

Automatisierungstechnik nach internationaler Norm programmieren (17)

Autor: Dr. Ulrich Becker

Fachzentrum Automatisierungstechnik und vernetzte Systeme im BTZ Rohr-Kloster

Mail: Ulrich.Becker@BTZ-Rohr.de

Beispiele für IT-Funktionen in der Automatisierungstechnik (Teil 1)

Die Folgen 15 und 16 führten ein in die Vernetzung von Automatisierungskomponenten mit Ethernet / TCP / UDP. Der Zugang zu den Controllern erfolgte über die gewöhnliche Netzcard des PC. Vernetzt man mit Ethernet, so steht dem Zugang eines Controllers zum weltweiten Netz (Web) grundsätzlich nichts im Wege. Damit stehen der Automatisierungstechnik eine Vielzahl der Internet-Technologien (IT) zur Verfügung. Die vorliegende Folge führt beispielhaft in einige IT-Funktionen ein und regt zur weiteren Arbeit und Weiterbildung auf diesem innovativen Gebiet an.

Systemadministratoren entscheiden über Zugangsmöglichkeiten

Solange wir im Labor oder in den Unternehmen in lokalen Automatisierungsnetzen arbeiten, sind - ähnlich wie beim Zugang des Programmiergeräts zum Controller bereits praktiziert - auch bei Nutzung von IT-Funktionen weniger Probleme zu erwarten. Verlassen wir aber diese lokalen Grenzen, so ist die Zusammenarbeit mit den Systemadministratoren der Unternehmen unverzichtbar. Nur diese legen fest, ob und wie wir von außen über Servereinstellungen und Firewalls hinweg einen Zugang zu Automatisierungskomponenten erhalten. **Bild 97** erinnert an Wege und mögliche Probleme beim Zugang zu Ethernet-Controllern über das Internet mit Hardware- und Software-Lösungen für Firewalls.

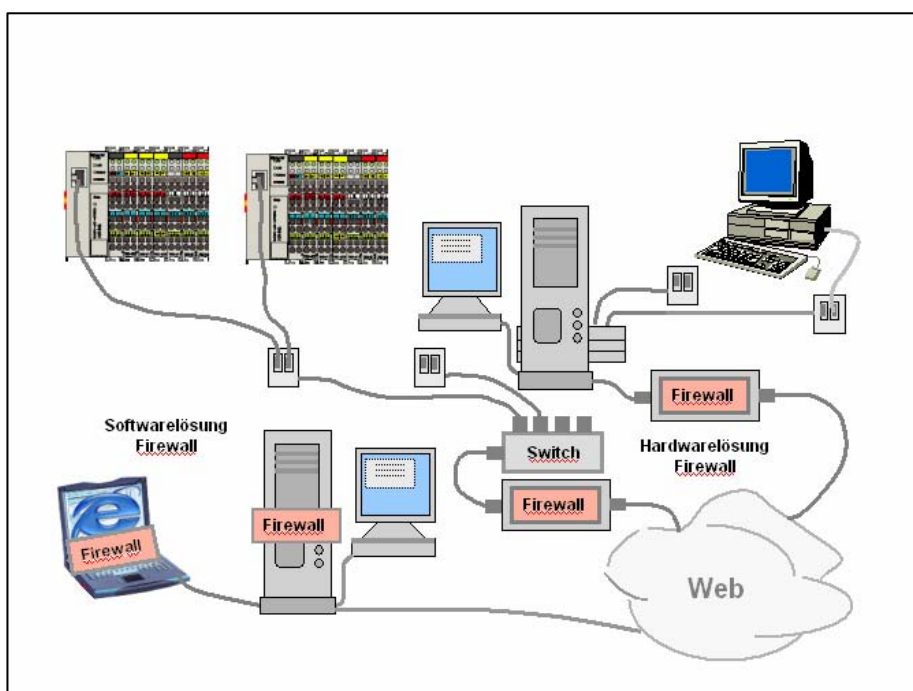


Bild 97: Wege und mögliche Hindernisse beim Zugang zu einem Controller über das Internet

