

Embedded Linux für industrielle Gateways

Klaus-Dieter Walter, SSV Embedded Systems
Hannover



Inhalt

- * Wer ist SSV Embedded Systems?**
- * Woher kommen unsere Erfahrungen mit (Embedded) Linux?**
- * Was sind industrielle Gateways?**
- * Linux und TCP/IP.**
- * Was ist ein Embedded Linux?**
- * Gateways mit Linux als industrieller Firewall.**
- * Reverse Proxy (einheitlicher Zugriff auf viele Webserver).**
- * VPNs und Managementwerkzeuge.**



Wer ist SSV Embedded Systems

* SSV Embedded Systems ist ein Geschäftsbereich der SSV Software Systems GmbH. In diesem Geschäftsbereich sind die Produktbereiche Single Board Computer, Industrie PCs und Terminals zusammengefasst.



Die DIL/NetPCs

* Ein typisches Beispiel ist der DIL/NetPC DNP/1110. Dieses Modul benötigt eine Grundfläche von nur 82*28mm und basiert auf einem DIL-64-Format.

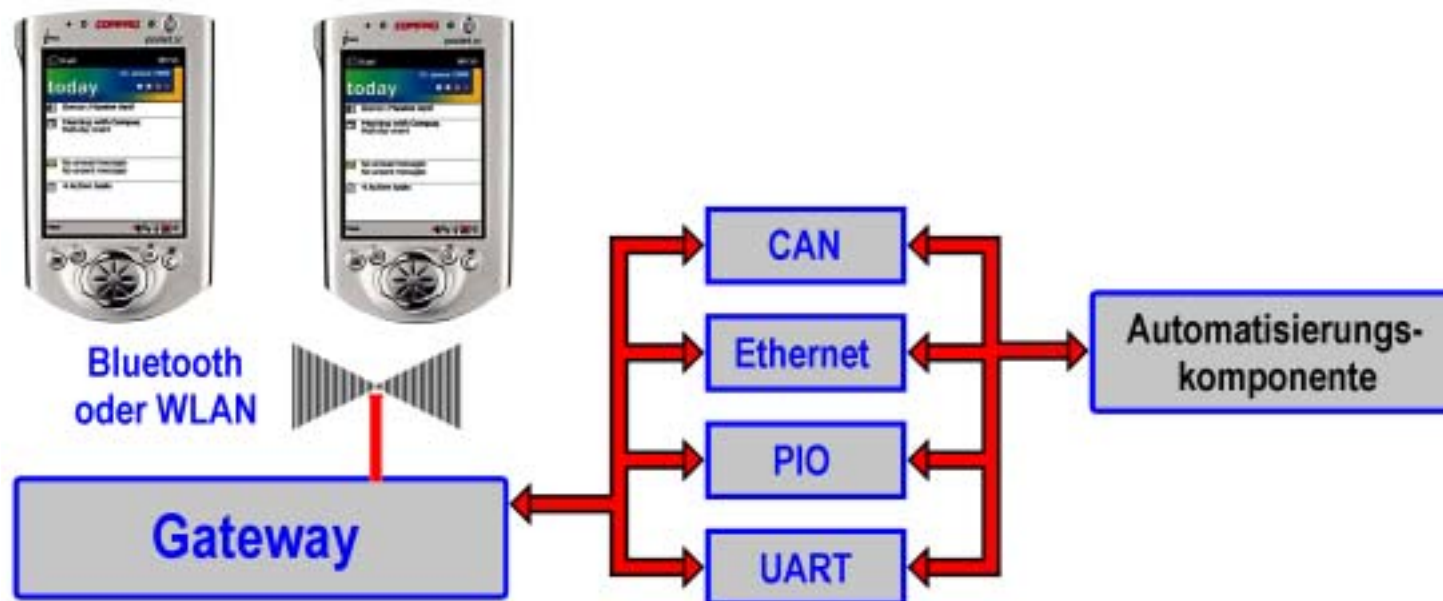


- * Intel-StrongARM-SA-1110 mit 206 MHz
- * Weiterentwicklung auf PXA255 (400 MHz)
- * 32 MByte SDRAM
- * 16 MByte Flash. ISP-fähig
- * 10/100 Mbps Ethernet-Interface
- * 20-Bit-Parallel-I/O
- * 2 serielle Schnittstellen
- * 8-Bit-Erweiterungsbus
- * 64-Pin-JEDEC-Format
- * Pinkompatibel zur 486-Variante



Industrielle Gateways

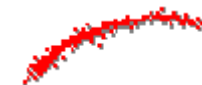
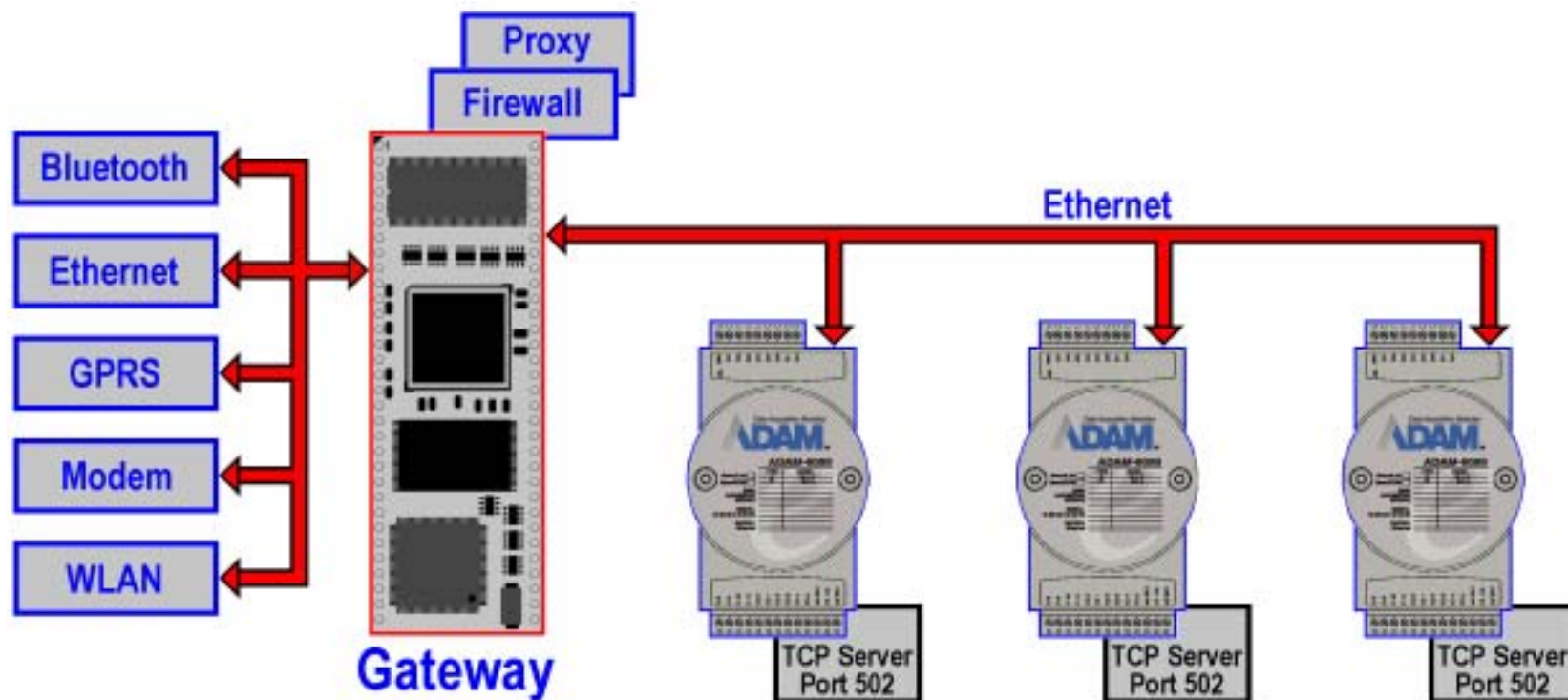
* Industrielle Gateways verbinden in der Regel beliebige Komponenten in der Automatisierungstechnik mit TCP/IP-basierten Netzwerken.



