
CA PROTOCOL EMULATION

1.1 GENERAL DESCRIPTION

This section briefly describes the Control Applications (CA) communication protocol for reference purposes only. The appropriate CA documentation should be consulted for complete details of the CA protocol.

The Control Applications standard SCADA protocol is an eight bit, asynchronous protocol designed to connect directly to computer communication ports. The protocol may be used either in a point-to-point or in a multi-drop configuration. The protocol can be used in half or full-duplex operation. Communications security is provided by a 16-bit calculated cyclic redundancy check (CRC). Also, control requests are protected by the use of a select-before-execute communication sequence.

All communications exchanges in CA protocol are initiated by the host. The remote cannot initiate any exchange with the host nor can the remote directly address or communicate with another remote. The remote transmits a response to the host for all valid messages sent by the host and addressed to the remote. The only exception to this is for broadcast (all station) messages which produce no response from any remote. Also, all messages received by the remote are validated by checking the header and trailer bytes. If these bytes are not valid, the remote will ignore the message; no action or response will be initiated.

1.2 Message Structure

A header message from the host to the remote is always eight bytes long. Only in the case of downloaded parameters (function code 46) are there additional data bytes appended to the 8 byte header message. Transmissions from a remote to the host are variable in length, up to a maximum of 262 bytes (256 bytes of data and 6 bytes header and trailer as described below). Once a transmission of data is initiated, it is in a continuous stream of eight bit bytes.

All messages consist of a header, data as required by the function code, and a trailer. The header consists of three bytes. The first byte is the sync byte. This byte will always be 0F_{HEX} for transmissions from the host to the remote and F0_{HEX} for transmissions from the remote to the host. The sync byte indicates the start of a message and the direction of the message. The second byte of the header is the RTU address. This is the hardware unit number assigned to each remote. Each remote on each communication line must have a

APPENDIX B

CA PROTOCOL EMULATION

unique address. Valid addresses are 0-254 with 255 reserved as the broadcast address. The third byte of the header is the function code. This function code may range from 0 to 255; however, not all possible function codes are currently used. Figure B-3 details all the CA function codes and identifies those that are implemented in the Comm-Troller.

The message trailer consists of 2 bytes for a transmission from the host and 3 bytes for a response from the remote.

The first byte of the response trailer from a remote is referred to as the Communications Protocol Adapter (CPA) status byte and is only used in the remote's response. This byte will be used by the remote to report certain error conditions, as shown in Figure B-1. The last two bytes of the trailer are a calculated 16-bit CRC.

0	REQUEST HONORED
1	INVALID POINT
2	CONTROL TIMEOUT
3	NO REPLY
4	ILLEGAL DOWNLOAD
5	CRC ERROR
7	SYNC ERROR
9	SEQUENCE ERROR

Figure B-1 CPA Status Codes

Figure B-2 shows the general format of a message exchange between a CA host and the Comm-Troller.

SYNC A	RTU ADDRESS	FUNCTION CODE	FUNCTION SPECIFIC DATA	FUNCTION SPECIFIC DATA	FUNCTION SPECIFIC DATA	CRC 16	CRC 16
--------	-------------	---------------	------------------------	------------------------	------------------------	--------	--------

SYNC B	RTU ADDRESS	FUNCTION CODE	DATA 1	DATA N	CPA STATUS	CRC 16	CRC 16
--------	-------------	---------------	--------	-------	--------	------------	--------	--------

Figure B-2 Typical CA Message

APPENDIX B

CA PROTOCOL EMULATION

Function Code	Description	Implemented
1	Read Status Data	Y
2	Read Analog Data	Y
3	Read Meter Data	Y
4	Read Latching Control	N
5	Read Setpoint Data	N
6	Read Meter Data	N
7	Read Calculated Floating Points	N
8	Read Parameters Integers	N
9	Read Parameters Floating Points	N
10	Read Frozen Analogs	Y
11	Read Frozen Meters	Y
13	Read Latched Status	N
14	Reset Latched Status	N
16	Read All Data	Y
19	Read RTU State	N
20	Read Tank Level Data	N
21	Reset RTU State	N
30/31	Momentary Control Select/Execute	Y
32/33	Latching Control Select/Execute	Y
34/35	Setpoint Select/Execute	Y
42	Reset Accumulators	N
43	Freeze Meters	Y
44	Freeze Analogs	Y
45	Freeze Analogs and Meters	Y
46	General Purpose Download	Y
129	Read External Status	N
130	Read External Analog Data	N
131	Read External Meter Data	N
158/159	External Momentary Control Select/Execute	N
160/161	External Latching Control Select/Execute	N
162/163	External Setpoint Select/Execute	N

