Modbus Slave Protocol Details

for

KALKI Protocol Gateway/GatewayLite

Product User Guide

Version – 1.0

KALKI Communication Technologies Pvt.. Ltd..,
#147, 2nd Floor, 5th Main, 7th Sector,
H.S.R. Layout, Bangalore,
INDIA – 560034.
Phone: 91-80-5721263
http://www.kalkitech.com

CONTENTS

1. Introduction

This document contains the details of configuring Modbus slave protocol for KALKI GatewayLite using "Easy Connect" Configuration utility.

2. Protocol Interoperability List

The types, which are not supported in KALKI GatewayLite, are stroked off.

2.1. Channel / Node Parameters

2.1.1 Channel Parameters for the Modbus TCP Slave

Channel Attributes	Default Value	Supported Values	Details
Channel Type	TCP/IP	TCP/IP	NA
IP Address or Host	--	--	Should specify the IP Address of the converter.
Port Number	502	Unreserved Ethernet ports	Indicates the TCP/IP Connection Port Number.
Network Delay	2 mSec	0 → 1000 mSec	Indicates the Network Propagation Delay. This network propagation delay will be considered while time synchronization.
First Char Wait	1 mSec	0 → 100 mSec	Delay between receiving a character and transmitting next character
Connect Timeout	2 mSec	0 →100 mSec	Indicates the IP connect time out

2.1.2 Channel Parameters for the Modbus RTU Slave

Channel Attributes	Default Value	Supported Values	Details
Channel Type	RS232	RS232/RS422/RS485	NA
Communication Mode	Full Duplex	Half Duplex/ Full Duplex	NA
Baud rate	9600 baud	600 → 19200 baud	Indicates the Baud Rate at which communicates.
Data Bits	8 bits	7/8 bits	Indicates the No of Data Bits
Stop Bits	1	1/2	Indicates the Number of Stop Bits
Parity	Even	Even/odd/none	Indicates the Parity Type

Port	Com1	Com1 →Com4	Indicates the Name of the Port
Flow Control	None	None/Hardware/Software	Indicates the Type of flow control.
CTS Delay	30 msec	0 → 100 sec	Indicates the Delay between rising of CTS signal by the modem and starting of a new transmission

2.1.3 Node Parameters

Node Attributes	Default Value	Supported Values	Details
Node Address	1	1 → 255	Indicates the Address of Remote Device. This is the physical station address which has to be set in the remote device.
Command Timeout	1 sec	0 → 10 sec	Maximum delay to wait for the command reply from the remote device.
Time Synchronization	Disabled	Enable / Disable	Modbus master can send time synchronization messages if this is enabled. Check Time Synchronization section for details.
Event Enable	Disabled	Enable / Disable	This enables the event queue. Check Event Queue section for details.
Event Buffer Address	75	Integer values	This indicates the starting address of the event buffer. Master has to read all the event details from this address. “Read Holding Register” is the function type used for reading this.
Event Monitoring Bit Address	70	Integer values	This indicates the address used for monitoring whether the events are available for read. Check Event Queue section for details.

2.2. Protocol Specific Functions:-

Function Types	Object Types	Supported Data Formats
Read Coil Status (FC = 1)	SI (Single Indications)	NA
	DI (Double Indications)	NA
Read Discrete Inputs (FC = 2)	SI (Single Indications)	NA
	DI (Double Indications)	NA
Read Holding Register (FC = 3)	AI (Analog Inputs)	Unsigned Single Register Signed Single Register Unsigned 32 bit (msw-lsw) Unsigned 32 bit (lsw-msw) Signed 32 bit (msw-lsw) Signed 32 bit (lsw-msw) Float Float (lsw-msw) Double
	PC (Pulse Counters)	Unsigned Single Register Signed Single Register Unsigned 32 bit (msw-lsw) Unsigned 32 bit (lsw-msw) Signed 32 bit (msw-lsw) Signed 32 bit (lsw-msw)
Read Input Register (FC = 4)	AI (Analog Inputs)	NA
Force Single Coil (FC = 5)	SC (Single Commands)	NA
Force Single Register (FC = 6)	AO (Analog Outputs)	Unsigned Single Register Signed Single Register Unsigned 32 bit (msw-lsw) Unsigned 32 bit (lsw-msw) Signed 32 bit (msw-lsw) Signed 32 bit (lsw-msw) Float Float (lsw-msw) Double
Force Single Coil (FC = 15)	DC (Double Commands)	NA
Force Multiple Register (FC = 16)	AO (Analog Outputs)	Unsigned Single Register Signed Single Register Unsigned 32 bit (msw-lsw) Unsigned 32 bit (lsw-msw) Signed 32 bit (msw-lsw) Signed 32 bit (lsw-msw) Float Float (lsw-msw) Double
Time Synchronization		
Event Transfer		

3. Protocol Mapping Details

3.1. Object Type: -

Each profile entry is classified according to it's type. Various available types and it's details are given below.