* Häufig kommen in diesem Zusammenhang auch Web-Technologien zum Einsatz (Web-basierter Fernzugriff per Browser, Web-basiertes Bedienen und Beobachten).

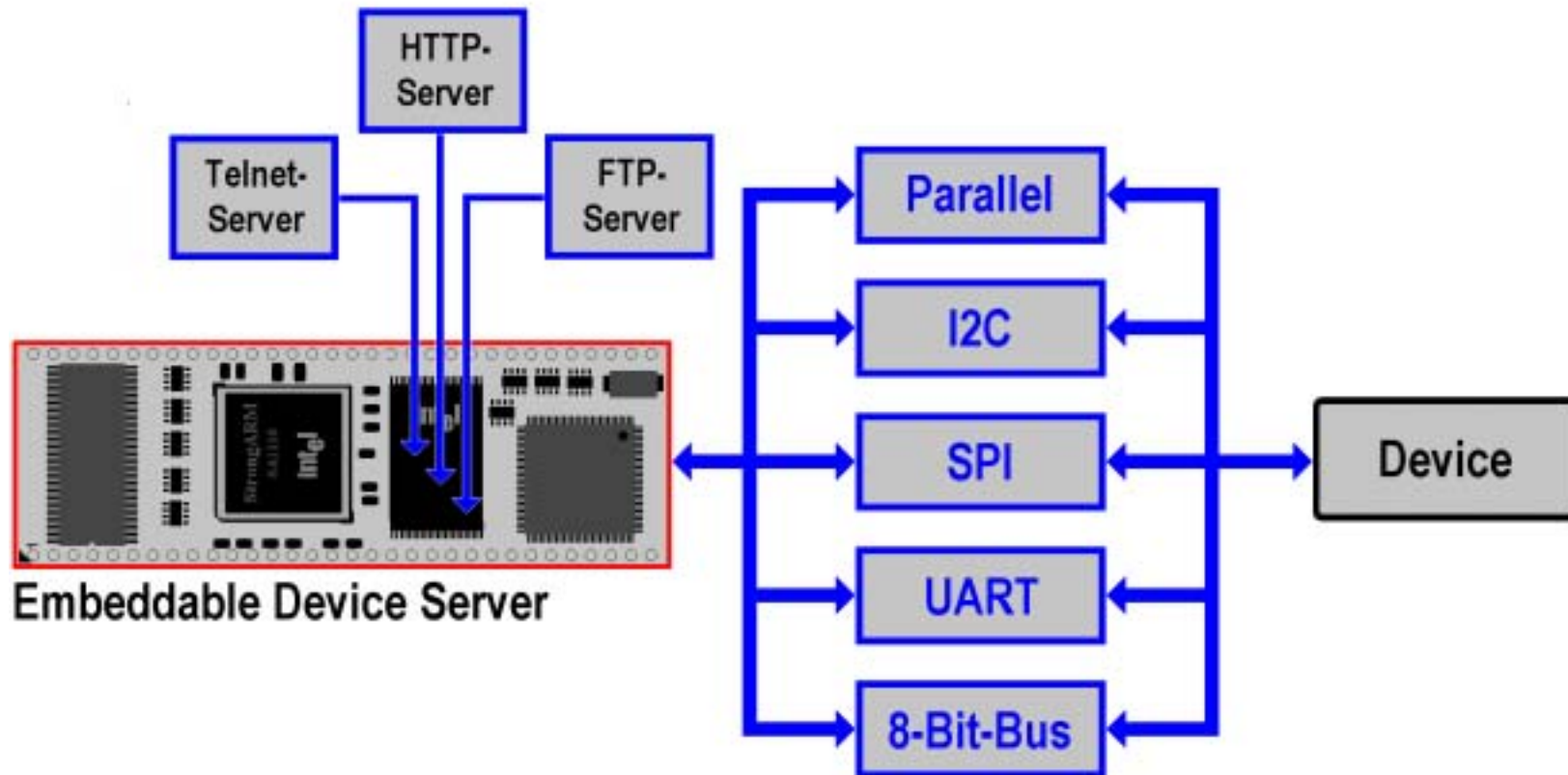
Industrielle Gateways

* Typisches Anwendungsbeispiel: I/O-Module mit Ethernet und Modbus/TCP. Das Gateway bildet einen Web-Proxy und eine Firewall.



