Radiometrix

Hartcran House, 231 Kenton Lane, Harrow, HA3 8RP, England

Tel: +44 (0) 20 8909 9595, Fax: +44 (0) 20 8909 2233

29 January 2008 **Application note 006**

Errors in the datastream ? Then everything is working normally

By Myk Dormer - Senior RF design engineer, Radiometrix

We engineers are simple creatures, and like to work in a world of absolutes. When a signal is applied to one end of a cable, it appears at the other. When a datastream is transmitted from one device, we anticipate that it will be received exactly as sent. Any deviation from this, and we look for faults, for software errors and faulty connections. But most of all, we consider these to be exceptions from the normal.

Radio links aren't like that. When planning to use a wireless data link, the engineer must accept that a certain incidence of data error is unavoidable. For usable links this can vary from a few ppm, to a few percent. But it is never zero:

A radio path is:

Noisy. As signal strength falls away with increasing range the signal to noise ratio of the baseband path falls (and so the error rate of the digital stream rises)

Subject to interference. RF energy from interfering sources (from other radio systems, and from the natural environment) can swamp the wanted signal, causing single errors, or whole bursts.

Unpredictable. Even when well 'in range' the signal strength can fall radically (by 20dB or more) due to fading. (Nulling of the wanted, direct path signal by out-of-phase echoes reflected from obstructions, geographical features, and even moving vehicles)

At this point it must seem like I'm implying that wireless links aren't usable at all (and most ISM band module manufacturers will gloss over what I'm describing, and do frequently make some sort of 'seamless cable replacement' claim for their products) but I'm not. What it is important to realise is that, while data errors are not frequent in a properly designed link operating within it's specified range, they will occur, and the design of the overall application must take this into account.

How to deal with data errors depends greatly on the amount of data being transmitted, and most importantly, what it is being used for. Techniques include:

1.**Ignore the error**: In applications using 'feedback-via-operator' (the user is observing the controlled device, and continues to activate the control until the desired occurrence) then a lost wireless instruction burst is at worst a mild annoyance.

Typical examples include remote controls and remote actuators, wireless keys and similar functions. In such cases, although no overt error correction is implemented, error detection is still important, as spurious operation of the controlled function is usually unacceptable (either during transmission of a command, or during idle). Sufficient burst identification data ('framing', 'synchronising' or 'addressing' words, combined with error detecting checksums, CRC or parity schemes) needs to be sent in addition to the actual command data, to allow a decoder to reliably discriminate between random noise in the absence of signal (or in the presence of interference) and the wanted command burst.

2. **Make the error statistically insignificant**: Where the failure to receive a given piece of data has safety implications (such as in alarm systems, or where dangerous processes are controlled) then multiple redundant transmissions of the same command can be used to swamp the effects of a given error, either by sending a sufficient number of command data bursts that the likelihood of all of them suffering errors becomes small enough, or by simply sending the command continuously and relying on the majority of identical commands being received correctly. (A method used in industrial machine and vehicle control)

In extreme cases, a fail safe approach can be taken, where the cessation of reception of the datastream (after a given time-out period) is taken to indicate the alarm condition.

A significant sub-class of this approach is the provision of forward error correction, where a relatively small amount of extra data is added to the message, which allows a suitably sophisticated decoding algorithm to correct for the effects of a limited number of bit errors. These 'FEC' techniques have attracted a huge amount of effort in recent years, and are now found in the Reed-Solomon coding schemes in CD recordings, and in the Viterbi algorithms used in cellular telephony.

3. **Send, acknowledge and re-transmit on error**: This is effectively an automated version of our first example. The datastream is broken up into discrete packet bursts, and after each packet the receiving unit transmits an 'acknowledge' back to the sender. If the sender fails to receive a valid acknowledge within a given time-out of sending the packet (due to an error in the packet or the ack' burst), it re-sends the same packet again.

This powerful technique is frequently used in high-end radio-modems, and is a feature of file-transfer software (such as Z-modem). Where the data must be received entirely intact and error free (such as when data logger files are downloaded, or computer binary files are transferred) then this is a preferred method.

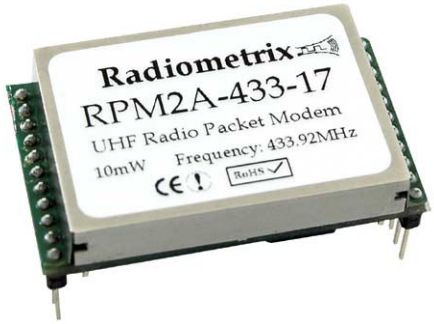

Fig 1: RPM2A radio modem features packet acknowledge and re-transmit

It is not problem-free, however, as it requires a bi-directional (transceive) link, combined with good error detection algorithms and, in the event of significant errors in the radio path, can deliver a very low overall data rate and require large data buffers at the transmitter.

There is no absolute 'correct' approach. Even the best error handling technique will fail when the radio environment is compromised (such as during electrical storms), or when the path loss is too high (= out of range).

It is up to the engineer to understand the imperfect nature of the wireless link, and design around it. Good luck!

Radiometrix Ltd

Hartcran House
231 Kenton Lane
Harrow,
Middlesex
HA3 8RP
ENGLAND
Tel: +44 (0) 20 8909 9595
Fax: +44 (0) 20 8909 2233
sales@radiometrix.com
www.radiometrix.com

Limitation of liability

The information furnished by Radiometrix Ltd is believed to be accurate and reliable. Radiometrix Ltd reserves the right to make changes or improvements in the design, specification or manufacture of its subassembly products without notice. Radiometrix Ltd does not assume any liability arising from the application or use of any product or circuit described herein, nor for any infringements of patents or other rights of third parties which may result from the use of its products. This data sheet neither states nor implies warranty of any kind, including fitness for any particular application. These radio devices may be subject to radio interference and may not function as intended if interference is present. We do NOT recommend their use for life critical applications.

The Intrastat commodity code for all our modules is: 8542 6000