Issue #66 - May 2013

Technical News

Industrial Electrical and Automation Products, Systems and Solutions

DNP3 Architecture
- Water Industry Case Study

Written by Lara Pournayeb
Product Manager – Micro Automation

INTRODUCTION

As water is one natural resource the human race cannot live without, the need to access and transport this essential liquid has been critical for centuries. Dating back to the Neolithic Era, the first water well was built to allow the humans at the time to fill up their vessels and carry them to their nearby settlements. While the need is still the same, we have come a long way, with today's technology providing us with pumping stations that allow us to move water from one place to another, often several kilometres in distance.

Electronic devices such as a Programmable Logic Controller (PLC) or Remote Terminal Unit (RTU) control the activities of the modern-day pumping station, usually via a Centralised Control Room with SCADA (Supervisory Control and Data Acquisition) remotely accessing the RTU of each substation. The operator located in the control room can then be notified when there are any pump faults, fluctuations in water levels, specific substation alarms or can simply record operational data.

Communication protocols define the rules to exchange data between the SCADA and the RTUs. In the early 1990s, the IEEE Power Engineering Society's Data Acquisition, Monitoring and Control Subcommittee conducted a task in determining existing communication protocols in a SCADA system. They found that many of the protocols actually increased the cost and the time of the design of the SCADA system. The two protocols that met most of the requirements for communication between SCADA and Intelligent Electronic Device were IEC 60870-5-101 and DNP3.

DNP3 (Distributed Network Protocol) has emerged as a standard for distributed communication in the water and electricity industry, which has a need for time-stamping, security and an open protocol. This capability has been available in RTUs for some time, however is becoming increasingly available in a wider range of hardware from many vendors. DNP3 allows time-stamping to be captured even when the system communication fails. This is critical in correcting major faults. Another aspect of DNP3 is the enhanced security with encryption and authentication. This edition of Technical News will focus on DNP3 architectures used for reliable and secure control of remote infrastructure such as water pumps, with an application example drawn from a live installation.

DNP3 – AN OVERVIEW

DNP3 defines a set of communication rules between various types of data acquisition and control equipment. DNP3 is a non-proprietary protocol developed to reliably, efficiently and securely exchange information between a remote master station and an outstation. A remote master station can be a SCADA or a real time server while the outstation is a Remote Terminal Unit (RTU), Programmable Logic Controller (PLC) or IED (Intelligent Electronic Device).

DNP3 is a layered protocol. The architecture supports 3 layers standard of the seven layer Open System Interconnection (OSI) model. A fourth layer, a pseudo-transport layer, resides in the application layer. This layer is responsible for message segmentation. Here we go into more detail about each of these different layers.

Physical Layer

The physical layer is the physical media through which the communication is being transmitted and received. Despite the increasing implementation of DNP3 over TCP/IP, the most common implementation is the serial communication such as RS-232 and RS-485. Copper, optical fibre and microwave can support physical media where the data interface allows data transmission from the source to the destination host.

Data link Layer

The data link layer is responsible for delivering messages while detecting error characteristics arisen from the physical media. The DNP3 message is structured as a frame. The DNP3 frame begins with a header and follows with a data section. The header provides two sync bytes indicating the start of a new frame. The 'length' element of the header specifies the number of octets in the remainder of the frame. In addition, link control, destination and source addresses identify which DNP3 device sent the message and to which device the receiver needs to respond. The data section called the data payload contains a pair of CRC octet for every 16 data octets. The maximum length of a frame is 292 octets. (See Figure 1).

Pseudo-Transport Layer

For messages larger than a single frame, the transmitting Pseudo-Transport layer partitions this single information in multiple frames. Each frame carries a byte which identifies the logical sequence within the originated message. At the receiving end, this layer has the responsibility of reassembling the frames. A rolling frame sequence number increments with each frame being received which allows detection of a dropped frame.

Application Layer

The application layer is the closest layer to the end user. When the data is larger than a single application layer message, this message is broken down to fragments. Fragments sent from the master station are typically requests for changed objects. Fragments from the outstations are typically responses to the master station.

Each application layer fragment begins with an application layer header followed by one or more object header/object combinations. The application layer header is composed of an application control code and an application function code. The application control code indicates if it is a single frame or one of a multi-fragment message, if a layer confirmation is requested for the fragment, if the fragment is part of unsolicited response, and indicates the rolling application layer sequence number. The application function code specifies the purpose of this fragment communication such as whether the fragment is part of a response to a master polling for information, whether the fragment is an unsolicited response (response without request from the master), read and write, plus additional functionality.