Object Types	Details
SI (Single Indications)	These are the single indications, which can hold a single binary value.
DI (Double Indications)	These objects can have values 0 → 3. '1' is considered as off state and '2' is considered as on state.
AI (Analog Input)	It can hold various analog values depending upon the data format specified.
PC (Pulse Counter)	It can hold various analog values depending upon the data format specified. It gets mapped to corresponding pulse counters present in the slave.
SC (Single Command)	It is a single command using which we can set either 0 or 1 to a corresponding address.
AO (Analog Output)	Using this we can set an analog set point to an address.
DC (Double Command)	It is a double command. '1' indicates off state and '2' indicates the on state.

3.2. Function Types: -

Kalki GatewayLite supports the following function Types.

- Read Coil Status (FC = 1)
- Read Discrete Inputs (FC = 2)
- Read Holding Register (FC = 3)
- Read Input Register (FC = 4)
- Write Single Coil (FC = 5)
- Write Single Register (FC = 6)
- Write Multiple Coils (FC = 15)
- Write Multiple Registers (FC = 16)

3.3. Data Formats: -

There are various types of data formats

- Unsigned Single Register
- Signed Single Register
- Unsigned 32 bit (msw-lsw)
- Unsigned 32 bit (lsw-msw)
- Signed 32 bit (msw-lsw)
- Signed 32 bit (lsw-msw)
- Float
- Float (lsw-msw)
- Double

3.4. Start Address:-

It is the starting offset address of modbus slave to which the master row gets mapped.

3.5. Number of Points: -

This implies the total number of points in the slave to which the master row gets mapped. This should not be greater than the number of points of the master row.

3.6. Scale: -

This is the factor by which the Modbus data gets multiplied before sending to the master. This is especially necessary when Modbus master does not support floating point data type and you want to send the decimal numbers to master. In this case you can map it to any other types and define the scale correspondingly. For e.g. you have a master protocol point, which can have, 2 decimal points and you want to send it through a signed single register data type. In this case you have to define the scaling factor as 100. After getting the data in the Modbus master, you have to divide it by 100 to obtain actual decimal number. The default value of this is 1.

3.7. Mode: -

Modbus standard does not specify anything about the various analog data types. So the data transfer depends upon how slave and master devices interpret the messages. "Mode" is used to interpret the messages differently. If mode is not selected (not ticked) the master will consider all the slave registers are having 16 bit register size. So in order to get a float data from slave, master will request for 2 registers. To get a double data master will request for 4 registers etc. If mode is selected master will assume that the slave register has as much size as data type. So in order to get a float, master will request for a register and slave will reply with 4 bytes of data. To get a double master will still request for a register and slave will reply with 8 bytes of data.

4. Event Queue Implementation In Modbus Protocol: -

Since modbus protocol standard does not support the event data transfer, as it's inherent feature, a custom implementation is necessary to support this functionality. Following are details required to configure event queue for modbus slave.

4.1. Event Configuration Details :-

Name	**"Easy Connect" Configuration parameter**	**Details**
Event Transmit Buffer Area	Starting address 'X' is configured as "Event Buffer Address" from Easy Connect.(**EBA**)	Read Holding Register X –-> X+9 (area to be read by Modbus Master for event data) Total of 10 register locations (20 Bytes) in the following sequence. (unsigned int - read only) • X → Input Address • X+1 → Function Code • X+2 → Status (value) • X+3 → Year • X+4 → Month • X+5 → Date • X+6 → Hour • X+7 → Minute • X+8 → Second • X+9 → Msec

Event size	Not Configurable	
Fill_EV_Buf	Configured as "Event Monitoring Bit Address" from Easy Connect. (**EMBA**)	This is a flag, which indicates whether any event is available in buffer for Modbus. Master has to read this data continuously and if it is set, go for the event read from Event Transmit Buffer Area. "Read Coil Status" (FC=1) function type is used to read this.
Read_EV_Buf	Value of this is ("Event Monitoring Bit Address" + 1)	This flag indicates the Modbus master has read the last event successfully. Master has to set this flag after it has read an event. The slave will clear the last event which was send to the master only after this flag is set. "Write Single Coil" (FC=5) function type is used to set this.