Eine mögliche Methode der Kommunikation zu Automatisierungskomponenten über das Internet ist die Technologie der Virtuellen Privaten Netze (VPN). **Bild 98** zeigt vereinfacht diese Zusammenhänge. Der Datentransport durch das öffentliche Netz erfolgt hierbei über gesicherte Tunnel wie in einem lokalen Netz, aber ohne direkte Verbindung. Die Verbindung wird verschlüsselt, nicht aber die Daten selbst. Eine aktuelle Protokollerweiterung für die Verschlüsselung ist IPSecurity (IPSec). Dafür gibt es spezielle IPSec-Softwaretools. Ein VPN-

Tunnel vom Typ Site-to-Site verbindet zwei lokale Netze über je ein VPN Gateway. Der Typ Site-to-End verbindet einen PC am Internet mit einem VPN Gateway am lokalen Netz auf der anderen Seite des Web.

Weiter müssen wir uns bewußt sein, dass ein Ethernet-Controller nur dann über das Web angesprochen werden kann, wenn er ständig Verbindung zum Internet unterhält. In großen Unternehmen mit dauerhaftem Internet-Zugang ist das denkbar. Auch wenn man heute häufig einen vorhandener DSL-Anschluß mitnutzen kann, wird dennoch in kleinen Automatisierungsanlagen wegen der Kosten kein dauerhafter Internetzugang geschaltet. Will man in diesem Fall Zugang zum Controller haben, so muß dieser selbst zunächst eine Verbindung zum Internet schalten. Dies kann z.B. durch Telefonanruf über spezielle Modems (z.B. Modem X1200 II von Bintec) erfolgen. Die Modems schalten nach Anruf über den D- oder B-Kanal des ISDN oder aber auch über analoge Telefonverbindung einen VPN-Tunnel. Andere Lösungen nutzen Internet Service Provider, welche nach geschütztem Anruf die VPN ermöglichen. Die Parametrierung der VPN-Modems kann mit dem Software-Tool „Hyperterminal“ im System Windows erfolgen, erfordert aber beträchtliche Einarbeitungszeit und Fachwissen. Alternativ können heute Kontrolle und Fernwartung von Automatisierungstechnik selbstverständlich auch über Telefonadapter und Telefonnetz allein gestaltet werden. Vorteilhaft ist dabei, daß insbesondere ISDN von sich aus bereits eine sichere Verbindung ist.

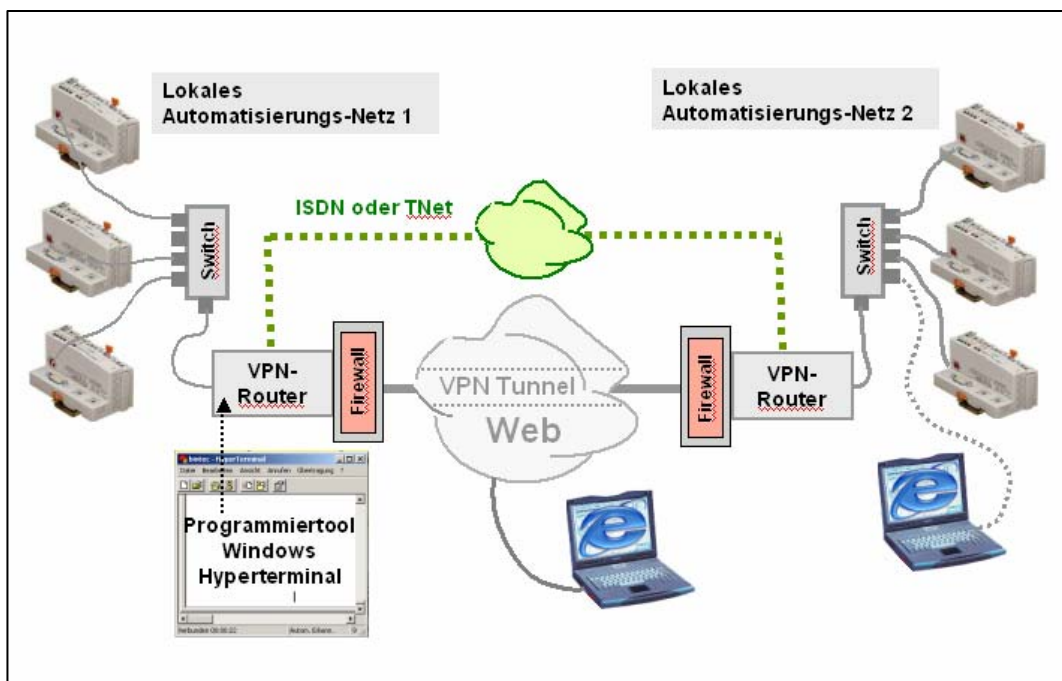


Bild 98: VPN für den Datentransfer im Internet (Tunnelung)

