Tech Talk
With Bob Dolph

RS-485: Old Soldiers Never Die

RS-422 and RS-485 are *recommended standards* (that is what the RS stands for) for system serial communications that have weathered the test of time. Would you believe that the RS-485 standard has been around since the early 1980s?

When you install an alarm system keypad, CCTV pan/tilt/zoom control or card access reader, there is a very good chance you are working with RS-485-type device drivers. Getting to know a little more about this standard will help a technician better understand how these systems communicate and keep running smoothly.

Standard Handles Up to 32 Devices on a Network

The RS-485 standard, also known as the TIA/EIA-485-A, is referred to as a "differential voltage" serial signaling circuit. It is a multidrop system that typically allows up to 32 devices to be connected into a network circuit.

Another standard, RS-422, is similar to the RS-485, but can only be used in a direct point-to-point communication. RS-422 devices cannot operate in RS-485 tri-state mode and therefore are not capable of multi-drop network operation.

There are two main versions of this circuit. Half-duplex consists of two twisted wires and full-duplex are two twisted pairs. In the half-duplex circuit, one device can only talk to other devices one at a time. In the full duplex mode, devices can send and receive at the same time, however a master/slave relationship must be configured for each pair.

For further investigation into these configurations, I suggest that you check out RS-485 reference Web sites such as www.rs485.com.

Transmitting Up to 10,000 Feet Is Possible

RS-485 communication circuits consist of a voltage level on each of two wires (-7V to +12V). Both wires reference their voltages to a single signal ground wire. At any given time, a differential voltage is established and is constant between the two twisted conductors A and B. Some vendors will reference wires A and B as - and + accordingly. When A voltage < B voltage, then the signal digit is a binary 1. When A voltage > B voltage, the signal digit is binary 0 (*see diagram below*).

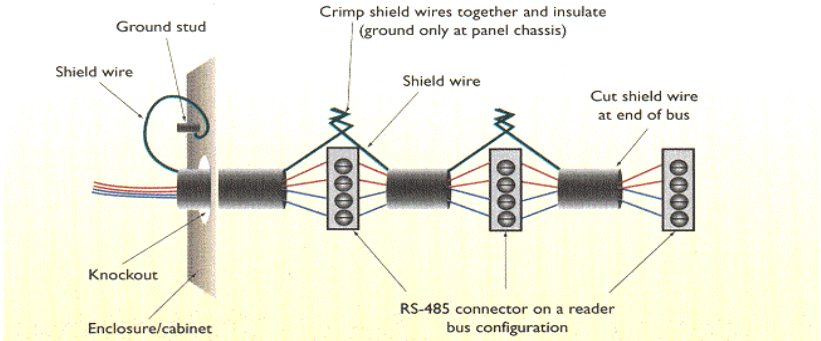
Properly terminated RS-485 networks can reliably transmit data over very long distances. The standard allows for distances up to 4,000 feet, however, many have reliably communicated up to 10,000 feet at lower baud rates. If cable runs are very long and go between buildings, it is highly recommended to use shielded cable for additional lightning suppression. Cables should also have a low capacitance for reliable data transfer, again, especially at high data rates.

The application range can vary widely with this technology, as many have bragged about sending data for considerable distances over standard twisted phone cable. If the twisted cable is in conduit, you may not need shielding. As always, check with your equipment and cable vendors when selecting material for large RS-485 network installations.

Daisy-Chaining Is the Optimal Configuration

Transmission speeds for an RS-485 network are specified at up to 10 Mbps. Typically, transmission rates are in the 1,200 Kbps to 9,600 Kbps range, which are considered slow by today's Ethernet standards. The trade-off for this slower

Grounding of an RS-485 Circuit



Signal ground wiring should be continuous and isolated from network devices, with final termination at the control panel.

Bob Dolph has served in various technical management and advisory positions in the security industry for 25 years. Bob currently is a training and products consultant for the security industry. He lives in Orlando, Fla.