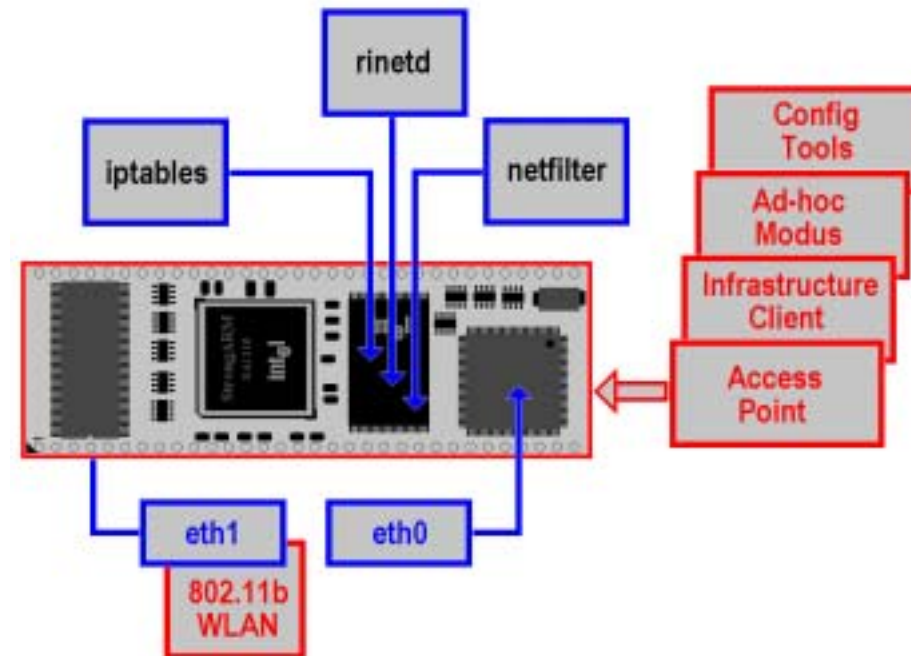
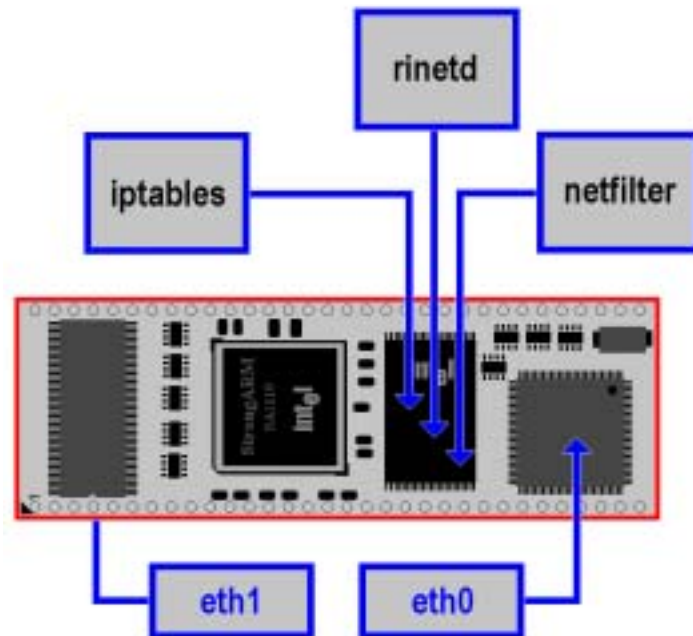
Industrielle Gateways

* Industrielle Gateways werden auch als Device Server eingesetzt, um andere - nicht vernetzungsfähige Systeme - in TCP/IP-Netzwerke einzubinden.



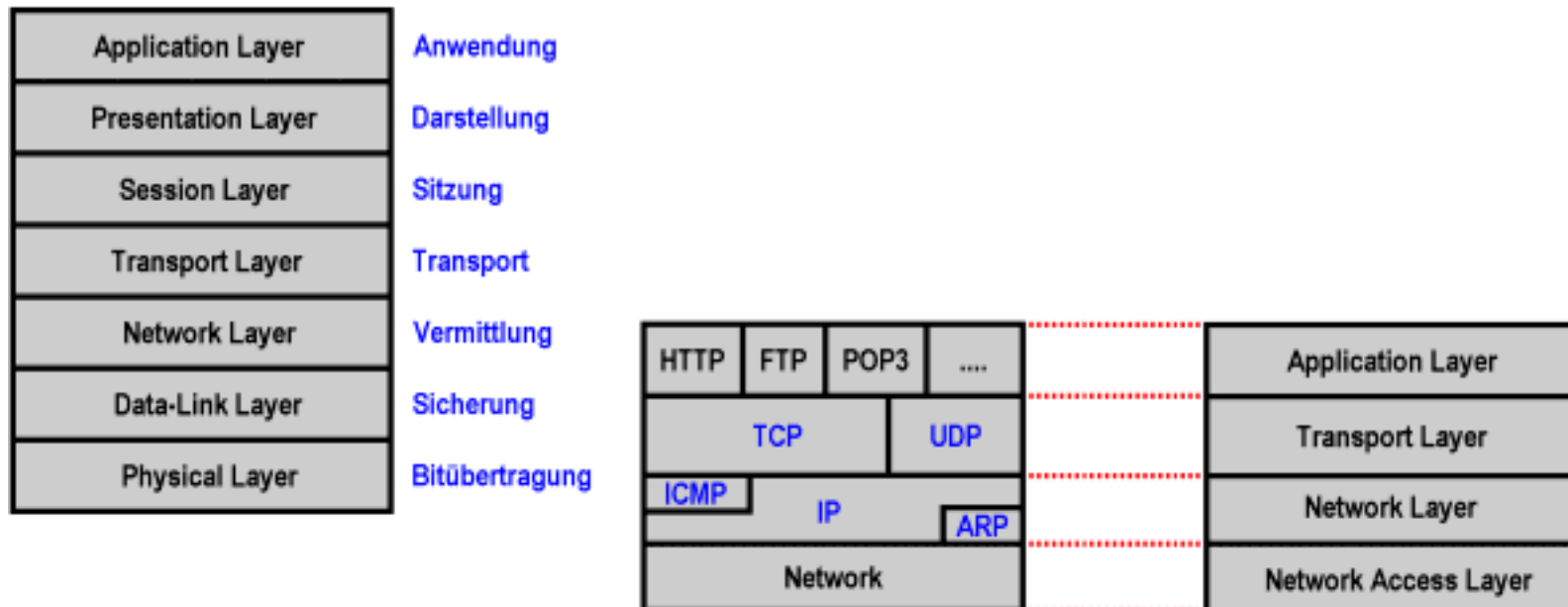
Industrielle Gateways

* Industrielle Gateways sollten unbedingt Schutzmechanismen gegen Angriffe und unerwünschte Zugriffe bieten.



Linux und TCP/IP

* Linux bietet einen TCP/IP-Protokollstack mit IPv4 und IPv6 sowie zahlreiche Client- und Serverprogramme für die Anwendungsschicht.