Die genannten Themen begründen, warum zukünftige Automatisierungstechniker die Zusammenarbeit mit Systemadministratoren, Informatikern und Programmierern suchen oder Dienstleitungen von Fachbetrieben für Netztechnik in Anspruch nehmen sollten. Ein weitere Grund dafür ist, dass bestimmte Internetfunktionen auch neuartige Aufgaben wie beispielsweise des Programmieren von HTML-Seiten erforderlich machen können. Andererseits sind Weiterbildung und Einarbeitung in grundlegende Zusammenhänge der Internet-Technologien angesichts des Wandels der Automatisierungstechnik dringend erforderlich! Allein schon die Fähigkeit, den versierten Fachkräften das Problem exakt nennen zu können, macht diese Arbeit lohnenswert!

In dieser Folge werden einige IT-Funktionen des programmierbaren Ethernet-Feldbus-controller WAGO 750-841 aufgezeigt. Ziel sind Anregungen, sich in Zusammenarbeit mit Fachleuten der Netztechnik solchen innovativen Aufgaben zu stellen.

Parametrierung und Kontrolle von Automatisierungskomponenten über Web-Browser

Eine naheliegende Nutzung der Internet-Technologien ist die Beobachtung des Zustandes von Controllern über das Web. Dazu wird im Browser – beispielsweise dem Internetexplorer - anstelle einer gewohnten Internetadresse die IP oder ggf. der Name des Controllers eingetragen. Ist der Controller im Netz erreichbar, so meldet er sich als Web-Server mit seinen internen Web-Seiten. Eine Reihe von Seiten sind bei der Werksauslieferung bereits eingetragen. Für eigene Zwecke können weitere Seiten ergänzt werden.

Bild 99 zeigt die Einstiegsseite des PFC WAGO 750-841 mit grundsätzlichen Informationen und der Übersicht der verfügbaren Web-Seiten im Bild links.

