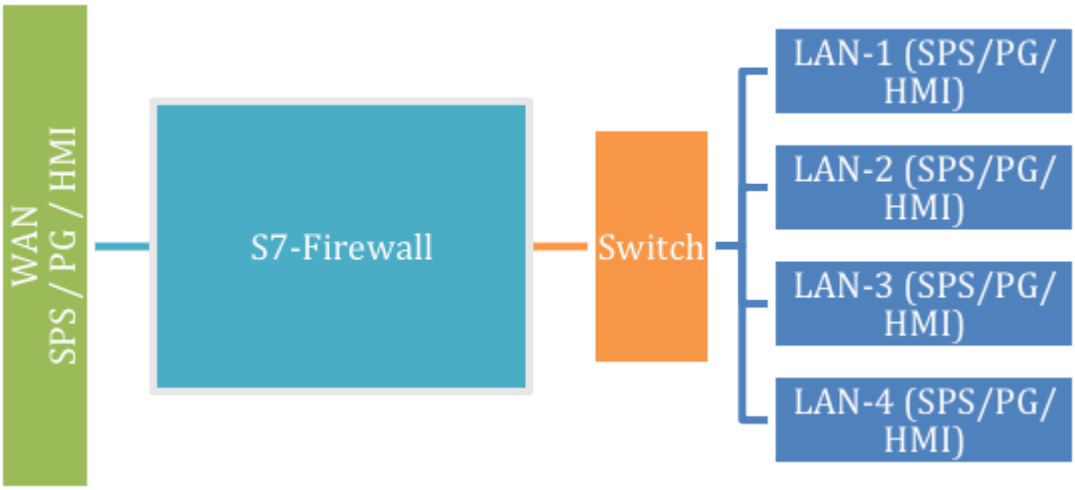
S7-Firewall Kurzanleitung

Dokumentation für die Version 1.19

1. Einführung

S7-Firewall ist eine skalierbare „SPS-Firewall„, die nicht nur IP/MAC-Adressen filtert. Für frei definierbare Verbindungen kann der Zugriff auf beliebige Datenbereiche der SPS eingeschränkt / festgelegt werden. S7-Firewall kann beliebig zwischen SPS- und Bedien- / Programmierebene eingebaut werden. S7-Firewall erkennt die Einbaurichtung automatisch. Es werden nur konfigurierte Verbindungen zugelassen.



2. Hardwareausführungen

2.1.Standardhardwareausführung

In der Standardausführung ist S7-Firewall mit einem WAN Port und 4 LAN Ports ausgeführt als Switch bestückt.

Betriebsarten	S7-Firewall
Services	DHCP Client/Server
	NTP Client/Server
Anschlüsse	1x WAN
	4x LAN-Port als Switch

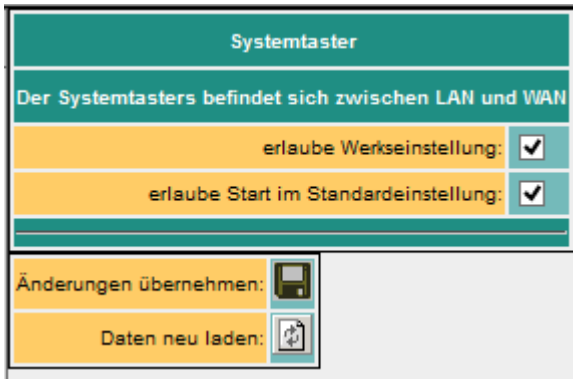
3. Konfiguration

In der Konfiguration können die Netzwerkeinstellungen etc. parametriert werden. Die Eingabeformulare sind in der Regel selbsterklärend. Gerne nehmen wir aber Anregungen von Anwendern entgegen, um die

Bedienung noch einfacher zu gestalten. Im Auslieferzustand sind folgende IP-Adressen eingestellt:
192.168.1.57
192.168.2.1
Sie haben folgende Optionen, per WEB-Browser S7-Firewall anzusprechen.
Am PC eine IP-Adresse aus dem entsprechendem Netzsegment vergeben (z.B. 192.168.1.100 oder 192.168.2.100) und den PC entsprechend mit LAN oder WAN über Ethernet verbinden. Im Browser http://192.168.1.57, bzw. http://192.168.2.1 eingeben.
Oder Sie stellen Ihren PC auf IP-Adresse automatisch beziehen und verbinden Ihn mit dem LAN-Port des S7-Firewall. S7-Firewall teilt dem PC automatisch eine IP-Adresse zu. Im Browser können Sie das Gerät mit: http://S7-Firewall ansprechen.

