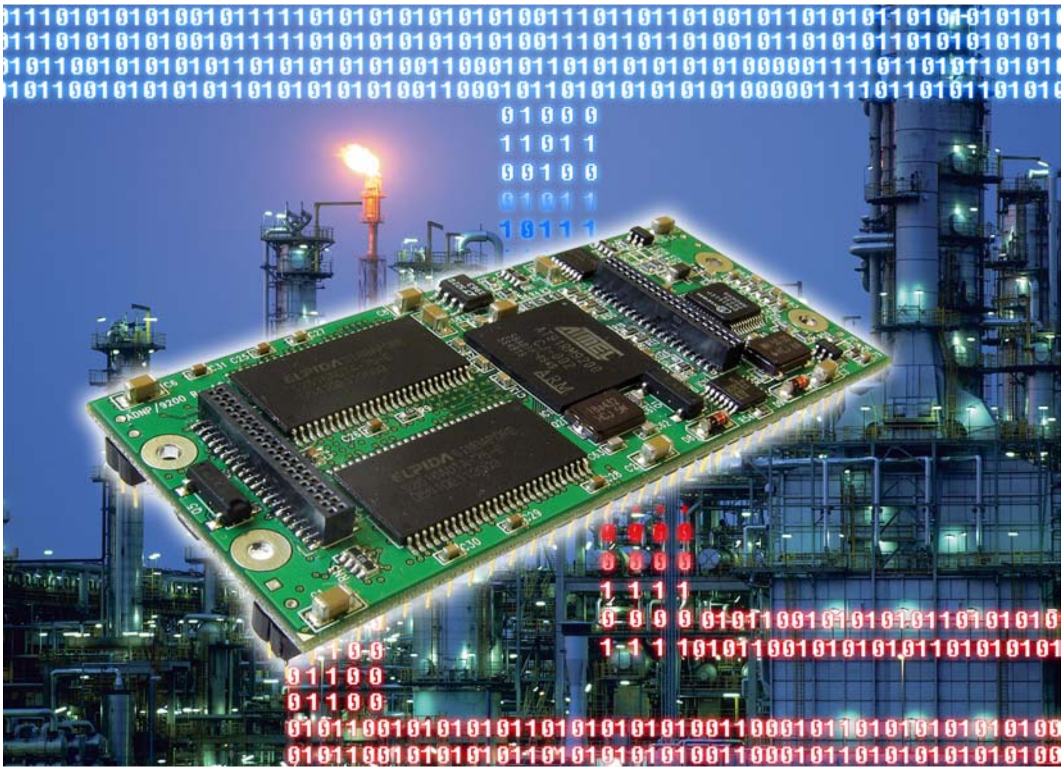
Embedded Gateway Server for Maintenance

Using IP-based embedded gateway server to consolidate the remote maintenance of multi-vendor systems increases system security and cuts costs.

Interface diversity in multi-vendor environments continues to grow. Established point-to-point links and fieldbus interfaces are being joined by a constant influx of real-time-capable Industrial Ethernet protocols. There are now 19 different techniques listed by the Reutlingen University web site [1] published by Prof. Dr. Schwager. In addition, a variety of wireless technologies (Bluetooth, IEEE 802.11-based WLAN, ZigBee) are gaining in popularity in the field of automation. Concepts and solutions for seamless and harmonized remote maintenance (remote access) are currently in short supply.



However, they are desperately needed, since each separate access attempt for remote maintenance (perhaps with a dedicated direct modem link or via the Internet) represents a potential weak spot with respect to system security and reliability. In addition, maintaining multiple access points can increase operating costs.

Introduction

For reasons of security and cost, a multi-vendor system should only have one access point for remote maintenance. Ideally, this access point should also support temporary interfacing with mobile computers, so that service engineers employed by the various manufacturers can access system components. However, the requirements to be met by a service gateway of this nature are high. First, this infrastructure component has to be able to support all conceivable interfaces that might be used at the field bus and control level. Second, sophisticated security mechanisms are required in order to protect the system against unauthorized access and encrypt communication.

