



Technical Brief AN241 Rev A1

Long Range RF for Large SCADA Systems

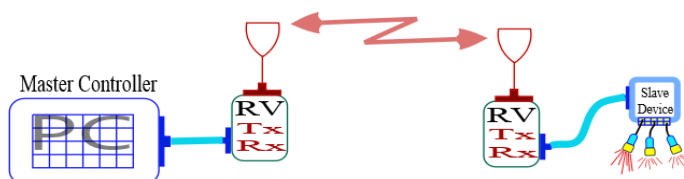
By John Sonnenberg

Raveon Technologies Corp

Summary

SCADA stands for Supervisory Control and Data Acquisition. The Data Radios from Raveon Technologies make ideal wireless modems for SCADA gateways and Remote Terminal Units (RTUs) in SCADA and telemetry systems.

Wireless Connection to SCADA Slaves (Long Range. Many miles)



The Tech Series versions have GPIO and FIO options to enable these *Tech Series* products to be complete SCADA RTUs, with many different input and output pins and features.

This Application Brief describes the general requirements for a wireless SCADA system to communicate with thousands or millions of remote devices.

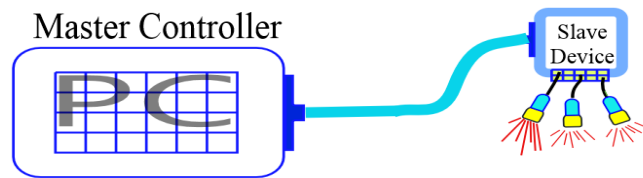
Many telemetry and SCADA systems run on private networks or connect things to the Internet. Raveon's wireless modems are excellent devices to connect your things to *Private Networks* or the *Internet*.



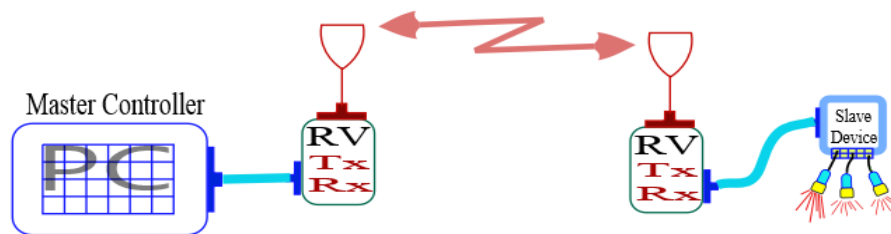
Wireless SCADA

A device or sensor is monitored by a Master Controller. The user may have something as simple as an LED indicator, or as complex as a computer server for the operator. Often this remote device is a Remote Terminal Unit (RTU) or Programmable Logic Controller (PLC). Each RTU has a device ID to identify which RTU to communicate with.

Typical SCADA System



When the distance between the Master Controller and the Slave being monitored is not trivial, a wireless link between the two sites becomes a logical means of connecting them. The RTU monitors the digital and analog parameters in the field, and when the Master queries the Slave, the Slave transmits data to the Master using a SCADA protocol.



Slave Addresses

A master device addresses a specific slave device by placing the 8-bit slave address in the address field of the message. The address field of the message frame contains two characters (in ASCII mode), or 8 binary bits. Valid MODBUS addresses are from 1-247.

On a wired MODBUS SCADA system, a Master can work with 1-247 Slaves. If you use a smart gateway like the Raveon CIGORN Gateway or just use N numbers of wireless Base Stations, you can communicate with up to $N \times 247$ slaves, which can be:

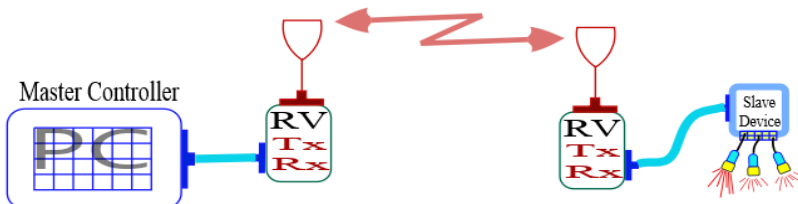
3 X 247 (741), 10 X 247 (2470), 32 X 247 (7904), 1000 X 247 (247,000).