4.2. Transmitting the Events :-

The events which are pending for transfer are filled in the transmit buffer (F-3 X→X+9) one by one. Using handshaking flag events are passed to Modbus master.

When there is new event present & Fill_EV_Buf flag is reset, new event is transferred in the transmit buffer and Fill_EV_Buf flag is set to indicate availability of event for Modbus Master. Filling of transmit buffer takes place one by one till all the events are sent.

Modbus master shall take the data from transmit buffer (F-3 X→ X+9) when the Fill_EV_Buf is set and Read_EV_Buf flag is reset. After reading the transmit buffer master will set the Read_EV_Buf flag. Upon receiving Read_EV_Buf, KSGL will reset Fill_EV_Buf and then reset Read_EV_Buf so that new event can be filled in transmit buffer.

Followings are the steps for getting the event from Modbus Slave

1. Query for the status of Monitoring bit addresses Fill_EV_Buf and Read_EV_Buf
   Function code- 1, Start Address- EMBA, No of Points- 2
   Response will be

EMBA	EMBA+1	Description
0	1	No event in queue and nothing to read
1	0	Event is available and is not read

2. If event is present, then poll for event details
   Function code- 3, Start Address-EBA, No of Points- 10
   Response details are shown in the above Configuration Details.

3.After reading the event set the point Read_EV_Buf
   Function code- 5, Address- EMBA+1, Value- ON
   Note the events which are read will not be removed from queue, unless this flag is set.

5. Time Synchronization in Modbus Slave: -

There are no specific function codes available in modbus protocol for time synchronization. So the specific functionality is achieved using the existing function code. The addresses used for this is taken on assumption that the specific address (under the same function code) is not used for any other purpose.

The master has to write the date and time in the specific registers and should send it to the slave stations. The slave will interpret it as time synchronization command and will get synchronized.

The time Synchronization has to be enabled from Easy Connect configuration tool to have time synchronization for modbus.

5.1. Time Sync Details: -

The **function code 16 (Write Multiple Registers)** is used to do the time synchronization. Analog and Unsigned Single Registers are used to send the time information from Master to Slave. The master has to write the date & time information in continuous registers starting from offset **9000** (the base of modbus address is 4XXXX). The higher register addresses are chosen to hold the time information. The date & time information has to be written by master and send to slave stations as given below.

Function Code: 16
Description: Write Multiple Registers
Format: Unsigned Single Registers
Base: 40000

Offset	Value
9000	Year (YYYY)
9001	Day (DD)
9002	Month (MM)
9003	Hour (HH)
9004	Minutes (MM)
9005	Seconds (SS)
9006	Milliseconds (XXX)

6. Mapping Details from other protocols: -

This section gives detailed idea of the data types in other master protocols, which can be mapped to specific Modbus slave types.

Modbus Slave types	MB-T1 MB-T2	MB-T3 MB-T4	MB-T5 MB-T6	MB-T7 MB-T8	MB-T9 MB-T10	MB-T11 MB-T12
IEC101/ 104 master types	14-M1 14-M2	14-M1 14-M2	14-M3 14-M4 14-M5 14-M6 14-M7 14-M8	14-C1 14-C2 14-C3	14-C1 14-C2 14-C3	14-C4 14-C5 14-C6 14-C7
IEC103 master types	103-T1 103-T2	103-T1 103-T2	103-T3 103-T4 103-T9	103-T20	103-T20	NA
Modbus master types	MB-T1 MB-T2	MB-T3 MB-T4	MB-T5 MB-T6	MB-T7 MB-T8	MB-T9 MB-T10	MB-T11 MB-T12
DNP3.0 master types	DN-T1 DN-T3	DN-T1 DN-T3	DN-T2 DN-T4	DN-T5	DN-T5	DN-T6
SPA master types	SP-T1 SP-T2	SP-T1 SP-T2	SP-T3 SP-T4	SP-T5 SP-T6	SP-T5 SP-T6	SP-T7
Courier master types	CR-T1 CR-T2	CR-T1 CR-T2	CR-T3	CR-T4 CR-T5	CR-T4 CR-T5	CR-T6

7. Protocol Type Details: -

IEC101/104 Type Details	
IEC101/104 types	**Type Details**
14_M1	Single Indication
14_M2	Double Indication
14_M3	Step position information
14_M4	Measured value, normalized value
14_M5	Measured value, Scaled value
14_M6	Measured value, short floating point value
14_M7	Integrated totals
14_M8	Bitstring of 32 bit
14_C1	Single command
14_C2	Double command
14_C3	Regulating step command
14_C4	Set point command, normalised value
14_C5	Set point command, Scaled value
14_C6	Set point command, short floating point value
14_C7	Set point command, Bitstring of 32 bit