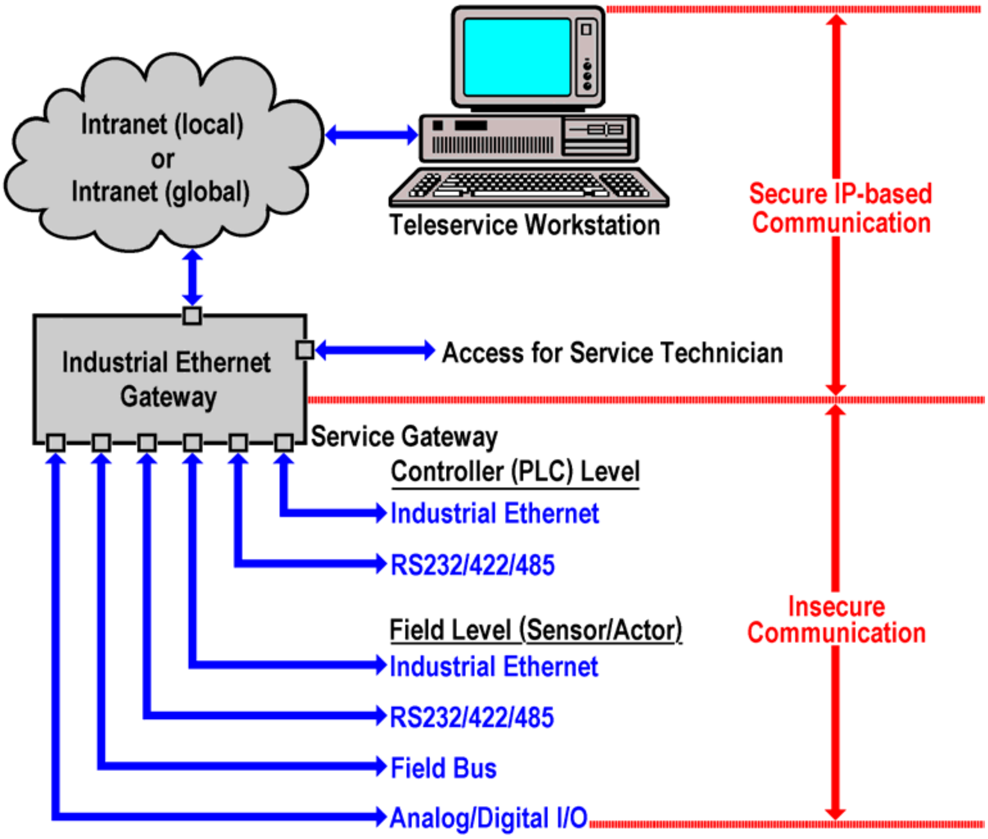


Figure 1: Industrial Ethernet gateway as a universal remote service gateway

Figure 1 illustrates a possible scenario with a embedded gateway server – like the DIL/NetPC ADNP/9200 [3] – at its center. Using this type of server as a service gateway facilitates uniform IP-based remote access to a multi-vendor system. On the automation side, the gateway offers the required interfaces via a plug-in card system. Communication at this level is usually non-secure. On the public IP side of the gateway (the remote service workstations used for remote maintenance and the access interface for service engineers), secure communication is achieved using the TCP/IP protocols SSH, SFTP and HTTPS. Data encryption is based on SSL.

Hardware IP Integration of Various Interfaces

The first thing to note at the control level is the variety of PLC systems. A uniform programming interface does not exist for PLCs. Industrial Ethernet and conventional serial interfaces (RS232/422/485) are required for remote access.

Should PPI or MPI special interfaces be required for Siemens S7-2xx and S7-3xx PLCs, these can be implemented using corresponding adapters.

Experience shows that there is the greatest diversity of interfaces at field level. Alongside Industrial Ethernet - some implementations of which involve a variety of real-time-capable special variants - we also find various field buses, serial links based on RS232/422/485 and special sensor/actuator interfaces which can only be addressed using analog or digital inputs/outputs.

