Report Title :
Gasmaster OEM Modbus Specification

Approvals	1:	Date:
Development Manager	2:	Date:
Project Manager	3:	Date:
Project Engineer		

Contents

1. INTRODUCTION

This document describes the MODBUS data interface for Gasmaster control panel.

The instrument uses the RTU protocol as described in the Modicon Modbus Protocol Reference Guide except as detailed in this document. Extensions and restrictions to the Modbus protocol that have been used in other Crowcon instruments are used here where these extensions and restrictions are known and appropriate.

1.1 Related Documents

[1] GM003 - Gasmaster Target Specification

[2] GM016 - Gasmaster Control Panel Detail Design Specification

[3] Modicon Modbus Protocol Reference Guide, MODICON Inc.

1.2 Note on Modbus Terminology and Registers

The standard Modbus specification [3] talks of 16 bit (one word) registers and numbers of data bytes. The interpretation of registers and words used in this document (and used by other Crowcon products using Modbus, but perhaps with different terminology) is as follows:

A register will refer to the address of a piece of data within the register map. A register may consist of one or more 16-bit words. Registers are uniquely identified by their address.

The size of a register (sometimes also confusingly referred to as the number of registers) - that is the amount of data at a particular register address - is referred to by the number of words it contains.

Restated, we have uniquely addressed registers referring to one or more words of data.

1.3 Abbreviations

Abbreviation	Meaning
ASCII	A character based transmission protocol which can be easily displayed in human understandable form. A weakness is it uses more bandwidth than RTU
CRC	Cyclic Redundancy Check – a message postfix used to determine if the message packet has been received without corruption.
FTM	Functional Test Mode – some registers to do with hardware and production testing only have the desired effect during FTM.
PLC	Programmable Logic Controller – part of the industrial IT network responsible for data collection and evaluation.
RTU	Remote Terminal Unit – a data format which requires the receiver to decode it to a human understandable form. It is normally binary encoded rather than ASCII.

2. Modbus Specification

The Gasmaster control panel only uses the RTU (remote terminal unit) communications mode, where each 8-bit byte in a message contains two 4-bit hexadecimal numbers, transmitted in binary (rather than as ASCII representations of hexadecimal numbers).

2.1 Data format

Basic data format is fixed to the following (11-bit format):

Data format is:	1 start bit
	8 data bits, least significant bit first
	no parity bit
	2 stop bits
Error check:	cyclic redundancy check (CRC)
Baud rate:	9600

2.2 Data Timing

Standard MOBUS defines a silent interval of 3.5 characters times to delimit data packets. However, a silent interval of 5.7mS is used to define the termination of a data packet – this assists PC software in transmitting data packages which conform.

The error condition described in [3] when there is a delay of 1.5 character times, but less than 3.5 character times between data, is not implemented – this can, apparently, cause problems with legacy systems and PC timings.

On receipt of a message requiring a response, the instrument will pause for a guaranteed period of at least 50mS before transmission will commence. Again, there may be timing problems on PC systems if this restriction is not applied.

2.3 Instrument Address

Each instrument on a communications loop requires a unique address in the range 1 – 247. This address may be set via the keys on the instrument front panel or by sending a MODBUS message to the instrument requesting a change of address – care should be taken not to have multiple instruments on one communications loop with the same address. Communications with multiple instruments at the same communications address is not defined.

2.4 Implemented Functions

The Gasmaster only implements two of the Modbus commands. These are:

03	-	Read Holding registers
16	-	Preset multiple registers

Both these commands will support multiple and single register reads and presets.

Where it is appropriate, when data is transmitted to the instrument, the instrument's non-volatile backup storage will be silently and automatically updated.

See [3] for details of message format and calculation of CRCs.

2.5 Data Types and Ranges

The following data types may be used, ranges in this table represent the maximum allowable and a smaller range may be specified in the register map.

