inhalte des Navigationsmenüs definiert.
 - Kopieren Sie die Datei `menu.prt`, die sich auf der Hilscher Communication Solutions DVD im Ordner `Examples & API > WebServer pages > Common > Port_1 > sx > pub` befindet, auf Ihren PC.

- Öffnen Sie die Datei mit dem Windows-Editor.
- Sie sehen den HTML-Code der Datei `menu.prt`:

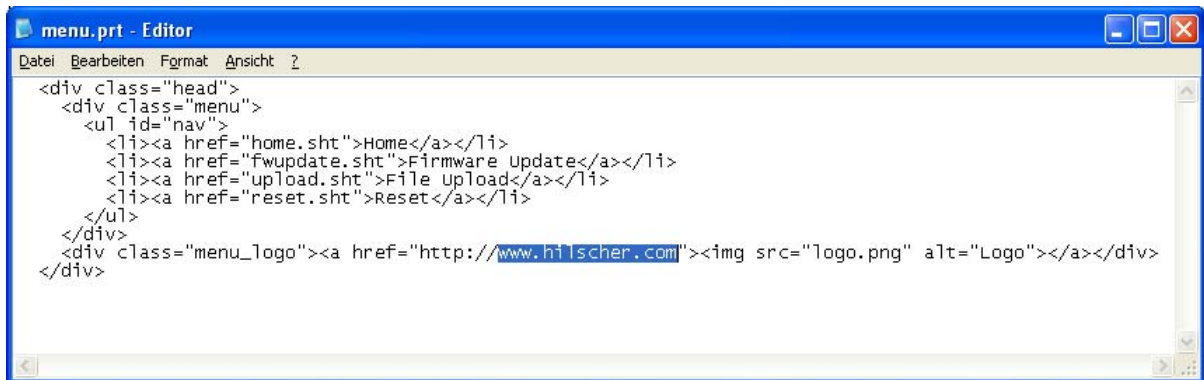


Abbildung 9: Hyperlink in `menu.prt` editieren

- Ersetzen Sie die Webadresse `www.hilscher.com` durch Ihre eigene Webadresse, z. B. `www.mustermann-automation.com`.
- Speichern und schließen Sie die Datei.
- Transferieren Sie die geänderte Datei `menu.prt` mittels File Upload auf den WebServer in den Ordner `pub` (siehe Abschnitt *File Upload* auf Seite 11). Dabei überschreiben Sie die alte `menu.prt` Datei.
- Sobald Sie eine Seite des WebServers erneut aufrufen und auf das Logo klicken, wird Ihr Browser auf Ihre Firmenwebseite weitergeleitet.

5.2.2 Beispiel 2: Design der Navigationsleiste ändern

Wenn Sie z. B. das Hintergrundbild der Navigationsleiste austauschen möchten, können Sie einfach die auf dem WebServer vorhandene Bilddatei `menubg.jpg`, die das Hintergrundbild enthält, durch eine gleichnamige Bilddatei ersetzen, die Sie per File Upload in den Ordner `pub` des WebServers hochladen. (Siehe Abschnitt *File Upload* auf Seite 11.) Für das Hintergrundbild sind Abmessungen von 932 (Breite) x 152 (Höhe) in Pixeln empfehlenswert.

Layout und Design der Seiten, die der WebServer anzeigt, werden im Cascading Style Sheet `style.css` definiert. Wenn Sie in der Navigationsleiste statt eines Bildes z. B. nur eine blaue Fläche als Hintergrund haben möchten, müssen Sie Änderungen im Style Sheet vornehmen. Gehen Sie hierzu wie folgt vor:

- Kopieren Sie die Datei `style.css`, die sich auf der Hilscher Communication Solutions DVD im Ordner `Examples & API > WebServer pages > Common > Port_1 > sx > pub` befindet, auf Ihren PC.
- Öffnen Sie die Datei mit einem geeigneten Editor-Programm.

☞ Sie sehen die in der Datei `style.css` enthaltenen Deklarationen:

```
* {
    font-family:Arial;
}

body {
    text-align:left;
    background-color:#E9E9EA;
}

/** NAVIGATION MENU **/
.head {
    margin:0; border:0; padding:0;
    height: 152px;
    max-width: 932px;
    background-color:#e01010;
    background-image:url(menubg.jpg);
    background-repeat:no-repeat;
    background-position:left top;
}

.menu {
    margin: 0; padding: 0;
    min-width: 28em;
    float: left;
}
```