3.1 Systemtaster, System zurücksetzen

Unter dem Punkt Systemtaster haben Sie zwei Möglichkeiten was beim Betätigen des Tasters erlaubt ist, es muss mindestens eine Option ausgewählt sein:



erlaube Werkseinstellungen	☑	Das Gerät kann in den Auslieferungszustand gesetzt werden
erlaube Start im Standardeinstellung	☑	Das Gerät wird auf die bereits gespeicherten Grundeinstellungen gesetzt

Achtung!
Benutzen Sie zum Konfigurieren einen der 4-Switch Ports, da es unter Umständen vorkommen kann, dass der WAN-Port nicht mehr ansprechbar ist
Setzen Sie das Gerät nie im laufenden Betrieb zurück. Trennen Sie das Gerät vom Produktionsnetzwerk und führen den Reset in einer autarken Umgebung aus. Der Konfigurationsrechner und das Gerät sollten währendessen nicht am Firmennetzwerk angeschlossen sein.

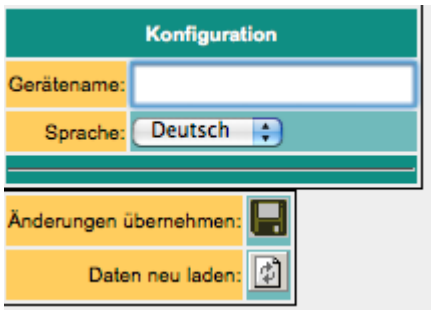
Keine Sorge wir nehmen beim Betätigen noch keinen Werksreset vor.
Der Taster verbirgt sich zwischen WAN und LAN-Ports (kleines Loch). Es sind nur die oben **aktivierten** Möglichkeiten verfügbar.

Gehen Sie wie folgt vor:

- z.B. Büroklammer bereitlegen
- Gerät stromlos machen!
- Ins Loch das Büroklammernende einstecken
- wieder einschalten
- wenn die vier LED’s erlöschen und nur noch die Power-LED an ist, den Taster mit Büroklammer gedrückt halten bis alle 4 LED’s schnell blinken
- Taster loslassen
- nun erscheint ein Art Auswahl. Wenn im gewünschten Zustand der Taster gedrückt wird, erfolgt die gewünschte Aktion

- Grundeinstellung
  - LED S3 (rechts unten) blinkt
    - Das Gerät bootet in der Grundeinstellung (Netzwerk / IP-Adressen des Auslieferzustandes werden verwendet). Nun können die gewünschten Änderungen an der Netzwerkeinstellung vorgenommen werden. Diese Einstellungen werden jedoch erst nach Neustart des Gerätes aktiv.
- Werkseinstellung
  - LED Power **und** S3 blinken
    - alle Einstellungen werden gelöscht

4. Konfiguration des Gerätes



Parameter	mögliche Einstellung	Routingrichtung / Zweck
Gerätename	„nach belieben“	
Sprache	deutsch	legt die Sprache der Bedienebene fest. Evtl. nach Änderung Ihrem WebBrowser die Seite neu laden.
	englisch	
Standard Gateway	fest (wie vorgegeben) von WAN über DHCP von WAN über PPPoE von LAN über DHCP von Modem über PPP	
1. DNS		
2. DNS		
Routing Mode	Büro	LAN → Routinginterface
	Maschine	Routinginterface → LAN
Routinginterface	WAN/IP	IP-Routing über WAN
	Modem	IP-Routing über Modem
	WAN/PPPOE	IP-Routing über PPPoE am WAN-Port
	WAN/OVPN	Routing über OVPN am WAN-Port
	WAN/Bridge	Ethernet-Routing am WAN-Port