UINT8	Single byte, unsigned data (8 bits), null padded in most significant bits to create a word.
	Range = 0 to 255
INT8	Single byte, signed data (8 bits), sign extended in most significant bits to create a word.
	Range = -128 to 127
UINT16	Two bytes, unsigned integer (16 bits), one word long, most significant byte first.
	Range = 0 to 65535
INT16	Two bytes, signed integer (16 bits), one word long.
	Range = -32768 to 32767
UINT32	Four bytes, unsigned integer (32 bits), 2 words, most significant word first.
	Range = 0 to 4,294,967,295
INT32	Four bytes, signed integer (32 bits), 2 words, most significant word first.
	Range = -2,147,483,648 to 2,147,483,647
TEXT nn	Text string, nn characters long, packed 2 characters per word, of length nn/2 words. Ordered with first character in high byte of first word. Null padded in least significant byte of last word if needed.
	Range 1-255. A zero byte can be used, and this will mark the termination of the string.
FLOAT	Floating point number, in IEEE-754 format.
ENUM nn	Data enumeration. A UINT16 where each number (counting from 0) refers to an option from a list of nn possibilities. In the Register map notes below, enumerations are listed in numeric order.
	Range 0 to the number of enumerations listed.
BIT nn	An array of nn bits, null padded as necessary in the most significant word, from the most significant bit to create a whole word. Length is nn/16 words.

2.6 Register Access Permissions

Permissions used in the register map following are:

R/W	Read and write always allowed
R	Read only. The information cannot be modified via Modbus.
R(W)	Read only, unless the security address (see control section below) has been set to the appropriate value, when the location is also write-able.

3. Register Map

Addresses 50 to 499 and 602 to 699 are reserved for Crowcon use. Do not send requests to these addresses.

3.1 Instrument Identification

Information about the instrument as a whole.

Address	Name	Words	R/W	Data Type	Notes/Example
1	Instrument identification	8	R	TEXT16	"Gasmaster"
2	Manufacturer	8	R	TEXT16	"Crowcon"
3	Software version	8	R	TEXT16	"V1 i1.01"
4	Instrument serial number	8	R(W)	TEXT16	A combination of works order number and line item, written as text.
5	System Name	8	R(W)	TEXT16	"free text here", whatever the customer wants to call their system. Helps in a multi drop scheme

3.2 Runtime Data

Address	Name	Words	R/W	Data Type	Notes/Example
500	Time	2	R	UINT32	Seconds since power up.
501	Status	1	R	BIT3	0-System Fault 1-Global Inhibit 2-Warning
502	System Fault 1	2	R	UINT32	Bit packed variable see section 3.2.1
503	System Fault 2	2	R	UINT32	Bit packed variable see section 3.2.1
504	System Warning 1	2	R	UINT32	Bit packed variable see section 3.2.1
505	System Warning 2	2	R	UINT32	Bit packed variable see section 3.2.1
506	Channel 1 Level	2	R	FLOAT	Gas level
507	Channel 1 Status	1	R	BIT6	Bit 0 – Alarm 1 Bit 1 – Alarm 2 Bit 2 – Undefined Bit 3 – Inhibit Bit 4 – Low Interpret Warning Bit 5 – Fault
508	Channel 2 Level	2	R	FLOAT	Gas level

Address	Name	Words	R/W	Data Type	Notes/Example
509	Channel 2 Status	1	R	BIT6	Bit 0 – Alarm 1 Bit 1 – Alarm 2 Bit 2 – Undefined Bit 3 – Inhibit Bit 4 – Low Interpret Warning Bit 5 – Fault
510	Channel 3 Level	2	R	FLOAT	Gas level
511	Channel 3 Status	1	R	BIT6	Bit 0 – Alarm 1 Bit 1 – Alarm 2 Bit 2 – Undefined Bit 3 – Inhibit Bit 4 – Low Interpret Warning Bit 5 – Fault
512	Channel 4 Level	2	R	FLOAT	Gas level
513	Channel 4 Status	1	R	BIT6	Bit 0 – Alarm 1 Bit 1 – Alarm 2 Bit 2 – Undefined Bit 3 – Inhibit Bit 4 – Low Interpret Warning Bit 5 – Fault

3.2.1 Fault and Warning Bit Packed Variable Definitions

The following table defines the mapping of status word bits to faults.