Figure B-3 CA Function Codes

1.3 Message Types

CA protocol communications exchanges can be divided into three types: data requests, downloads and control requests. In data requests, the host transmits a message requesting data values from the remote. The remote responds by transmitting the requested data values. These data values may be discrete, analog, accumulator, calculated variables, remote parameters, RTU status, analog outputs or discrete outputs. The format of the data types are as required by the CA host. Some variations may exist from site to site provided the host and remote are consistent in the data format (e.g. if the host expects BCD accumulator values, the remote must transmit BCD accumulator values). Note that the Comm-Troller does not do any processing on the data collected from the PLC. The PLC ladder logic must perform any data formatting that is required prior to placing the information in the data area which is read by the Comm-Troller.

Downloads consists of two messages from the host computer to the remote. The two messages are sent in succession by the master and are composed of a header and appended data bytes. The header message will contain the number of data bytes appended to the header message. The number of data bytes does not include the two trailing CRC bytes. The remote responds with an echo of the header message information along with a CPA status indicating validity of receipt of data. After the download data has been received the Comm-Troller will transmit the block of information to the designated PLC. There are six (6) download subfunctions. The header configuration section allows each subfunction to be downloaded to a specific PLC in the cluster, or broadcast to all the PLC's in the cluster with a subfunction code of FF_{HEX}.

Control requests are defined as any message from the host requesting the remote to change the state of a field device or to change or modify an internal condition of the remote. Control requests for changes to field devices require two message exchanges between the host and the remote. This will be referred to as select-before-execute. The select message is sent first followed by the execute message. After both messages have been received with no error the Comm-Troller will send the actual control command to the PLC.

1.4 CA CONFIGURATION TABLE

The CA configuration table layout is shown in the following figures.

APPENDIX B

CA PROTOCOL EMULATION

BYTE	DESCRIPTION
0	RTU Number
1	Number of PLC's
2,3	Not Used
4	Baud Rate
5	Parity
6	Number of Stop Bits (1 or 2)
7,8	Control De-select Time (10ms inc)
9	"Anaheim" Option
10-13	Not Used
14	On/Off Option Select
15-19	Not Used
20	PLC for Download 0
21,22	Start Address for Download 0
23,24	Flag Address for Download 0
25	PLC for Download 1
26,27	Start Address for Download 1
28,29	Flag Address for Download 1
30	PLC for Download 2
31,32	Start Address for Download 2
33,34	Flag Address for Download 2
35	PLC for Download 3
36,37	Start Address for Download 3
38,39	Flag Address for Download 3
40	PLC for Download 4
41,42	Start Address for Download 4
43,44	Flag Address for Download 4
45	PLC for Download 5
46,47	Start Address for Download 5
48,49	Flag Address for Download 5

Figure B-4 Configuration Header

APPENDIX B CA PROTOCOL EMULATION

BYTE	DESCRIPTION	BYTE	DESCRIPTION
0	PLC Address	29	# Bytes per Data Type 7
1	# Bytes per Status Input Card	30-	# of Data Type 7
2	# Status Input Cards	31,32	Start Address Data Type 7
3,4	Start Address for Status Inputs	33	# Bytes per Data Type 8
5	# Bytes per Analog Input Card	34	# of Data Type 8
6	# Analog Input Cards	35,36	Start Address Data Type 8
7,8	Start Address Analog Inputs	37	# Bytes per Internal Status
9	# Bytes per Accumulator Input	38	# of Internal Status Cards
10	# Accumulator Inputs	39,40	Start Address Internal Status
11,12	Start Address Accum. Inputs	41	# Bytes per Latching Status
13	# Bytes per Digital Output	42	# of Latching Status Cards
14	# Digital Output Cards	43,44	Start Address Latching Status
15,16	Start Address Digital Outputs	45	# Bytes per Data Type 11
17	# Bytes per Analog Output	46	# of Data Type 11
18	# Analog Output Cards	47,48	Start Address Data Type 11
19,20	Start Address Analog Output	49	# bytes per Data Type 12
21	# Bytes per Calculated Integer	50	# of Data Type 12
22	# Calculated Integers	51,52	Start Address Data Type 12
23,24	Start Address Cal. Integers	53	# Bytes Per Data Type 13
25	# Bytes per Data Type 6	54	# of Data Type 13
26	# of Data Type 6	55,56	Start Address of Data Type 13
27,28	Start Address Data Type 6	57	First Byte of Table for Next Plc

Figure B-5 PLC Data Configuration

1.4.1 CA Configuration Header

Byte #0 in the configuration header is used to define the RTU address to which the Comm-Troller will respond when communicating with the CA host. This entry is an 8-bit binary number in the range of 0 to 254 (00000000 to 11111110)

Byte #1 is used to define the number of PLCs in the system. This entry is a 4 bit binary number which is right justified in the byte. The valid range for this number is from 1 to 8 (00000001 to 00001000). The Comm-Troller will use this number to determine the number of PLC Configuration blocks to read.