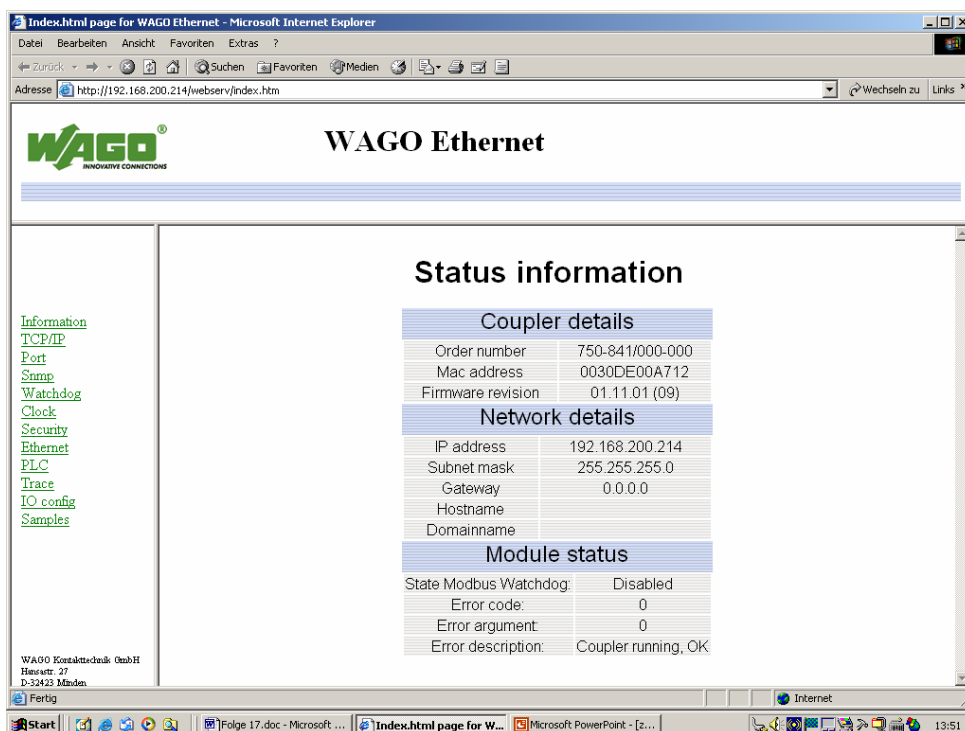


Bild 99: Zugang zu einem Controller mittels Internet Browser und IP-Adresse, links die Übersicht der verfügbaren Web-Seiten.

Interessant ist die Seite „Port“ (**Bild 100**). Sie erlaubt uns nach Eingabe eines Benutzernamens und eines Kennwortes (werkseitige Voreinstellung: Admin, wago) die Kontrolle, welche Protokolle im Controller aktiviert sind. Dies ist von Bedeutung, wenn wir beispielsweise die Protokolle BootP oder FTP nutzen oder deaktivieren wollen. Im PFC nach Bild 100 wurden die Protokolle FTP, HTTP, Modbus TCP sowie die Codes für CoDeSys und WebVisualisierung freigeschaltet. Dagegen wurde das Protokoll BootP zum Eintrag einer IP-Adresse in den Controller (siehe Folge 4) pflichtgemäß abgeschaltet, weil dieser sonst nach jedem Einschalten mit Spannungswiederkehr den Eintrag einer IP über BootP erwartet. Die Vielzahl der verfügbaren Protokolle verweist wiederum auf Themenfelder, die dem „klassischen Automatisierungstechniker“ zunächst nicht geläufig sind und bei denen fortwährender Weiterbildungsbedarf besteht.

Schaltet man das Protokoll DHCP im Controller frei, so kann der PFC auch mit einer dynamisch vom DHCP-Server vergebenen IP-Adresse arbeiten. Mit DHCP übernimmt der Controller nach dem Einschalten für die Zeitdauer seiner Kommunikation oder für eine festgelegte „Mietzeit“ eine der freien IP-Adressen des lokalen Netzwerkes. Der DHCP-Server steht im lokalen Netz. Seine Einrichtung ist genau wie die Einrichtung des Fernzugriffs über das Internet Aufgabe des Systemadministrators.

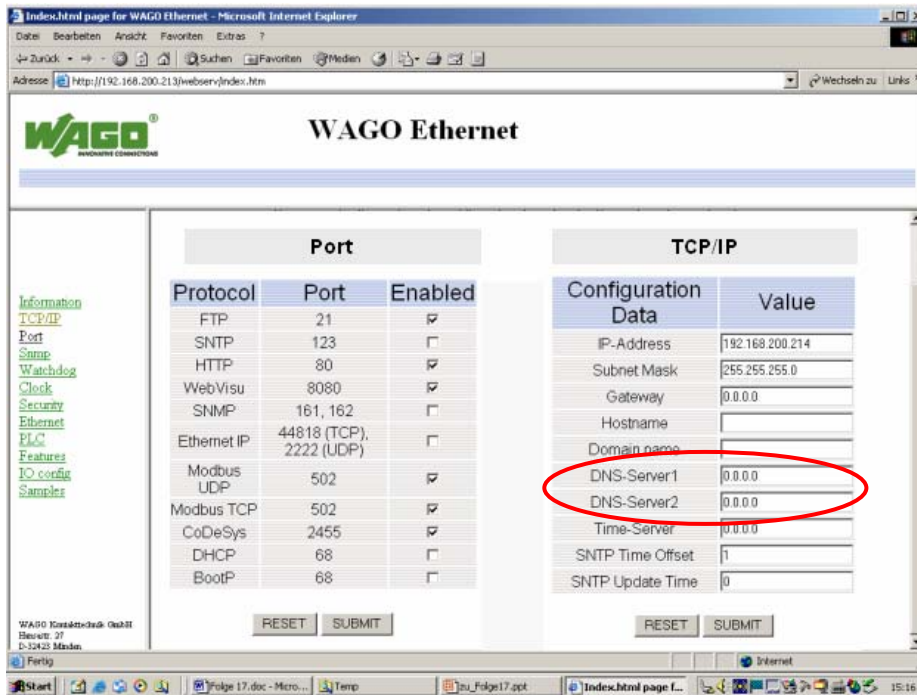


Bild 100: Inhalt der Web-Seiten Port und TCPI/IP (Seiten im Bild montiert)

