ARGA CONTROLS INC.

DNP 3.0 and Modbus RTU Protocols

USER GUIDE

March 27, 2000

Version 2a

ARGA CONTROLS
(626) 799-3314
www.argacontrols.com

Table of Contents

1.0 Overview

This document describes protocol support software for the Arga Controls Analog Meter IED. At this time, the Arga Meter can be configured to support either DNP 3.0 or Modbus RTU protocol. This document describes protocol implementation features for each of these protocols, plus operation of the meter configuration program which allows you to select the target protocol and set all relevant operational parameters.

This document assumes that the user is familiar with technical aspects of the selected protocols. The DNP 3.0 Basic 4 Document Set (from the DNP User's Group) describes the DNP 3.0 protocol, and the Modicon Modbus Protocol Reference Guide (from Modicon) describes the Modbus RTU protocol. Either of these, in conjunction with this document, provides complete information on how to communicate with the Arga Controls IED.

2.0 DNP 3.0

2.1 General

This implementation supports single fragment request messages from the host and can generate single segment responses. A fragment is a maximum of 60 bytes. Each fragment will be returned as one data link layer frame. Each data link layer frame is a maximum of 65 bytes long. If a multiple fragment request is sent to the Arga Controls IED, then only the first fragment will be processed. This implementation does not support unsolicited responses. The Arga Controls IED will respond to user level confirm requests from the host. The Arga Controls IED will generate user level confirm requests to the host if configured to do so.

This implementation does not support application level retries. It does support data link layer retries initiated by the host and if so configured, supports data link layer retries initiated by the Arga Controls IED.

2.2 DNP 3.0 Function Code Set

The following DNP function request codes are supported. Use of other function codes by the host will cause Bit 0 ("Function code not implemented") to be set in the second byte of the IIN of the response.

Code	Meaning
0	Confirm
1	Read
2	Write
13	Cold Restart (Comm Card Only)
14	Warm Restart (Comm Card Only)
15	Initialize Data to Defaults (Acknowledged but otherwise ignored)
16	Initialize Application (Acknowledged but otherwise ignored)
17	Start Application (Acknowledged but otherwise ignored)
18	Stop Application (Acknowledged but otherwise ignored)
22	Assign Class

2.3 DNP 3.0 IIN Response Code

The IIN field is fully supported. The following applies to the Arga Controls IED implementation of the DNP 3.0 protocol.

Byte	Bit	Description
1	1	Class 1 data available - always zero.
1	2	Class 2 data available - always zero.
1	3	Class 3 data available - always zero.
1	4	Time-synchronization required - always zero.
1	5	Outputs off-line - always zero.
1	6	Device Trouble - always zero.
2	3	Buffer overflow - frame data received or generated exceeds 65 bytes total, reset by host.
2	4	Request in process - always zero.
2	5	Configuration corrupt - always zero.

2.4 DNP 3.0 Object Types

The following object types are supported. Use of other object types will cause Bit 1 ("Requested objects(s) unknown") to be set in the second byte of the IIN of the response.

DNP Type	Object	Var'n	Description
S-32-R	30	1	32-Bit analog input
S-16-R*	30	2	16-Bit analog input
S-32-R	30	3	32-Bit analog input without flag
S-16-R	30	4	16-Bit analog input without flag
	52	1	Time Delay, Coarse (in response to restart func)
RS	60	1	Class 0 (Statics Only)
RS	60	2	Class 1 (Events Only)
RS	60	3	Class 2 (Events Only)
RS	60	4	Class 3 (Events Only)
W	80	1	Internal Indications

The DNP type code is of the form x-yy-zzz where:

x = S	Static
y = 16	16 bit analog input
y = 32	32 bit analog input
zzz = R	Point be read by DNP function code 1
zzz = W	Point can be written by DNP function code 2
*	Default variation if variation zero specified

The code in the "DNP type" column above specifies which object type and variations that can be used with a particular DNP command, such as read or write, etc. Use of other object types or variations, or use of an object in DNP commands other than as specified above will cause Bit 1 ("Requested objects(s) unknown") to be set in the second byte of the IIN of the response. Specifying undefined index points will be reported in the IIN as "Parameter Error".

An item in the above table marked with an asterisk is the variation returned if variation zero is specified or a class scan is used with a read command. All analog inputs are 16 bits internal to the Arga Controls IED, and will be sign extended if a 32 bit output variation is requested.

All object/index codes are supported in DNP requests except qualifier code 11 (free-format).

The DNP 3.0 protocol allows the application (Arga Controls IED) to select the qualifier and in some cases, the variation that will be returned in the response to a request from the host. The following conventions are used by the Arga Controls IED implementation of DNP 3.0.