Since the release of DNP3 communication protocol, the main uptake has been within the water and electrical industry where the master operations centre has a need to monitor all the main activities and equipment for each substation. This edition of Technical News will provide an overview of the SCADA system used for the ACTEWAGL water pumps stations and how DNP3 has been successfully implemented in a new water pump station.

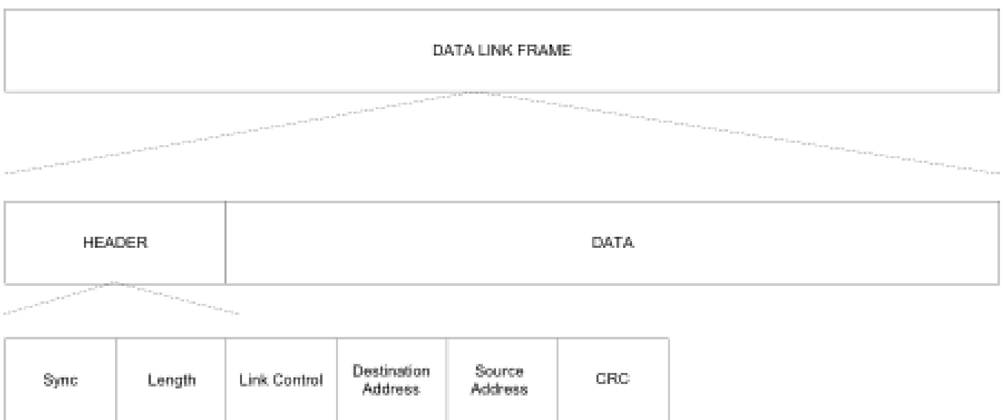

Figure 1: DNP3 Data Link Frame

WATER INDUSTRY CASE STUDY: ACTEWAGL

ACTEWAGL DNP3 System Architecture

The DNP3 system architecture adopted by ACTEWAGL is a multi-drop single master/multiple outstations network. In this network, the master SCADA system polls information from 24 remote pump stations. The master requests information from the first pump station and then moves to the next pump station for its data. When the master station receives data from the last pump station, it rolls back to the first outstation. This process is continuously performed with an interval of 2 minutes. The communication media is based on a 450 MHz full duplex two-way radio communication system. Each outstation has a YAGI antenna placed on the rooftop pointing the direction of a central radio repeater site. Each data radio in the outstations can hear messages from the master but only the outstation with the correct identification status can respond to the messages addressed to it (see Figure 2).

Pump Station Overview

This new water pump station is located 13km north of the city of Canberra. The outstation reports to the ACTEWAGL office headquarters, about 8km away. Two water pumps are installed in this outstation, with one water pump active at all times, while the other pump is on standby. If one pump fails, the second pump will start operating. The water pump system pumps water to a nearby reservoir through to the suburb (high zone below 690m contour level). (see Figure 3).

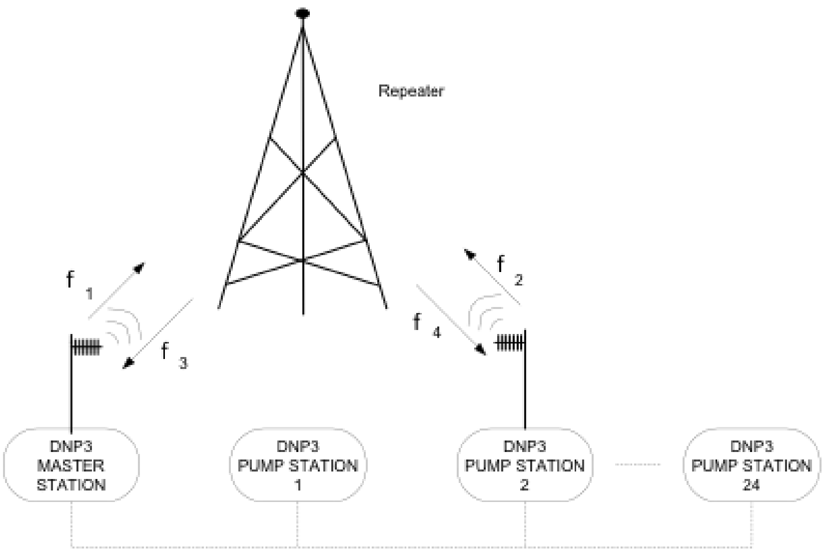

Figure 2: ACTEWAGL DNP3 Architecture

Figure 3: Water Pump Station

Pump Station Control room overview

The Allen-Bradley® MicroLogix 1400 (series B) PLC is at the centre of all communications in the outstation. Most of the equipment such as magnetic flow meter and sensors signals are connected to the PLC. The controller regularly scans changes of the input and processes this change via a buffer holding the data so that it can later respond to the master. The input changes may also change the outputs. The 450 MHz data radio is connected to the PLC and supports DNP3 communication. The information sent over the DNP3 link includes the measurements of analog flow data, analog suction and discharge pressure of the water pump, the open/close bi-state of the valves, the status of the UPS and the system alarms.