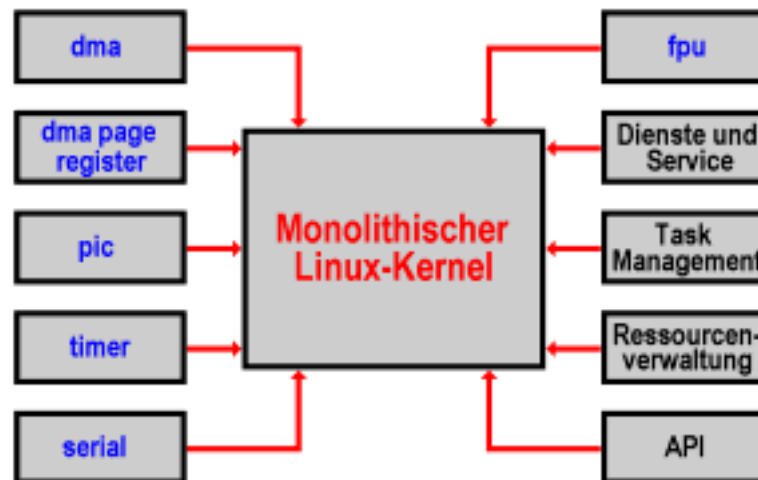


* Der Linux-TCP/IP-Stack ist ausgereift und stabil. Da er im Quellcode vorliegt, werden eventuelle Sicherheitslücken (zum Beispiel *Buffer Overflow*) schneller erkannt und beseitigt.



Embedded Linux

* Es gibt kein spezielles „Embedded Linux“. Es wird lediglich die beispiellose Skalierbarkeit von Linux ausgenutzt.



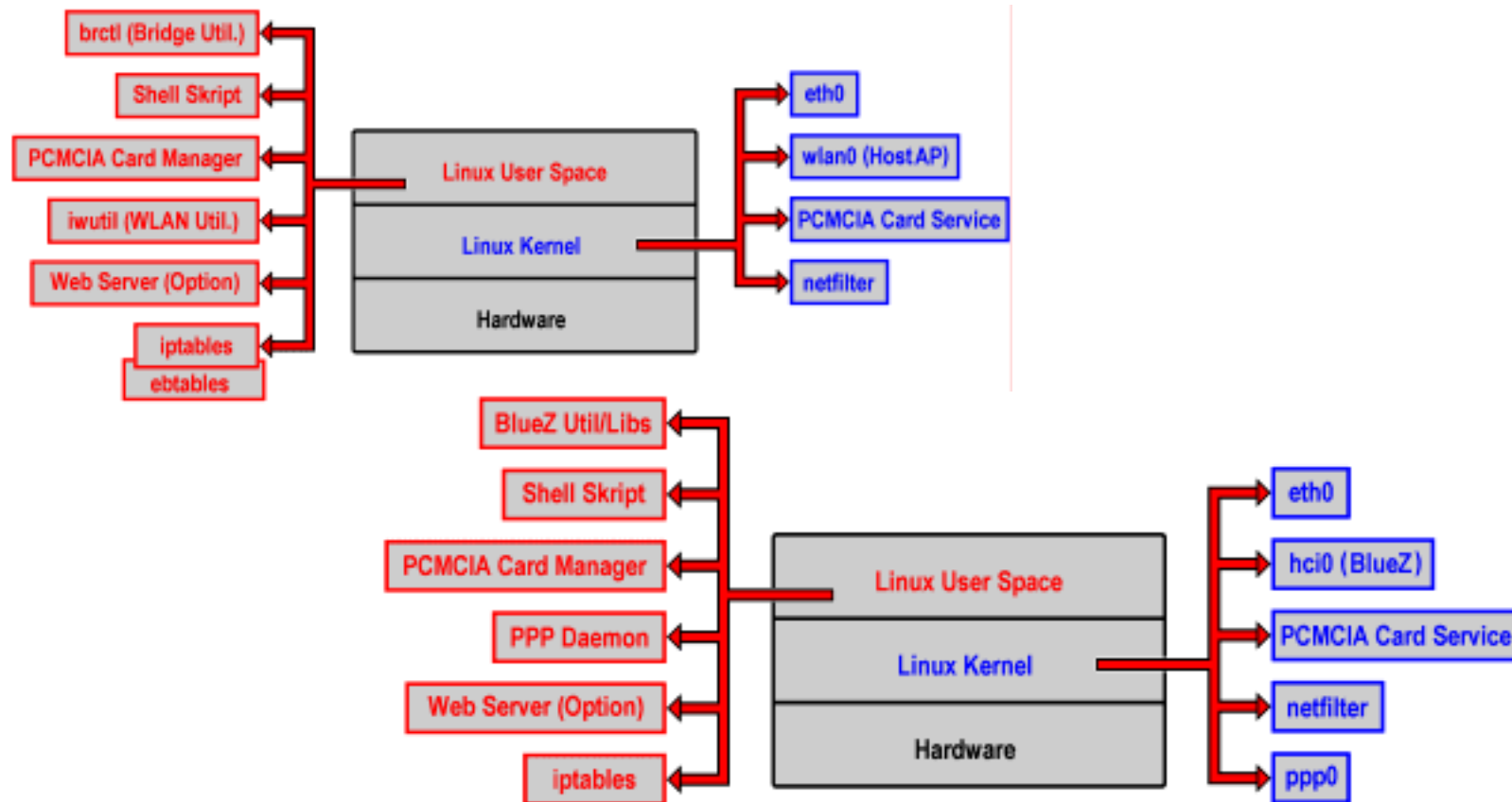
* Das größte Problem beim Erzeugen eines Embedded Linux ist meistens der Boot Loader.

* Besonders hilfreich ist, dass (fast) alles im Quellcode zur Verfügung steht (Open Source).



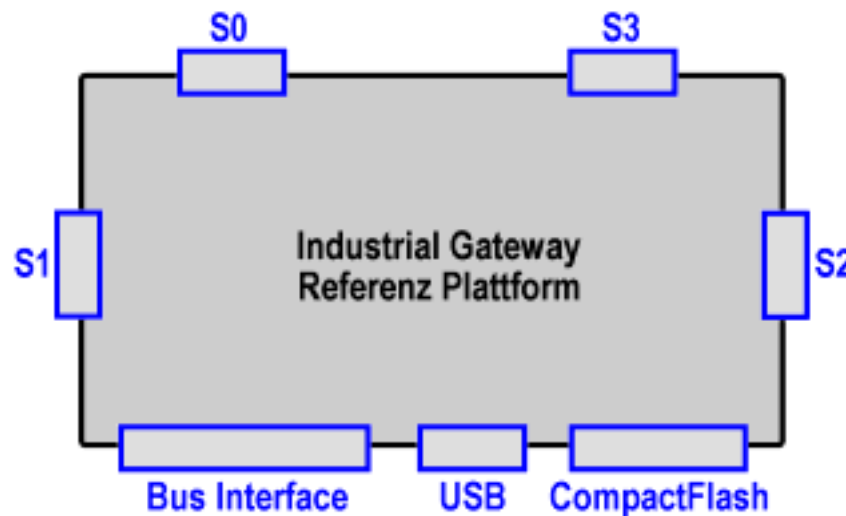
Embedded Linux

* Es gibt sehr viel Zubehör, um ein Embedded Linux für Gateways zu erstellen. Auch Bluetooth- und WLAN-Konfigurationen sind möglich.