5. Netzwerkeinstellungen

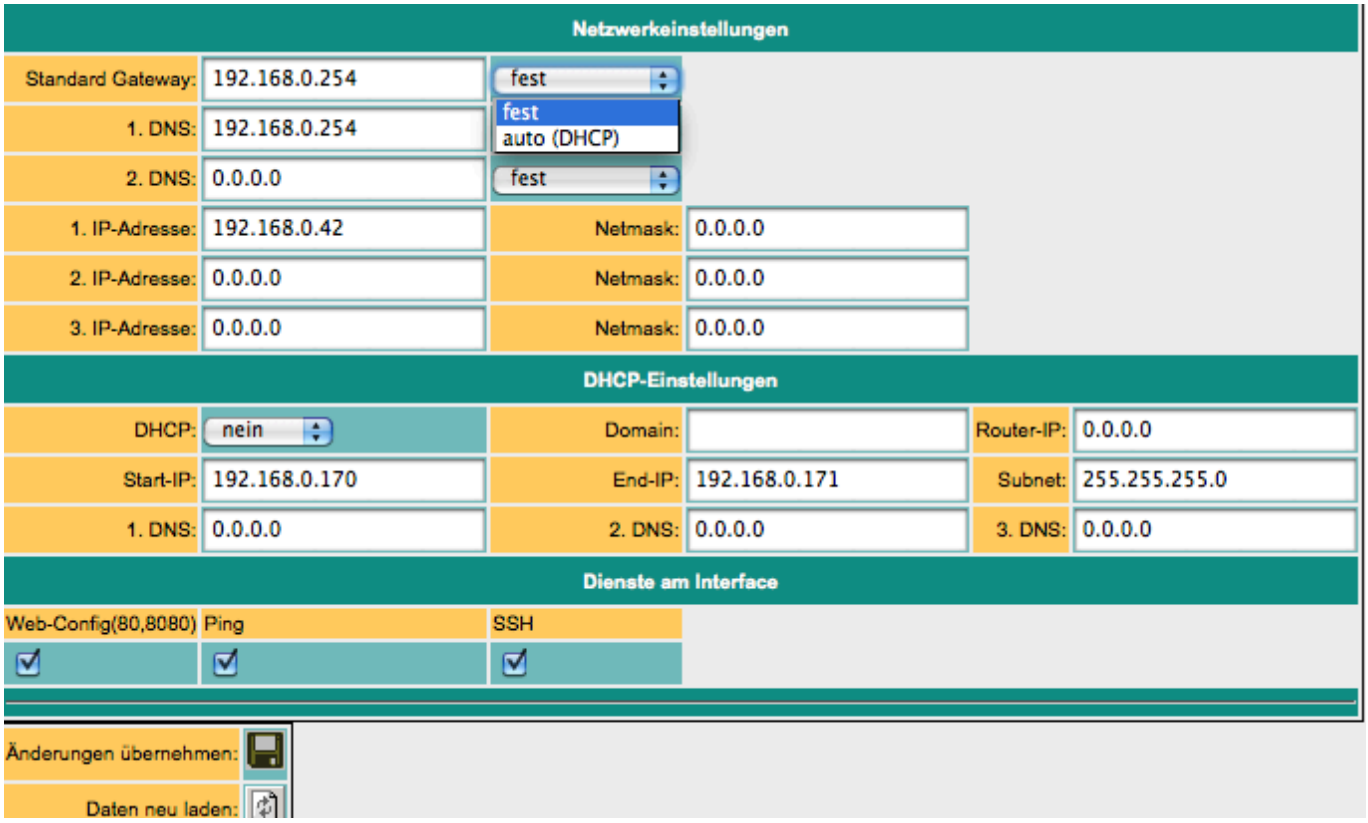


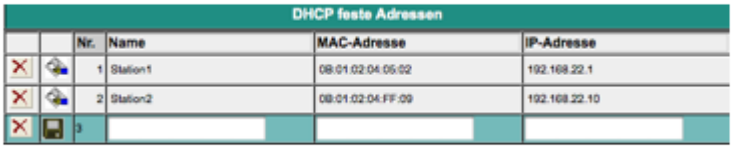
Abb. 6: Netzwerkeinstellungen

Parameter	mögliche Einstellung	Zweck
Standard Gateway	fest (wie vorgegeben) über DHCP	
1. DNS		
2. DNS		
1-3. IP-Adresse mit Netmask	IP-Adresse / Netmask	Wenn Netmask 0.0.0.0 wird die Netmask automatisch berechnet, je nach A,B,C-B Netz. z.B. 192.168.0.x → 255.255.255.0 10.x.x.x → 255.0.0.0
Bei Verwendung fester IP-Adressen ist mindestens die 1. IP-Adresse zu konfigurieren. Ansonsten startet das Gerät mit der Werkeinstellung.		
DHCP	nein	kein DHCP verwenden Die restlichen DHCP-Parameter werden nicht verwendet
	Client	Das Netzwerkinterface wird als DHCP-Client und bezieht die IP-Adresse automatisch von einem DHCP-Server. Die restlichen DHCP-Parameter werden nicht verwendet
	Server	Das Netzwerkinterface betreibt einen DHCP-Server. Die restlichen HCP-Parameter sind zu parametrieren.
Start-IP	Start-IP-Adresse	Start-IP-Adresse beim Betrieb als DHCP-Server
End-IP	End-IP-Adresse	End-IP-Adresse beim betrieb als DHCP-Server
Subnet	Subnetadresse	Adresse des Subnets für die Vergabe der IP-Adressen als DHCP-Server
Domain	Frei	Name der Domain bei der Verwendung als DHCP-Server