Auch die Vergabe von Namen an PFC 841 ist möglich. Der Controller unterstützt das Domain Name Systems (DNS). DNS wandelt Namen in IP-Adressen und umgekehrt. Grundlage für DNS ist eine weltweit verteilte Datenbank, und die Namen werden von DNS-Servern verwaltet. Nach Namensvergabe kann ein Teilnehmer im Internet anstelle mit der eher ungewohnten IP-Adresse mit seinem Namen lokalisiert werden. Dies ist im Internet allgegenwärtige Methode. Für einen PFC 841 können bis zu zwei DNS-Servern angegeben werden (Bild 101 rechts). Das Einrichten übernehmen Internet Provider und Systemadministrator.

Um sich im lokalen Netz die Arbeit zu erleichtern und Namen statt IP-Adressen zu verwenden, kann man DNS umgehen und die Namen in der Windows Datei „hosts“ verwalten. Ein Beispiel zeigt **Bild 101**. Im Windows Explorer wurde unter *Programme \ WINNT \ System 32 \ drivers \ etc* in der Datei „hosts“ zwei Alias-Namen für IP eingerichtet, im Bild die Namen PFC_213 und PFC_214. Danach kann der Controller auch unter diesem Namen mit dem Browser erreicht werden (Bild 102 unten rechts).

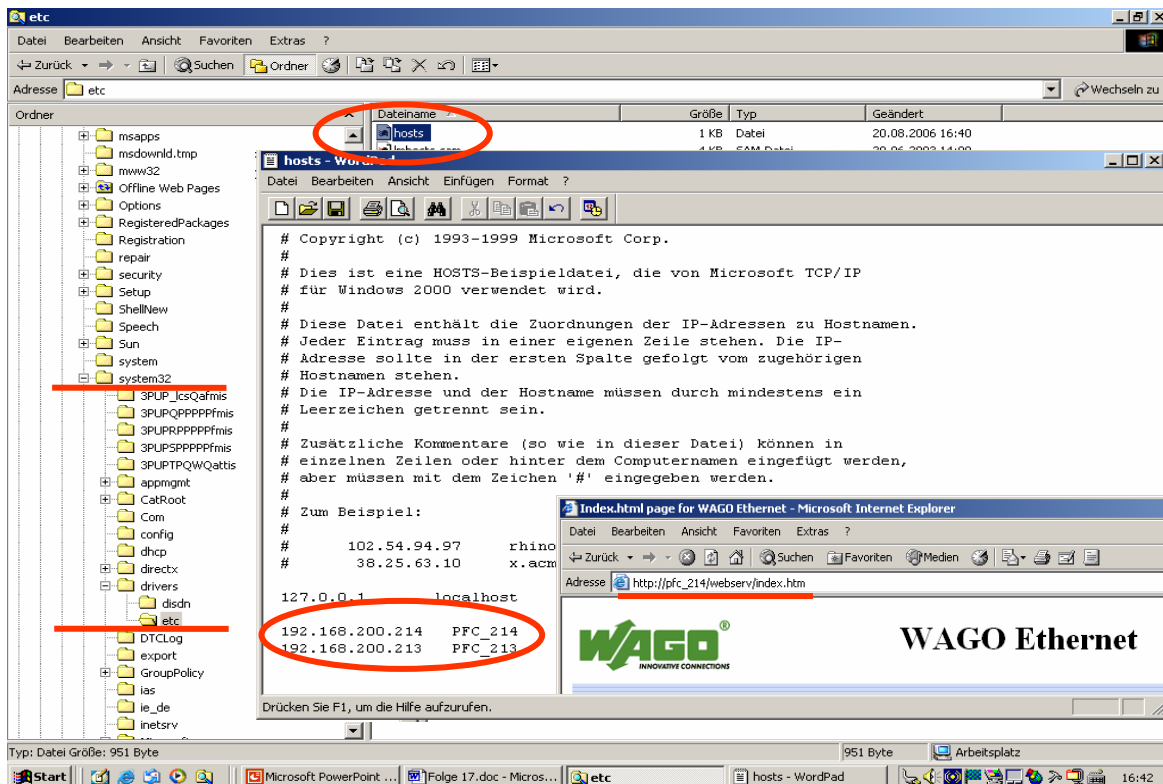


Bild 101: Einstellungen im System Windows für die Vergabe von Namen an Controller im lokalen Netz