Bit identity	Fault identity	Fault meaning
0 System Fault 1	1	Measurement system failure on ADC zero signal
1 System Fault 1	2	Measurement system failure on ADC span signal
2 System Fault 1	3	Battery Flat – shutting down
3 System Fault 1	4	Battery Low – not much time before shutdown
4 System Fault 1	5	Relay power supply fail – P12V not in expected range
5 System Fault 1	6	Main supply fail – power from main supply is not within expected range
6 System Fault 1	7	NVM hardware fail – there was a problem erasing or writing to on chip flash non volatile storage.
7 System Fault 1	8	No valid data in NVM at powerup - Loaded default parameters
8 System Fault 1	9	Common alarm low relay coil open circuit fault
9 System Fault 1	10	Common alarm high relay coil open circuit fault
10 System Fault 1	11	Common fault relay coil open circuit fault
11 System Fault 1	12	Channel 1 Alarm Low relay coil open circuit fault
12 System Fault 1	13	Channel 1 Alarm Low relay coil open circuit fault
13 System Fault 1	14	Channel 2 Alarm Low relay coil open circuit fault
14 System Fault 1	15	Channel 2 Alarm Low relay coil open circuit fault
15 System Fault 1	16	Channel 3 Alarm Low relay coil open circuit fault

Bit identity	Fault identity	Fault meaning
16 System Fault 1	17	Channel 3 Alarm Low relay coil open circuit fault
17 System Fault 1	18	Channel 4 Alarm Low relay coil open circuit fault
18 System Fault 1	19	Channel 4 Alarm Low relay coil open circuit fault
19 System Fault 1	20	Channel 1 ESU fan stalled
20 System Fault 1	21	Channel 2 ESU fan stalled
21 System Fault 1	22	Channel 3 ESU fan stalled
22 System Fault 1	23	Channel 4 ESU fan stalled
23 System Fault 1	24	Channel 1 ESU fan slow
24 System Fault 1	25	Channel 2 ESU fan slow
25 System Fault 1	26	Channel 3 ESU fan slow
26 System Fault 1	27	Channel 4 ESU fan slow
27 System Fault 1	28	Channel 1 Signal Over range
28 System Fault 1	29	Channel 2 Signal Over range
29 System Fault 1	30	Channel 3 Signal Over range
30 System Fault 1	31	Channel 4 Signal Over range
31 System Fault 1	32	Channel 1 Signal Under range
0 System Fault 2	33	Channel 2 Signal Under range
1 System Fault 2	34	Channel 3 Signal Under range
1 System Fault 2	35	Channel 4 Signal Under range
3 to 31 System Fault 2		Never Set

The following table defines the mapping of status word bits to warnings.

Bit identity	Warning identity	Warning meaning
0 System Warning 1	1	Supervisor mode
1 System Warning 1	2	Global inhibit active
2 System Warning 1	3	Testing audio visual alarm
3 System Warning 1	4	Service / calibration due
4 System Warning 1	5	Common Alarm Low relay forced
5 System Warning 1	6	Common Alarm High relay forced
6 System Warning 1	7	Common Fault relay forced
7 System Warning 1	8	Detector 1 stabilising
8 System Warning 1	9	Detector 1 input low
9 System Warning 1	10	Detector 1 initiated inhibit
10 System Warning 1	11	Channel 1 inhibited
11 System Warning 1	12	Channel 1 input simulated
12 System Warning 1	13	Channel 1 output forced
13 System Warning 1	14	Channel 1 alarm low relay forced

Bit identity	Warning identity	Warning meaning
14 System Warning 1	15	Channel 1 alarm high relay forced
15 System Warning 1	16	Detector 2 stabilising
16 System Warning 1	17	Detector 2 input low
17 System Warning 1	18	Detector 2 initiated inhibit
18 System Warning 1	19	Channel 2 inhibited
19 System Warning 1	20	Channel 2 input simulated
20 System Warning 1	21	Channel 2 output forced
21 System Warning 1	22	Channel 2 alarm low relay forced
22 System Warning 1	23	Channel 2 alarm high relay forced
23 System Warning 1	24	Detector 3 stabilising
24 System Warning 1	25	Detector 3 input low
25 System Warning 1	26	Detector 3 initiated inhibit
26 System Warning 1	27	Channel 3 inhibited
27 System Warning 1	28	Channel 3 input simulated
28 System Warning 1	29	Channel 3 output forced
29 System Warning 1	30	Channel 3 alarm low relay forced
30 System Warning 1	31	Channel 3 alarm high relay forced
31 System Warning 1	32	Detector 4 stabilising
0 System Warning 2	33	Detector 4 input low
1 System Warning 2	34	Detector 4 initiated inhibit
2 System Warning 2	35	Channel 4 inhibited
3 System Warning 2	36	Channel 4 input simulated
4 System Warning 2	37	Channel 4 output forced
5 System Warning 2	38	Channel 4 alarm low relay forced
6 System Warning 2	39	Channel 4 alarm high relay forced
7 to 31 System Warning 2		Never Set