The outstation also monitors the water level of the reservoir. The communication is a point-to-point data link where the PLC is connected to a 900 MHz data radio via an RS-232 serial port. In this outstation, the MicroLogix 1400 PLC acts as a host computer while the modem converts the analog measurement into a digital data stream. The communication protocol, DF-1, between the PLC and the data radio is vendor specific. The Allen-Bradley DF-1 communication protocol specifies a link layer frame as 8 data bits, no parity, and a maximum baud rate of 19,200 bps. (See Figure 4 & 5)

The Allen-Bradley PanelView Components Human Machine Interface (HMI) is installed on the door of the control cabinet. This HMI gives the user the ability to visualise vital information from the control equipment, including the water level of the reservoir, valves operation, the drives voltage, the suction and discharge pressure of the water pumps, fire and intruder alarms.

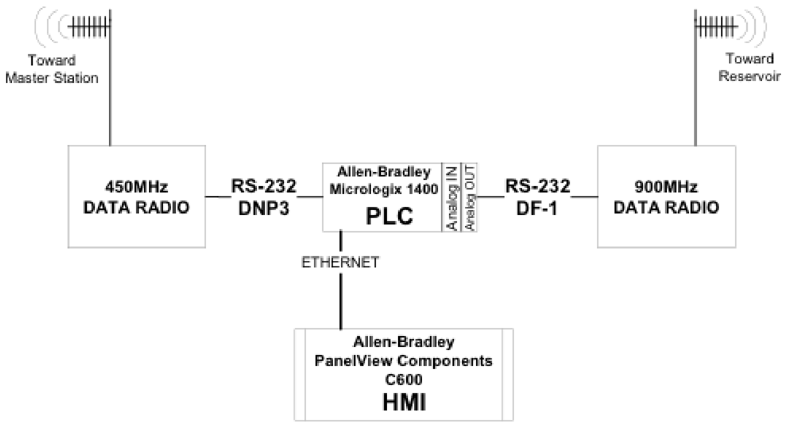

Figure 4: Outstation communication overview

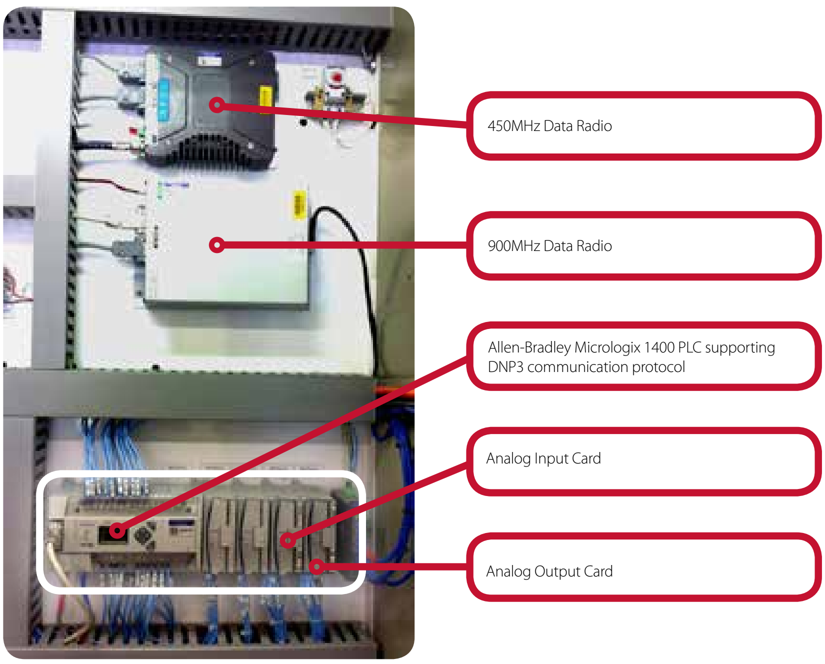

Figure 5: Outstation communication equipment overview

Outstation Database Structure

In the DNP3 communication protocol, any object is associated with an object group, a variation and the index of the array. At the outstation, the DNP3 MicroLogix 1400 PLC organises data into data types called objects. 60 analog input signals, 20 analog outputs signals, 64 binary inputs and 16 binary outputs signals correspond to changes in the suction and discharge pressure of the water pump, with the water flow measurement and binary alarms all polled to the office headquarters. Each data type is grouped into object groups. The controller is set with 4 data groups: analog inputs, analog outputs, binary inputs and binary outputs. Each element of the array is labelled with indexes.