Raveon's data radio modems have 16-bit ID codes so Radios Modems can have 2^{16} (65535) unique IDs for each radio.

Going Wireless

Telemetry Gateway

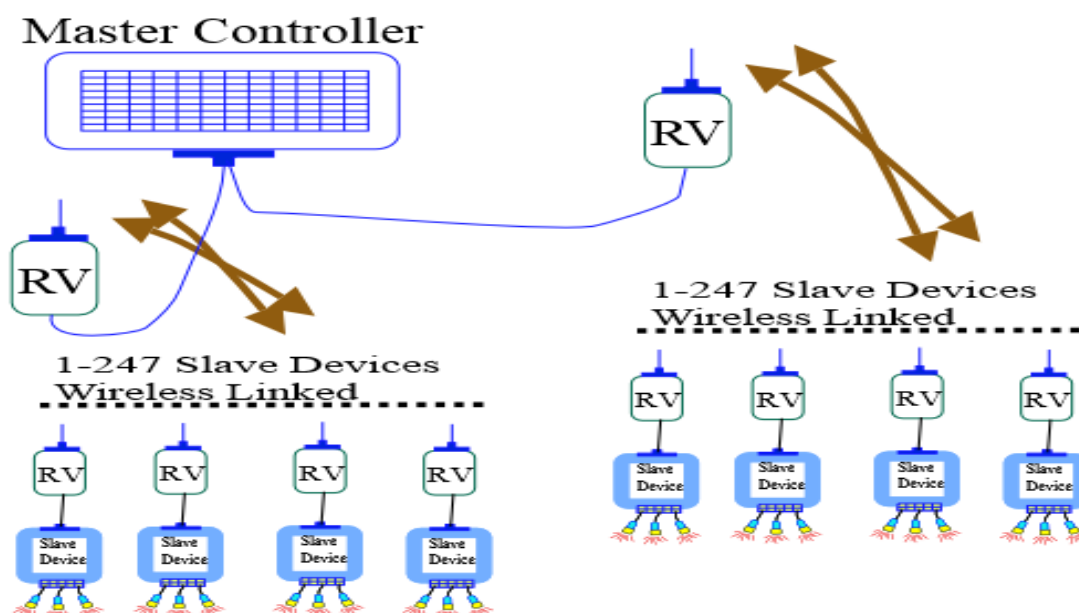
Wireless modems are the gateway to the wireless telemetry system. When a system uses MODBUS or any other ASCII, RTU, or serial protocol, a Data Radio Modem is the telemetry gateway to dozens or hundreds of remote devices communicating over the radio channel.



In remote areas, outdoors, the Slave device is inside of a waterproof enclosure, and the Radio Modem can be included within the enclosure also. Place the radio's antenna outside the enclosure.

