SIA-B Specific CT´s

Self & Dual Powered Overcurrent & Earth Fault Protection Relay

SELF POWERED

MODBUS RTU PROTOCOL MANUAL

1. MODBUS RTU PROTOCOL

This document describes the steps to follow to read and write data on the SIA-B relay, as per the ModBus/RTU protocol. The memory map is described further on.

The standard ModBus/RTU protocol is used, so any program or PC can communicate easily with the equipment.

The SIA-B always acts as a slave, which means that it never initiates communications. The master is always responsible for initiating communications.

Only a subset of the ModBus/RTU functions is implemented:

- Reading function 3.
- Writing function 16.

The ModBus/RTU protocol is independent from the hardware. Therefore, the physical layer can exist in different hardware configurations: RS232, RS485, fiber optic or Ethernet.

Specifically, the relay has a front USB emulating a RS232 port with a “half-duplex” data stream.

Each byte of data is transmitted asynchronously and is made up of 1 start bit, 8 data bits, 1 stop bit and 1 parity bit, if this is how it is programmed. Therefore, the data has 10 or 11 bits, depending on whether or not it includes parity.

The address of the single front port can be configured but the rest of the parameters are fixed: the speed is 19200, without parity and with 1 stop bit.

The master must know the address of the slave that it is going to communicate with. No unit will act on requests from the master if the message is not addressed to them. The exception is when the 0 address, or “broadcast” address, is used, in which case the relay will act but will not send an answer of any type.

Communications are made in packages or frames, which are groups of data that are sent asynchronously. The master transmits a frame to the slave, and the slave then replies with another frame (except in the case of “broadcast” messages).

The end of the frame is marked by a dead time or silence time in the communication medium. The length of this time of silence varies depending on the transmission speed, as it is equivalent to 3 characters.

The following table shows the generic package format that is valid for transmission and reception. However, each function has its own peculiarities, as will be described further on.

1.1. ModBus packaged format

CUSTOMER ADDRESS	1 byte	Each device on a communication bus must have a unique address, otherwise two different units could reply simultaneously to the same request. All ports of the relay will use this address which can be set a value between 1 and 247. When the master transmits a frame with the slave address to 0 indicates a Broadcast. All the slaves in the communications bus will carry out the requested action, but no one will reply to the master. The Broadcast will only be accepted to write, as it makes no sense to make a read request in the Broadcast, as no one will reply this request.
FUNCTION CODE	1 byte	This is one of the function codes supported by the equipment. In this case, the only function codes supported are 3 to read and 16 to write. When the slave has to reply with an exception one of these frames, it is indicated by putting 1 in the most important bit of the correspondent function. Thus, an exception for the function 3 will be indicated with a 83 as a function code; and an exception for the function code 16 or 0x10 in hexadecimal, will be indicated with an 0x90.
DATA	N bytes	This part consists of a variable number of bytes, depending on the function code. It may include: addresses, data lengths, settings, commands or exception codes sent by the user.
CRC	2 bytes	Control code of two bytes. The ModBus/RTU includes a 16 bit CRC in each frame, to detect errors. If the slave detects an erroneous frame, based on a CRC that is not correct, it won't take any action, nor will reply anything to the master. The management of the CRC is LSB-MSB.
DEAD TIME	Necessary time to transmit 3,5 Bytes	A frame is terminated when nothing is received for a period of 3,5 bytes. It means: 15 ms at 2400 bps 2 ms at 19200 bps ...etc.

1.2. Function codes

HEX DEC CODE	MODBUS NAME	DEFINITION	COMMENT
0x03 3	Read Holding Registers	Reading of Any Value	This function allows the master to read 1 or more consecutive addresses of a relay. The registers always are of 16 bits, with the most important byte at first. The maximum number of registers to be read in a package is 60.
0x10 16	Preset Multiple Registers	Script	This function allows writing one or more registers that represent one or more settings. The registers are values of 2 bytes of length, transmitted with the most important byte at first. The maximum number of register to be written in a package is 60.

1.3. Exceptions responses

The error codes defined by the ModBus protocol are as follows:

01	**ILLEGAL FUNCTION**	The slave does not support any function with the function code received in this message.
02	**ILLEGAL DATA ADDRESS**	The master is trying to do an operation in a wrong address.
03	**ILLEGAL DATA VALUE**	The slave has detected that the value sent by the master is not valid.
04	**SLAVE DEVICE FAILURE**	Indicates an error occurred in the slave while trying to execute the request of the master.
05	**ACKNOWLEDGE**	Generic recognition.
06	**SLAVE DEVICE BUSY**	The slave is busy and unable to perform the required operation.
07	**NEGATIVE ACKNOWLEDGE**	Generic non-recognition.

