White Paper

Remote Connection Options For Monitoring, Troubleshooting and Maintenance of Control Devices for OEM Machine Builders

INSYS Microelectronics · Coventry · United Kingdom
www.insys-datacommunication.co.uk

Introduction:

Each year an OEM machine-builder can spend thousands of pounds on expensive on-site intervention costs (including related travel expenses) in many cases to arrive on site and find that a simple fix or parameter adjustment is all that was required. This whitepaper discusses the options available to OEM machine builders to avoid unnecessary costs by using a remote connection to the electrical control equipment. This means that typical operations such as equipment maintenance programs, configuration changes or PLC programming can be handled directly from the OEM business premises or other remote locations.

This paper deals with the physical connection methods and assumes that any locally approved User Access and Authentication Policies and IT Procedures are followed. Also any remote control of plant and machinery should be fully assessed and understood and follow the appropriate machinery safety directives.

It is important to consider the functional requirements for remote access as they impact the solution used. The different scenarios for remote access to plant and machinery have a range of characteristics, including who the user is (role – including internal employees, partners, and suppliers) and where the user is located (physical and network location). Each case will have different considerations and requirements. When considering implementing remote access, the following questions will help identify the available choices:

- What is the functionality and frequency of connection?
- What connections are available, telephone lines, internet, mobile phone networks?
- Is there an existing “partner” remote access policy - the ability and process to add partners (OEM, SI, vendor, contractor)?
- What types of connections are supported by the remote equipment?

In the following pages we take a general look at the options available.

Telephone Modems

Still the most common form of remote access connection is via the Public Switched Telephone Network (PSTN). PSTN exists all over the world and is much standardised. Analogue modems transmit digital data using a normal telephone network - any analogue modem or GSM adapter can act as receiver. This solution is easy to implement, can be cost effective but may be limited for some requirements.

A point-to-point connection is made over a telephone line with a modem close to the remote device and a modem at the control centre. Installation costs can be high if a new phone line is needed, but you only pay for the connection time thereafter. This could be expensive for international calls; otherwise this is a cost-effective solution for occasional connections with small or medium amounts of data.

A continuous connection can be rented if required, this is called a Leased Line Connection, but these are now falling out of favour due to speed limitations and costs.

The connection speed for PSTN is relatively slow at a nominal 56K bits/second, but quicker than sending an engineer.

This is a reasonably secure connection unless a malicious individual has knowledge of the telephone number. Many industrial modems support security features such as Caller ID and Security Call-back. Unwanted connections can also be managed at the site by an operator physically disconnecting the modem cable and connecting it when needed.

PSTN Modems are normally limited in functionality and user interface. Most are configured and controlled with a terminal program using a simple command-line set of instructions conforming to a standard called the AT command set.

For reliable industrial applications where the modem is close to the connected device a DIN-rail mount industrially hardened device is recommended. Some modems are built with embedded inputs and outputs to allow for connection control, alarm notification or reset of the modem or connected device.

A good fit for a PSTN modem connection would the occasional fault finding of a Programmable Logic Controller (PLC) application. Most PLC manufacturers include capability for this type of connection in both the hardware (serial ports) and programming software.

Most Programmable Logic Controller (PLC) manufacturers include capability for modem connections in both the hardware (serial ports) and programming software.

So what if a PSTN line is not available or costly to install?

The mobile telephone network (radio) is a viable alternative to the PSTN connection. The GSM network is the basis for worldwide transmission of voice, data and text messages to mobile end devices. For industrial use, data is transmitted using the following services:

- *Circuit Switched Data (CSD)* - Data transmission via a voice channel (just like a normal modem)
- *SMS* - Sending and receiving short text messages
- *GPRS/EDGE* - Packet-switching data service, usually via an internet connection

GSM modems are fitted with mobile phone SIM cards and act very similar to a PSTN modem when making a point-to-point connection. When using Circuit Switched Connections (CSD) the data rate is 9.6Kbits/second. This makes CSD slower than PSTN but adequate for remote PLC diagnostics. The connection speed may frustrate the user when uploading new programs or making on-line program changes.