BOB'S TIPS

- Remember to include the signal ground wire when ordering cable for an RS-485 circuit.
- Connect signal ground wire to chassis earth grounded only at the control panel end.
- Shielded cable is often nto need but is preferred for extra reliability.
- Connect multiple devices in a dasiy-chain network topology.
- For troubleshooting, install isolation switches for hard-to-access equipment.

speed is higher reliability of data transfer at long distances. One cable manufacturer specifies RS-485 network cable distances of up to 10,000 feet at 1,200 Kbps and 4,000 feet at 9,600 Kbps. Since data packets are typically small, this mode of transmission is still often acceptable.

The best network topology for RS-485 networks it daisy-chaining. Avoid configurations such as star, ring and long stubs as you can run into reflection problems. Termination resistors are typically not needed at distances less than 4,000 feet and speeds lower than 19.2 Kbps.

If termination resistors are needed, they must be placed at each end of the network and be equal to the impedance of the network, which is typically 100 ohms to 120 ohms. National Semiconductor (www.national.com) has a good paper on termination configurations for RS-485 networks.

Grounding Should Be at the Control Panel End

Electromagnetic interference (EMI) and radio frequency interference (RFI) reception transmitted to or from an RS-485 signal circuit is virtually eliminated by the A/B balanced circuit configuration. The twisting of the wires makes them consistently equidistant from each other. Any induced surge voltages will affect wires A and B equally, thereby not influencing the overall voltage differential.

Since the voltage differential remains constant, the signal is not dramatically affected by outside interference. This is sometimes referred to as *common mode rejection*.

One of the biggest problem areas with RS-485 equipment installations is with grounding of the circuit. Grounding should be done at only one end, and that should be at the control panel end. (*See Diagram* >>) Since RS-485 networks can be up to 4,000 feet long, connecting to earth grounds at several locations can create ground loops and upset the differential voltage levels, thereby affecting signal transmission. This can cause a conflict if surge suppression devices are connected at various ground locations in the network.

Companies such as Ditek (www.ditekcorp.com) and MCG Electronics (www.mcgsurge.com) provide surge protection devices for a variety of networks, including RS-485. Some RS-485 communication devices incorporate optical isolation, which is highly desirable. Check to see if the manufacturer has provided this feature.

Repeaters Help Update Technological Capabilities

The use of converters and repeaters can provide additional flexibility in mixing old technologies with new. An RS-232 to RS-485 converter will allow access to an existing PC serial port. It will also allow a remote connection via modem and phone line. A universal serial bus (USB) conversion is another popular option.

An RS-485 to Ethernet converter will allow interfacing old RS-485 devices to more modern networks and even to the Internet. Repeaters are handy when additional distances are needed due to higher transmission rates. Check out B&B Electronics (www.bb-elec.com) for more information.

Isolation, Lightning Suppression Are Key

Troubleshooting RS-485 driven devices can be challenging due to the long distances between devices. Even though the devices are connected in a parallel manner, one slightly damaged device can take down the whole network. This is all the more reason for good isolation and lightning suppression.

Let's take the scenario of lightning hitting an access control system with RS-485-driven card readers. A lightning surge can put stress on the internal protection diodes in the RS-485 drivers, causing the device to work fine on the bench in the shop but not perform properly in the actual network. Indications of device damage can be as subtle as a sudden increase in transmission errors.

In this case, a normal RS-485 driver would drop about 8 millivolts (mv), while the slightly damaged unit dropped 150 mv. The large voltage drop was not noticeable by itself on a bench test, but was critical in affecting the overall differential voltage in a multiple device network in the field.

To troubleshoot this problem, it was necessary to remove all devices from the network, monitor the differential voltage we talked about earlier with a DVM and then replace the devices one at a time. When replacing, look for a substantial voltage drop to find the bad unit. This is also typically a standard repair process for keypads in an alarm system as they often internally use RS-485 drivers.

One final tech suggestion is to strategically place, during the system's installation, service switches for temporarily isolating hard-to-access devices during troubleshooting.