Abbildung 10: Ausschnitt aus `style.css`

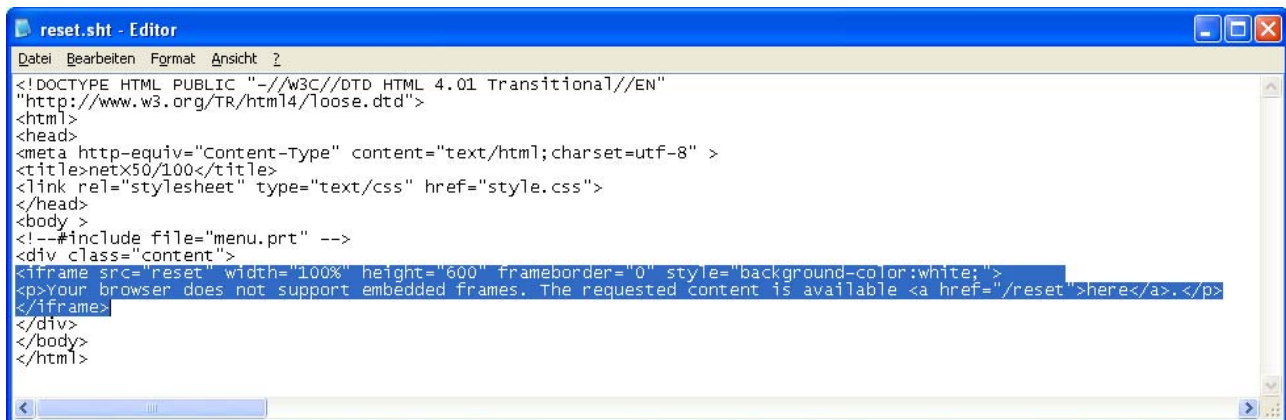
- Navigieren Sie zu dem Selektor `.head` im Abschnitt `*** NAVIGATION MENU ***` und entfernen Sie das Hintergrundbild, indem Sie den Zeichenstring `background-image:url(menubg.jpg);` löschen. Ändern Sie anschließend die Hintergrundfarbe, indem Sie hinter dem Parameter `background-color` den Zeichenstring `#e01010` (steht für Rot) durch einen Wert für Blau ersetzen, z. B. `#0000FF`.
- Speichern und schließen Sie die Datei.
- Transferieren Sie die geänderte Datei `style.css` mittels File Upload auf den WebServer in den Ordner `pub` (siehe Abschnitt *File Upload* auf Seite 11). Dabei überschreiben Sie die alte `style.css` Datei.
- ☞ Sobald Sie eine Seite des WebServers erneut aufrufen, wird die Navigationsleiste mit blauem Hintergrund angezeigt.

5.2.3 Beispiel 3: Neue Webseite einbinden

Sie können eigene Webseiten auf den WebServer hochladen und Links auf diese Seiten in die Navigationsleiste einfügen. Wenn Sie z. B. eine Webseite einbinden möchten, die eine Arbeitsanweisung enthält, gehen Sie folgendermaßen vor:

1. Erstellen Sie die Webseite, die die Arbeitsanweisung enthält. Sie können hierfür eine bereits vorhandene Webseite als Template verwenden.
- Kopieren Sie die Datei `reset.sht`, die sich auf der Hilscher Communication Solutions DVD im Ordner `Examples & API > WebServer pages > Common > Port_1 > sx > pub` befindet, auf Ihren PC.
 - Öffnen Sie die Datei mit einem geeigneten Editor-Programm.

- Sie sehen den HTML-Code der Datei `reset.sht` (zur besseren Übersichtlichkeit wurden in der nachfolgenden Abbildung Zeilenumbrüche eingefügt):