SMS messaging is a very useful feature for many applications as it can provide a very good Alarm Notification solution. When considered as part of an overall pro-active maintenance or site-support program, SMS alarm notification fits well into the remote access picture. For example a machine can use an SMS message to notify the engineer of a potential or real problem and he can then 'dial-in' to take remedial action. This has significant benefits to machine uptime and plant efficiency.

Call costs are usually higher for GSM Circuit Switched Connections (CSD) than a PSTN call but the installation cost is cheap compared to installing a new PSTN line. Special low-use contracts are available if using the SIM card and modem as an SMS alarm notification service.

GSM Connections (CSD) are slower than PSTN at 9.6Kbits/second. This is just adequate for remote PLC diagnostics, however the connection speed may frustrate the user when uploading new programs or making on-line changes.

Mobile Cellular Internet Modems

The General Packet Radio Service (GPRS) and Universal Mobile Telecommunications System (UMTS or 3G – stands for 3rd Generation) are both services which extend from within the GSM network. GPRS and 3G are used for transmitting data over the mobile phone network in a packet-oriented way. Data packets occupy several channels at the same time whenever data needs to be transmitted. This dynamic allotment of resources means the bandwidth utilization is optimised providing higher data rates and the advantage of payment according to data volume, not connection time. A drawback of the system is that the available bandwidth may drop when many users try to access the network at the same time.

GPRS is good for applications with stable monthly data volumes, such as SCADA or Monitoring applications. It can be costly for irregular connections with higher data volumes such as PLC fault finding.

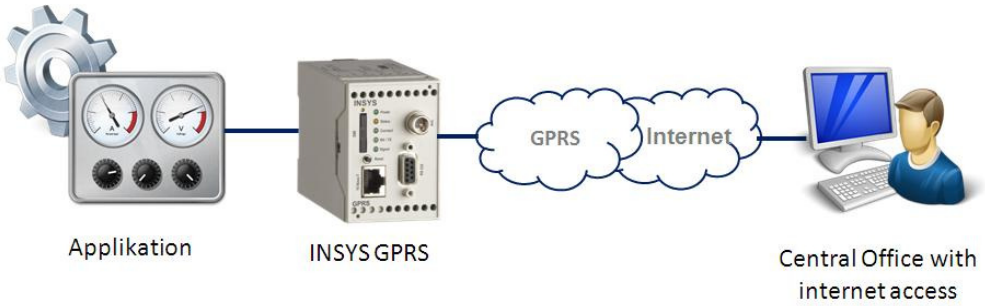
In addition, the data is also compressed by means of special coding processes so as to ensure a further data rate enhancement. This allows you to set up a virtual dedicated line at a very low cost, for sending many small data packets (e.g. measurement values).

GPRS and 3G both support internet protocol (IP), this allows an IP address to be assigned dynamically to the mobile equipment. A GPRS or 3G connection is established by reference to the Access Point Name (APN) of the SIM card provider.

Once cellular modems are connected to the internet (IP based) they integrate easily to IT-based applications, such as PC networks including Virtual Private Networks, browser based applications and real-time data feeds to enterprise applications. One of the most useful aspects is the roaming ability of Laptop computer connectivity to these networks, allowing an engineer to get a connection from many locations using a Wi-Fi hot-spot or USB 3G modem, often referred to as a dongle.

GPRS modems - What do you need?

- An application with a cable-connected GPRS modem
- An available GSM/GPRS network
- A SIM card with an activated GPRS service
- A remote station with access to Internet or the GPRS network



The maximum bit rate in the GPRS network is theoretically 171.2kBit/s. Standard commercial devices afford a maximum bit rate of 85.6kBit/s. In practice, however, data rates around 50kBit/s are typical; this is the equivalent of the average bit rate of an analogue 56k modem.

A GPRS enabled SIM card is required and the following points should be considered when choosing a provider:

- Basic charge per month with GPRS
- Monthly Included volume (1 MB, 5 MB, etc)
- Billing Block size (1kByte, 10kByte, etc)
- Billing period (e.g. 24 h)

There are many Industrial SIM card providers that have contracts specifically configured for Industrial applications. Below is an example of typical SIM card basic contract costs based on a single SIM card contracted over 2 years.

