MSI TEC

PRODUCTIVITY THROUGH TECHNOLOGY

MSI TEC offers a full line of motion control and industrial automation products and services,backed by an experienced team of automation engineers.

For assistance with your application, call us at 866-397-7388 or email info@msitec.com.

Learn more at www.msitec.com.

M2M Device Networking

Getting Started in Global Device Networking and Communications

Smart companies know that information is power. Companies that have a crystal clear picture of their operations, customers, and supply chain are able to make better decisions, operate with greater productivity and less waste, and offer enhanced services that inspire customer loyalty… often creating new profit centers.

Today, most businesses rely on networks for sharing information among employees and customers. Yet this is only a small piece of the information that can be shared. Machines and appliances – essentially any electronic or electro-mechanical device with a sensor, controller or microprocessor – contains a great deal of information about its status, performance and usage. The ability to extract raw data from a device, machine or appliance and convert that data into useful information transforms the decision-making from an art to a science. Moving light years beyond isolated HMI (human machine interface) and SCADA (supervisory control and data acquisition) systems that pass limited amounts of data, you can now leverage Internet, Wi-Fi and Celluar technologies to relay information anywhere, anytime. This unique combination of factors has converged into a powerful new paradigm known as M2M (machine-to-machine, machine-to-man and machine-to-mobile).

M2M constitutes the next notable phase of the information age, a phase which promises to be even more explosive than anything we have seen yet. Though still in the infant stages, M2M markets are projected to exceed 100 million connections and $700 billion in revenues by 2010 (see Figure 1 below).

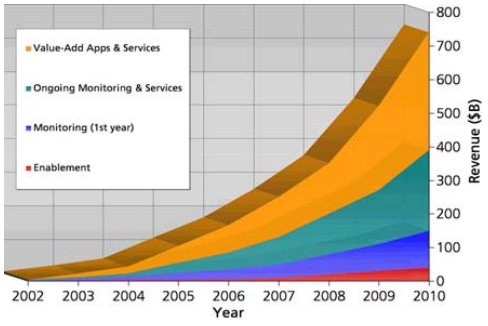

Figure 1: M2M markets are projected to exceed 100 million connections and $700 billion in revenues by 2010. Source — Harbor Research Group

Using simple plug-and-play modules, you can now connect devices directly into legacy systems and create peer-to-peer device networks. With M2M device networking, intelligent devices, however remote, are capable of relaying data and sending alerts, alarms, and commands to cell phones, PDAs, databases and other intelligent devices. Devices can also be “Web-enabled” and accessible using a standard Web browser. This article outlines how to implement push and pull data transfer strategies in an M2M environment with just a few basic components and factors to consider.

M2M Components

There are basically four components in an M2M system: 1) the intelligent device (machine or appliance) where the data originates, 2) the gateway that extracts and translates data, 3) the network which serves the data and 4) the remote client which ultimately receives the data. M2M software applications are optional but can facilitate communications, enable Web access and provide the user interface.

The Intelligent Device:

Where The Data Originates

Intelligent devices include PLCs, I/O modules, and sensors — essentially any device, machine or appliance containing a microprocessor. These devices are programmed to read, and sometimes react, to actions and conditions such as motion, voltage, pressure, flow, or temperature. Any device that has the capability to act or react to a command, communicate with other devices, control or be controlled, can broadcast data in an M2M application.

The Gateway:

Translates and Passes The Data To The Network

The gateway is responsible for extracting raw data from the intelligent device and preparing it for the network. Gateways are typically hardware but can also be a combination of hardware and software.

Gateways use a protocol such as Modbus or a proprietary device driver to interact with the intelligent device, and translate the data into a format that another device, software application or human can understand. The gateway can also act as, or interact with, a Web server to serve files to Web browsers, allowing multiple simultaneous connections to Web pages. Gateways may also have other enhanced functionality such as the ability to convert media types (e.g., serial to Ethernet). For example, a gateway such as Advantech's WebLink can communicate with intelligent devices via serial, Ethernet, and/or USB connections. With a PCMCIA cellular modem acting as the network connection, the WebLink can also collect and send data via cellular service.