Daten lesen und schreiben über das Web

Von besonderem Interesse ist die Kontrolle aktueller Zustände von Variablen, Eingängen oder Ausgängen über Internet oder lokales Netz mit einem Internet Browser. Dies ist beim PFC 841 allerdings etwas aufwändiger. So sind Texte in HTML zu erstellen und als Web-Seite im Verzeichnis „Sample“ des Controllers abzulegen. In die HTML-Texte werden sogenannte Plugins eingebettet, die das Lesen oder Schreiben bestimmter Adressen bewirken. Ein solches Plugin für das Lesen des Eingangswortes 0 im Dezimalformat lautet beispielsweise in HTML:

```
<!--#READPI ADR=IW0&FORMAT=%d-->
```

Die erforderlichen Arbeitsschritte für diese Aufgabe zeigt **Bild 102**. Zum ersten erstellen wir in HTML eine Tabelle, in deren Felder die gewünschten Variablenwerte sichtbar werden sollen. Eine solche sehr einfache Tabelle zeigt Bild 103 rechts unten. Ein Ausschnitt des dafür erforderlichen HTML-Textes ist in **Bild 103** mit einigen Anmerkungen zu sehen. Für solche Aufgaben nehmen wir die Hilfe eines Informatikers oder anderer Web-Fachleute in Anspruch. In diese Ausführungen wurden Ergebnisse eines Praktikums von Herrn Marcus Müller einbezogen, dem ich zu Dank verpflichtet bin.