Referenzmodell

- * Ein industrielles Gateways kann viele unterschiedliche Schnittstellen besitzen, welche Linux-Unterstützung benötigen.



S0: RS232

S1: Ethernet

S2: Ethernet, PPP, PPPoE

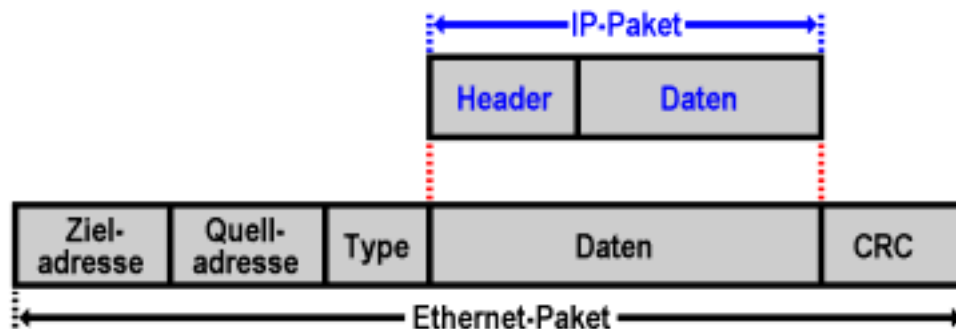
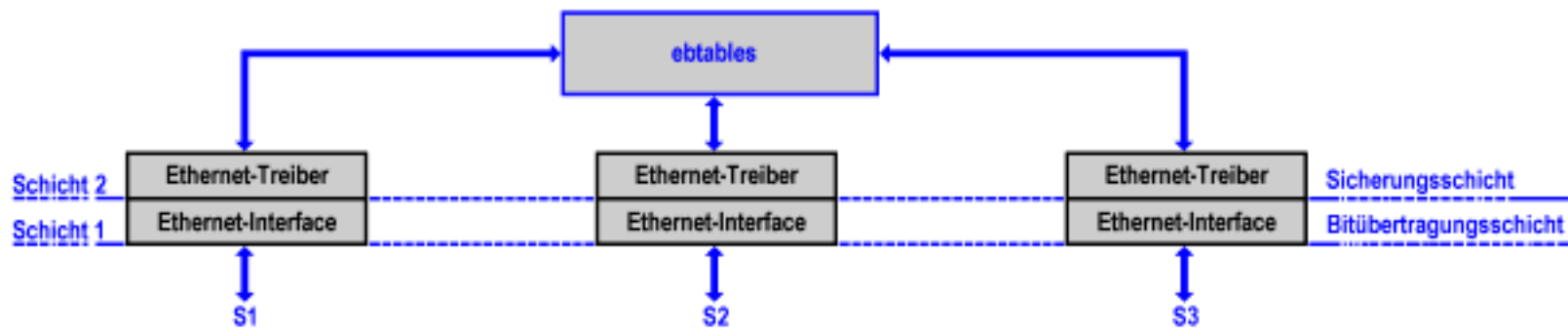
S3: Ethernet (DMZ)

USB: Konfiguration, Log-Dateien

- * Über das Bus-Interface können zum Beispiel WLAN-Schnittstellen, Feldbus-Anbindungen oder sonstige Spezialschnittstellen realisiert werden.
- * Auch die Erweiterung mit Crypto-Coprozessoren ist geplant.

Paketfilter

* *ebtables* ermöglicht das Filtern von Paketen im Layer 2 (Data Link Layer, Network Access Layer). Es sind sehr wirkungsvolle ACLs möglich. Sogar ein MAC-Adressen-NAT ist realisierbar.

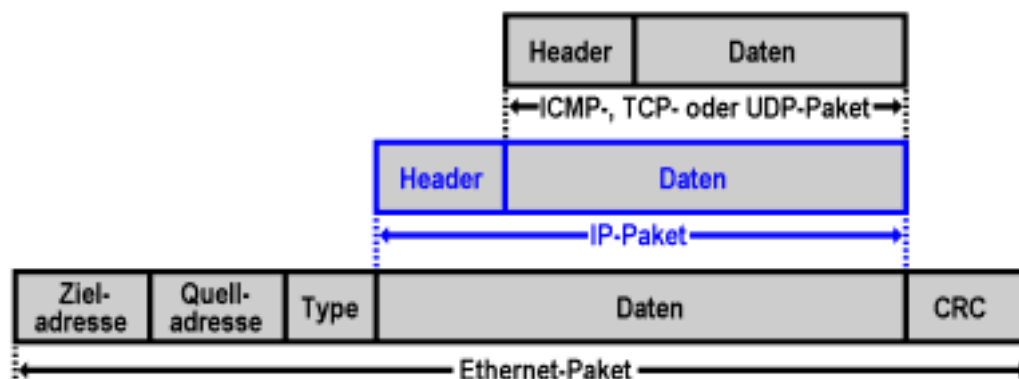
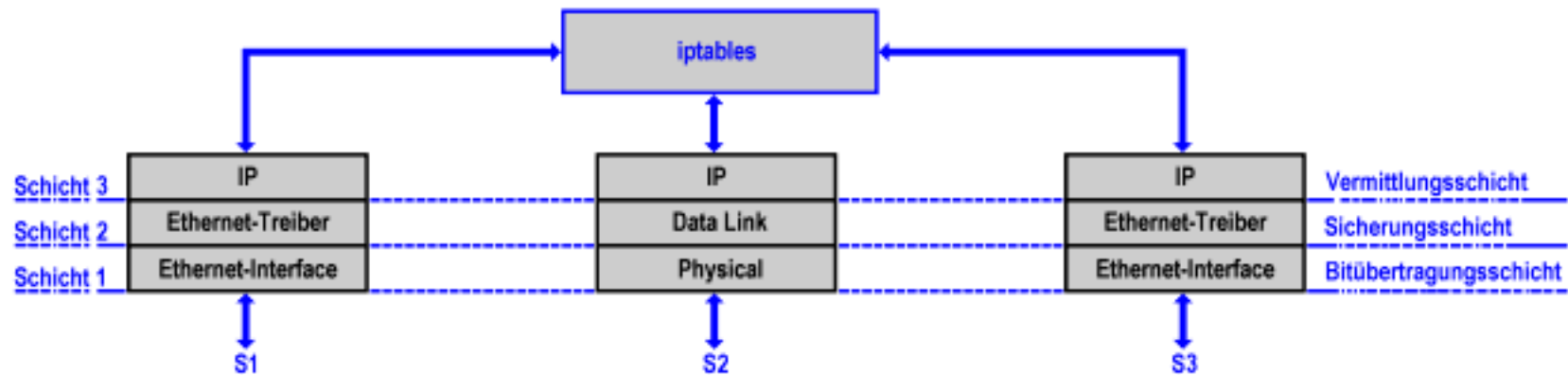


- * Ethernet-Protokollfilter
- * MAC-Adressenfilter
- * ARP-Kopfdatenfilter
- * MAC-Adressen-NAT



Paketfilter

* *iptables* ermöglicht das Filtern von Paketen im Layer 3 (Network Layer). Dabei werden auch die Protokolle im Layer 4 (Transport Layer) ausgewertet.