Parameter	mögliche Einstellung	Zweck
Router-IP	IP-Adresse	Ist die IP-Adresse, die beim Betrieb als DHCP-Server als Gateway weitergegeben wird

Der WAN/LAN-Port hat gemeinsame IP-Adressen Es können bis zu 3 verschiedene IP-Adressen und Subnetze konfiguriert werden. Der Port kann auch als DHCP-Server oder Client betrieben werden. Die notwendigen Daten für die IP-Zuordnung werden hier eingegeben. Für den Betrieb als DHCP/Server können feste Zuordnungen MAC-IP-Adresse festgelegt werden. (Siehe weiter unten, „DHCP feste Adressen). Weiter wird festgelegt, welche Services am Port zur Verfügung stehen (Web-Konfig), Ping , SSH (nur für Entwickler)

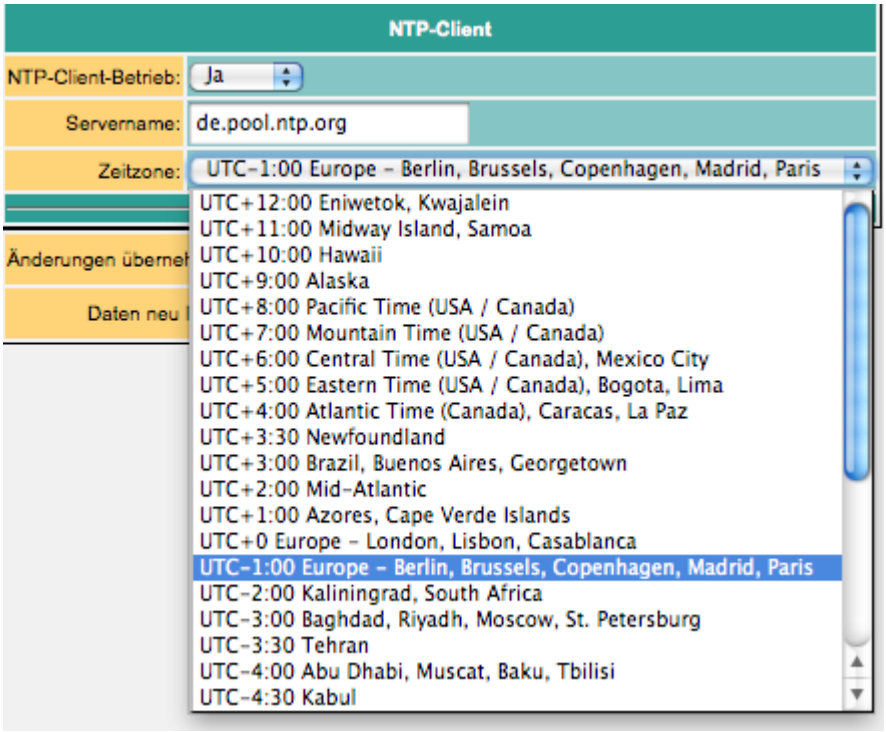
6. DHCP Feste MAC /IP-Adresszuordnung



Wird der eingebaute DHCP-Server (am WAN oder LAN) betrieben, kann es sinnvoll sein bestimmten IP-Teilnehmern immer dieselbe IP-Adresse zuzuteilen. Hier können Sie festlegen welche MAC-Adresse welche IP-Adresse erhält.

7. NTP-Client

Damit S7-Firewall immer mit aktueller Uhrzeit läuft haben wir einen NTP-Client implementiert. So kann sich S7-Firewall automatisch über Internet oder mit einem anderen im Netz verfügbaren TimeServer Datum und Uhrzeit synchronisieren \\

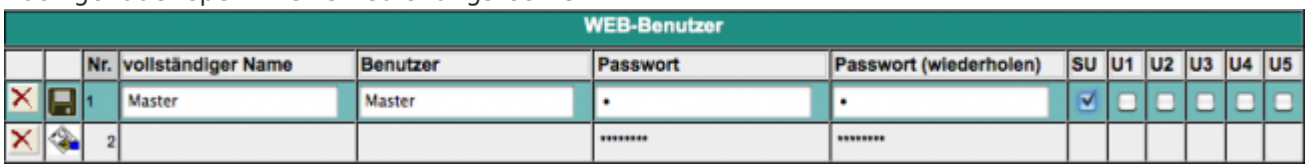


Parameter	mögliche Einstellung	Zweck
NTP-Client-Betrieb	ja	schaltet NTP-Client ein oder aus.
	nein	

