ISEP

Integrated Systems Engineering & Products

PROTOCOL CONVERTER

MODBUS RTU TO CM4

Technical Manual

DOCUMENTED BY

ISEP

Updated: 14 Dec 2001

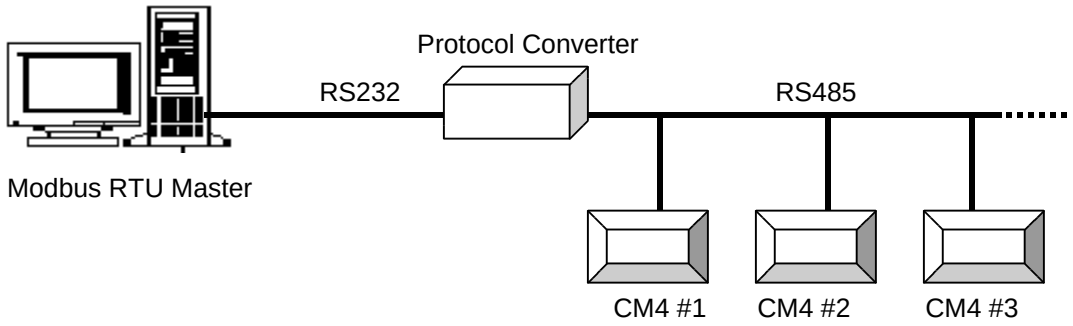
Table of Content

1 Introduction

The MODBUS RTU to CM4 Protocol Converter by ISEP facilitates data communications between a MODBUS RTU master and one or more CM4 monitor. It does this by converting MODBUS RTU queries to equivalent CM4 commands. The CM4 commands are transmitted on a RS-232 bus and only the CM4 monitor whose address matches responds. Upon receipt of the CM4 response, the converter will translate it to MODBUS RTU recognizable by the MODBUS RTU master device.

2 System Configuration

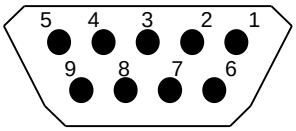
In the monitoring system, one or more CM4 monitor could be monitored. A PC is used as the MODBUS RTU master. The CM4 monitors are the slave devices. The converter is connected to MODBUS RTU master as a slave via the RS232 port. The converter is connected to CM4 monitors as a master via the RS232 port.. The system configuration is shown below.



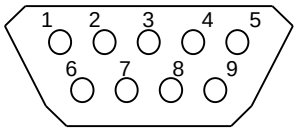
3 Converter Description

The converter is designed to sit on a shelf or platform.

The pin description for the 9 pin D connector is shown below.



9 Pin Female Connector (CM4 Port)	
Pin #	Description
2	Rx
3	Tx
5	Ground
rest	No connection



9 Pin Female Connector (MODBUS Port)	
Pin #	Description
2	Tx
3	Rx
5	Ground
rest	No connection

4 Overview of Communication Process

This section provides an overview of the communication processes that takes place within the CM4 monitor, the MODBUS RTU master and the protocol converter.

The protocol converter begins a series of events upon receiving a valid MODBUS RTU query from the MODBUS RTU master. Currently, the valid query is Read Registers. The converter will ignore any queries other than those stated above.

On power up, the converter monitors the MODBUS RTU port continuously for queries. The converter will only respond to queries with the function codes 4 which correspond to the query mentioned above.

Upon receipt of a valid query, the converter will convert the MODBUS RTU query to a CM4 command. After which, it will send out the command and waits for a response from the CM4 monitor..The converter can send multiple Query (five function codes of CM4) to CM4 depending on the starting no. of the register and the number of registers requested by the MODBUS RTU. The maximum amount of time, that is allowed between the time the last byte of the command is sent from the converter to the time the CM4 monitor responds, is 1000 milliseconds That is around 8000 milliseconds, that is the maximum amount of

time that a MODBUS RTU master can wait for the response from the converter after a query for maximum no.of registers have been sent. If no response is received from the CM4 monitor, the converter will abort the communication process of the current query and wait for a new MODBUS RTU query. The whole communication process of the current query could be finished before the MODBUS RTU master send next query.

If an error- free response is received from the CM4 monitor, the converter will convert it to a MODBUS response. The converter then sends this response back to the MODBUS RTU master.