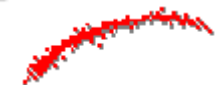
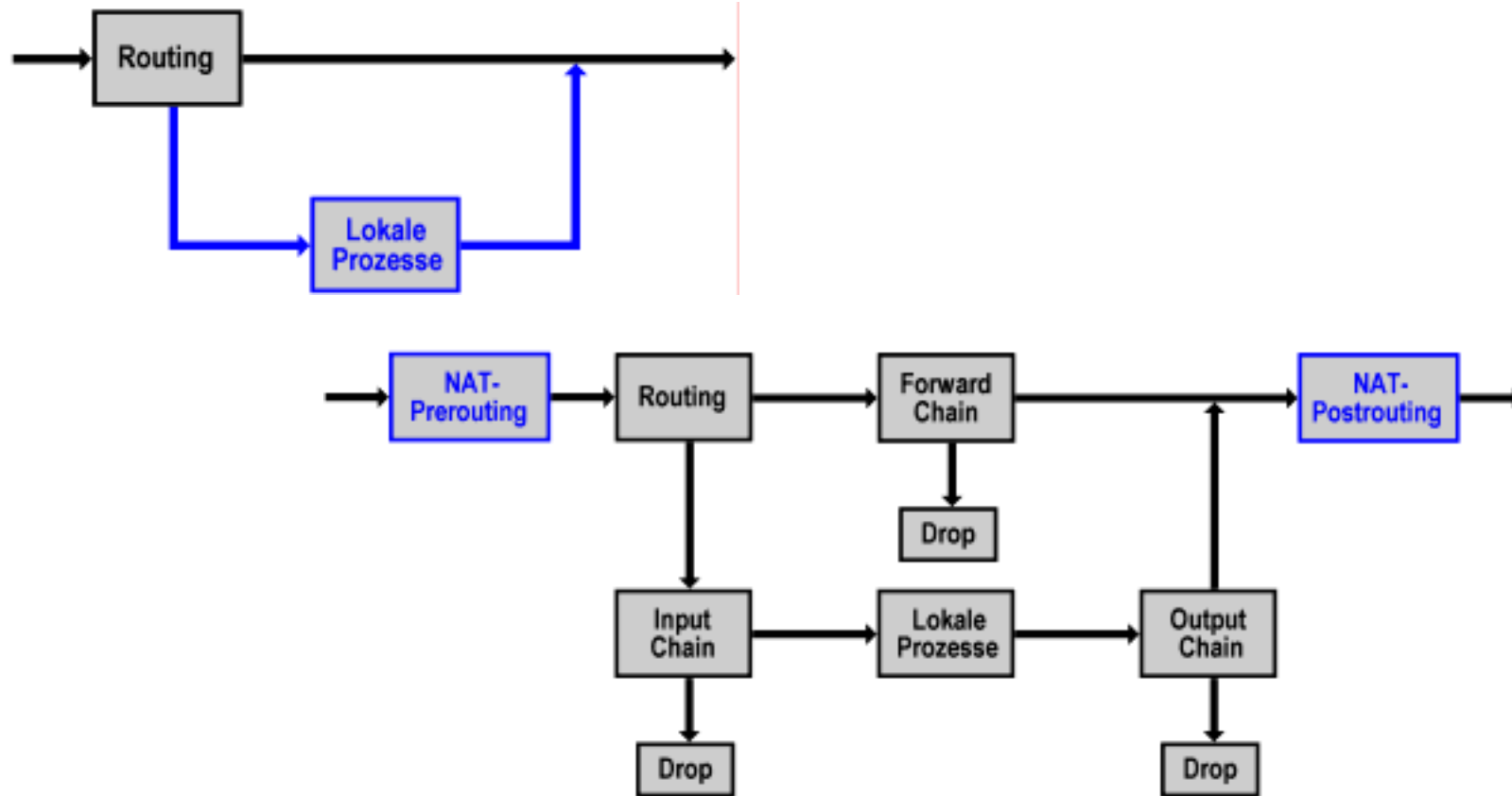


- * SPI-Filter für UDP & TCP
- * Inbound/Outbound NAT
- * PAT (Port Adr. Translator)
- * Skriptdateien mit Regeln



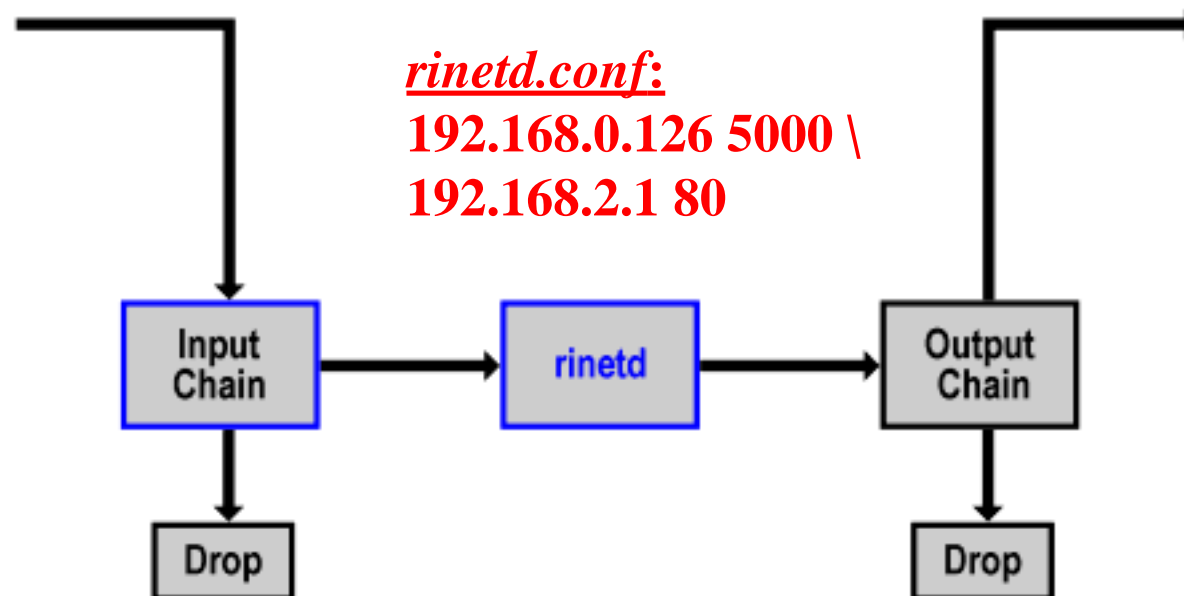
Paketfilter

* Die Pakete durchlaufen verschiedene Stationen innerhalb des Linux-Kernels. Standardmäßig wird an drei verschiedenen Stationen gefiltert.