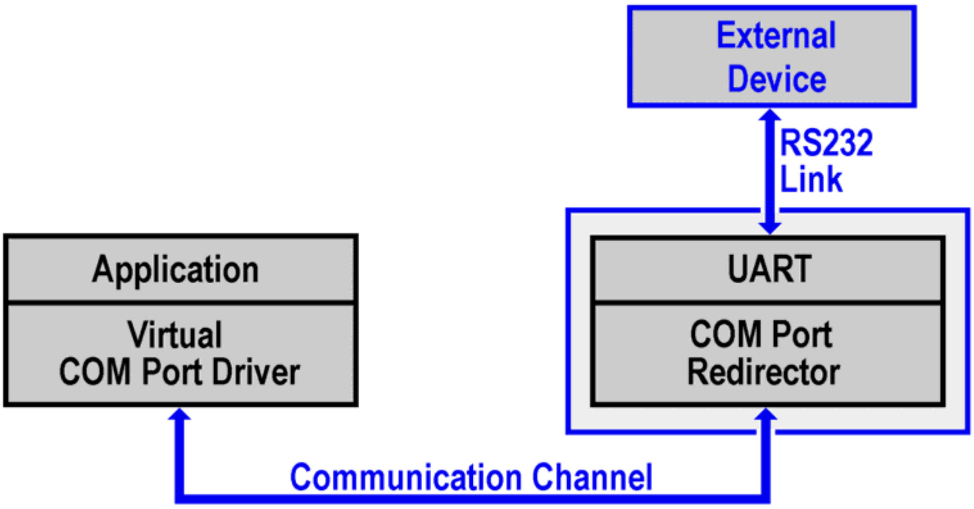


Figure 2: VCOM port drivers support COM ports located at significant distances

For serial interfaces at control and field level, the ADNP/9200 can work as what is known as a COM port redirector. A redirector of this type is linked at one end to the relevant functional unit (e.g., a PLC) via an internal UART (in other words, the physical chip for implementation in a serial interface) (Figure 2). The other end is connected to an IP-based communication channel, at the end of which there is a virtual COM port driver (VCOM driver) which might run, for example, on the remote service workstation in Figure 1. This transmission channel can, for example, be simulated by an Ethernet LAN or any other TCP/IP-capable connection. Even the Internet has been considered as a link between VCOM driver and COM port redirector. In other words, a Windows-based remote service workstation can, for example, use a virtual COM port and a corresponding COM port redirector to access a COM port located (very) far away from it in order to allow PLC programming software to access the PLC without the need for any changes. As a COM port redirector, the gateway server in Figure 1 links its serial interfaces to IP networks with total transparency, thereby allowing uniform remote access.

As most field buses (e.g., Interbus and Profibus) can be implemented using serial interfaces, the technique described above based on a COM port redirector and virtual COM port driver can also be used to gain remote access for maintenance purposes. However, CAN is an exception. This field bus is linked to an IP-based network in a different way. If CANopen is being used as an application protocol at control or field level, the implementation of CiA specifications CiA309 (Interfacing CANopen with TCP/IP [2]) is recommended. In an application of this nature, the ADNP/9200 gateway server in Figure 1 would work as what is known as a CANopen gateway server. If access to the subordinate CAN protocol levels via TCP/IP is required, a converter software program, for example (such as the SSV IGW/400-CAN Smart Command Line Interpreter (SCLI)), will suffice. This software supports transparent access to multiple CAN field bus systems at control and field level via a TCP socket connection.