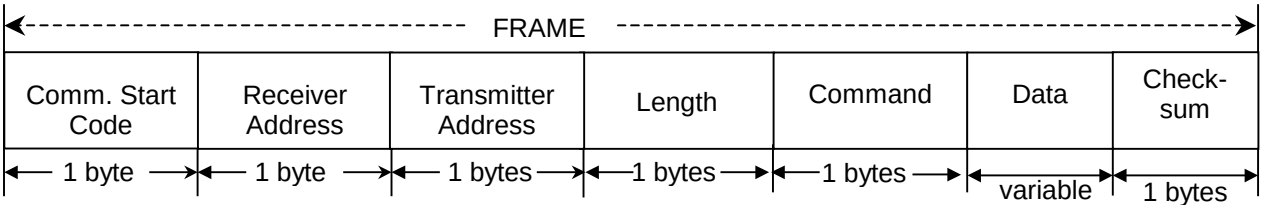
For both communication ports of the converter, the converter will do the error check first after a packet is received. The CRC-16 code of the MODBUS RTU query and the checksum byte of CM4 response are used for error check. If a response from CM4 monitor with errors in its checksum, the converter will ignore this response and wait for next query from the MODBUS RTU master. The converter will not re-transmitted the CM4 commands to the CM4 monitors and send response to the MODBUS RTU master if no error-free response is received from the CM4 monitors. If a query with errors is received, the converter will ignore this query and wait for next query.

If no response is received from the converter after the MODBUS RTU master sent the query, check the converter first. If the Tx LED of the CM4 port still flash after a query is received on the MODBUS port, that means the converter work well and the CM4 monitor should be check. Otherwise, power off the converter and power up again. The converter will start the communication process described above automatically.

5 Description of CM4 protocol

The CM4 monitor is the slave device and the converter issues commands as a master. Upon receipt of a valid frame (with no errors), the CM4 monitor responds with corresponding data.

This section describes the various message formats and definition of the CM4 protocol used in protocol converter. The message fields for a typical message are shown below:



Comm. Start Code: A byte 0x40 would signal a start of the communication packet.

Receiver Address: Range over 0 to 255. For responses from slave to master , this is always 0. For requests from master to slave ,this must match the slave's address (1-255). No broadcast message can be sent to all the devices because the address in the frame must be defined for a unique device.

Transmitter Address: Range over 0 to 255. For requests from master to slave, this is always 0. For responses from slave to master, this must match the slave's address (1-255).

Packet Length: Range over 0 to 255. This lists the packet's total number of bytes from the Comm. Start code to (and including) the checksum byte. A maximum of 250 data bytes are allowed.

Command: this command instructs the receiver what action must be performed.

Data: This section of the packet is optional. The bytes sent or received could be optional parameters or data.

Checksum: it's the two's complement of the unsigned summation of all the preceding bytes in the packet. The checksum is least significant byte (8-bits) of the sum of the bytes in the packet exclusive-Ored with 0xFF plus one. This value ends the packet.

Only four commands are implemented in the converter. They are *Get System Information, Get Unit Status, Get Current Point Status and Get Fault History.*

The details of 4 commands are shown below. An example of each command is also given below. The address of the CM4 monitor communicated is set to 1.

Get System Information (command code-0x30):

This command requests information about the slave system only and the software version currently in use.

Example:

0x40	0x01	0x05	0x30	0x8A

Checksum = (0xFF + 0x01) – (0x40 + 0x01 + 0x05 + 0x30) = 0x8A

Get Unit Status (command code-0x31):

This command requests the current condition or status of the slave. This command allows the master to inquire about the general operation condition of the system.

Example:

0x40	0x01	0x05	0x31	0x89

Get Current Point Status (command code-0x37):

This command queries an individual point for its current status. There are total 4 points.

Example: For point #1

0x40	0x01	0x06	0x37	0x00	0x82

Example: For point #2

0x40	0x01	0x06	0x37	0x01	0x82

Get Fault History (command code-0x3D):

This command will query the unit for the latest fault.

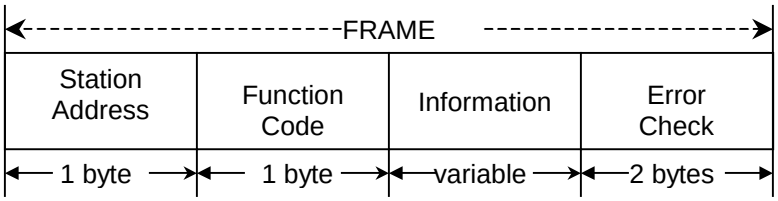
Example:

0x40	0x01	0x05	0x3D	0x7D

6 Description of MODBUS RTU

RTU protocol is a query – response protocol for communication between an RTU device and a host computer capable of communicating using protocol. The host computer is the master device and it transmits a query to a RTU slave, in this case the protocol converter, which responds to the master. The protocol converter as the RTU slave is not allowed to query but only respond to the master.