The default qualifier used for all responses to a DNP read request is the qualifier supplied on the input request. However, if the input request qualifier is 6 (all points) then the output qualifier is set to hex 07 (one byte single field quantity).

A scan of class 0 (object 60, variation 1) will return all static data. Since this device only supports static analog inputs (not analog events), a scan of other classes (object 60, variations 2, 3, or 4) will not return any data. A scan for all data (object 60, variation 0) will also return all static data points.

In the flags returned with some of the object variations, the "On-line" bit is always one, and all other bits are always returned as zero.

The DNP cold or warm restart functions will generate a time delay object in the response message specifying a time delay of ten seconds. The response will also request an application

level confirm. When this confirm is received from the host, then the IED will halt all activity. This will cause the watch dog timer to time out and reset the IED. Five seconds after the watch dog reset, the IED will again respond to DNP requests from the host.

2.5 DNP 3.0 Point List

The analog inputs can be configured to be uni-polar (0 through 4095 units, or 0 through 4.9988 volts) or bi-polar (-2048 through +2047 units, or -5 through +4.9976 volts). The upper and lower limits may several units less due to ground reference voltage corrections. The ground reference voltage (a small number of milli-volts) is subtracted out of all reported data.

The reported analog values are filtered and smoothed. Samples of the input are taken at a 240 Hz rate. Then four subsequent samples are averaged to create an average input value. This effectively filters out 60Hz and 120Hz sine wave noise on the analog input. Each of the six input channels is sampled in the same fashion on a round robin basis, so an average input value is generated for each channel at a 10 Hz rate.

The average input value is then smoothed by adding 1/4 of the new average value to 3/4 of the previous historical input value. This then becomes the new historical input value which is reported to the host via DNP 3.0.

The actual number of points that can be addressed by DNP 3.0 commands is configurable, from one point (index 0) though 6 points. The analog data acquisition, filtering and smoothing, as described above, is always done on all six analog input channels.

Analog Input Points:

Point Index	DNP Type	Description
0	S-16-R	Channel #1 Analog Input
1	S-16-R	Channel #2 Analog Input
2	S-16-R	Channel #3 Analog Input
3	S-16-R	Channel #4 Analog Input
4	S-16-R	+5 volt reference
5	S-16-R	Ground Reference

3.0 Modbus RTU

The Modbus/RTU protocol is much simpler than DNP 3.0. The only functions codes supports are **Read Holding Registers** (function code 3) and **Read Input Registers** (function code 4). The response to both requests is identical. A request forany other addresss will generate an ILLEGAL FUNCTION response.

Either request can be made for up to 6 analog values. The address of the first analog value is user selectable. The other five point's addresses are at the next five sequential addresses. A request for any other address will generate an ILLEGAL DATA ADDRESS response.

The first four analog points return values for analog channel inputs 1 to 4. The fifth point is the +5 volt reference, and the 6th is the ground reference (as listed in section 2.5).

4.0 General Notes

4.1 Delay

There is a five second delay from initial power application to when the Arga Controls IED will start responding to master commands on the RS-485 port. This delay is to allow stabilization of various components of the Arga Controls IED before communication begins. It also allows time for the IED to respond to a request for a custom initialization program that will set parameters into the EEPROM contained in the IED.

4.2 RS-485 Serial I/O Interface

The RS-485 serial I/O data communication port can be configured as a two wire or a four wire interface via hardware jumpers. Both the meter initialization program ("TERM3.EXE") described below, and the host processor communicate with the meter IED via the RS-485 serial interface. Some of the considerations for successfully using this interface are described next.

The RS-485 standard differs from the RS-422 standard primarily in that the hardware line drivers and receivers are designed for multi-drop operation, i.e. more than one meter can be connected to the line at the same time. Host interfaces designed to the RS-422 standard might not successfully or reliably operate with the RS-485 interface in the meter interface because of different electrical characteristics.

Proper termination of the ends of the multi-drop line with termination resistors is essential. (120 OHMS) Pay close attention to the polarity of the line, an unintended reversal will disable all communication. For long lines, the electrical characteristics of the cable become important. Details of both the cable and termination resistor characteristics are described in the RS-485 standards document.

Although there can be many active receivers on a multi-drop line, there can only be one active transmitter, or else a "collision" will occur and data transmissions will be corrupted. It is important that proper delays be introduced after receiving a frame of data before transmitting a response. Otherwise the other end will not have time to disable its transmitter and enable its receiver. The result will be loss of part of the response, and probably the effect will be to disable all communication.

The "W" parameter of the meter IED is used to adjust this time delay for transmissions

originating at the meter. It defaults to 30 milli-seconds, and must be increased to at least 200 milli-seconds when the meter is attached to the Applied Systems Engineering COMM64 RTU Test Set. A similar timeout must be included for transmissions originating at the host. In the case of the Applied System Engineering test set, this delay is supplied by the 8 milli-second RTS/CTS delay enabled in the RS-232 to RS-485 converter box.