Bytes #2 and 3 are reserved for use as a Radio Delay Timer. The current implementation of the CA protocol in the Comm-Troller ignores these bytes.

Byte #4 is used to define the baud rate which will be used while communicating with the CA Host. This entry is a binary number which is right justified in the byte. Valid selections are: 300 baud (00000100), 600 baud (00000101), 1200 baud (00000110) , 2400 baud (00001000), 4800 baud (00001001) and 9600 baud (00001011).

Byte #5 is used to select the host communication line parity bit. Valid settings for this byte are: No Parity (00000000), Odd Parity (00000001) and Even Parity (00000010).

Byte #6 is used to select the number of Stop Bits to use when communicating with the CA host. Valid selections are: 1 Stop Bit (00000001) or 2 Stop Bits (00000010)

Bytes #7 and 8 are used to define a "Control De-Select Time". The timer is used to qualify the execute command on CA Select-before-Execute control commands. If the execute command is not received within the time-out period specified the Comm-Troller will abort the current select operation and return to normal operation. The timer is a 16-bit binary value with each count equal to 10 msec. Byte 7 is the most significant and byte 8 the least significant.

Byte #9 is used to indicate the "Anaheim" option. If this byte is non-zero, the Comm-Troller will use a second select message (identical to the first and within the timeout period) as an execute message. If the byte is zero then a proper execute message will be required to complete the command. This option derives its name from the unique mode of operation of the CA host at Shell in Anaheim.

APPENDIX B

CA PROTOCOL EMULATION

B-8

Bytes #10, 11, 12 and 13 are not recognized by the Comm-Troller for the CA protocol.

Byte #14 is used to select whether or not the ON/OFF byte in momentary commands will be used when processing the command. If set to zero, the ON/OFF byte will be ignored in momentary control operations. If non-zero the ON/OFF byte will be checked. If the ON/OFF byte is 0 the specified point will be turned OFF then ON. If the ON/OFF byte is non-zero the specified point will be turned ON then OFF.

Byte #15 is the PLC "SWAP" enable flag. If this byte is non-zero any failure detected by the Comm-Troller while communicating with the PLC will result in an automatic switch-over to a backup PLC. The backup PLC must have exactly the same configuration information as the primary PLC. The backup PLC address must be address 0B_{HEX}. If the backup PLC subsequently fails the Comm-Troller will attempt to switch back to the primary unit. If this byte is zero then a switch will not be attempted.

Bytes 16, 17, 18 and 19 are not used for the CA Comm-Troller.

Byte #20 is used to specify the PLC address to use for download subfunction 0. This is the PLC to which the data sent with the download will be transferred.

Bytes #21 and 22 are used to specify the starting address within the PLC to place the data received.

Bytes #23 and 24 are used to specify a memory location in the PLC which will be set to FFFF_{HEX} whenever a download function has been completed.

Bytes #25, 26, 27, 28 and 29 are used the same way as bytes 20 thru 24, except for download subfunction 1.

Bytes #30, 31, 32, 33 and 34 are used for download subfunction 2

Bytes #35, 36, 37, 38, and 39 are used for download subfunction 3

Bytes #40, 41, 42, 43 and 44 are used for download subfunction 4

Bytes #45, 46, 47, 48 and 49 are used for download subfunction 5

1.4.2 PLC Data Configuration for CA Protocol

The PLC Data Configuration section(s) are each 57 bytes long. There is one section for each PLC connected to the Comm-Troller. The number of PLCs and thus the number of configuration sections to read is defined by byte #1 in the header section of the configuration table.

Byte #0 is used to define the address of the PLC on the Data Highway. The first PLC must be at address 0A_{HEX}.

Byte #1 is used to define the number of bytes of data for each status input card. Normally it will be set to 2 because each input card in an Allen-Bradley provides 16 bits of status information. In special applications however, PLC ladder logic could be used to form "cards" of any width.

Byte #2 is used to define the number of status input cards associated with this PLC. A total of 256 bytes of status input information can be defined per Comm-Troller.

Bytes #3 and 4 define the starting address in the PLC for the status input data.

Bytes #5, 6, 7 and 8 are used in a similar fashion to define the Analog input cards for the PLC. A total of 256 bytes of analog input information can be defined per Comm-Troller.