Modbus Type Details		
Modbus types	**Type Details**	**Supported Formats**
MB-T1	Single Indication, Read Coil status	NA
MB-T2	Single Indication, Read Discrete inputs	NA
MB-T3	Double Indication, Read Coil status	NA
MB-T4	Double Indication, Read Discrete inputs	NA
MB-T5	Analog I/P, Read Input Registers	NA
MB-T6	Analog I/P, Read Holding Registers	Signed Single Register Unsigned Single Register Signed 32 bit Register (lsw – msw) Signed 32 bit Register (msw – lsw) Unsigned 32 bit Register (lsw – msw) Unsigned 32 bit Register (msw – lsw) Float (lsw – msw) Float (msw – lsw) Double
MB-T7	Single Command, Force single coil	NA
MB-T8	Single Command, Force multiple coils	NA
MB-T9	Double Command, Force single coil	NA
MB-T10	Double Command, Force multiple coils	NA
MB-T11	Analog O/P, Force single register	Signed Single Register Unsigned Single Register
MB-T12	Analog O/P, Force multiple registers	Signed Single Register Unsigned Single Register Signed 32 bit Register (lsw – msw) Signed 32 bit Register (msw – lsw) Unsigned 32 bit Register (lsw – msw) Unsigned 32 bit Register (msw – lsw) Float (lsw – msw) Float (msw – lsw)

IEC103 Type Details	
IEC103 types	**Type Details**
103-T1	Time Tagged Message (103 TYPE = 1)
103-T2	Time Tagged Message With Relative Time(103 TYPE = 2)
103-T3	Measurands I (103 TYPE = 3)
103-T4	Time Tagged Measurands with Relative Time. (103 TYPE = 4)
103-T5	Identification (103 TYPE = 5)
103-T9	Measurands II (103 TYPE = 9)
103-T20	Write general commands (103 TYPE = 20)
103-T21	Directory

DNP3.0 Type Details	
DNP3.0 types	**Type Details**
DN-T1	Binary Input
DN-T2	Analog Input
DN-T3	Binary Output Status
DN-T4	Analog Output Status
DN-T5	Binary Output Command
DN-T6	Analog Output Command

SPA Type Details				
SPA types	**Type Details**	**Supported Data Types**	**Supported Data Formats**	**Update Methods**
SP-T1	Single Indications	I, O, S, V, M, C	Bits, Hex, Real, Long Int	Polling , Events , polling & events
SP-T2	Double Indications	I, O, S, V, M, C	Bits, Hex, Real, Long Int	Polling , Events , polling & events
SP-T3	Analog Inputs	I, O, S, V, M, C	Bits, Hex, Real, Long Int	Polling
SP-T4	Pulse Counters	I, O, S, V, M, C	Bits, Hex, Real, Long Int	Polling
SP-T5	Object Commands	I, O, S, V, M, C	Bits, Hex, Real, Long Int	NA
SP-T6	Double Commands	I, O, S, V, M, C	Bits, Hex, Real, Long Int	NA
SP-T7	Analog Outputs	I, O, S, V, M, C	Bits, Hex, Real, Long Int	NA

Courier Type Details			
Courier types	**Type Details**	**Supported Data Formats**	**Update Methods**
CR-T1	Single Indications	NA	Polling , Events , polling & events
CR-T2	Double Indications	NA	Polling , Events , polling & events
CR-T3	Analog Inputs	UnsignedInteger (1Byte) – 24H UnsignedInteger (2Bytes) – 25H UnsignedInteger (4Bytes) – 26H SignedInteger (1Byte) – 28H SignedInteger (2Bytes) – 29H SignedInteger (4Bytes) – 2AH CourierNumber (4Bytes) – 2CH Extended Courier (6Bytes) --30 H IEEE floating Format (4Bytes)--34 H	Polling
CR-T4	Single Commands	Indexed String Courier Number	NA
CR-T5	Double Commands	Indexed String Courier Number Two bits setting command	NA
CR-T6	Analog Outputs	UnsignedInteger (1Byte) – 24H UnsignedInteger (2Bytes) – 25H UnsignedInteger (4Bytes) – 26H SignedInteger (1Byte) – 28H SignedInteger (2Bytes) – 29H SignedInteger (4Bytes) – 2AH CourierNumber (4Bytes) – 2CH Extended Courier (6Bytes) --30 H IEEE floating Format (4Bytes)--34 H	NA