

# **DNP<sub>3</sub> PROTOCOL AND RADIO DATA NETWORKS**

*A white paper by Neville Findlater, GM, Radata Systems NZ.*



First published 10/04

# DNP<sub>3</sub> PROTOCOL AND RADIO DATA NETWORKS

*A white paper by Neville Findlater, GM, Radata Systems NZ.*

First published 10/04

## Introduction

DNP<sub>3</sub> has been widely adopted in countries around the world as a “standard” for Electricity Network SCADA Communications. When using DNP<sub>3</sub> (and for that matter many other SCADA protocols) one has to be aware of the RF environment and the special factors using RF brings.



*Images courtesy of Dataradio COR Ltd.*

DNP<sub>3</sub> is a powerful and extremely versatile protocol and is a good choice for RF networks for many reasons. One should however keep in mind the effect of using the different Classes and Levels of DNP<sub>3</sub> data because the RF network typically has restricted bandwidth. Network performance may determine what you use. The performance factor alone will have a significant effect on the type of RF communications network you adopt for SCADA. Performance is often the key in Electricity SCADA communications.

## DNP<sub>3</sub> Requirements

For Effective SCADA Communications the RF network must transfer information

- **Quickly**
- **Efficiently**
- **Accurately**
- **Completely**
- **Economically**
- **Repeatedly**

## Choosing Radio Data Technology

Let's look a little closer at some of those requirements. Keep in mind the SCADA Protocol (DNP3) already provides addressing, data type, time synchronisation, time stamping, unsolicited reporting (if allowed) file transfer, and multiple objects. All protected by error detection and backed by retries if required.

A typical DNP3 frame includes ... Sync, Length, Link Control, Destination Address, Source Address, CRC and user data.

**Quickly and Efficiently.** The first question is, why choose a radio that adds unnecessary overhead? You already have all the overhead required for good communications in the protocol. This clearly implies that real-time radio modems that do not add overhead have a distinct advantage over packet radios which add overhead in their packet structure. As an example, a real-time radio-modem can offer a 2.5 times better throughput at 9600 bps than a packet radio-modem. Is this important you ask? Well yes, think of it like this. Real-Time radio-modems will support 2.5 times more remote devices on the network than packet OR will allow you to gather 2.5 times more data OR will allow you to gather that data 2.5 times more often. If you have large numbers of devices on your network or lots of data to gather, this is an important consideration. In fact, with multiple fragment replies the advantage can be even greater than this.

Now lets look at “**completely**”. Packet radio-modems break the data into packets for transmission. At the far end this often means data is delivered in bursts with small time gaps where the packet boundaries were. The issue then becomes how long should the remote device wait after receiving part of a DNP3 message or frame, before deciding that the message is incomplete and rejecting it. Different implementations of DNP3 may treat this in different ways so while some devices may dump the data as bad, others will wait long enough to allow it through. Integrators can well do without this kind of complication. If a retry occurs initiated by the packet radio then the gaps can be quite large. Possibly up to a second or more. You can see from this that retries initiated by the radios are not necessarily a good thing. With real-time radios on the other hand there is no limit to the size of a data message. The whole message can be sent in one transmission. So once again real-time radio-modems have the advantage.

Lets consider “**repeatedly**”. Keep in mind here that every millisecond of network time is important for optimum network throughput.

With packet modems the time taken for data to actually be sent can depend on a number of factors such as the size of radio packet, the size of the message to be transmitted, and the time-out used to determine the end of a message etc. The repeatedly factor translates a range of times from some minimum to a maximum which may be considerably larger. Note the times mentioned on packet radio brochures are sometimes misleading as a result. In real-time radios the delay from initi-



ating transmission until data is on the network is always the RTS/CTS delay required by the radio. This is a fixed time which depends on the network data rate. It is always the same time for every transmission. Repeatability then is an other another real-time advantage.