The Network:

The Connectivity That Serves Data To The Remote Client

In an M2M application, the network is like any other network: it is the connection that allows data to pass from one place to another. The four most popular network connectivity choices in an M2M system are:

Wired Ethernet
Wireless (802.11x, Bluetooth, 802.15...)
Cellular
POTS (Plain Ol' Telephone Service)

Wired Ethernet is often used when the intelligent device is part of an existing LAN or can be connected to an existing LAN. The device can then be accessed by another device, software application, or human at the same location, or via the Internet using the existing Internet connection on the LAN. Wired Ethernet is completely secure as long as any Internet connections on the LAN are carefully protected by a firewall. A local area network also has, by far, the highest data transfer rates.

Wireless is a good choice when wires are not feasible and devices are within short range of each other. Wireless technology is cost-effective, secure, and stable, but very limited by distance. With a wireless network, you can create an always-on connection between the intelligent device and an existing LAN or other wireless-

Advantech offers a full line of embedded computing and I/O units for remote monitoring and control applications.

Advantech's WebLink 2059 (shown above) is a fully functional, application-ready embedded computer. The 2059 is ideal for acting as the M2M Gateway.

The WiSer Serial to 802.11b Gateway by OTC Wireless is a cost-effective method to retrofit legacy devices and attach them to your LAN or other wireless devices.

Nokia and Sierra Wireless are two major players in the forefront of wireless and cellular hardware.

enabled device, with the data transfer rate much higher than a cellular or wired modem. Security is more of an issue than with wired connections. Rather than a standard firewall, wireless devices require different security measures, for example encryption or IPSec. Currently, the two most popular wireless technologies are Wi-Fi (802.11x) and Bluetooth. Zigbee (802.15) is a new wireless protocol designed specifically for direct machine-to-machine communications.

Cellular data modules and cards are becoming increasingly popular for M2M networks. Cellular data transfer overcomes most limitations of distance and location. Cellular tends to be more expensive than other connection types and is not the best choice for applications that require high bandwidth and real-time, always-on access to the device. In many situations, however, cellular is the only feasible choice. Additional security measures such as client-initiated VPNs (virtual private networks) are often used with cellular Internet connections to ensure the integrity of the device.

POTS remains popular because of its low cost and security. POTS can be used for both direct dial connections and Internet connections. POTS is a good choice for applications that do not require heavy data transfer as it continues to be a slower method of delivery. DSL (Digital Subscriber Line) running over POTS is quite a bit faster and can be configured for an always-on, firewall-secured connection at a relatively low price.

Other network possibilities include Satellite Internet Service, GPS Technologies, dedicated long-range RF, Infrared and more. These are seldom used due to a combination of factors including price, distance or stability.

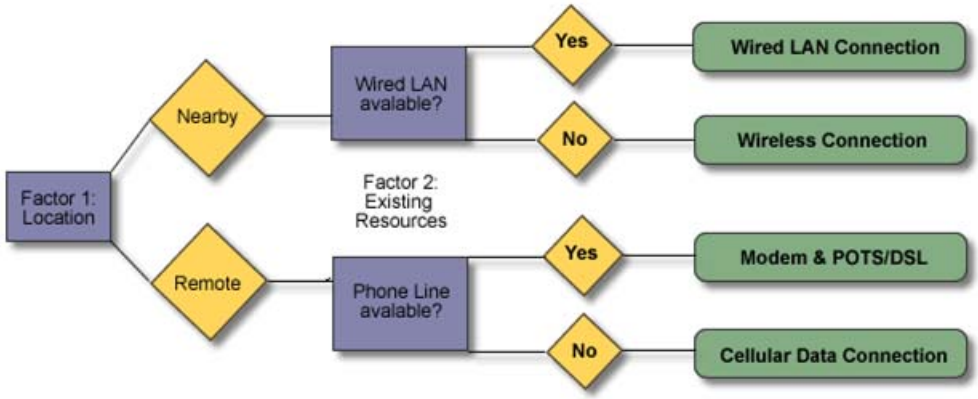

Figure 2: Choosing the right network is based on location and availability of existing resources.

It may seem confusing when choosing a network type but it is usually quite simple. The network of choice is, in most cases, dictated by two factors: location and existing resources including the availability of phone or data lines. Figure 2 above shows the decision process based on these factors.