Parameter	mögliche Einstellung	Zweck
Servicename	IP-Adresse / Domainname des NTP-Servers	Geben Sie hier die IP-Adresse bzw. den Domainnamen des gewünschten NTP-Servers ein. Achten Sie darauf, dass dieser Server über den angegebenen Routing weg erreichbar ist.
Zeitzone	Zeitzone, in der S7-Firewall betrieben	notwendig, damit S7-Firewall die korrekte Ortszeit besitzt

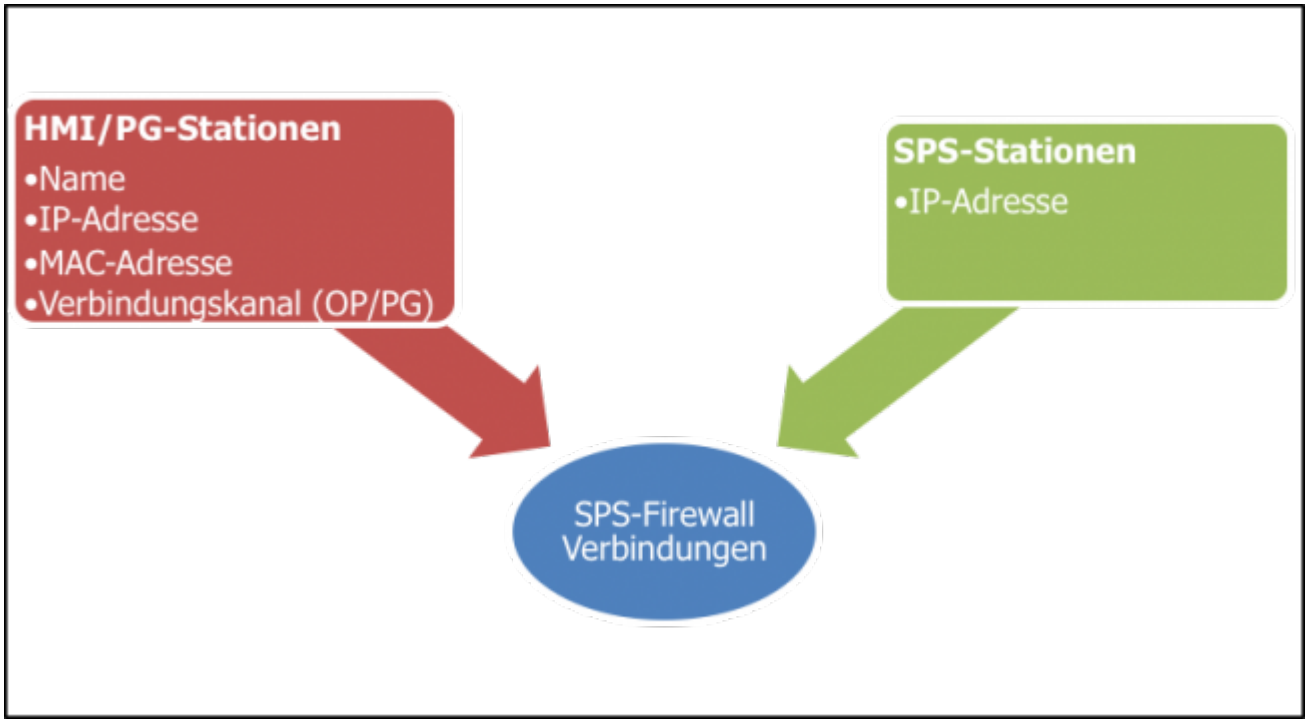
8. Web-Benutzer

Hier die Maske für die Eingabe der WEB-Interface Benutzer. Pro Benutzer können verschiedene Berechtigungen vergeben werden. Grundsätzlich darf nur ein Anwender mit „SU„ Änderungen vornehmen. U1 – U5 darf das Interface nur bedienen. In den S7-Firewall-Erweiterungsmodulen besitzen „U1“ – „U5„ noch genauer spezifizierte Bedienungsrechte.

