EE Times Connecting the Global Electronics Community

designlines INDUSTRIAL CONTROL

Design How-To

Replacing RS-232 with 802.11n wireless

N. Venkatesh, Redpine Signals

6/10/2009 05:00 PM EDT

The Wired Setup

The monitoring and control of medical equipment and devices are often carried out from a separate controller or server. The server may be in the vicinity of the equipment or may be at a remote location. Traditionally, a common means of connecting the two is via an RS-232 serial interface. Consider a set of sensors controlled by a sensor unit as shown in Figure 1. The accumulated data is transferred to a monitor via a serial interface.

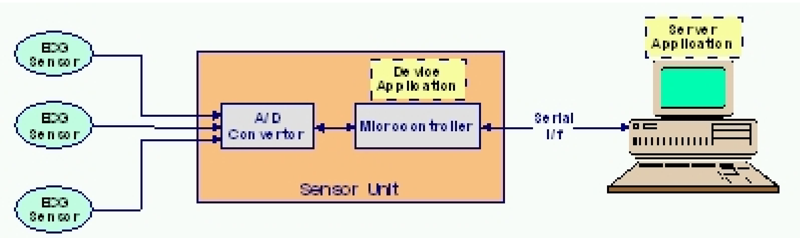

Figure 1: Sensor Unit and Interface to Monitor

(Click on image to enlarge)

The multichannel A/D converter is typically within the microcontroller unit. The periodically sampled data is encapsulated in a predetermined packet format and sent on to the Monitor via the UART interface of the microcontroller.

The applications running on the microcontroller and the monitor (or server) ensure the means to transfer the sensor data meaningfully. The device application encapsulates the data using a protocol negotiated with the receiver of the data (the server in this case). The obtained data would be de-capsulated on the corresponding peer before passing it to the application. Figure 2 illustrates this process.

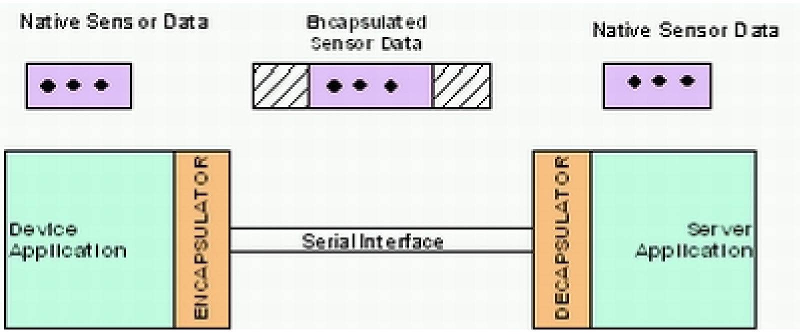

Figure 2: Wired Connection

(Click on image to enlarge)

There are many methods of encapsulation - one example for encapsulation of IP data is SLIP (Serial Line Internet Protocol). SLIP is a packet framing protocol that defines a sequence of characters that frame IP packets on a serial line. It provides no physical addressing or error control, for which it depends on upper-layer protocols. SLIP simply sends the data and then sends a signal marking the end of the data.

The Basic Wireless Setup

The wired connection in Figure 1 can be replaced by a wireless one based on 802.11 WLAN by connecting the device and the server with a serial to Wi-Fi bridge. The serial to Wi-Fi bridge provides a means of transporting the device data either employing layer-3 protocols or directly bridging it to the corresponding Wi-Fi bridge at the server.

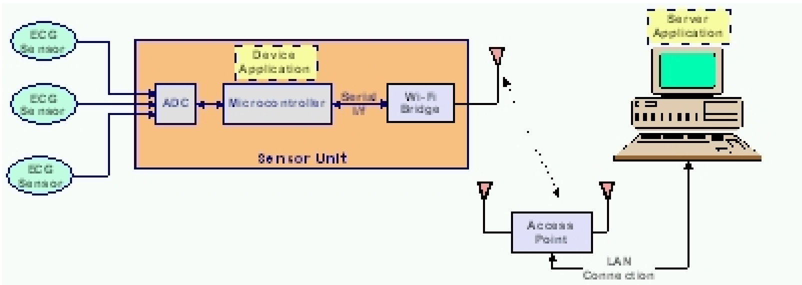

Figure 3: Wireless Connectivity in the Infrastructure Mode

(Click on image to enlarge)

There are many advantages to using 802.11 Wi-Fi connectivity in medical devices. Firstly, Wi-Fi is close to being ubiquitous, especially in medical establishments, and therefore no special provisions need be done at the infrastructure end. Secondly, the use of standard TCP/IP transport, as opposed to proprietary protocols, enables the monitors or servers to be present practically anywhere " within the premises on the LAN, or at any remote location via the internet. Thirdly, in comparison to alternatives like Zigbee or Bluetooth, WLAN provides longer range, higher throughput, and with the right implementation, better energy efficiency through the use of higher data rates translating to longer battery life.

The Wireless Transport Mechanism using TCP/IP

The serial to WiFi bridge frames an IP packet from the data obtained through the device and transmit to any other node in the network as shown in the figure 4.