The RTU data transferred consists of 8-bit binary characters with an optional parity bit. No control characters are added to the data block; however, an error check (Cyclic Redundancy Check) included as the final field of each query and response to ensure accurate transmission of data. The message fields for a typical message are shown below:



Only 1 function (Read Registers) is implemented in this protocol converter.

6.1 Cyclic Redundancy Check (CRC-16) Calculation

The pseudo code for calculation of the CRC-16 is given below.

Preset byte count for data to be sent.
Initialize the 16-bit remainder (CRC) register to all ones.
XOR the first 8-bit data byte with the high order byte of the 16-bit CRC register. The result is the current CRC.

INIT SHIFT: Initialize the shift counter to 0.

SHIFT: Shift the current CRC register 1 bit to the right.
Increment shift count.
Is the bit shifted out to the right (flag) a 1 or a 0?
If it is a 1, XOR the generating polynomial with the current CRC.
If it is a 0, continue.
Is shift counter equal to 8?
If NO, return to SHIFT.

If YES, increment byte count.
Is byte count greater that the data length?
If NO, XOR the next 8-bit data byte with the current CRC and go to INIT SHIFT.
If YES, add current CRC to end of data message for transmission and exit.

6.2 Read Registers Query

Byte Number	Field
0	Address
1	Function Code(3L)
2	Starting Register No. *Hi Byte*
3	Starting Register No. *Lo Byte*
4	Number of Registers *Hi Byte*
5	Number of Registers *Lo Byte*
6	CRC-16 *Hi Byte*
7	CRC-16 *Lo Byte*

Example (This query is for Get System Information):

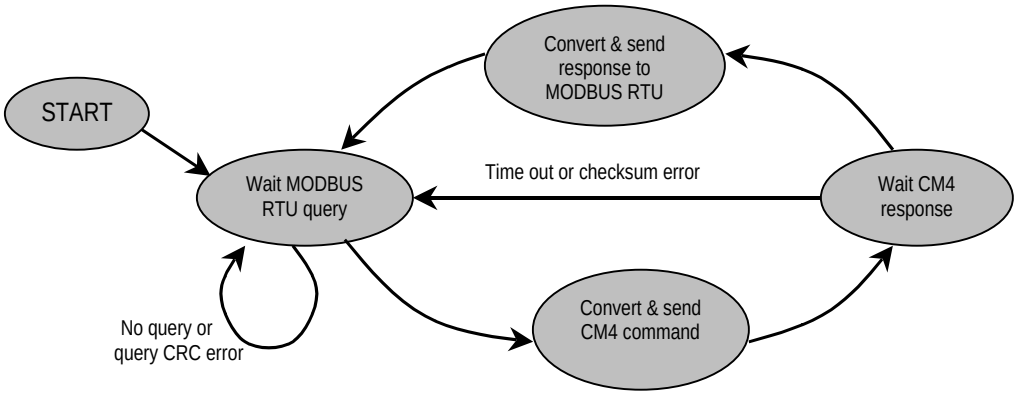
0x01	0x04	0x75	0x31	0x00	0x0B	0x2B	0x89

0x01: the CM4 monitor address is 1.
0x03: function code.
0x7531: the starting point No. is 30001.
0x000B: the number of registers
0x2B89: CRC-16