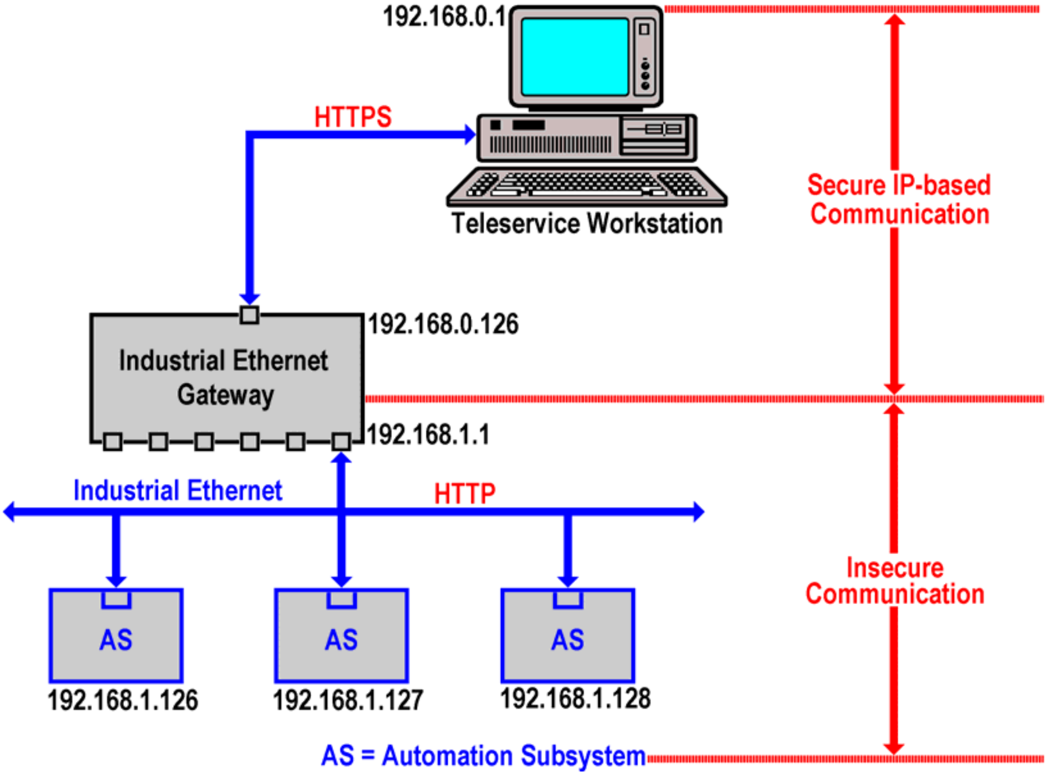


Figure 3: Use of HTTPS/HTTP proxy for web server security in the AS

If the PLCs and field devices already have Industrial Ethernet interfaces, the gateway server will function primarily as a proxy. In this context, implementation of the non-secure TCP/IP application protocols (e.g., Telnet, FTP, HTTP, TFTP) in their counterpart secure versions (SSH, SFTP, HTTPS) is of particular importance. Furthermore, appropriate access protection based on user profiles must be implemented for access by system operators. Figure 3 illustrates a technique for secure access to non-secure HTTP-based web servers in automation components via secure HTTPS.

Data Servers for Service and Maintenance

Thanks to its ability to interface with all major modules at control and field level, an ADNP/9200 embedded gateway server can also serve as a central database for system maintenance. In order for multi-vendor systems to be maintained and serviced effectively, informative and up-to-date data material is vital. Ultimately, it must always be assured that the service engineers working for the individual manufacturers are able to carry out the necessary work without impairing the function of modules supplied by other manufacturers. In this respect, a central database is a vital tool. An embedded gateway functioning as a data server [4] can perform a total of four important database tasks:

1. Saving of all alarm and fault messages: All relevant messages associated with a system should be time-stamped and stored in a database. This will enable the events leading up to a system failure to be tracked.

2. Recording of important operating parameters: In addition to operating times providing the basis for proactive (preemptive) maintenance, important operating parameters such as the temperatures of individual modules, voltage fluctuations and interruptions, excess speeds and important user access attempts (e.g., shutting down and starting up a system) can be stored in the embedded gateway server's database.

3. Central storage of configuration data: The majority of modules in a system will have specific configuration data which can be used to adapt a module for use in a given system. This data should be available on the data server.

4. Logging of all service activities: Faults frequently occur directly after service and maintenance work has been carried out. In a multi-vendor system in particular, it is, therefore, vital to have a virtual log book recording all work carried out. This enables more complex error sources to be tracked down much more quickly.

Furthermore, a comprehensive image of the associated system can be stored on a data server of this type, providing all service engineers with the overview they need of the links between the individual components within the overall system.

Security

In addition to the use of secure TCP/IP protocols such as SSH, SFTP and HTTPS and the associated SSL required, an embedded gateway server also needs to have a powerful IP packet filter. This software function filters all incoming and outgoing IP data traffic at packet level. It provides a means of checking MAC and IP source and target addresses, port numbers and other protocol parameters. Only packets meeting a specific set of rules and regulations can pass through the gateway. All other packets are rejected.

An IP packet filter of this type can be implemented using netfilter/iptables [5] in conjunction with an embedded Linux operating system as a software basis for the gateway. The netfilter/iptables software modules are also used in numerous IT firewalls, thereby proving their suitability for practical application. The Firewall Builder can be used to create the set of rules and regulations [6]. This support software can be used on an external PC. Featuring an advanced user interface, it supports the editing of filter rules at the click of a mouse on a transparent graphics-based display. The rules and regulations created using the interface are then simply transferred to the gateway, where they are subsequently applied.

Conclusion

For reasons of security, remote access to multi-vendor environments via Internet or intranet is a particularly critical issue. A single central gateway can reduce the access paths to a system. In conjunction with corresponding configuration settings, an embedded gateway of this type can be used to maximize access protection and functional security.

References

[1] Reutlingen University web site: http://www.real-time-ethernet.de/
[2] CiA (CAN in Automation) web site: www.can-cia.org
[3] Product descriptions for DILNet/PC ADNP/9200: www.dilnetpc.com
[4] Product descriptions for IGW/400-CAN: www.ssv-comm.de.
[5] Software and application descriptions for ADNP/9200: www.dilnetpc.com.
[6] Netfilter/iptables web site: http://www.netfilter.org/
[7] Firewall Builder web site: http://www.fwbuilder.org/

Contact

SSV Embedded Systems
Heisterbergallee 72
D-30453 Hannover
Tel. +49-(0)511-40000-0
Fax. +49-(0)511-40000-40
Email: sales@ist1.de
Web: www.ssv-embedded.de
Web: www.dilnetpc.com

Please note

This document is written only for the internal application. The content of this document can change any time without announcement. There is taken over no guarantee for the accuracy of the statements.

INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED 'AS IS' WITHOUT WARRANTY OF ANY KIND. The user assumes the entire risk as to the accuracy and the use of this document. Some names within this document can be trademarks of their respective holders.