The Remote Client:
The Destination Of The Information

For purposes of this article, the “remote client” is defined as hardware or software that receives the data. Clients can be cell phones, database software applications, Web browsers (e.g., Internet Explorer™ or Netscape™), email clients (e.g., MS Outlook™ and smart messaging (SMS) devices (e.g., the BlackBerry™), among others.

M2M Software Applications:
Communications, Web Access and User Interface

Third party applications or custom software programs are used to facilitate machine-to-machine communications, provide an operator interface, and provide Web browser access and Internet presence. One such program is Advantech Studio (A-Studio) provides all of the necessary tools to communicate with the device, Web-enable the application, and deliver data securely to all levels of the enterprise. A-Studio provides a user friendly "drag and drop" programming environment. Microsoft's .NET platform also provides the tools necessary to program a custom M2M application for both embedded and non-embedded platforms.

A-Studio from Advantech is a fully customizable M2M programming suite featuring user interface and communication tools. It offers built-in device drivers and Web accessibility.

Design Strategies

When considering M2M implementation, there are basically two infrastructure design strategies: the push strategy or the pull strategy. Push implies that the intelligent device initiates communications, sending data through a stand-alone gateway over the network to a remote client. Pull implies that a central database servers polls the intelligent device, pulling in data through the network. The two strategies can also be combined as a "hybrid" to fit the exact needs of the application.

Push Strategy

Using the push strategy (Figure 3), the intelligent device is configured to recognize pre-defined conditions and trigger the device to send alarms, alerts, emails, data and commands. For example, if the temperature in a room rises above a predetermined point, the intelligent device sends a command via the gateway to a PLC or I/O unit to enable power to a cooling device, and forwards an email to a technician's cell phone.

Push systems tend to be a more difficult to monitor – you may not know if the device has failed to establish communications when it needs to — the more remote the device, the harder it is to confirm. Push is less expensive, however, because it does not require an always-on connection. The gateway simply connects over the network on an as-needed basis to send data to the remote client. The initial investment is also usually less expensive since the gateway acts as a stand-alone solution and no data servers or additional equipment is necessary.

Pull Strategy

The pull strategy assumes that a server exists on the network and is tasked with polling the intelligent device(s) for data on a periodic basis (Figure 4). The server can then broadcast the data (using XML, ODBC or other database connectivity) throughout the enterprise, sending alerts, alarms, messages, or commands to other devices. For example, a central server can monitor several remote cell phone towers via the Internet using Modbus over TCP/IP. Let's say the beacon light on one of the towers fails. The application running on the server recognizes the failure which triggers a local alarm, sends an email alert over the Internet to the FCC, and forwards a cell phone message to a technician. At that point, the technician can browse to a Web page through a Web-enabled cell phone in order to acknowledge the alarm and enter an estimated time for the repair. All of this information can be made available to an enterprise software application or authorized company staff.

Figure 4—Example of the "**Pull Strategy**". A server pulls data from the remote intelligent devices. The data is stored in a database from which it can be broadcast and made accessable via a variety of network protocols.

The pull method is generally more reliable because it enables you to "monitor the monitor", checking the server to make sure it is consistently establishing communications with the intelligent device. The pull method is more costly because it requires a server and an always-on, LAN, dial-up, or Internet connection to ensure continuous error reporting.

Push / Pull Strategy

A combined push/pull method is recommended when you need to be able to access the intelligent device at any time and rely on the intelligent device to take action when an event is triggered. If the remote gateway is connected to the Internet, and acting as a Web server, the push/pull method introduces many other issues outside of network connectivity: it requires a static IP address for each intelligent device which demands greater security precautions such as individual firewalls.

No matter what the application, gateway, or strategy, the key is that information is delivered in a more efficient fashion where it is needed, when it is needed. M2M is helping make business smarter in the way they access and utilize information. Companies are now able to see, listen, and collectively provide intelligent action remotely across the enterprise, all as a result of M2M technologies. M2M enables corporations to protect assets, reduce downtime, optimize resources, and deliver data throughout the enterprise. It also allows OEMs to provide online service to their customers.