3.3 Channel Control

Channel 1

Address	Name	Words	R/W	Data Type	Notes/Example
540	Channel 1 Inhibit	1	R/W	ENUM1	No inhibit Channel inhibit

Address	Name	Words	R/W	Data Type	Notes/Example
541	Channel 1 Action Zero	1	R/W	ENUM2	Idle Perform Zero Zero Fail Set to "Perform Zero" then wait for "Idle" or "Zero Fail". If "Zero Fail" then write to set it back to "Idle".
542	Channel 1 Cal Level	2	R/W	FLOAT	The concentration of the cal gas.
543	Channel 1 Cal Action	1	R/W	ENUM2	Idle Perform Cal Cal Fail (Input) Cal Fail (Gain) Set to "Perform Cal" then wait for "Idle" or "Cal Fail". If "Cal Fail" then write to set it back to "Idle".
544	Channel 1 OP Cal Control	1	R/W	ENUM3	Normal/Idle Measure Low mA Measure High mA Cal Fail For operation see Note 1 below.
545	Channel 1 OP Cal Level	2	R/W	FLOAT	Measured mA level. For low mA range is 3 to 5. For high mA range is 19 to 21.

Note 1 – Operation of OP Cal Control; Set to "Measure Low mA" system then requires a measured value of mA to be written to 545. A valid low mA value will move OP Cal Control to "Measure High mA" and an invalid value will move OP Cal Control to "Cal Fail". With the control set to "Measure High mA" the system requires a measured value of mA to be written to 545. A valid high mA value will move OP Cal Control to "Normal/Idle" and will cause the output calibration offset and scale values to evaluated and an invalid value will move OP Cal Control to "Cal Fail". "Cal Fail" values when read should be overwritten by "Normal/Idle" and the calibration operation started again.

Channel 2

Address	Name	Words	R/W	Data Type	Notes/Example
550	Channel 2 as per channel 1				

Channel 3

Address	Name	Words	R/W	Data Type	Notes/Example
560	Channel 3 as per channel 1				

Channel 4

Address	Name	Words	R/W	Data Type	Notes/Example
570	Channel 4 as per channel 1				

3.4 System Control

Address	Name	Words	R/W	Data Type	Notes/Example
600	Accept Reset	1	R/W	ENUM1	Idle, Cause Accept Reset Automatically reverts to idle when action complete
601	NVM control	1	R/W	ENUM4	Idle, Save Parameter Config, Restore Parameter Config, Clear Parameter Config, Save Text Config, Restore Text Config, Clear Text Config. Automatically reverts to idle when action complete

3.5 Event Log

3.5.1 Event Log Map

This section specifies the Modbus map for events. For a complete explanation of the use of the controls and the format of the event data refer to section 3.5.2. Event data is always read in blocks of 10 events for efficiency of communications.

Address	Name	Words	R/W	Data Type	Notes/Example
700	Read control	1	R/W	ENUM 2	Abort read, Reset, Next Block, Clear Log (not imp)
701	Service event time and date	2	R(W)	UINT32	Seconds since 1 Jan 1970.
702	Event 1 time	2	R	UINT32	Time of event
703	Event 1 IDs	1	R	UINT16	Event ID and ID byte
704	Event 1 data word	2	R	UINT32	Event data word
705	Event 2 time	2	R	UINT32	Time of event
706	Event 2 IDs	1	R	UINT16	Event ID and ID byte
707	Event 2 data word	2	R	UINT32	Event data word
708	Event 3 time	2	R	UINT32	Time of event
709	Event 3 IDs	1	R	UINT16	Event ID and ID byte
710	Event 3 data word	2	R	UINT32	Event data word
711	Event 4 time	2	R	UINT32	Time of event
712	Event 4 IDs	1	R	UINT16	Event ID and ID byte
713	Event 4 data word	2	R	UINT32	Event data word
714	Event 5 time	2	R	UINT32	Time of event
715	Event 5 IDs	1	R	UINT16	Event ID and ID byte