Use Multiple Raveon Base Stations

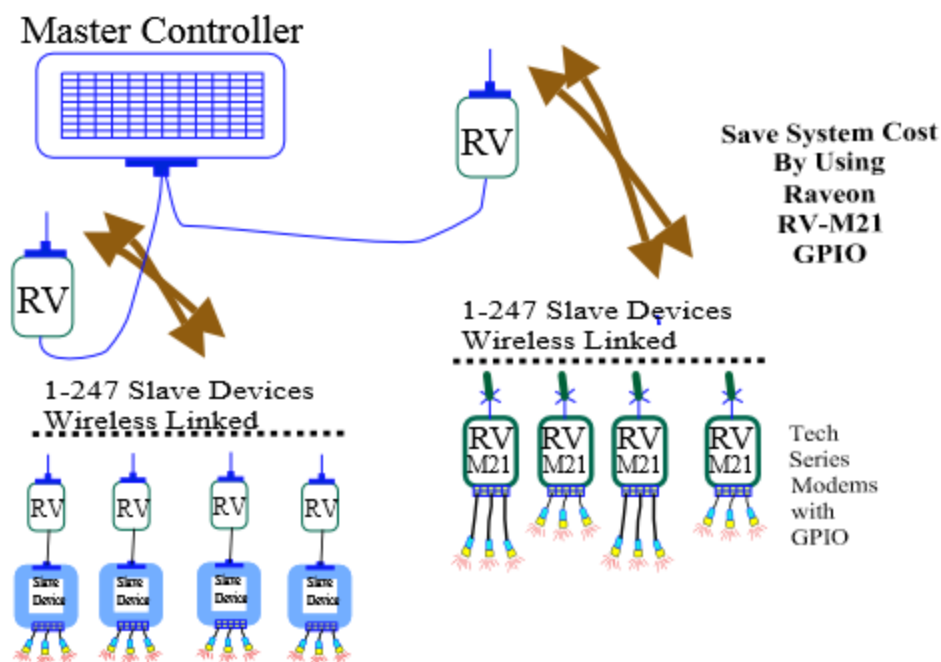
If a Master Controller is connected to multiple Radio Modems acting as Base Stations talking to Slave Devices over radio frequencies, then many more Slaves can be accessed. 2 base modems can communicate with 494 Slaves. 20 base modems can communicate with 4940 Slaves. The Raveon data radio modems shown here (RV) can be used as the base stations and as the modems for the SCADA devices. Different groups with different radio base station RVs can have unique GROUP IDs, so groups don't interfere or cross-communicate.