Weitere Möglichkeiten

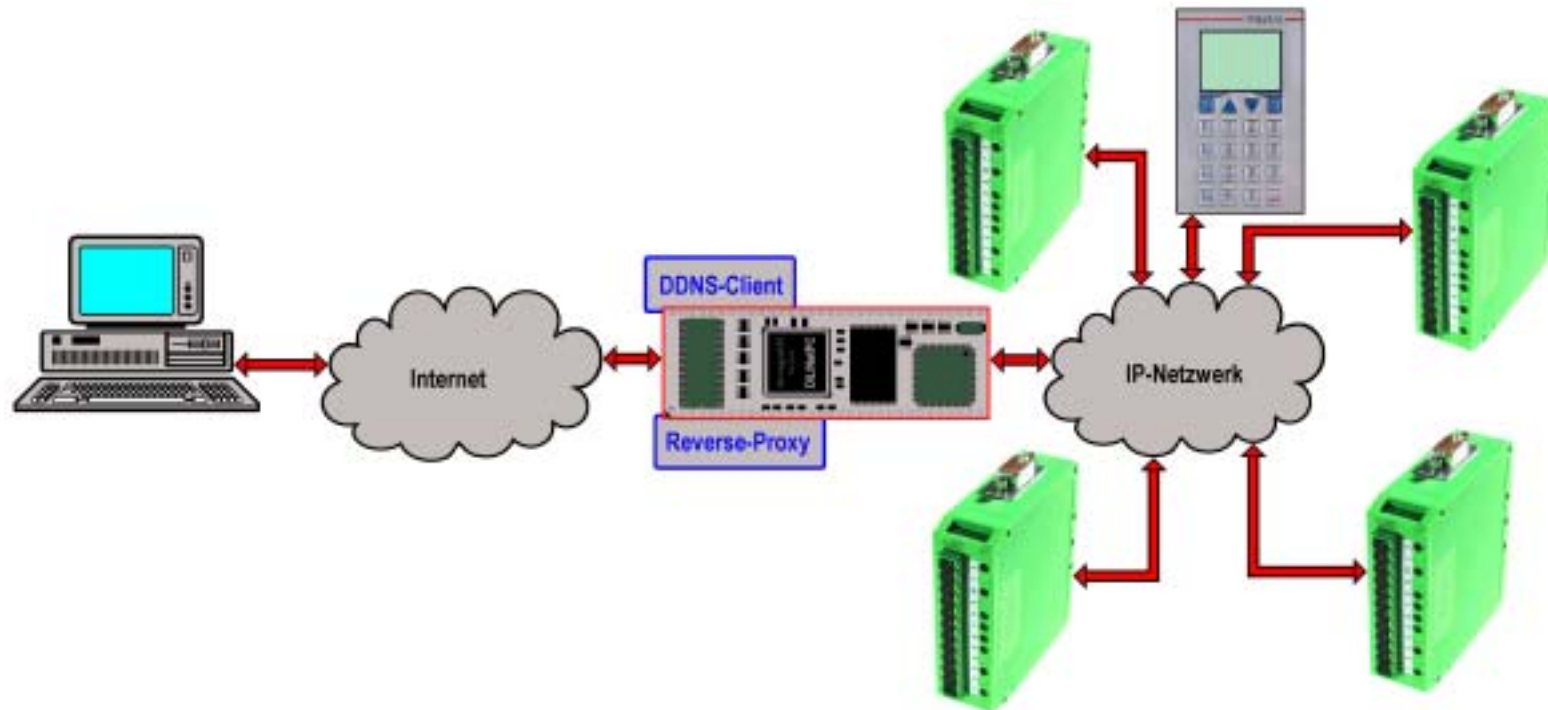
* Auch lokale Prozesse können zusätzliche Sicherheitsfunktionen anbieten. Ein Beispiel wäre der TCP-Redirector *rinetd* (Internet Redirection Server).



* Durch *rinetd.conf* im Beispiel werden alle Pakete für 192.168.0.126:5000 an 192.168.2.1:80 umgeleitet. Der Forward Chain ist ausgeschaltet.

Reverse Proxy

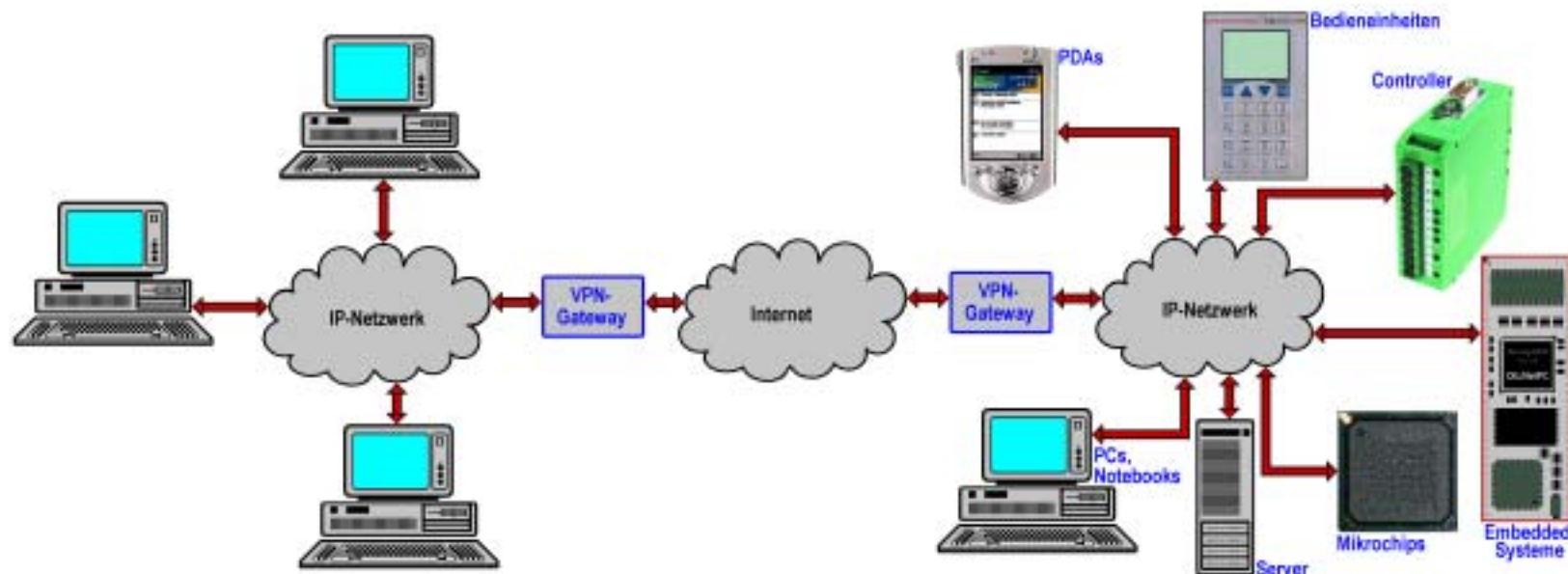
* Zahlreiche Automatisierungskomponenten besitzen heute bereits einen eingebauten Webserver (Konfiguration, Service, Bedienen- und Beobachten).