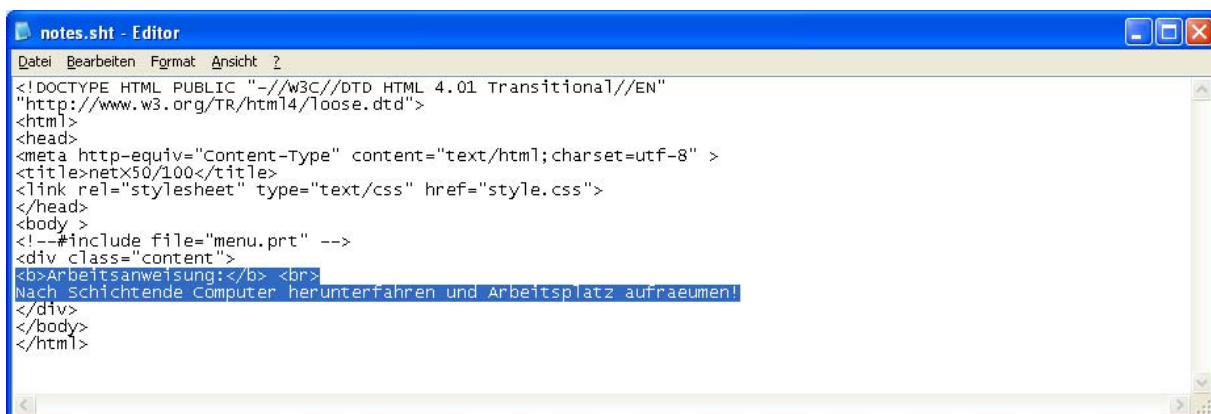
```

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" >
<title>netx50/100</title>
<link rel="stylesheet" type="text/css" href="style.css">
</head>
<body>
<!--#include file="menu.prt" -->
<div class="content">
<iframe src="reset" width="100%" height="600" frameborder="0" style="background-color:white;">
<p>Your browser does not support embedded frames. The requested content is available <a href="/reset">here</a>.</p>
</iframe>
</div>
</body>
</html>

```

Abbildung 11: `reset.sht` als Template für eigene Webseite verwenden – `iframe` Element löschen

- Löschen Sie das `iframe`-Element aus dem HTML-Code (d. h. den Zeichenstring von einschließlich `<iframe src="reset"...` bis `</iframe>`) und fügen Sie an gleicher Stelle den Text Ihrer Arbeitsanweisung ein.



```

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" >
<title>netx50/100</title>
<link rel="stylesheet" type="text/css" href="style.css">
</head>
<body>
<!--#include file="menu.prt" -->
<div class="content">
<b>Arbeitsanweisung:</b> <br>
Nach Schichtende Computer herunterfahren und Arbeitsplatz aufräumen!
</div>
</body>
</html>

```

Abbildung 12: `reset.sht` als Template für eigene Webseite verwenden – eigenen Text einfügen

- Speichern Sie die Datei z. B. als `notes.sht`. Achten Sie darauf, dass der Dateiname nicht mehr als acht Zeichen aufweist und die Dateinamenerweiterung `.sht` lautet.
- Transferieren Sie die Datei `notes.sht` mittels File Upload auf den WebServer in den Ordner `pub` (siehe Abschnitt *File Upload* auf Seite 11).

- 2. Link auf neue Webseite in die Navigationsleiste einfügen. Hierfür müssen Sie in der Datei `menu.prt`, die die Inhalte des Navigationsmenüs definiert, den Hyperlink ergänzen.
- Kopieren Sie die Datei `menu.prt`, die sich auf der Hilscher Communication Solutions DVD im Ordner `Examples & API > WebServer pages > Common > Port_1 > sx > pub` befindet, auf Ihren PC.
- Öffnen Sie die Datei mit dem Windows-Editor
- Sie sehen den HTML-Code der Datei `menu.prt`:

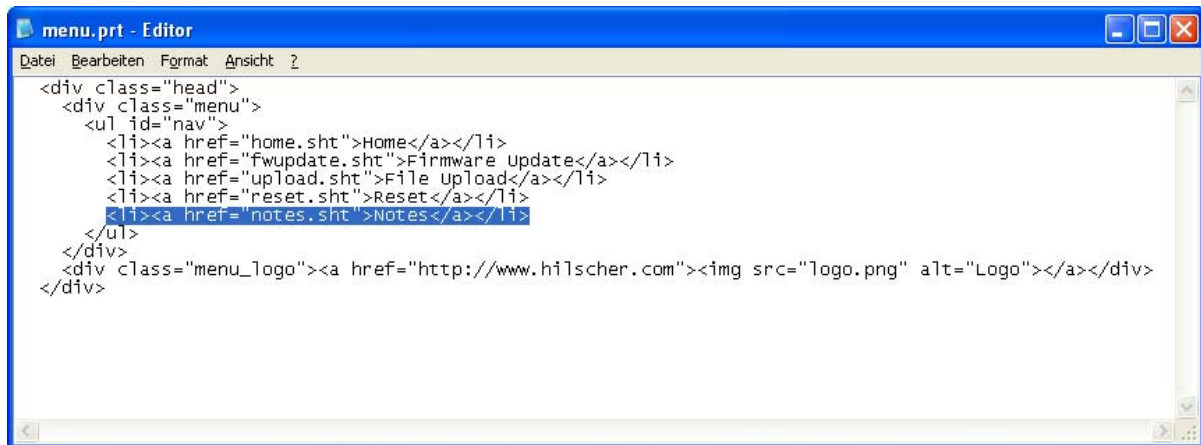


Abbildung 13: Hyperlink auf neue Webseite einfügen

- Fügen Sie den Hyperlink
`Notes` ein.
- Speichern und schließen Sie die Datei.
- Transferieren Sie die geänderte Datei `menu.prt` mittels File Upload auf den WebServer in den Ordner `pub` (siehe Abschnitt *File Upload* auf Seite 11). Dabei überschreiben Sie die alte `menu.prt` Datei.
- Sobald Sie eine Seite des WebServers erneut aufrufen, sehen Sie den neuen Hyperlink in der Navigationsleiste und können Ihre neue Webseite aufrufen, indem Sie auf den Link klicken oder die IP-Adresse samt Dateinamen (`http://<IP-Adresse>/notes.sht`) in die Adresszeile des Browsers eingeben.