If millions of Slaves need to be accessed with Modbus, Modbus can access millions of devices over radio waves, and Raveon's Cigorn Gateway can route the Modbus messages to the correct base station for millions of devices.

Use Thousands Per system, and Save Cost

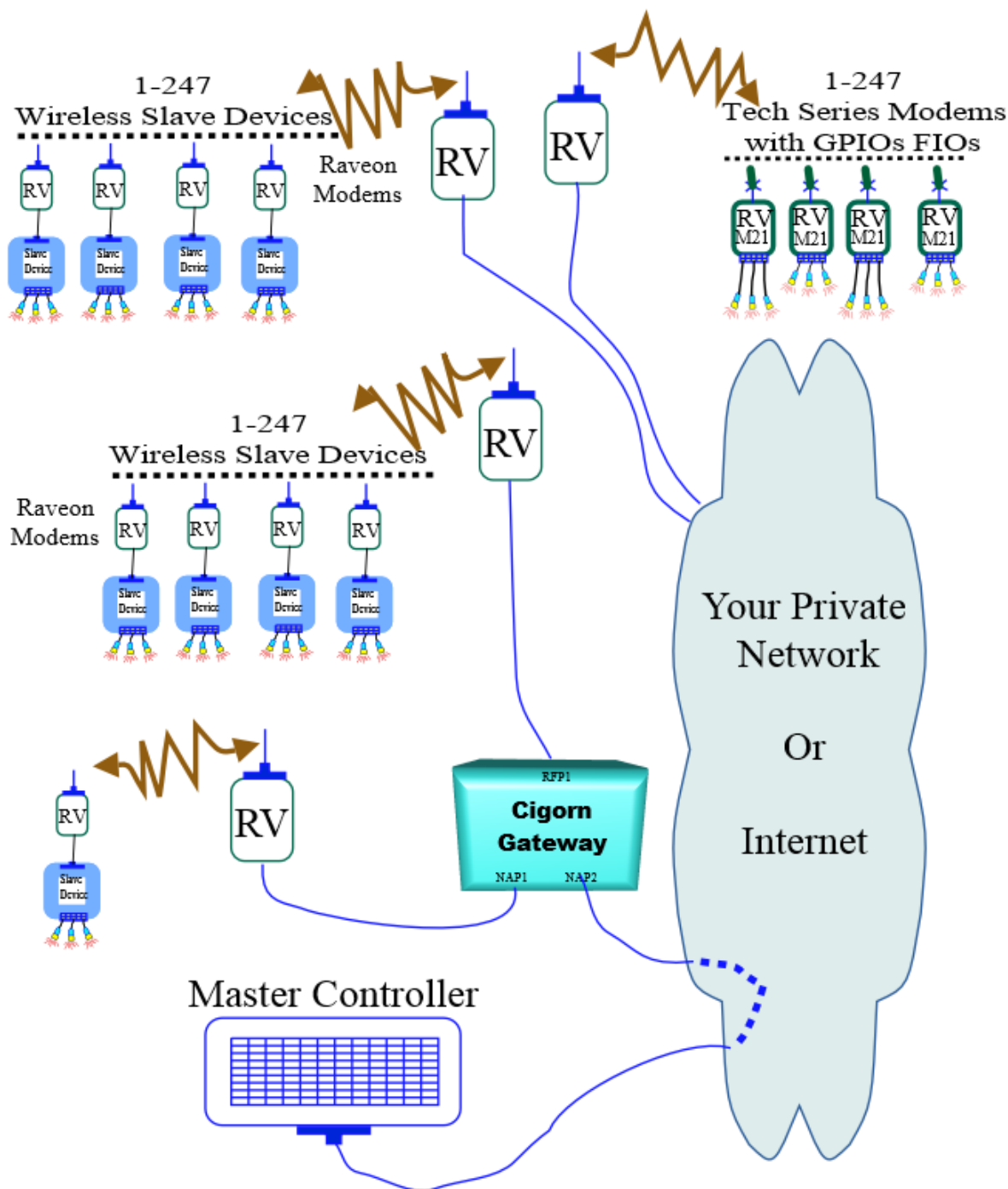
Reduce your system cost by eliminating many Slave Devices. Raveon's Tech Series GPIO option can work long-range wirelessly and act as an RTU Slave to read sensors and switches, and control devices that are switched with digital, DC, or open drains.