716	Event 5 data word	2	R	UINT32	Event data word
717	Event 6 time	2	R	UINT32	Time of event
718	Event 6 IDs	1	R	UINT16	Event ID and ID byte
719	Event 6 data word	2	R	UINT32	Event data word
720	Event 7 time	2	R	UINT32	Time of event
721	Event 7 Ids	1	R	UINT16	Event ID and ID byte
722	Event 7 data word	2	R	UINT32	Event data word
723	Event 8 time	2	R	UINT32	Time of event
724	Event 8 Ids	1	R	UINT16	Event ID and ID byte
725	Event 8 data word	2	R	UINT32	Event data word
726	Event 9 time	2	R	UINT32	Time of event
727	Event 9 Ids	1	R	UINT16	Event ID and ID byte
728	Event 9 data word	2	R	UINT32	Event data word
729	Event 10 time	2	R	UINT32	Time of event
730	Event 10 Ids	1	R	UINT16	Event ID and ID byte
731	Event 10 data word	2	R	UINT32	Event data word

3.5.2 Event Log Register Descriptions

Read Control

Used to set up the log ready for reading.

Reset – resets event log control to start at the beginning of the log. It also loads the first block of 10 event records ready for reading.

Next Block – Loads subsequent blocks of event records ready for reading.

Clear – not implemented yet (may become more relevant if the event log is ever implemented in NVM), at present this value causes an exception.

Typical Modbus sequence for reading events

Register (Operation)	Data	Comment
700 (write)	1	Resets the event log to present the oldest event as event 1.
702 to 731 (read)	**	Reads a block of 10 events
700 (write)	2	Presents the next 10 events.
702 to 731 (read)	**	Reads the next block of 10 events. When these are scanned one of the events indicates end of list.
700 (write)	0	Terminate log read operations

Service event time and date

This data is stored in NVM and used to create the service event. This value should be modified only after the system has been serviced.

Event block – time, identities, data word.

Time is defined as a count of seconds since powerup. The device reading the events will have to convert this to a date and time format for display to the user based on the current system clock reading (register 500).

Event Description	**Event ID** **1 byte**	**Event Data** **1 byte**	**Additional Data 4 bytes**
Alarm Low Entered	1	Channel ID	0
Alarm Low Exited	2	Channel ID	Peak level while in alarm (or trough level for falling alarms) [FLOAT]
Alarm High Entered	3	Channel ID	0
Alarm High Exited	4	Channel ID	Peak level while in alarm (or trough level for falling alarms) [FLOAT]
Detector comes online	5	Channel ID	0
Accept Reset	6	0	0
Warning Set	7	Channel ID Or 255 for system warning	Warning ID
Warning Cleared	8	Channel ID Or 255 for system warning	Warning ID
Power Status change	9	New power status ID	0
Power Level	10	0	When running on battery Vsys is logged every 60 secs [FLOAT].
Fault State Entered	11	Channel ID Or 255 for system fault	Fault ID
Fault State Exited	12	Channel ID Or 255 for system fault	Fault ID
Config Change	13	2 = Config Block B 3 = Config Block A 4 = Text	CRC16
NVM Repaired (redundant from V1, i1.01)	14	2 = Config Block B 3 = Config Block A 4 = Text	0
Service Event	254	0	Time and Date in seconds since 1st Jan 1970 [UINT32].
End of Event List	255	255	0

Event Data definitions

Data Description	Values
Channel ID	Channel 1 = 1, Channel 2 = 2, Channel 3 = 3, Channel 4 = 4,
Power status ID	Mains OK = 0, Mains fail = 1, Mains fail accepted = 2, Battery Low = 3, Battery Cut Off = 4.
Fault ID	TBD

NOTE that the system will store a maximum of 300 events in RAM, i.e. if power is removed or the system resets the events will be lost.

A Service event is a special case because the event data contains the date of the last service. This data is stored in NVM and the service event is reconstituted whenever a system reset occurs.

Clear log

At present does nothing so therefore not implemented.

4. Exception Respsonses

Gasmaster will respond to errors as described in [3], with the following exception codes being supported:

1 – Illegal function	function code not supported (i.e. not 3 or 16)
2 – Illegal data address	invalid/unknown register address, invalid number of registers, invalid number or words for the specified registers, write to read only register
3 – Illegal data value	Invalid number or enumeration code or data type
6 – Slave device busy	An attempt has been made to write to configuration data which is accessible from the instrument's front panel menu system whilst a user is using the menu system. This error prevents the apparent inconsistencies of data changing whilst an operator is using the instrument.