GPRS Preferred SIMs		
Package	**Annual Service Charge**	**Includes**
UltraLow	£36.41	1MB Data
Low	£45.90	12MB Data
Low	£64.26	36MB Data
Medium	£74.35	60MB Data
Medium	£109.20	120MB Data

Data correct as of January 2010.

It is important to understand that the GPRS architecture has a security firewall that blocks connection requests from the Internet to GPRS Devices (modems) for security reasons. This is no problem as long as the GPRS devices initiate the connection to the internet. There are several solutions to get around this, so some thought must be given to which solution is used. See options below:

Leased Line Mode
The GPRS device (modem) can be configured to connect after power-up to a pre-configured IP address or URL. The device then maintains the connection ("always on"). After the connection is established, data transfer is possible in both directions.

Security Call Back
The GPRS device (modem) can be triggered to make a connection by an SMS message or telephone call-back to the device. Some modems can be triggered to establish a connection by on-board inputs.

Fixed IP SIM card
The GPRS device (modem) can be installed with a Fixed IP SIM card. The SIM card provider then provides the user a secure log-in to access only his devices. Device–to-Device access is possible. This Fixed IP SIM card solution carries an extra cost but ensures security as there is no access to the devices from the internet. This is also very easy to install as all the security settings are in place at the SIM card provider.

The Fixed IP SIM option means that the modem has only one addressable location. Therefore a routing technology called port forwarding is required to give separate routes if more than one device is connected to the modem, for example a network (Ethernet) of IP devices such as PLCs or computers. Not all GPRS modems support port forwarding.

Virtual Private Network (VPN)
The GPRS modem establishes a secure Client/Server relationship with the control centre through the GPRS firewall. Once established data transfer is possible in both directions through the VPN tunnel. The control centre must have a reachable IP address on the internet using a fixed Public IP address or URL. This solution is especially useful for users with multiple sites or machines (clients) as the connections are easy to manage. However the initial set up can be complex first time out and a GPRS modem/router with VPN capability is required and carries an extra cost.

The VPN solution is also advantageous if the remote site has a network (Ethernet) of IP addressed devices. The remote site network is addressable directly across the VPN.

The following criteria will influence the chosen methods:

National and/or worldwide connections	Mobile phone services vary in different parts of the world. Fixed IP SIM cards may not be available and will probably incur higher charges.
One provider or provider independent	A single provider will reduce unit costs for multiple SIM cards. However they may not provide a service in some parts of the world.
Quantities	Connection management may prove an issue with multiple SIM card and IP addresses. A VPN will be easier to manage.
Data security	Exposed IP addresses can cause security issues. A Private IP address and a VPN are very secure
Costs	Fixed IP SIM cards are more expensive but easier to set-up. Who pays the on-going SIM contract?
Skills of integrating company	VPNs can be complex to configure. Fixed IP is simple.
Application	How much data and how often?

Of course there are applications in which GPRS is not the ideal choice for transmitting data. In cases where there is,

- a permanent transmission of huge amounts of data
- a need for a permanently available wide band
- protocols with critical timing

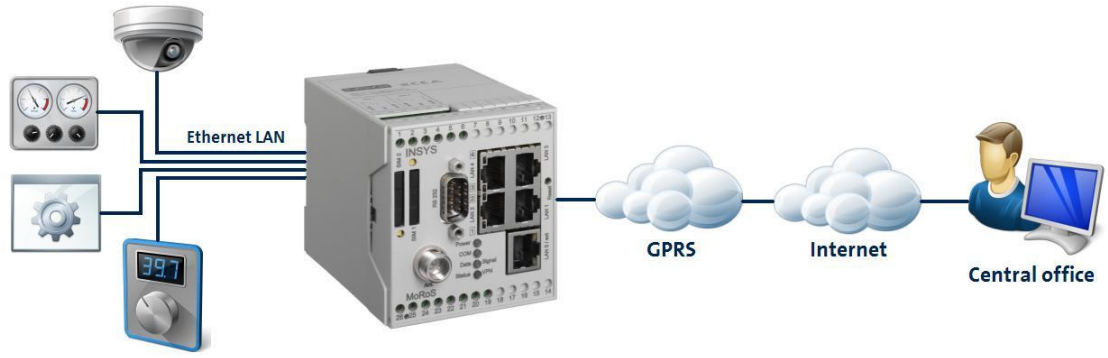
In summary the use of GPRS is of particular interest,

- Wherever there is a need for a dedicated line
- Where a landline would be too costly because of a remote location
- Where high costs for overseas connections are incurred
- Where a number of devices have to be read out in succession/simultaneously
- Where there is often a need for transmission of small data volumes.