Most MODBUS slave devices can only report when queried. All Raveon SCADA slaves can respond to MODBUS inquiries and can have their registers and IOs managed by the Master Controller. The RV-M21 and RV-M22 radio modems have General Purpose IO (GPIO) SCADA IO pins built into the modems and the Flexible Digital IO (FIO) option has 8 TTL IO pins with SCADA features for digital inputs or outputs.

Cigorn Gateway for Network Routing and Connecting to Millions.

Raveon's Ethernet gateway router called CIGORN can route your messages to and from the devices and the base stations you want to use. It can communicate with dozens of base stations, and each of the base stations can talk to 247 different SLAVE devices or Tech Series SCADA products.



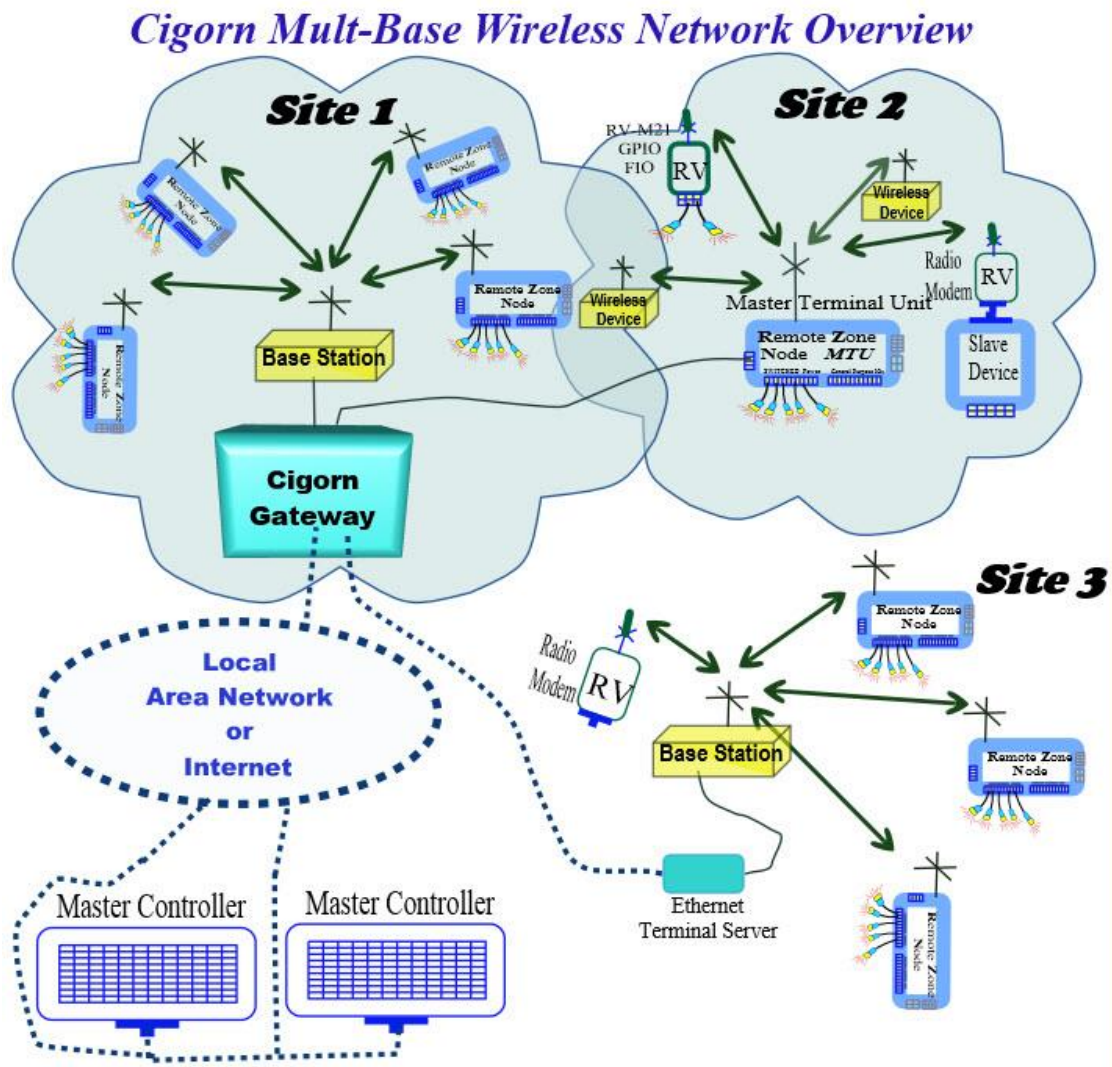
The Raveon data radio modems shown above (RV) can be used as the base stations and as the modems for the SCADA devices. The Cigorn can be configured to route as you want, so dozens of base stations can be used, talking to even millions of radio modems or slave devices.

Even MODBUS devices with the same MODBUS ID can be on different radio local systems talking to a local base station, and the radios in the local area only receive the messages sent to their group. Other nearby groups won't get the other group's messages

because each RV base station group can be setup with unique group IDs and the Cigorn will route messages to the specific group the way you want.

Cigorn Router Communicates with Many Base Stations

In your system, each base station can talk to hundreds of radios, and each radio can talk to 1-10 SCADA devices with RS-485.



Cigorn can be configured to work the way you need your network to work. So your Master Controller software will work perfectly with the system without having to modify the Master Controller code.