**Collision avoidance.** The other factors mentioned under “requirements” are mostly provided for by the DNP<sub>3</sub> protocol. However, one additional factor that must be considered regarding network efficiency is how collisions can be avoided on the network. Collisions consume time which reduces network throughput and therefore efficiency. The radio-modems used should provide a means by which the SCADA and RTU’s can determine if the network is available for data transmission. If this decision is left to the radio-modems, (something that is often claimed as an advantage of packet radio-modems) then the SCADA has lost control of the data. Duplicate data can appear in the network because while one message is buffered in the radio waiting for network access, the RTU can decide to send another because it hasn’t received a reply. In real-time systems the radio never has buffered data. With real-time, serial DCD is generally used to warn the peripheral devices that the network is busy. The random timers built into peripheral devices which support DNP<sub>3</sub> then ensure collisions are avoided or at least minimised. See attached flow chart.

How do real-time radios-modems work then? These radios are generally controlled by RTS and CTS. The equipment also provides DCD for collision avoidance and it may also support other serial lines for programming modes or other requirements. Of course data is sent and received via serial TXD and RXD. So let’s look a a simple data transmission sequence from an RTU. Firstly the RTU looks at the DCD line to see if the network is busy. If the network is clear it asserts RTS, looks at CTS and waits. When the radio is ready to transmit data it asserts CTS. The RTU sees this and then sends its data. When the last character has been sent RTS is unasserted and the RTU is ready to receive. This is the most efficient control method. Should the RTU lack the ability to look for CTS, all is not lost. By waiting a pre-set time after asserting RTS a similar result can be obtained. Remember that for real-time radio-modems the RTS/CTS delay is always known. On the receive side if the RTU sees that DCD is asserted it should be ready to receive data.

Radata Systems has supplied many RF networks for DNP<sub>3</sub> communications in New Zealand and the Pacific Islands. These networks have varied from simple “Point to Multipoint” networks through to “Repeater” networks and complex “Backbone” networks with “Drop and Insert” at intermediate sites. The number of RTU’s or remote devices which are supported on these networks varies from system to system. Generally the number able to be supported is determined by network performance and the way in which DNP<sub>3</sub> is utilised by the SCADA system. That is to say whether Class I, Class, II or class III is used. Also the acceptable poll cycle time if polling is used exclusively. There are simple tools available to calculate poll cycle time for various networks implementations. Radata Systems can supply you with these tools. Note the radio network does not impose how many RTU’s are supported by the network. The SCADA operational requirements are what impose these limits. How long can you wait before knowing about a

change of state, how long can you wait before polling for data at a particular site etc. Real-time has all the advantages in terms of performance so is the logical choice for DNP<sub>3</sub> SCADA communications.

**Economically.** When considering the economics of radio data networks it is important to consider “whole of life” costs particularly when comparing with “public network” solutions. The pay-back for private network RF data solutions is typically quite short and return on investment or IRR quite high. Also because the communications for your SCADA are critical to the SCADA operation, making a technology decision based on cost alone is not a wise idea.

**Serial port considerations.** An important thing to look for is that the DNP<sub>3</sub> field device has the facilities needed to interface with your radio network while meeting the criteria listed under requirements. As a starting point look for RTS, CTS, DCD, RXD, TXD and GND on the serial port. CTS is not essential if appropriate timers are included in the RTU but DCD is required unless you can tolerate collisions on the network or are using polling exclusively. It is surprising how many sophisticated DNP<sub>3</sub> devices are available that have poorly implemented serial communications facilities so look carefully at these requirements.

## DNP<sub>3</sub>

Now a little about DNP<sub>3</sub>. As you are probably aware there are several classes of data in DNP<sub>3</sub> and these can be retrieved from the field devices in several ways. Class 1 is the highest priority followed by Class 2 and then Class 3.

Because RF network bandwidth is limited and you may have many devices on the network it is important not to waste network time. Using report by exception is one way of minimising data traffic. This means that only that data which has changed since the last communication is retrieved. Also it may not be necessary to retrieve Class 3 data with every poll. Similarly Class 2. Remember it is possible to retrieve data in several classes at one pass and this feature can again be used to again minimise traffic and optimise your network performance.

The organisation that controls DNP<sub>3</sub> recognises that supporting all the features of DNP<sub>3</sub> is probably not necessary for every device. Some field devices have limited memory and performance available and do not need specific features, while other devices must have the more advanced features to accomplish their task effectively and safely. The DNP<sub>3</sub> protocol therefore categorises complexity into three levels. At the lowest level (1) only very basic functions must be provided and all and others are optional. Level (2) handles more functions, objects and variations, and level (3) is even more complex and sophisticated.