6 Zugriff auf Verzeichnisse

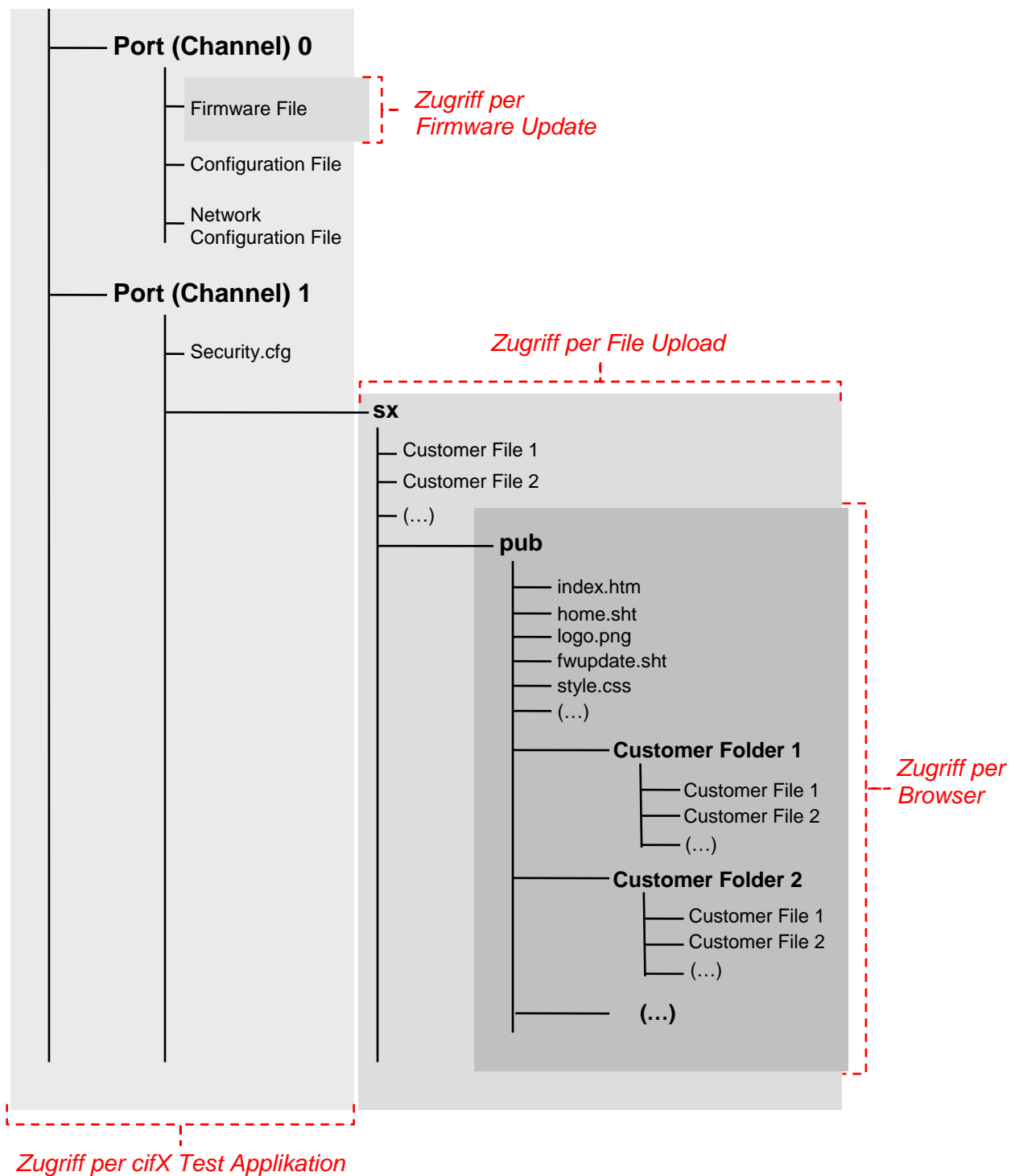


Abbildung 14: Zugriff auf Verzeichnisse des Systems

7 Anhang

7.1 Abbildungsverzeichnis

Abbildung 1: Startseite WebServer (Darstellung im Internet Explorer, kann in anderen Browsern abweichen).....	8
Abbildung 2: Firmware Update (Darstellung im Internet Explorer, kann in anderen Browsern abweichen)	9
Abbildung 3: File Upload (Darstellung im Internet Explorer, kann in anderen Browsern abweichen)	11
Abbildung 4: Reset (Darstellung im Internet Explorer, kann in anderen Browsern abweichen)	14
Abbildung 5: Zeichenketten in Beispieldatei security.cfg.....	17
Abbildung 6: Auswahl des Channel in cifX Test Applikation	19
Abbildung 7: Zugangsverwaltungsdatei übertragen	20
Abbildung 8: Dateien in File Explorer anzeigen und löschen	21
Abbildung 9: Hyperlink in menu.prt editieren.....	24
Abbildung 10: Ausschnitt aus style.css	25
Abbildung 11: reset.sht als Template für eigene Webseite verwenden – iframe Element löschen.....	26
Abbildung 12: reset.sht als Template für eigene Webseite verwenden – eigenen Text einfügen.....	26
Abbildung 13: Hyperlink auf neue Webseite einfügen	27
Abbildung 14: Zugriff auf Verzeichnisse des Systems	28

7.2 Tabellenverzeichnis

Tabelle 1: Änderungsübersicht.....	3
Tabelle 2: Abkürzungen	3
Tabelle 3: Liste der Geräte und Firmware mit integriertem WebServer	5
Tabelle 4: Übersicht der Webseiten und deren URLs	7
Tabelle 5: HTTP-Funktionen direkt aufrufen	7
Tabelle 6: Bedienelemente Firmware-Update	10
Tabelle 7: Bedienelemente Datei-Upload.....	12
Tabelle 8: Bedienelemente Dateien löschen	13
Tabelle 9: Gruppen und deren Rechte	16
Tabelle 10: Benutzer-Passwort-Rechte-Matrix der Beispieldatei security.cfg	17

7.3 Kontakte

Hauptsitz

Deutschland

Hilscher Gesellschaft für
Systemautomation mbH
Rheinstrasse 15
65795 Hattersheim
Telefon: +49 (0) 6190 9907-0
Fax: +49 (0) 6190 9907-50
E-Mail: info@hilscher.com

Support

Telefon: +49 (0) 6190 9907-99
E-Mail: de.support@hilscher.com

Niederlassungen

China

Hilscher Systemautomation (Shanghai) Co. Ltd.
200010 Shanghai
Telefon: +86 (0) 21-6355-5161
E-Mail: info@hilscher.cn

Support

Telefon: +86 (0) 21-6355-5161
E-Mail: cn.support@hilscher.com

Frankreich

Hilscher France S.a.r.l.
69500 Bron
Telefon: +33 (0) 4 72 37 98 40
E-Mail: info@hilscher.fr

Support

Telefon: +33 (0) 4 72 37 98 40
E-Mail: fr.support@hilscher.com

Indien

Hilscher India Pvt. Ltd.
New Delhi - 110 025
Telefon: +91 11 40515640
E-Mail: info@hilscher.in

Italien

Hilscher Italia srl
20090 Vimodrone (MI)
Telefon: +39 02 25007068
E-Mail: info@hilscher.it

Support

Telefon: +39 02 25007068
E-Mail: it.support@hilscher.com

Japan

Hilscher Japan KK
Tokyo, 160-0022
Telefon: +81 (0) 3-5362-0521
E-Mail: info@hilscher.jp

Support

Telefon: +81 (0) 3-5362-0521
E-Mail: jp.support@hilscher.com

Korea

Hilscher Korea Inc.
Suwon, 443-810
Telefon: +82-31-204-6190
E-Mail: info@hilscher.kr

Schweiz

Hilscher Swiss GmbH
4500 Solothurn
Telefon: +41 (0) 32 623 6633
E-Mail: info@hilscher.ch

Support

Telefon: +49 (0) 6190 9907-99
E-Mail: ch.support@hilscher.com

USA

Hilscher North America, Inc.
Lisle, IL 60532
Telefon: +1 630-505-5301
E-Mail: info@hilscher.us

Support

Telefon: +1 630-505-5301
E-Mail: us.support@hilscher.com