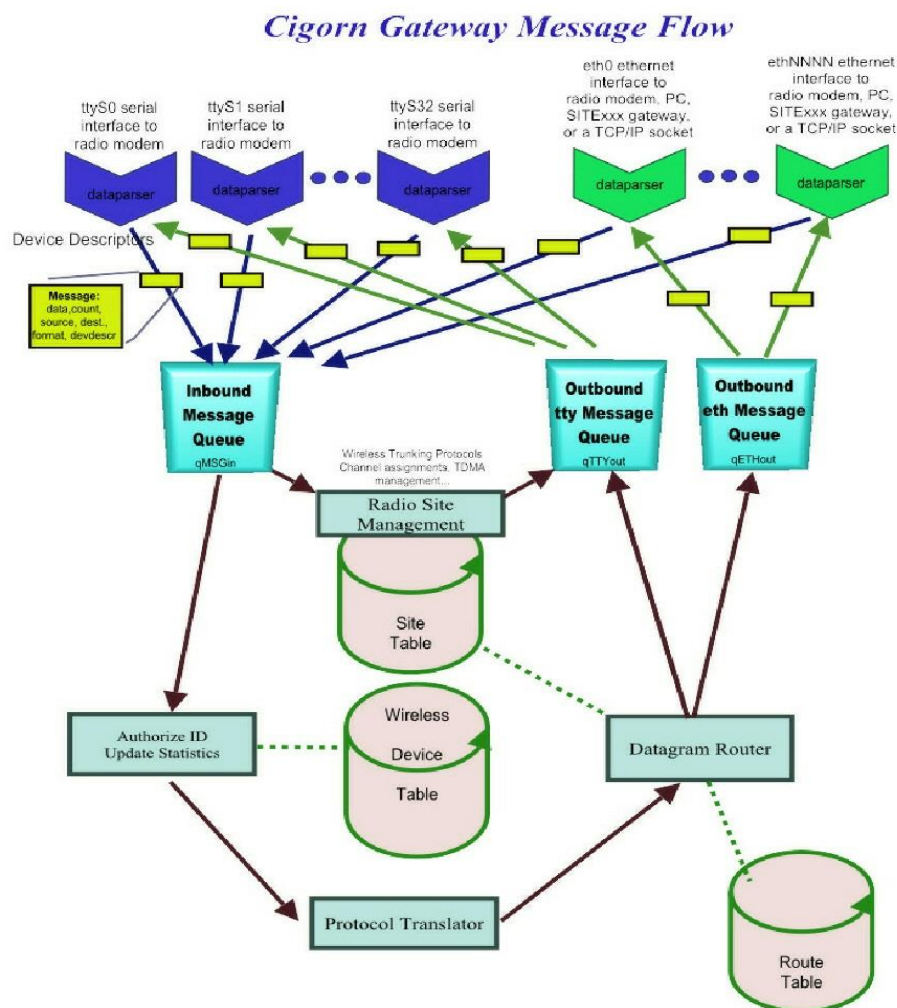
Message Routing

A primary function of the Cigorn gateway software is to route messages to/from the proper wireless device. Messages may originate from a number of different sources:

- Another wireless device on the system
- From a device connected to the Cigorn system, such as a transducer or another computer
- From the Cigorn gateway itself

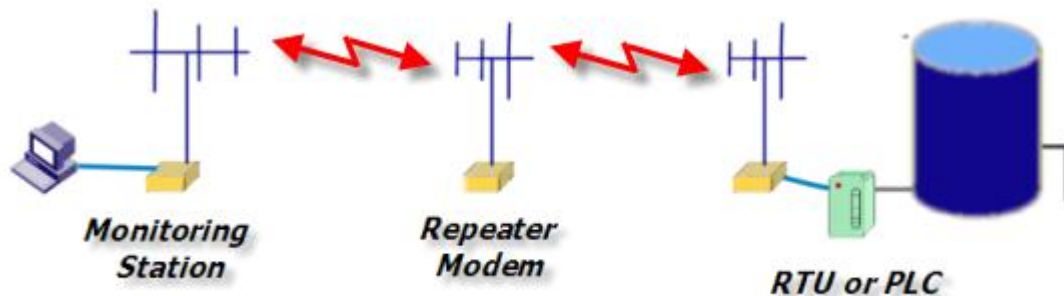
Routes can be as simple as:

- Route all data from TCP/IP port 1000 to TCP/IP port 1001.
- Route all data from RS-232 serial port 1 to RS-232 serial port 2.
- Route all GPS position data from an RV-M7 radio on serial port 1 to 50 IP addresses on 50 remote computers.