UMTS/3G Modems

Just about all the concepts and requirements that have been discussed for GPRS apply to 3G. However the 3G network is much faster with data rates up to 384kBit/s (3,6Mbps for HSDPA and HSUPA if supported). These are rates which can match some broadband connections and bring mobile communications into the application areas of live CCTV and computer remote access.

These modems are ideal for linking Ethernet networks together making remote support of multiple PLC sites attractive.



Internet Technology

Many industrial sites will have some form of Internet connection. This could be a cost effective and easy way to achieve remote access to OEM plant and machines. We have already discussed using the internet with mobile phone (radio) modems and routers but this section looks at wired internet connections including **Asymmetric Digital Subscriber Line** (**ADSL**) broadband modems and Internet routers.

Each Internet connection is provided by an Internet Service Provider (ISP) and will have a reachable IP address at the router. This is the basic target for any remote connection.

Port forwarding is a routing technology that is easy to implement in most routers, so no extra hardware is required. A particular PORT address is routed to the IP address and PORT of a device on the site network behind the router. This effectively makes the device visible on the internet but can only be accessed by addressing the appropriate IP address and port.

Internet Technologies can offer very cost effective remote connections. If your connection can be integrated into an existing Internet router this may even be free!

As the remote device is effectively reachable from the internet this method is deemed insecure by many IT departments and some sites will simply ban this method. This would be an excellent method if the site had a dedicated Internet public IP address that could be used, for example a dedicated broadband connection.

Example Router Port Forwarding Configuration

active	delete	Protocol	Port	to IP address	to port
☑	☐	TCP	1024	192.168.100.15	80
☑	☐	TCP	44818	192.168.100.15	44818

In the above example any packets that are addressed to the routers reachable IP address but at specific ports 1024 or 44818 will be routed to the device at IP address 192.168.100.15 Port 80 and port 44818 respectively.

One of the most useful aspects is the roaming ability of Laptop computer connectivity to IP networks, allowing an engineer to get a connection from many locations using a Wi-Fi hotspot or USB 3G modem, often referred to as a dongle.

Virtual Private Networks (VPN) provide secure connections over the internet. A client/server relationship is established between the remote device and the control centre. If the client device (router) can reside inside the site network then it just uses an outgoing internet connection (no settings required in end user router) to contact the server device (router or PC) at the control centre. Once a VPN is established two-way traffic can travel between the server and the client encapsulated in a secure tunnel.

Many hardware solutions are available for VPN tunnels and some consideration needs to be given to the merits of each. Some are difficult to configure correctly and need a little more planning and effort to configure requiring the skills of an IT engineer.

It is possible to get an off-the-shelf VPN or remote device management solution where 3rd party service centres mange your VPN connections for you, including router set ups. This is a more costly option with less flexibility but will be beneficial where the user has little or no IT knowledge and chooses not to interfere with existing company networks.