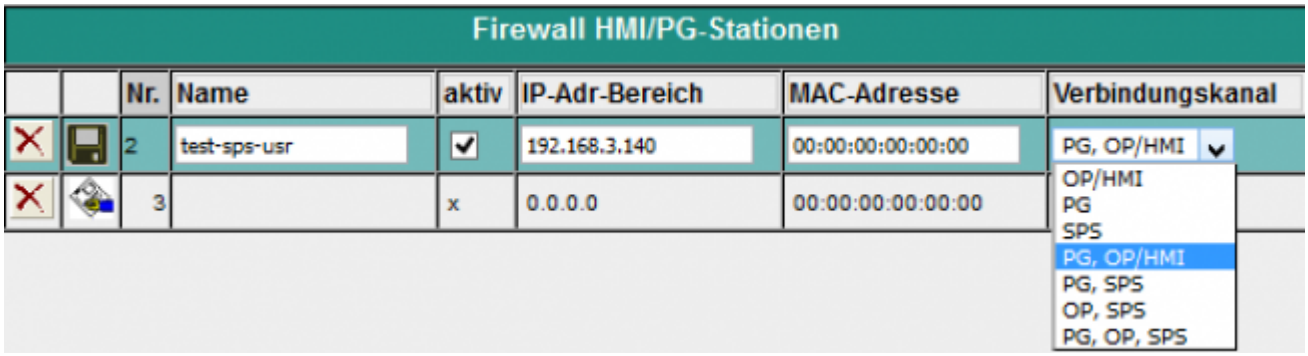


9. S7-Firewall-Einstellungen

Die SPS-Firewall-Verbindungen ergeben sich aus der Kombination aus HMI/PG-Station und SPS-Station

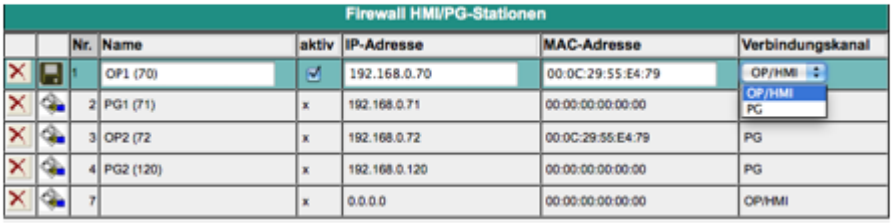


10. Eingabe der HMI/PG-Stationen



Parameter	mögliche Einstellung	Zweck
Nr.	automatisch	fortlaufende Nummer
Name	frei vom Benutzer einzugeben	Name der Station
aktiv	ja (x)	Verbindungen mit dieser Station werden von der Firewall verarbeitet
	nein ()	Verbindungen mit dieser Station werden nicht verarbeitet, d.h sie werden geblockt
IP-Adresse	IP-Adresse des HMI / PG-Gerätes	Identifikation des Absenders Eingabe unbedingt notwendig
MAC-Adresse	MAC-Adresse des HMI / PG-Gerätes	Identifiziert das HMI/PG zusätzlich über die MAC-Adresse. 00:00:00:00:00:00 bedeutet, dass die MAC-Adresse nicht geprüft wird. Bei ungleich 0 muss die MAC-Adresse der Station mit der Eingabe übereinstimmen
Verbindungskanal	verwendeter Kanal der Verbindung	In der Simatic S7 stehen PG- und OP-Kanäle zur Verfügung. Dieser Kanal wird als zusätzliches Merkmal zur Identifikation des Absenders verwendet. Auf jedem der beiden Kanäle sind sowohl PG- als auch OP-Funktionen möglich. Bediengeräte / WinCC etc. verwenden in der Regel OP-Kanäle. Dieser Kanal ist für HMI-Geräte auch der empfohlene. Die Siemens PG-Software verwendet grundsätzlich den PG-Kanal. Leider ist verschiedene Software am Markt im Einsatz, welche nicht über das Knowhow verfügt, diesen Kanal einzustellen. Dies herauszufinden geht über das LOG-File. Eine vernünftige HMI-Software, respektive der zugehörige Softwaretreiber versorgt die Einstellbarkeit dieses Kanals. Soll z.B. vom selben Rechner aus PG und HMI laufen (IP/MAC PG/HMI identisch) bleibt nur noch der PG/OP-Kanal zur Identifikation des Absenders.

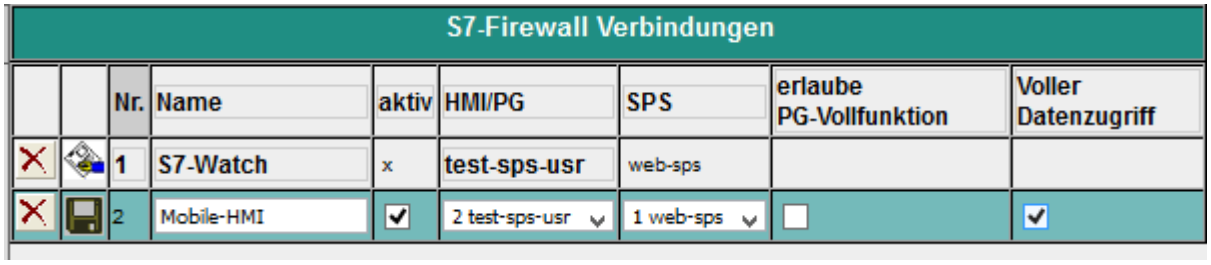
11. Eingabe der SPS-Stationen



Parameter	mögliche Einstellung	Zweck
Nr.	automatisch	fortlaufende Nummer
Name	frei vom Benutzer einzugeben	Name der Station
aktiv	ja (x)	Verbindungen mit dieser Station werden von der Firewall verarbeitet
	nein ()	Verbindungen mit dieser Station werden nicht verarbeitet, d.h sie werden geblockt
IP-Adresse	IP-Adresse der SPS-Station	Identifikation des Absenders Eingabe unbedingt notwendig