On a two wire RS-485 interface, it is expected that the receiver will "hear" all transmissions on the line, including transmissions originating in the same unit as the receiver. The meter program expects this echo and compensates for it. In the Applied Systems Engineering test set, the "Half Duplex Filtering" option must be selected in the SystemParams menu to compensate for the echo.

To trouble shoot the RS-485 connection, use the Applied Systems Engineering test set to repeatedly send a Reset Link frame (DNP) or Read Holding Registers (Modbus) message. For DNP, the "Source" address is the host address, and the "Dest" address is the meter address set into the EEPROM meter parameters. For Modbus, there is only a "Slave" address, which must correspond to the meter address. You can then use an oscilloscope to track the transmission all the way to the meter, and then back to the test set.

For DNP 3.0, the asynchronous transmission format is 8 bits, one stop bit, and no parity. For Modbus, this is selectable from the configuration program. (The configuration program always operates as 8 bits, 1 stop, no parity, but can configure the on-line communication differently.) The time sequence order of bits is start bit (mark, zero), the data bits (low order first), then the stop bit (spacing, one). Idle line is set to spacing (one or high) until the transmitter is turned off. The state of the line is then indeterminate. Note that the line is differential, and a two wire differential connection to the oscilloscope should be made to eliminate spurious information in the display.

If there is insufficient delay between receive and transmit, the first part of the first character may be truncated. If there is a polarity reversal in the cable connections, bits will be inverted. Be sure to first attach the oscilloscope to the Tx output of the RS-232 to RS-485 converter box to establish the correct polarity in the oscilloscope display, since this is the point that defines the polarity for the rest of the system.

4.3 Meter Initialization and Parameter Setting

The Arga Controls Analog Meter IED includes an EEPROM that contains various operating parameters. These parameters can be changed by configuration program running in an IBM PC or equivalent which is connected to the IED via the RS-485 serial connection. This IBM PC program "TERM3.EXE" allows interactive setting of the parameters stored in the IED EEPROM and also can test the analog inputs.

Upon startup, the TERM3.EXE program first requests the appropriate communications port on the PC, "COM1" or "COM2". This is the port that is connected to the IED via an RS-232 to RS-485 converter box. It next asks if a 2-wire or 4-wire RS-485 interface is being used. Finally it enters the main menu routine where the current EEPROM parameters are displayed, and a menu of commands to change these parameters, or enter the analog input test is displayed.

Before displaying the main menu, the meter is polled and if it is already in DNP mode, the "TERM3.EXE program will not get a response. After a couple of seconds the message "Waiting for meter to respond, use CTRL-C to exit to DOS" will be displayed. You can then choose to exit to DOS or reset the meter. The meter will respond to the TERM3.EXE program only during the first five seconds after it is powered up or a watchdog reset has occurred. Otherwise the meter will automatically enter the on-line processing mode.

So the recommended sequence is to first start up the TERM3.EXE program and then power up or reset the meter. Note that no unit addressing is used by the TERM3.EXE program. This means that only one meter on the RS-485 line may be in configuration mode at a time.

The main menu will appear on the IBM PC screen as follows:

Protocol Software For ARGA Controls
Copyright (c) 1994, 1996 by Applied Systems Engineering, Inc.
All Rights Reserved.

To change a parameter, enter a command character followed by a parameter value of 1 to 5 digits followed by Enter. Use Esc to cancel, backspace to rubout.

You will next be presented with the current values of all parameter settings, and the ability to change any of them. You change a parameter by entering the parameter's identification letter followed by the new value and a carriage return.

4.3.1 Parameters Supported by All Protocols

Bn sets an analog input to bi-polar mode. In bi-polar mode, voltages less than or equal to -5 volts are reported as -2048 units. Voltages greater than or equal to 4.9976 are reported as 2047 units. The value of "Un" can range from 0 through 4. Channel 5 is fixed as bi-polar to properly set the ground reference value.

Cn sets the number of analog points that can be addressed by read commands. All six channels are always read, filtered, and smoothed. Setting this parameter to less than six will reduce the number of points available to be accessed from the host.

Dn Protocol type. 1=DNP, 2=Modbus

Gnnnnn is the inter-character gap timeout in micro-seconds. It is set by default to two character times at the given baud rate, whenever the baud rate is set. After the baud rate is set, the gap can be modified as needed. Must be greater than 0 and less than 65535 microseconds. If an inter-character gap timeout occurs during a frame read, then the frame will be deemed corrupted, and discarded. This timeout value must be large enough to accommodate the maximum expected inter-character delays generated by the host computer, yet as small as possible to maximize throughput.