Repeating For Extended Range

For ultra-long communication ranges, high RF noise environments or obstructed line of sight applications it may be necessary to use a repeater to establish a reliable communications link.



Incorporated in all Raveon Data Radio Modems, where allowed by regulation, is a **store-and-forward repeater** function. The repeater function works in the Packet Mode. A repeater can extend the range of a system by 2-20X, depending upon how high-up above the average terrain the repeater is mounted. Repeater systems are often 100 to 500 square miles per repeater.

The following table shows a typical repeater system configuration in packetized mode.

AT Command	Monitoring Modem	Repeater Modem	Remote Modem	Notes
ATMY	1000	2000	0001-0999	Individual unit address for this particular modem. Each remote modem should get a unique ID.
ATDT	0001	N/A	1000	Destination address to send data to.
ATMK	F000	0000	F000	Address mask. F000 means that to receive, the first digit of the MYID must match the first digit of the TOID.
ATXR	0	1	0	Enable/Disable repeater function. Only enable it on the particular radio that will be the repeater.
ATX1	N/A	1000 0000 1000 0000	N/A	In the repeater, set the addresses this unit will store-and-repeat to/from. By setting the repeater address mask to 0000, this repeater will repeat any and all data packets.




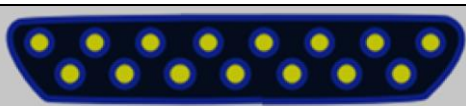
Tech Series Serial Communications

Refer to application note **AN236 (SerialComm)** for more detailed information on serial communication for telemetry. Raveon's Tech Series radio modems come with a myriad of IO options such as RS232, 485, 422, USB, and GPIO. Serial protocols have various advantages.

Serial Protocol Comparison Chart

	RS-232	RS-422	RS-485	USB
Cable	Single ended	Single ended multi-drop	Multi-drop	Single ended
Number of Devices	1 transmitter 1 receiver	1 transmitter 10 receivers	32 transmitters 32 receivers	1
Communication Mode	Full duplex	Full duplex, Half duplex	Full duplex, Half duplex	Full duplex
Maximum Distance	50 feet at 19.2 kbps	4000 feet at 100 kbps	4000 feet at 100 kbps	20 feet
Max Data Rate (50 feet)	1 mbps	10 mbps	10 mbps	100mbps

The Tech Series radio enclosure from Raveon is the most flexible radio platform in the industry. Options include 6 I/O options, multiple RF band options, GPS option, wide/narrow channels, Arduino option, MODBUS option, and wide DC input voltage range.

I/O Connector Type	Connector Code	IO Function
	S	RS232
	U	USB
	G, T, F	GPIO RS422 RS485
	A, D	Analog, FIO

For SCADA systems, a typical configuration is to have the radio modem connected to the HID/computer via an RS-232 serial port. The RTUs in the field usually use RS-485, so the radio modems connected to the RTUs should have the RS-485 option installed. A system may mix RS232 and RS485 modems with no adverse consequences.

Buffer Status

Tech Series radios have a command ATJF that will allow the user to set the CTS threshold. By default, this is set to 80% of the buffer's size. When the internal data buffer of the M21 reaches this threshold, the CTS hardware handshake line is negated.

The user may change this threshold. If you want the modem's CTS line to indicate when the buffer is empty (all data has been transmitted), then set the **ATJF** parameter to 1 (**ATJF 1**). This will have the effect of negating CTS whenever there is any data in the M21's data buffer. When all data has been transmitted over-the-air, the CTS line will be asserted again. It is a handy way to receive a hardware indication that a transmission has gone out, and the radio is ready for more data.

Regardless of the ATJF setting, the radio modem's data buffer can hold thousands of bytes of data, queuing them up to be sent over the air. The ATJF command only affects the threshold where CTS is asserted, not the size of the internal data buffer.

For additional information, contact:

Raveon Technologies Corporation

2320 Cousteau Court

Vista, CA 92081 - USA

Phone: 1-760-444-5995

Fax: 1-760-444-5997

Email: sales@raveon.com