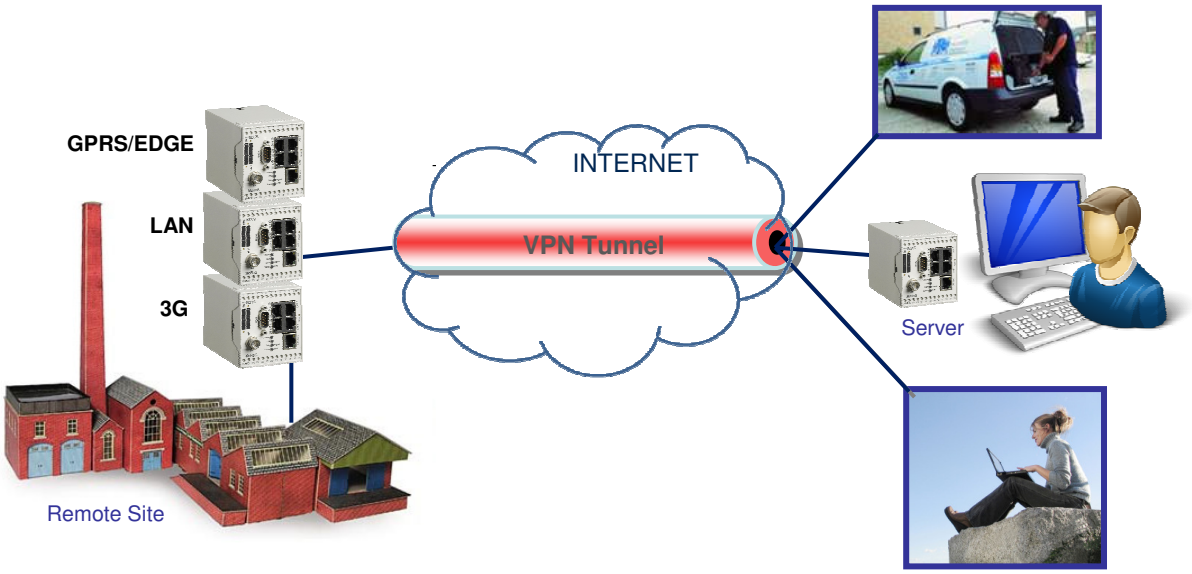
Working Case Study

Here we look at an example of remote access that allowed a machine-builder to connect to his machines world-wide to provide fault finding during commissioning. This meant he didn't have to send a control engineer to each installation but could use a smaller commissioning team on-site.

This machine-builder had the following criteria:

- Worldwide solution
- Common approach
- Self sufficient – minimal impact on customers IT department.
- Industrial devices mounted in Control Cabinets
- Multiple (max 4) Ethernet control devices at each machine.
- Engineer access from anywhere

These requirements fitted a VPN solution. Each machine was fitted with a combination modem, router and switch from a common family of devices. Choosing a wired internet (LAN) connection or a GPRS/3G modem connection if no existing internet was available. The VPN solution allowed the machine mounted client device to establish an always on connection back to the machine-builders offices where he had a matching server. Control engineers could connect to the VPN server as clients and access any other client machine. Even engineers on the move could connect back to the server as long as they had an internet connection.



The big benefits for this OEM machine-builder were:

- Savings and utilisation of the control engineers
- Performance and flexibility of the solution.

There was also an investment in the future as he could use the remote connection to offer further support services to his customer that created an on-going revenue stream.

On the negative side the VPN required an IT skill-set to configure and a fixed IP internet connection at the OEM offices.

Summary

For OEM machine-builders the choice of a remote access communication method varies depending on the application conditions. It is always worth talking to your communication provider(s) as early as possible about which is the best solution. Early consultation may allow other elements of the application to be changed in order to facilitate a better overall solution. For example choosing an Ethernet Programmable Logic Controller (PLC) instead of a serial version will allow easier integration to the Internet.

It's not so easy to find a company that offers a wide enough range of products to meet all the above options. It is more difficult to find a company that will work with you from initial concept through to post-sales support.

Insys Microelectronics offer a wide range of products for embedded use and also complete devices for control cabinets, 19" racks and desktop devices. Beyond this, INSYS offers a comprehensive project support to develop and construct customer-specific devices - we are a competent prototype partner.

It is our range of standard products for control cabinets that are particular interest to OEM Machine Builders seeking connectivity to their machines and control equipment. Insys have Industrial DIN-rail mounted PSTN modems, GSM/GPRS/3G modems and routers, some which incorporate Port forwarding, serial to Ethernet conversion and VPN capabilities to cover a wide range of needs.

INSYS MICROELECTRONICS UK
The Venture Centre, Sir William Lyons Road, Coventry. CV4 7EZ
Tel: +44 (0)2476 323237 • Fax: +44 (0)2476 323236
Email: sales@insys-datacommunication.co.uk
Web: www.insys-datacommunication.co.uk