6.3 Read Registers Response

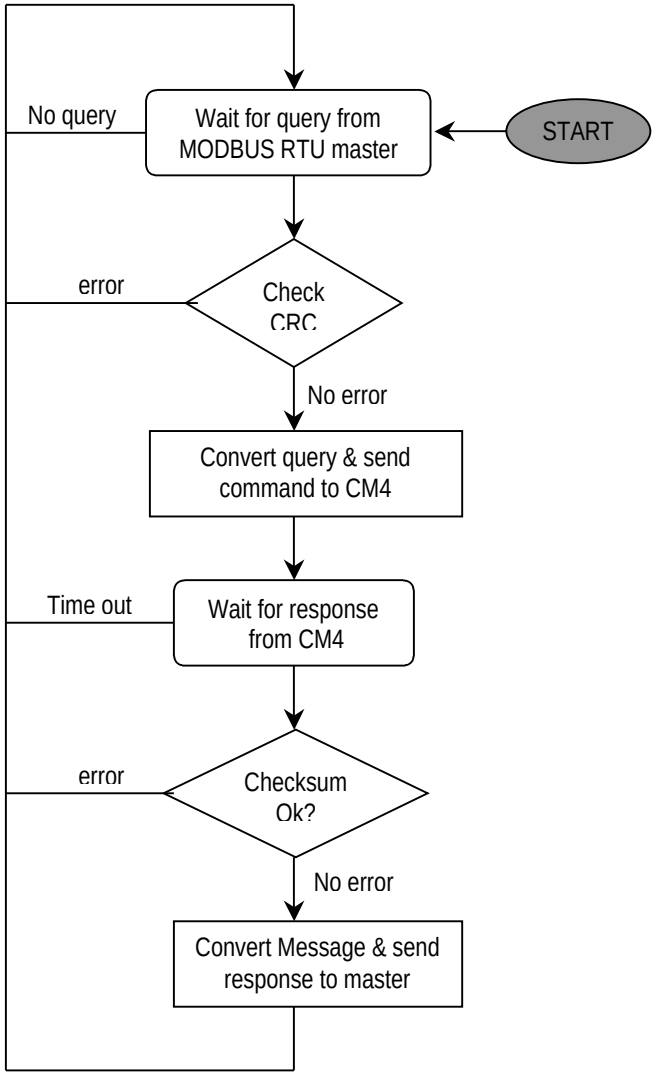
Byte Number	Field
0	Address
1	Function Code(3L)
2	Byte Count
3 to 3+ByteCount –1	*Register Hi Byte*
4 to 4+ByteCount –1	*Register Lo Byte*
4+Byte Count	CRC-16 *Hi Byte*
5+Byte Count	CRC-16 *Lo Byte*

7 State machine diagram



State Machine for Modbus-to-CM4 Protocol Converter

8 Flow Chart of the Protocol Converter



Flowchart of the Converter

9 Data Array Maps

The data are 16-bit integer.

Current Point Status

Point #1

Address	Function
30001	CM4 Year
30002	CM4 Month
30003	CM4 Day
30004	CM4 Hour
30005	CM4 Min
30006	CM4 Sec
30007	MDA Gas Abbreviation
30008	
30009	
30010	Format Code
30011	Flow Rate (current flow)
30012	TWA Start Year
30013	TWA Start Month
30014	TWA Start Day
30015	TWA Start Hour
30016	TWA Start Min
30017	TWA Start Sec
30018	TWA End Year
30019	TWA End Month
30020	TWA End Day
30021	TWA End Hour
30022	TWA End Min
30023	TWA End Sec
30024	TWA Concentration
30025	Last Concentration
30026	Alarm Status
	Status

Point #2

Address	Function
30027	CM4 Year
30028	CM4 Month
30029	CM4 Day
30030	CM4 Hour
30031	CM4 Min

30032	CM4 Sec
30033	MDA Gas Abbreviation
30034	
30035	
30036	Format Code
30037	Flow Rate (current flow)
30038	TWA Start Year
30039	TWA Start Month
30040	TWA Start Day
30041	TWA Start Hour
30042	TWA Start Min
30043	TWA Start Sec
30044	TWA End Year
30045	TWA End Month
30046	TWA End Day
30047	TWA End Hour
30048	TWA End Min
30049	TWA End Sec
30050	TWA Concentration
30051	Last Concentration
30052	Alarm Status
	Status

Point #3

Address	Function
30053	CM4 Year
30054	CM4 Month
30055	CM4 Day
30056	CM4 Hour
30057	CM4 Min
30058	CM4 Sec
30059	MDA Gas Abbreviation
30060	
30061	
30062	Format Code
30063	Flow Rate (current flow)
30064	TWA Start Year
30065	TWA Start Month
30066	TWA Start Day
30067	TWA Start Hour
30068	TWA Start Min
30069	TWA Start Sec
30070	TWA End Year
30071	TWA End Month
30072	TWA End Day

30073	TWA End Hour
30074	TWA End Min
30075	TWA End Sec
30076	TWA Concentration
30077	Last Concentration
30078	Alarm Status
	Status

Point #4

Address	Function
30079	CM4 Year
30080	CM4 Month
30081	CM4 Day
30082	CM4 Hour
30083	CM4 Min
30084	CM4 Sec
30085	MDA Gas Abbreviation
30086	
30087	
30088	Format Code
30089	Flow Rate (current flow)
30090	TWA Start Year
30091	TWA Start Month
30092	TWA Start Day
30093	TWA Start Hour
30094	TWA Start Min
30095	TWA Start Sec
30096	TWA End Year
30097	TWA End Month
30098	TWA End Day
30099	TWA End Hour
30100	TWA End Min
30101	TWA End Sec
30102	TWA Concentration
30103	Last Concentration
30104	Alarm Status
	Status