The DNP3 communication protocol represents data with a defined format called variation. In the case of this outstation, the PLC generates a 16-bit integer value with event time for all data types. The Micrologix 1400 PLC supports time-stamping which is a powerful feature of the DNP3 communication protocol. An event time is generated when the value of the data object changes. The event time is synchronised with the PLC Real Time Clock (RTC) which closely matches the occurrence time.

DNP3 data collection scheme

In DNP3, a static data is the current value of a device. The communication is efficient when the master polls event data. A DNP3 event data is generated when a significant change has occurred with static data. At this water pump station, the master requests events data from the MicroLogix 1400 PLC. No static data is retrieved. The master can provide instructions to the PLC to report all static data at the sacrifice of available bandwidth and increase in polling time. The PLC used at this pump station has a buffer which allows events to be stored until a master retrieves the entire buffer. The user has configured the PLC to store up to 1,000 events in the buffer.

In DNP3, an event can be classified into one of three classes. A class 1 event is considered having higher priority than class 2 and higher priority than class 3, sequentially. The user layer can request the application layer for data from any of the three classes or any combination of them. At this water pump station, the PLC is set to place all group data in Class Poll 1. All events data are considered equally important.

As an example, if the water pump pressure is higher than 20 psi indicating a current higher than 20 mA, then the change in the analog value is stored as an event in the PLC buffer with the associated time-stamp. This event also triggers a binary output alarm which is polled by the master station. This will indicate to the operator at office headquarters that an instrument within the outstation is malfunctioning. In case an intruder is detected by one of the sensors in the outstation, a binary input to the PLC changes state. Within two minutes, this information is reported to the master station which notifies the operator. As a further example, when the power fails, the PLC and vital communication equipment are connected to a UPS. However, the pump station pressure and flow measurement equipment are not connected to a UPS. The analog data changes from a reading value to a null value. Each event associated with a time-stamp is stored in the buffer. When the power is turned back on, the analog data changes from no value to a measured reading. The operator can access the log file from the master station database when the power failure has occurred and the duration of this power failure. The user can then troubleshoot and diagnose the cause of this power failure.

Unsolicited Event responses

The MicroLogix 1400 PLC installed at this outstation has the capabilities to trigger a response without any request from the master station. The user may set the PLC with unsolicited mode for prioritising the events which requires immediate action from the master. The DNP3 unsolicited mode can be associated with a particular class event. In other words, the user can set the PLC to poll data from class 1, 2, 3 or any combination of these whenever an unsolicited response occurs. This reduces the time required to poll event data and hence increases bandwidth. ACTEWAGL has disabled this mode of the PLC as all event data has been allocated equal priority in the communication system.

CONCLUSION

The DNP3 open communication protocol has been rapidly adopted by the water,, oil and gas, mining, irrigation and electricity industries as DNP3 offers many advantages over conventional protocols. While most of the existing protocols follow token-passing methods, DNP3 communication is based on event data reports. This prevents redundant data being transmitted, which maximises available bandwidth, critical for long distance communications. DNP3 also incorporates Class Polls and unsolicited messaging, which is beneficial when the slave requests immediate action from the master. Time-stamping of each event is another major advantage for the user. This is useful when an abnormal event occurs and troubleshooting of the outstation is required. In addition, DNP3 is an open protocol and supported by many devices.

The DNP3 protocol continues to grow in feature-set whilst retaining reliability and security across the communication backbone.

SOURCES

Allen-Bradley, Micrologix 1400 User Manual, Publication 1766-UM001F-EN-P, March 2011,

http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1766-um001_-en-p.pdf

DNP3 Primer, Revision A, 20 March 2005, www.dnp.org

Triangle Micro Works, Inc, DNP3 Overview, Revision 1.2, February 22, 2002, www.trianglemicroworks.com

Scan the QR code to download the eCatalogues App

Scan the QR code to download the Variable Speed Drives App

If you would like previous copies of Technical News, please complete the following form and **fax to NHP on (03) 9429 1075**.

Name: .... Title: .... Company: ....

☐ **Please post to:** address ....

....

Telephone: (   ) .... Fax: (   ) ....

☐ **Please email to:** .... **Issue number:** ....

To find out what issue number you require or to download all previous editions of NHP's Technical News, simply visit **www.nhp.com.au/media** and navigate to 'Catalogues & Literature'

Editorial content: Please address all enquiries to marketing@nhp.com.au.