Bytes #9, 10, 11 and 12 are used to define accumulator inputs. A total of 256 bytes of accumulator information can be defined per Comm-Troller.

Bytes 13, 14, 15 and 16 are used to define control outputs. A total of 64 bytes of control output information can be defined per Comm-Troller

Bytes #17, 18, 19 and 20 are used to define analog outputs. A total of 64 bytes of analog output information can be defined per Comm-Troller.

Bytes #21, 22, 23 and 24 are used to define calculated integers. A total of 256 bytes of calculated integer information can be defined per Comm-Troller.

Bytes #25, 26, 27 and 28 define data "type 6". This is a generalized data type which can be used as the application requires. A total of 256 bytes of type 6 information can be defined per Comm-Troller.

APPENDIX B

CA PROTOCOL EMULATION

B-10

Bytes #29, 30, 31 and 32 define data "type 7". A total of 256 bytes of type 7 information can be defined for each Comm-Troller.

Bytes #33, 34, 35, and 36 define data "type 8". A total of 256 bytes of type 8 data can be defined for each Comm-Troller.

Bytes #37, 38, 39 and 40 define Internal Status Data Type. A total of 32 bytes of internal status information can be defined per Comm-Troller.

Bytes #41, 42, 43 and 44 define Latched Status Data. A total of 32 bytes of latched status information can be defined per Comm-Troller.

Bytes #45, 46, 47 and 48 define data "type 11". A total of 128 bytes of type 11 information can be defined per Comm-Troller.

Bytes #49, 50, 51 and 52 define data "type 12". A total of 128 bytes of type 12 information can be defined per Comm-Troller.

Bytes #53, 54, 55 and 56 define data "type 13". A total of 128 bytes of type 13 information can be defined per Comm-Troller.

1.5 JUMPER SELECTIONS FOR CA PROTOCOL

The Comm-Troller jumper selections and EPROM part numbers for CA protocol operation is detailed in the following figure.

JUMPER	POSITION	JUMPER	POSITION
J2	1-2	J10	NOT USED
J3	NOT USED	J11	1-2
J4	NOT USED	J12	1-2
J5	NOT USED	J13	NOT USED
J6	1-2	J14	NOT USED
J7	1-2	J15	1-2
J8	NOT USED	J16	NOT USED
J9	NOT USED	J17	NOT USED

CA Protocol Communication is on Port P1 (top port), Allen-Bradley
Communication is on Port P2 (center port)

U13 = #127-015-X U23 = #127-014-X

Figure B-6 Jumper Selections for CA

APPENDIX B

CA PROTOCOL EMULATION

1.6 EXAMPLE CONFIGURATION FILE

The following figures detail a sample configuration file for a typical CA protocol application. The configuration information is based on the following information:

Protocol	CA6800
PLC Type	PLC2/17
Comm. Data	Leased Line, 1200 baud, 1 stop, no Parity
Num. of PLCs	One
Num. of Status	144
Num. of Analogs	5
Num. of Accums	6
Num. of Controls	112
Num. of Setpoints	6
Desired location of configuration table at word 710 ₈	
Desired starting location of data at word 300 ₈	
Desired location for Config. Table address pointer 700 ₈	

Figure B-7 Example System Info.

1.6.1 Comm-Troller Switch Settings

The location of the word which points to the start of the configuration table must be specified by setting the three (3) address selection switches on the Comm-Troller. For this example the switch selections are:

- Pointer Address = 700₈ (octal word address)
- = 1600₈ (octal byte address)
- = 380_H (hex byte address)

Set Comm-Troller switches to 038 (least significant 0 is implied)

APPENDIX B

CA PROTOCOL EMULATION

1.6.2 Example Table Entries

PLC WORD	VALUE (HEX)	PLC WORD	VALUE (HEX)
700	0390	741	0A02
710	3401	742	0901
711	0000	743	8002
712	0600	744	0501
713	0100	745	9204
714	C800	746	0601
715	0000	747	9C02
716	0000	750	0701
717	0000	751	B402
720	0000	752	0601
721	0000	753	C200
722	0000	754	0000
723	0000	755	0000
724	0000	756	0000
725	0000	757	0000
726	0000	760	0000
727	0000	761	0000
730	0000	762	0000
731	0000	763	0000
732	0000	764	0000
733	0000	765	0000
734	0000	766	0000
735	0000	767	0000
736	0000	770	0000
737	0000	771	0000
740	0000	772	0000
		773	0000
		774	0000
		775	00XX

Figure B-8 Example
Table Entries