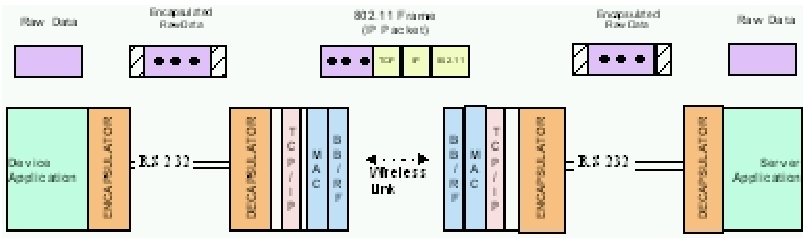

Figure 4: Wireless Connection through a Wi-Fi Bridge

(Click on image to enlarge)

The serial to Wi-Fi bridge incorporates a built-in TCP/IP stack, thereby abstracting the application devices of the nature of network with which the data transmission/reception is done.

Transmission involves the following steps:

1. The device encapsulates the data as mentioned in the above section.
2. The serial to Wi-Fi bridge attached to the device decapsulates the obtained data.
3. The decapsulated data is passed through the TCP/IP stack in the serial to WiFi bridge forming an IP packet.
4. The IP packet, fragmented if necessary, is framed in WLAN MAC format and transmitted through the WLAN air interface.

The following are the actions performed by the serial to Wi-Fi bridge on the server side for reception of the packet.

1. The WLAN interface receives and reassembles the IP packet.
2. The received IP packet is passed through the TCP/IP stack, with its integrity verified.
3. The payload in the IP packet is extracted.
4. The application on the serial to Wi-Fi bridge encapsulates the data obtained before sending the data through the serial interface of the server.
5. The server decapsulates the data obtained from the bridge.

Wireless Peer to Peer Transport

The serial to Wi-Fi bridge transfers a proprietary packet by using a delimiter to identify the encapsulated data obtained from the device. Figure 5 and 6 depict such transfers. This mode is potentially a proprietary one and the wireless connection used is mainly in an IBSS or ad-hoc mode.

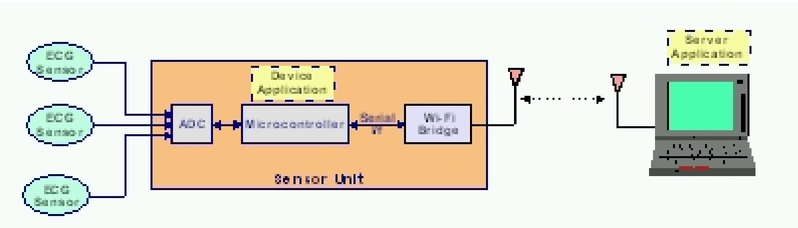

Figure 5: Wireless Connectivity through the Ad-hoc Mode

(Click on image to enlarge)

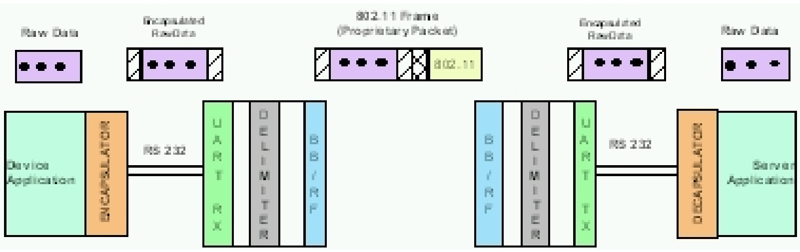

Figure 6: Wireless Transport without TCP/IP

(Click on image to enlarge)

In this scheme, the following are the actions performed for the transmission:

1. The device encapsulates the data as mentioned in the section 1.
2. The serial to WiFi bridge receives the data from the device and adds the delimiter. This delimiter provides a way for the peer (bridge) to identify the encapsulated data.
3. The data along with the delimiter is transmitted through the RF.

The following are the actions performed by the serial to WiFi bridge on the server side for the reception of the packet.

1. The WLAN interface receives and assembles the packet.
2. The received packet is processed to obtain the encapsulated data. The delimiter is used to identify the start of a data frame.
3. The extracted data is sent through the serial interface of the server.
4. The server decapsulates the data obtained from the bridge.

802.11n Benefits

Current serial to Wi-Fi solutions are largely based on 802.11b or 802.11g. Future enterprise networks are, however, likely to be predominantly 802.11n based, and recent serial to Wi-Fi products like Redpine's RS9110-N-11-22 are started catering to the 802.11n needs of the market. The IEEE 802.11n standard primarily provides for high throughput, high-efficiency, and long range data connectivity, and includes the use of multiple antennas and transmit-receive chains. However, the standard also includes a single-stream mode that is intended to provide the benefits of 11n to low-power small form-factor devices including sensor nodes. The use of single-stream 802.11n WLAN in these client devices provides the following benefits:

- Higher throughput and lower transmit times " achieved through better efficiency in PHY and MAC.
- Longer range " through use of multiple antennas at the access point
- Preservation of 802.11n network capacity " the presence of legacy 802.11a/b/g clients forces the 11n nodes to use protection mechanisms and results in overall drop in network capacity. 802.11n helps avoid this.

Summary
802.11 WLAN, or Wi-Fi, is an ideal wireless transport mechanism for medical applications that currently employ the RS-232 serial interface for connectivity between sensors, devices, instruments, and monitoring equipment. Wi-Fi is ubiquitous as well as flexible " enabling a variety of connection methods including peer-to-peer and infrastructure modes spanning both the local network as well as the wide area network. In particular, the 802.11n WLAN standard would provide the benefits of range, throughput performance, and interoperability; and would remain an ideal solution for these applications through future network upgrades.

About the author
N.Venkatesh has more than 23 years of experience in communications engineering with expertise in wireless systems design, chip design, telecommunications and optical networking. He is responsible for leading the development of wireless systems at Redpine's development center. He can be reached at n.venkatesh@redpinesignals.com