12. Eingabe der S7-Firewall Verbindungen

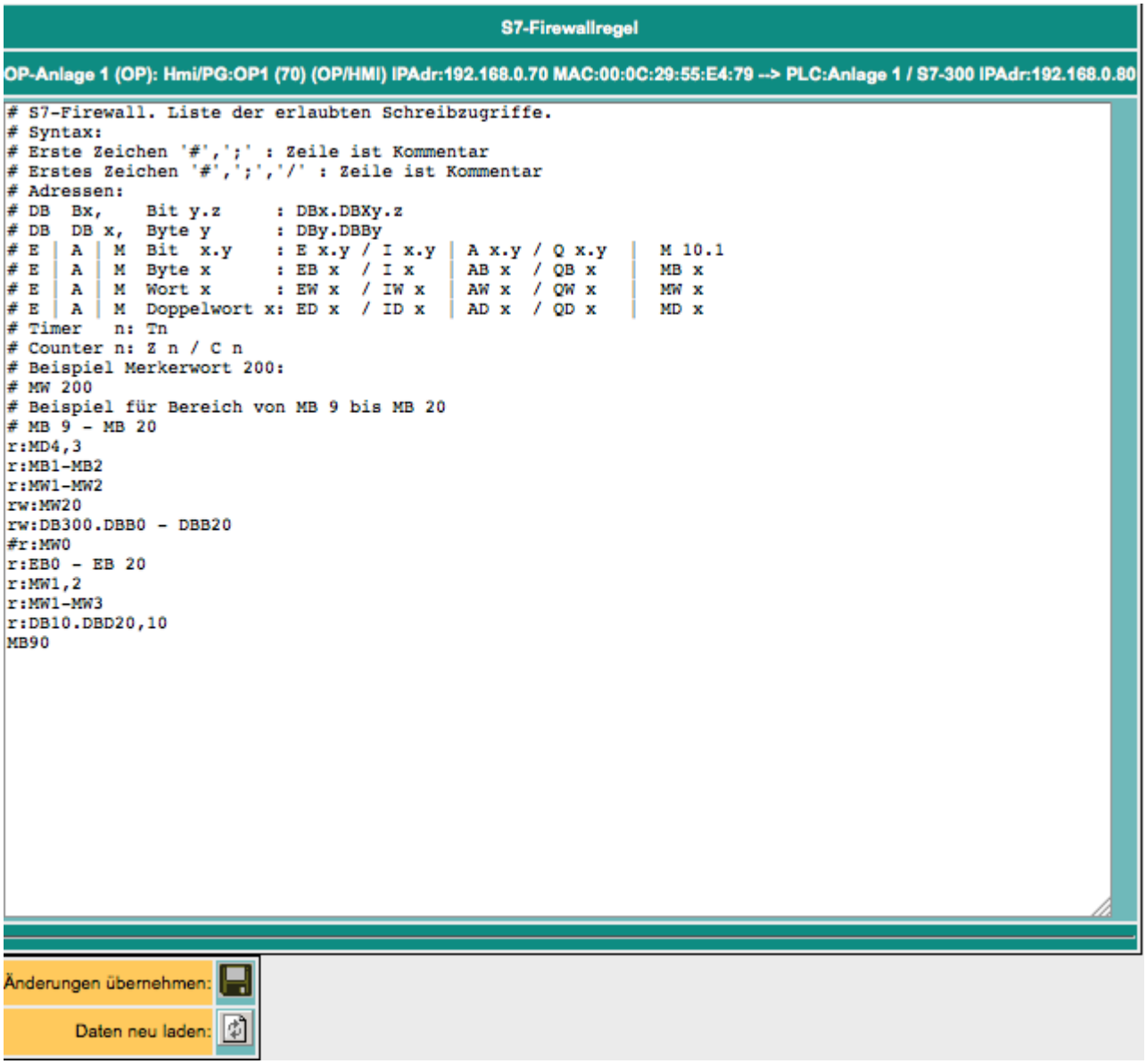
Die Verbindungen werden aus der Kombination HMI/PG-Station und SPS-Station gebildet. Jede HMI/SPS-Station kann mehrfach verwendet werden. Bei Änderung von Mac- oder IP-Adresse muss diese nur zentral in der HMI/PG-Station bzw. SPS-Station geändert werden. Jeder Verbindung wird eine Verbindungsregel zu geordnet. Ist „erlaube PG-Vollfunktion“ selektiert, so ist diese Verbindung ein Vollzugriff. In Zukunft wird dieser Zugriff näher unterteilt werden können (Definierte Bausteine lesen / schreiben, SPS Start/Stop, Urllöschen , Systemdaten (lesen/schreiben).