Unit Status

Address	Bit	Function
30105	0-15	CM4 Year
30106	0-15	CM4 Month
30107	0-15	CM4 Day
30108	0-15	CM4 Hour
30109	0-15	CM4 Min
30110	0-15	CM4 Sec
30111	0	Current Operating mode
	1	Keyboard Lockout state
	2	Key pad status
	3	Chemcassette counter status
	4	2mA Fault operation
	5	Point Lock-ON
	6-7	Point Locked
	8	Data Format
	9-12	Points enable when No Lock on
	13	Relay state
	14	Relay Latching state
	15	Alarm Simulation state
30112	0-15	Flash memory remaining
30113	0-15	Chemcassette windows remaining
30114	0-15	Chemcassette days remaining
30115	0-15	Internal Filter
30116	0-15	External Filter
30117	0-15	Flow Rate Point 1
30118	0-15	Flow Rate Point 2
30119	0-15	Flow Rate Point 3
30120	0-15	Flow Rate Point 4
30121	0	Optics have been calibrated
	1-4	Optics test results
	5-7	Undefined
	8-15	Maint. Status

System Information

Address	Bit	Function
30122	0-15	CM4 Year
30123	0-15	CM4 Month
30124	0-15	CM4 Day
30125	0-15	CM4 Hour
30126	0-15	CM4 Min
30127	0-15	CM4 Sec

30128	0-15	Serial# (product code 851 is assumed)	
30129	0-7	Software Rev.	Major
	0-8		Minor
30130	0-15		VIP (0xFFFF as default)
30131	0-15	Prom Check Sums	MSB PROM
30132	0-15		LSB PROM
30133	0-7	Status	

Get Fault History

Address	Bit	Function	
30134	0-15	CM4 Year	
30135	0-15	CM4 Month	
30136	0-15	CM4 Day	
30137	0-15	CM4 Hour	
30138	0-15	CM4 Min	
30139	0-15	CM4 Sec	
30140	8-15	# of fault (0-4 maximun)	
30141	0-15	Year of Fault	
30142	0-15	Month of Fault	
30143	0-15	Day of Fault	
30144	0-15	Hour of Fault	
30145	0-15	Min of Fault	
30146	0-15	Sec of Fault	
30147	8-15	Fault #	
30148	8	Point Status	General fault bit
	9-10		Point # where fault occured
	11-13		Undefined
	14		Previously Read
	15		Instrument Fault
30149	0-15	Year of Fault	
30150	0-15	Month of Fault	
30151	0-15	Day of Fault	
30152	0-15	Hour of Fault	
30153	0-15	Min of Fault	
30154	0-15	Sec of Fault	
30155	8-15	Fault #	
30156	8	Point Status	General fault bit
	9-10		Point # where fault occured
	11-13		Undefined
	14		Previously Read
	15		Instrument Fault
30157	0-15	Year of Fault	
30158	0-15	Month of Fault	
30159	0-15	Day of Fault	

30160	0-15	Hour of Fault	
30161	0-15	Min of Fault	
30162	0-15	Sec of Fault	
30163	8-15	Fault #	
30164	8	Point Status	General fault bit
	9-10		Point # where fault occured
	11-13		Undefined
	14		Previously Read
	15		Instrument Fault
30165	0-15	Year of Fault	
30166	0-15	Month of Fault	
30167	0-15	Day of Fault	
30168	0-15	Hour of Fault	
30169	0-15	Min of Fault	
30170	0-15	Sec of Fault	
30171	8-15	Fault #	
30172	8	Point Status	General fault bit
	9-10		Point # where fault occured
	11-13		Undefined
	14		Previously Read
	15		Instrument Fault

Get Floating Status

Point #1

Address	Bit	Function
30173	0-15	CM4 Year
30174	0-15	CM4 Month
30175	0-15	CM4 Day
30176	0-15	CM4 Hour
30177	0-15	CM4 Min
30178	0-15	CM4 Sec
30079	0-7	Status
30180	0-7	Flow rate 1
30181	0-7	Point Status 1
30182	0-7	Flow rate 2
30183	0-7	Point Status 2
30184	0-7	Flow rate 3
30185	0-7	Point Status 3
30186	0-7	Flow rate 4
30187	0-7	Point Status 4
30188	0-15	Concentration for Point 1 data
30189	0-15	
30190	0-15	Concentration for Point 2 data
30191	0-15	

30192	0-15	Concentration for Point 3 data
30193	0-15	
30194	0-15	Concentration for Point 4 data
30195	0-15	