



Machine control going www **Opportunities and risks when connecting a control system to the Internet**

Over the last few years control systems have undergone drastic technological enhancements. Where the classic approach of using microcontrollers as a Programmable Logic Controller – PLC – was industry standard in the past, today's machine control is based on PC technology adopted for the harsher environments found in industrial applications. By applying this technology onto a machine control system a great variety of PC features is now embedded within the actual control. At the same time the World Wide Web brought electronic communication and networking the virtually everyone. The combination of the Internet and embedded PC based controls now open opportunities especially in the areas of remote maintenance and diagnostics that are mutually beneficial for both the manufacturer and user of a production machine. Though features like TCP/IP, web server, VNC, VPN, email have been available for around 2 years now they have not been adopted by many OEMs also because of security concerns and necessary implementation efforts of their customers. This article will provide an overview of available technology and show methods on how to maximize on diagnostics with minimal risk and implementation effort.

Get connected – how to establish a remote connection with a machine controller

Mainly there are two methods how to access machine controller remotely, either via an analog modem line or via the Internet. Both methods have advantages and disadvantages, which are examined a little closer.

Modem connection

Accessing a controller through an analog phone line via a dedicated modem has been available for a number of years. The advantages of this solution are:

- Relatively low configuration effort. The modem needs to be connected to the controller and both modem and controller need to be configured to ensure proper communication.
- Independence from IT infrastructure. Since the modem uses a dedicated phone line, there is no integration of the machine into the local LAN necessary.

However there are also several disadvantages:

- The communication speeds are limited to about 56 kbps.
- Standard fax modems are not designed for industrial use and industrial modems are rather expensive.
- The modem requires a dedicated analog phone line and therefore can't easily be integrated into phone systems. Instead of simply using up an extension number, they need their own main line which may also result in extra monthly phone costs.
- Each machine controller within a plant may require its own modem.
- The caller also needs a PC with a modem connected to a dedicated analog phone line.
- Security can be an issue as there is no protection to verify the caller, which means that anybody calling the phone number might be able to tamper with the modem settings or even the connected controller.



- The controller can be diagnosed with the development suite only. In an integrated controller all other integrated PC technology features briefly mentioned above typically can't be utilized. For example while it is possible to monitor variables in the controller and update the program, it is not possible to view the screens.
With the integration of Serial Line IP (SLIP) most of the integrated PC technology features also become available via modem. SLIP basically transforms the IP protocol typically communicated via Ethernet to a serial connection that can also be established between two modems. To utilize SLIP on the controller it simply needs to be configured. On the PC of the caller a dial-up network connection needs to be set up.
While SLIP greatly increases the functions available via a modem line, all other listed disadvantages still remain.

Internet connection

With the migration of PC technology into machine controllers accessing them via the Internet has been made possible, offering a number of advantages, but also some disadvantages.

Advantages:

- Higher bandwidth depending on the internet connection speed between the controller – e.g. end user site – and the remote access location – e.g. OEM site.
- No additional hardware required on either side as only an Ethernet port connected to the LAN is required on either side.
- No extra monthly service costs.
- Any number of controllers can be accessed within a plant as long as they are all connected to the plant's LAN.
- Properly configured, a high level of security can be achieved, limiting who can access the controller.

Disadvantages:

- The main disadvantage is the necessary configuration effort on both sides – the controller and the remote access location – to ensure proper communication and security.

While the configuration of a remote connection to a machine controller via the internet should not be the responsibility of a controls engineer – instead it should be setup between the IT departments of the companies involved – let's briefly discuss a few basic elements about networking.

For a computer to communicate with a machine controller over Internet, it must have an **IP address**. An IP address is a unique 32-bit number that identifies the location of your computer on a network. When IP addressing first came out, everyone thought that there were plenty of addresses to cover any need. Theoretically, you could have 2^{32} unique IP addresses. With the explosion of the Internet and the increase in home and business networks, the number of available IP addresses is simply not enough.

This is where **Network Address Translation (NAT)** comes to the rescue. NAT allows a single device, such as a router, to act as an agent between the Internet (or "public network") and a local (or "private") network. This means that only a single, unique IP address is required to represent an entire group of computers.



A local network uses IP addresses only internally. Most of the network traffic in a local network is local within the network, so it doesn't travel outside the internal network. The IP addresses of any device connected to a local network are typically so-called unregistered IP address. Now if any computers that use unregistered IP addresses wants to communicate with the outside world, it must use NAT.

NAT is used by the router is configured to translate unregistered (inside, local) IP addresses, that reside on the private (inside) network, to registered IP addresses. This happens whenever a device on the inside with an unregistered address needs to communicate with the public (outside) network.

Using NAT, any computer having assigned an unregistered IP address can be accessed through the internet as long as the registered (public) IP address, which is unique, is known. This means that a single public IP address can serve many private IP addresses behind it.

One of the best methods to establish is a secure connection through a **Virtual Private Network (VPN)**.

Basically, a VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site.