I means initialize EEPROM parameters to defaults. The protocol is set to DNP 3.0. The baud rate is set to 19,200 baud. The host address is set to 3, the meter (IED) address is set to 2, all analog channels are set for bi-polar operation, all six channels can be accessed, data link confirms are disabled, application level confirms are disabled, the delay after receive and before transmit is set to 30 milli-seconds, the data link primary timeout is set to one second, the receive character timeout is set to two character times at the default baud rate (19,200 bps), and the number of data link primary retries is set to ten.

Mnnnnn is the meter (IED) address. Can be any value between 0 and 65534 inclusive. The value 65535 is reserved as the "all stations" address and should not be specified as an address.

Rnnnnn is the baud rate. The "TERM3.EXE" operates at a fixed 9600 baud rate. The communication serial data rate can be set between 300 and 19200 baud inclusive. If a rate less than 300 is specified, then 300 is used. If a rate greater than 19200 is specified then 19200 is used. In between these limits, only certain rates are available, due to the design of the baud rate generator. The rate is 57600 divided

by an integer ranging from 3 through 192 inclusive. Some of the more commonly used rates that can be generated are: 19200, 14400, 9600, 7200, 4800, 3600, 2400, 1800, 1200, 600, 300.

T means start analog input testing. The analog input test is terminated by the ESC key. During the analog input test, the values of all six analog channels are displayed on the IBM PC screen in real time. The display can be used to observe the calibration of each channel. There are two numbers displayed for each channel. The first is the computed voltage for each channel. If the channel is configured as bi-polar, then this number will be -5.0000 to +4.9976 volts. If the channel is configured as uni-polar, then this number will be 0.0000 to +4.9988 volts. The second number is the number of units, ranging from -2048 through +2047 for bi-polar, and ranging from 0 through +4095 for uni-polar inputs. Note that value displayed is smoothed, filtered, and with ground reference voltage adjustment. Thus, with the exception of the ground reference channel, these analog values are the same as reported to the host. For the ground reference channel, the value reported will always be zero, whereas during this analog test, the ground reference channel (last two numbers on the display line) will show the actual ground reference offset, usually a few milli-volts, plus or minus.

Un sets an analog input to uni-polar mode. In uni-polar mode, voltages less than or equal to zero volts are reported as zero units. Voltages greater than or equal to 4.9988 are reported as 4095 units. The value of "Un" can range from 0 through 4. Channel 5 is fixed as bi-polar to properly set the ground reference value.

Wnnnnn is the minimum delay in milli-seconds after message reception before a response can be transmitted. Its default is 30 milli-seconds, but this value must be increased to at least 200 milli-seconds when the IED is being used with the Applied Systems Engineering C64-COM Test Set (not required for C64-BCOM or C64-PCM). Failure to increase this timeout will cause the Test Set to ignore part or all of transmissions from the IED.

X means exit this setup procedure and start on-line protocol processing. The meter must be reset to re-enable the EEPROM parameter setting mode.

4.3.2 Parameters for DNP Protocol Only

Ennn is the number of data link layer primary retries. Can range from 0 through 255.

Hnnnnn is the host address. Can be any value between 0 and 65534 inclusive. The value 65535 is reserved as the "all stations" address and should not be specified as an address.

Ln indicates data link layer confirms. If value is not zero then confirmation at the data link layer is enabled. This means that "User Data With Confirm" and ACK will be used for all user data transmissions from the IED to the host. If the "Ln" value is zero then "Unconfirmed User Data" frames will be used for all user data transmissions to the host.

Pn indicates application level confirms. If the value is not zero then confirmation at the application layer is enabled. This means that the "CON" confirmation bit will be set in the application control byte of all response headers sent by the IED to the host. The host is expected to respond with application level confirmation messages. Application level retries by the IED are not supported and no retry attempts will be made if the host does not respond with a confirmation frame. If the host does not respond with a confirmation frame as expected, no special action is taken, i.e., the lack of a user level confirmation is ignored by the IED. If the "Pn" value is zero the "CON" confirmation bit will not be set in the application control byte of response headers sent by the IED to the host and no confirmation frames will be expected from the host.

Snnnnn is the data link layer primary timeout in milli-seconds. This timeout is activated whenever the IED is acting as a DLC primary, i.e. when the IED is transmitting a data frame with a DLC confirm or the IED is transmitting a reset link frame. The timeout is not used for unconfirmed data frames or when the IED is acting as secondary and transmitting ACK, NACK, or other secondary frames.

4.3.3 Parameters for Modbus Protocol Only

Hnnnnn Starting register address. Address of the first analog point.

?n Parity type. ?=Odd, ?=Even, ?=None