* Mehrere Server können zu einer Website zusammengefasst werden. Es wird nur eine IP-Adresse (ein DNS-Name) veröffentlicht.

VPN-Gateways

* Für Linux stehen auch zahlreiche Erweiterungen zur Verfügung, um VPNs zu realisieren (IPsec, Client-to-Site VPN, Site-to-Site VPN).

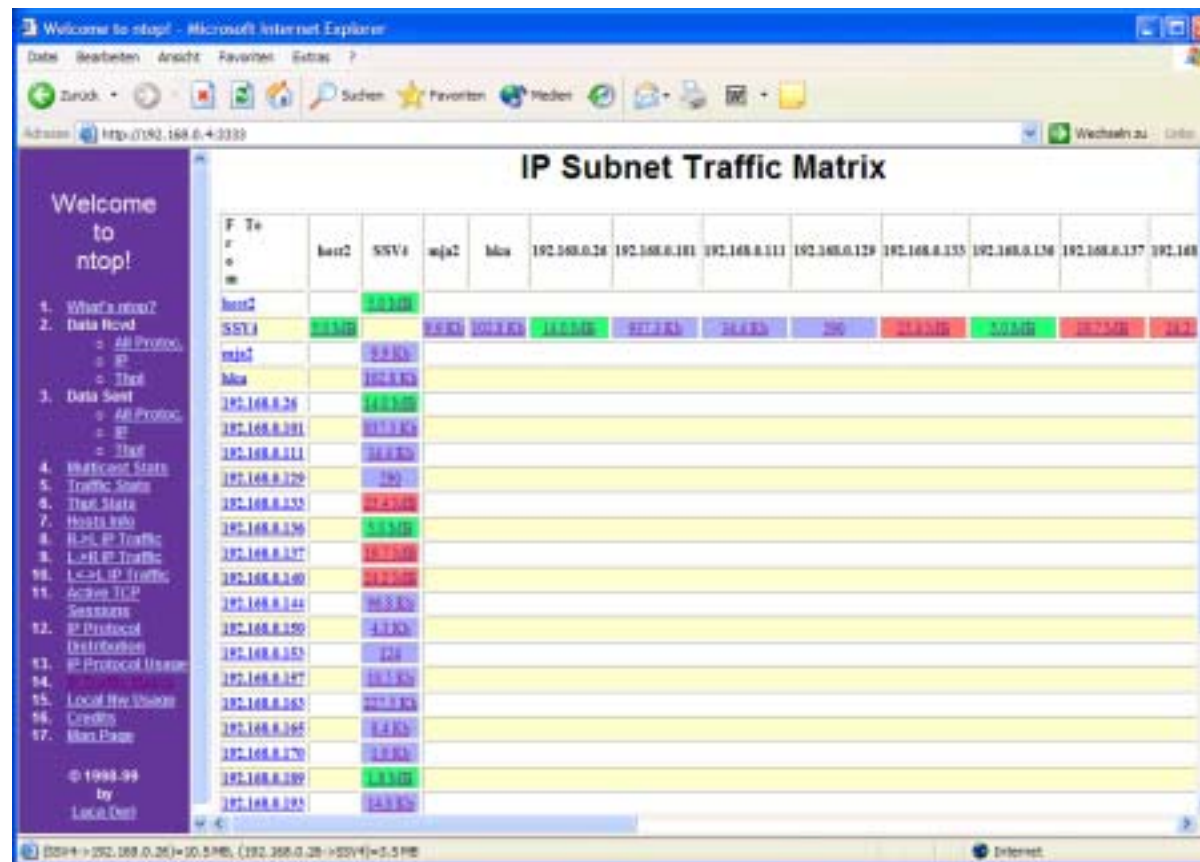


* VPN-Gateways legen einen „Tunnel“ durch das Internet. Dadurch entsteht eine vollständig abgesicherte Punkt-zu-Punkt-Verbindung.



Managementwerkzeuge

* Auch ein industrielles Gateway sollte überwacht werden. Für diese Aufgabe kann ein Embedded Linux zum Beispiel mit *ntop* ausgerüstet werden.



AMSEL

* Zusammen mit *.vantronix* arbeiten wir an einer Linux-Distribution, welche in erster Linie auf industriellen Gateways zum Einsatz kommen soll.



AMSEL
Advanced Modular Secure Embedded Linux

New Security Linux Distribution
for Embedded Systems

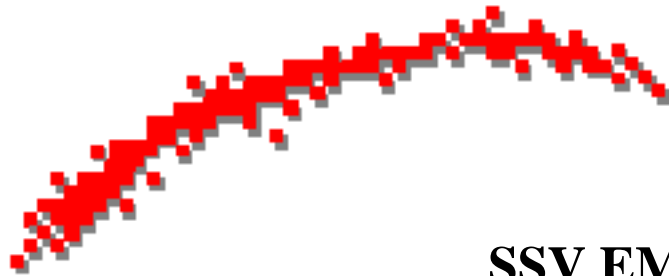
Key Features:

- IPsec VPN
- Router/Firewall configuration
- SPI packet filtering

www.amselinux.com

DIL/NetPC included





**SSV EMBEDDED SYSTEMS
HEISTERBERGALLEE 72
D-30453 HANNOVER
TEL.: +49-(0)511-40000-0
FAX.: +49-(0)511-4000040
WWW.DILNETPC.COM
WWW.SSV-EMBEDDED.DE
EMAIL: INFO@IST1.DE**

File: gateways.ppt Revision: 2.0 - 12.02.2004