Proper setup of a VPN network guarantees maximum security of the connection and allows only configured users to connect to the machine controller. Typically the VPN is configured at the user's fire wall, where a machine controller may be connected to a **Demilitarized Zone (DMZ)**.

A DMZ is a network area that sits between an organization's internal network and the Internet. The point of a DMZ is that connections from the internal and the external network to the DMZ are permitted, whereas connections from the DMZ are only permitted to the Internet. Controllers in the DMZ may not connect to the internal network. This allows the DMZ's machine controllers to provide services to both the internal and external network while protecting the internal network in case intruders compromise a host in the DMZ. For someone on the external network who wants to illegally connect to the internal network, the DMZ is a dead end.

Once a remote connection to a machine controller has been established, several features are now available to send and receive information to and from the machine controller.

Those features are:

- **Online diagnostics with the development suite** for the machine controller application, e.g. B&R's Automation Studio. Once the IP address of the machine controller can be reached, all of the debugging, diagnostics, and download functions are available no matter where the PC or the controller is located, just as if the controller was connected to the PC running Automation Studio through a short Ethernet cable.
- VNC stands for "**Virtual Network Computing**" and is a system that can be used to remotely control the desktop of another computer. Keyboard input and mouse movements and clicks are transferred over the network from the client to the server. In the other direction, changes to the screen's contents are transferred from the server to the client. TCP/IP is used as the network so that nearly any Internet-capable network connection can be used (including e.g. dial-in modems).



B&R's controllers offer a VNC server; in other words, it can be controlled from other computers if they are using a suitable VNC client. By using VNC the contents of the screen can now be shown on a remote computer. It is possible to limit the access to a view only, so accidental operator inputs from a remote location can be locked out. It is also possible to program a separate visualization that can only be shown through VNC, which would allow the remote operator to see data on a different set of screens that are not to be seen by the local operator.

In either use-case, VNC is a big leap forward in visually seeing what is happening on a machine.

- **FTP or File Transfer Protocol** is used to transfer data from one computer to another over the Internet, or through a network.
Specifically, FTP is a commonly used protocol for exchanging files over any TCP/IP network, such as LANs and the Internet. There are two computers involved in an FTP transfer: a server and a client. The FTP server listens on the network for connection requests from other computers. The client computer, running FTP client software, initiates a connection to the server. Once connected, the client can do a number of file manipulation operations such as uploading files to the server, download files from the server, rename or delete files on the server and so on.
B&R controllers have a FTP server implemented. This allows a local or remote access to any files that need to be obtained from the machine controller, such as production data, log files, or machine configuration and setup files.
- A **Web Server** enables the display and input of process values on a standard internet browser using intranet connections. B&R controllers have a Web Server implemented as part of their operating system.
HTML pages are created using a HTML editor (i.e. MS FrontPage) and transferred directly via FTP or the "Publish FrontPage Web..." function to B&R Automation Runtime.
A standard internet browser enables these pages to be called and displayed from the Web Server. Through active server pages (ASPs), variables can be output or modified using HTML pages.
A Web Server allows remote monitoring and control of a machine independent of the local machine visualization. Unlike VNC no viewer software is required and other browser functions, like playing videos or opening PDF documents stored on the machine controller can be displayed via the Web Server. A practical usage is to show enhanced machine tutorials displaying those types of files on a computer connected to the machine controller for diagnostics, especially for machines where a Windows based visualization would be too expensive.
- **Simple Mail Transfer Protocol (SMTP)** is the de facto standard for email transmissions across the internet. SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified and then the message text is transferred. It is a client-server protocol, where the client transmits an email message to the server. B&R controllers have a SMTP based email function available. This allows the machine controller to automatically send email messages locally within the network or to any email address over the internet, as long as the authentication to the SMTP server where the controller is installed is configured. It is also possible to attach files to the email. Practical examples are pro-active maintenance emails, machine production statistics gathered for each shift in a .csv file that is sent at the end of the shift and much more.



Summary

This paper explained in simple terms methods to configure a connection from a remote location to a machine controller. The additional efforts when connecting a controller to a company network and access it via the Internet are by far outweighed by the benefits that are gained. Typically configuration has been the task of a company's IT department and while this will also be true for some time in the future this paper also briefly took a look at some of the necessary configuration tools.

Most importantly there are several features available in B&R's controllers that in the past required a PC. Features like VNC, FTP, Web Server, and SMTP greatly add to the information an OEM can obtain from a machine installed at any end user site without being in front of it. Utilizing those features opens a lot of opportunities in troubleshooting any problems, or simply getting data out of a machine from anywhere in the world, where previously it could only be done when being right in front of it.

Robert Muehlfellner
Director of Automation Technology
B&R Industrial Automation Corp.

For more information on B&R contact:
B&R Industrial Automation Corp.
1325 Northmeadow Parkway, S-130
Roswell, GA 30076
Phone: (770) 772-0400
Website: www.br-automation.com
Email: sales.us@br-automation.com