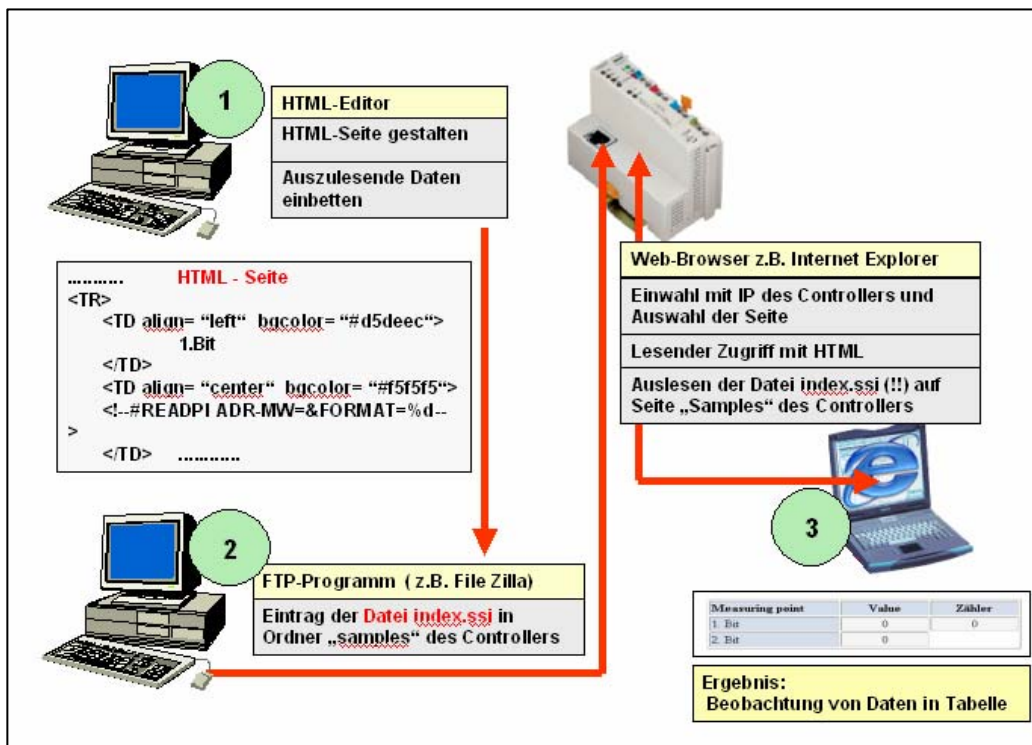


Bild 102: Arbeitsschritte zum Erstellen einer Web-Seite im PFC für die Kontrolle von Variablen über das Netz

```

<html>
<body>
  <META HTTP-EQUIV="refresh" content="1" /> /meta>
  <H2>
    Lesender Zugriff mit HTML
  </H2>
  <TABLE align="center" border="1">
    <TR>
      <TH width="150" align="left" bgcolor="#d5deec">
        Measuring point
      </TH>
      <TH width="100" align="center" bgcolor="#d5deec">
        value
      </TH>
      <TH width="100" align="center" bgcolor="#d5deec">
        Zähler
      </TH>
    </TR>
    <TR>
      <TD align="left" bgcolor="#d5deec">
        1. Bit
      </TD>
      <TD align="center" bgcolor="#f5f5f5">
        <!--#READPI ADR=IX0.0&FORMAT=%d-->
      </TD>
      <TD align="center" bgcolor="#f5f5f5">
        <!--#READPI ADR=MW0&FORMAT=%d-->
      </TD>
    </TR>
    <TR>
      <TD align="left" bgcolor="#d5deec">
        2. Bit
      </TD>
      <TD align="center" bgcolor="#f5f5f5">
        <!--#READPI ADR=IX0.1&FORMAT=%d-->
      </TD>
    </TR>
  </TABLE>
</body>
</html>

```

Zeitintervall der Aktualisierung der Daten in sec.

Einbettung der zu lesenden Daten

Bild 103: Auszug eines HTML-Textes für die Gestaltung einer Tabelle mit Dateneintrag

Mit Hilfe eines FTP-Programms übertragen wir diese Datei im zweiten Schritt in das dafür vorgesehene Verzeichnis selbsterstellter Web-Seiten des Controllers. **Bild 104** zeigt beispielhaft die grundlegende Vorgehensweise bei der Arbeit mit dem FTP-Softwaretool „File Zilla“. Im dritten Schritt können wir nun nach Einwahl in den Controller mittels Web Browser diese Seite und damit die aktuellen Werte von Variablen betrachten.

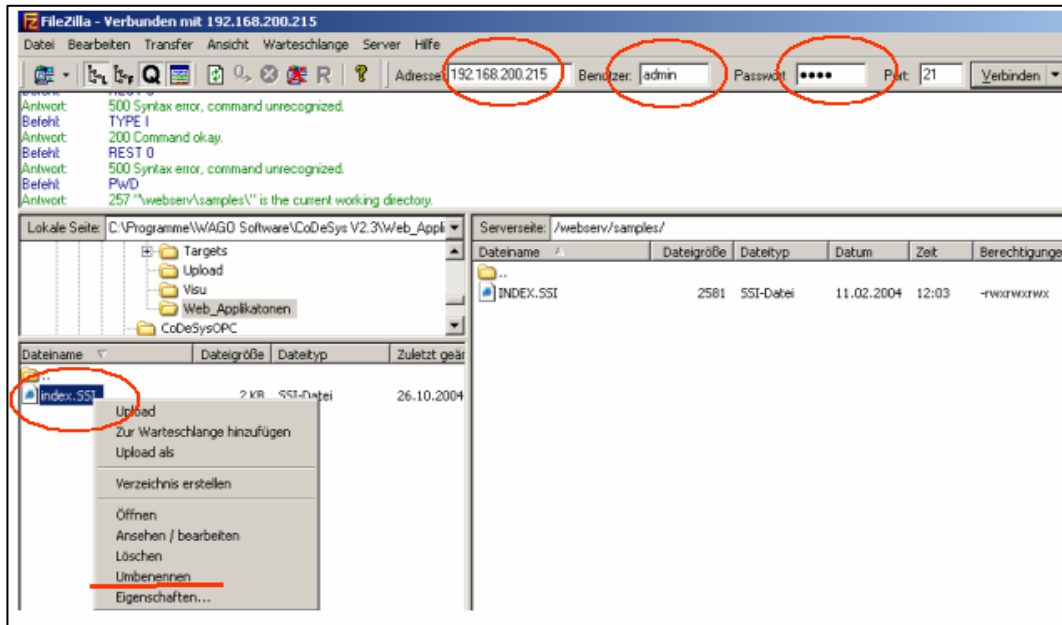


Bild 104: Eintrag der Datei index.ssi in die Webseiten des PFC mittels FTP-Programm „FileZilla“.