Parameter	mögliche Einstellung	Zweck
Nr.	automatisch	fortlaufende Nummer
Name	frei vom Benutzer einzugeben	Name der Verbindung Dient zugleich als „Link„ zum Öffnen und Bearbeiten des Regelscripts.
aktiv	ja (x)	diese Verbindung wird von der Firewall verarbeitet
	nein ()	diese Verbindung wird nicht verarbeitet, d.h. sie wird geblockt
erlaube PG-Vollfunktion	ja (x)	Diese Verbindung ist eine PG-Verbindung und darf alle Funktionen ausführen
	nein ()	Diese Verbindung ist eine Eingeschränkte Verbindung. Es sind nur Zugriffe auf die freigegebenen Funktion und Datenbereiche, wie im zugehörigen Regelscript definiert, erlaubt.

13. Das Regelscript

Im Regelscript werden die Datenbereiche bzw. mögliche Zugriffe für die jeweilige Verbindung festgelegt. Das Script kann über den Link des Namens der Verbindung erreicht werden. \\



Syntax des Regelscripts

erste(s) Zeichen	Funktion	Rest der Zeile
#	die Zeile ist ein Kommentar	freier Text
Doppelschrägstrich		
(kein Zeichen, es folgt gleich Operand/Bereich)	der folgende Bereich ist nur zum lesen (readonly)	Operand / Bereich siehe weiter unten
r:		
w:	der folgende Bereich ist nur zum schreiben (writeonly)	
rw:	der folgende Bereich lesbar und schreibbar (read/write)	

In eine Regelzeile kann ein einzelner Operand, oder ich ein Bereich eingegeben werden.

Beispiel für die Eingabe von einzelnen Operanden: (Quelle aus Siemens STEP-S7 PG-Software)

Erlaubter Operand	Datentyp	Beispiel (Mnemonik Deutsch)	Beispiel (Mnemonik Englisch)
Eingang I Ausgang I Merker	BYTE	EB 1 I AB 10 I MB 10	IB 1 I QB 10 I MB 10
Eingang I Ausgang I Merker	WORD	EW 1 I AW 10 I MW 10	IW 1 I QW 10 I MW 10
Eingang I Ausgang I Merker	DWORD	ED 1 I AD 10 I MD 10	ID 1 I QD 10 I MD 10
Peripherie (Eingang I Ausgang)	BYTE	PB 0 I PEB 0 I PAB 1	PB 0 I PIB 0 I PQB 1

Erlaubter Operand	Datentyp	Beispiel (Mnemonik Deutsch)	Beispiel (Mnemonik Englisch)
Peripherie (Eingang I Ausgang)	WORD	PW 0 I PEW 0 I PAW 1	PW 0 I PIW 0 I PQW 1
Peripherie (Eingang I Ausgang)	DWORD	PW 0 I PED 0 I PAD 1	PD 0 I PID 0 I PQD 1
Zeiten	TIMER	T 1	T 1
Zähler	COUNTER	Z 1	C 1
Datenbaustein	BOOL	DB1.DBX 1.0	DB1.DBX 1.0
Datenbaustein	BYTE	DB1.DBB 1	DB1.DBB 1
Datenbaustein	WORD	DB1.DBW 1	DB1.DBW 1
Datenbaustein	DWORD	DB1.DBD 1	DB1.DBD 1

Hinweis: Die Eingabe von „DB0. ..“ ist aufgrund interner Benutzung nicht erlaubt.

Beispiel für die Eingabe von Bereichen, mit Anzahl der Einheiten:

ab Merker 60, 10 Byte: MB60, 10

ab DB10, Datenwort 2, 5 Worte: DB10.DW2, 5

Hinter dem Komma folgt die Anzahl der gewünschten Einheiten (je nach Adressart, BOOL, BYTE, WORD, DWORD)

Beispiel für die Eingabe von Bereichen mit „von“ – „bis„:

Merker Byte 70 bis Merker Byte 200: MB 70 – MB 200

Ausgang A 10.2 bis Ausgang 14.7: A 10.2 – A14.7

Einfach nach Startoperanden mit ,-, den Endoperanden (Endadresse) angeben. Die Endadresse wird inkludiert!

Inhaltsverzeichnis