Fazit:

Diese Folge brachte den ersten Teil einer Einführung in Themen zur Nutzung von Internet-Technologien in der Automatisierungstechnik mit Busklemmen. Am Beispiel des PFC WAGO 750-841 wurde das Lesen des Status sowie Lesen und Schreiben ausgewählter Variablen im lokalen Netz und über Internet vorgestellt. Stets ist zu unterscheiden, ob in einem lokalen Netz oder aber über diese Grenze hinweg im Web kommuniziert wird. Die Ausführungen regen an, bei solchen Fragen die Zusammenarbeit mit Systemadministratoren und IT-Fachleuten zu suchen. Da effektive Zusammenarbeit andererseits Wissen erfordert, sollten sich auch Fachkräften der Automatisierungstechnik grundlegenden Fragen der Netzwerktechnik und des Internets stellen.

Der zweite Teil dieses Themas erscheint in Folge 19 und beschäftigt sich u.a. mit erforderlichen Arbeitsschritten für das ereignisgesteuerte Versenden von E-Mails durch PFC.

Glossar:

DHCP	Dynamic Host Configuration Protocol: Das Protokoll ermöglicht die Konfiguration des Netzes und insbesondere die Vergabe der IP-Adresse von einem DHCP-Server aus. Aus einem Pool möglicher IP wird dem PFC dabei eine freie IP für die Zeit seiner Kommunikation im Netz vergeben.
DNS	Domain Name Systems: DNS gehört zu den Internetprotokollen und ist einer der wichtigsten Dienste im Internet. Seine Aufgabe ist die Auflösung der Domain-Namen und Zuordnung von IP-Adressen, so dass Webseiten wie im Internet üblich mit einem Namen angesprochen werden können. Technisch besteht DNS aus einer weltweit verteilten Datenbank, welche alle Namen verwaltet.
Firewall	engl. „Brandwand“. System aus Software- und / oder Hardwarekomponenten, welche den Zugriff auf ein Netzwerk beschränken. Insbesondere kann damit der Datenaustausch zwischen lokalen Netzen und dem Internet kontrolliert und von Bedingungen abhängig gemacht werden. Firewalls werden in PC und Netzwerkkomponenten wie Routern installiert.
FTP	File Transfer Protocol: Protokoll zum Austausch von Daten zwischen Netzteilnehmern, auch über die Grenzen von Betriebssystemen hinweg. Mit FTP werden u.a. HTML-Seiten und Programmcodes in einen PFC eingetragen.
HTML	Hyper Text Markup Language: Sprache für Dokumente im Web. Mit HTML werden Hypertext-Dokumente geschrieben.
HTTP	Hyper Text Transfer Protokoll: Grundlegendes Protokoll des Internet. Web-Server benutzen das Protokoll zur Übermittlung von Text, Bildern und anderen Daten im Web. Im PFC 841 dient der HTTP Server zum Auslesen der dort abgespeicherten HTML-Seiten.
IT-Funktionen	IT steht hier für Internet-Technologie
PlugIn	Zusatzsoftware oder auch feststehende, unveränderliche Softwareteile oder Programmzeilen
Virtual Private Network (VPN)	dt.: Virtuelles Privates Netz. Für die Zeitdauer der Kommunikation geschaffenes virtuelles Netz für den Transport privater Daten durch ein öffentliches Netz.
VPN Tunnel	Eine VPN-Verbindung erfolgt über einen gesicherten Tunnel. Dieser ermöglicht die Einbettung von Daten eines Netzwerk-Protokolls in ein anderes Protokoll. Für die Parametrierung des Tunnels gibt es spezielle Tunnel-Software. Die Sicherung des Tunnels – nicht der Daten an sich ! – erfolgt häufig mit der Protokollerweiterung IP Security (IPSec).