1.4. Data type

TYPE	LENGTH	DESCRIPTION
UCHAR	1/2	Integer without sign of 1 byte
BYTE	1/2	Integer with sign of 1 byte
BIT16	1	Gathered bits type, groups of 16. E. g.: 0x1A41 = 0001101001000001b
BIT32	2	Gathered bits type, groups of 32.
ENUM	1	Integer without sign of 16 bits. Each of the values that the integer can be will have a correspondence in the auxiliary list of the database. I this list is the correspondence chain which must be shown for each of the values. Memory will only receive an integer value. E. g.: 0, 1 Correspondence to “CLOSED”, “OPEN”
DENUM	2	Integer without sign of 32 bits
UINT	1	Integer without sign of 2 bytes
INT	1	Integer with sign of 2 bytes
LONG	2	Integer without sign of 4 bytes
FLOAT	2	Number in floating decimal point “Float” of 4 bytes
ASCIIxx	xx/2	String: Length variable character chain. Final of String marked with ‘\0’. E. g.: “ABC” 0x41x42x43x00....
FH	5	Year(UINT).month(UCHAR).day(UCHAR).hour(UCHAR).minutes(UCHAR).seconds(UCHAR).hundredth(UCHAR).thousandth(UINT)
EVENT2	10	Criteria Directory (UINT), Event Identifier (UINT), Value (UINT), Associated Measure (float), Date and Time (FH)
EVENTO2	11	Antiquity (UINT), Event (EVENT2)

When a data format takes up more than 1 byte, it is always sent, firstly the most significant BYTE and lastly the lowest significant BYTE by communications.

DENUMCURVE	0	IEC 60255-151 inverse
	1	IEC 60255-151 very inverse
	2	IEC 60255-151 extremely inverse
	3	Definite time
DENUM 5060Hz	0	60Hz
	1	50Hz
DENUM NOYES	0	NO
	1	YES
DENUMBAUD	0	4800 bauds
	1	9600 bauds
	2	19200 bauds
	3	38400 bauds
DENUM LANGUAGE	0	English
	1	Spanish
	2	Depending on model
DENUM TRIPVOLT	0	12 Vdc
	1	17 Vdc
	2	22 Vdc
	3	24 Vdc

1.5. General Memory map

Function	Description	Start address	Number of registries	Format	
16	Write the Directory of Event	1	1	UINT	
16	Write the number of the Setting List	6	1	UNIT	
03	Read of Model and Version	100	44	ASCII88	
16	Write access code	168	2	UCHAR4	See Passwords and Access Levels
03 and 16	Date and Time	170	5	FH	
16	Selection of Command	200	1	UINT	See commands map
16	Confirmation of Command	201	1	UINT	See commands map
03	Serial number	252	2	LONG	
03	Equipment identifier	254	44	ASCII88	
03	Read and Delete the oldest Event	400	11	EVENTO2	See events list
03	One event reading	410	11	EVENTO2	See events list
16	Delete All Events	420	1	dummy	
16	Write fault report index	8000	1	16	Write fault report index
16	Write event index from a fault report	8002	1	16	Write event index from a fault report
03	Fault report reading	8123	11	03	Fault report reading

1.5.1. States Map

The function code implemented to State reading is is 0x03 (Read Holding Registers)

The number of registries for all states is 2.

Address	Description	Bit	Event NO	Status	Associated Measurement
500	General	00	1	Trip	Imax (A)
		01	2	External Trip	-
		02	6	No Trip Power	-
		03	7	50 Hz	-
		04	8	Trip Block Enable	-

		05	16	Measure Error	-
		06	17	Ready	1: Vaux power 2: Self-powering 4: USB power
		07	19	Settings Changed	-
		08	21	Set Date/Time	-
		09	22	Local Communication	-
		10	23	Factory Settings	-
		11	24	EEPROM Error	-
		12	28	EEPROM Changed	-
		13	32	Events Error	-
		15	15	Reset	-
		16	49	Pickup (*)	Imax (A)
		-	30	New DFR	DFR number
		-	46	Identification	-
		-	48	Events Erased	-

Address	Description	Bit	Event NO	Status	Associated Measurement
502	Local COM	00		Local communication	
		01		HMI Activity	
		25	8	Reset thermal image	

Address	Description	Bit	Event NO	Status	Associated Measurement
504	50	00	01	50 Phase A Pickup	IA (A)
		01	02	50 Phase B Pickup	IB (A)
		02	03	50 Phase C Pickup	IC (A)
		03	04	50 Pickup	Imax (A)
		09	05	50 Phase A Trip	IA (A)
		10	06	50 Phase B Trip	IB (A)
		11	07	50 Phase C Trip	IC (A)
		12	08	50 Trip	Imax (A)

Address	Description	Bit	Event NO	Status	Associated Measurement
506	50/51	00	01	51 Phase A Pickup	IA (A)
		01	02	51 Phase B Pickup	IB (A)
		02	03	51 Phase C PIckup	IC (A)
		03	04	51 Pickup	Imax (A)
		08	05	51 Phase A Trip	IA (A)
		09	06	51 Phase B Trip	IB (A
		10	07	51 Phase C Trip	IC (A)
		11	08	51 Trip	Imax (A)

Address	Description	Bit	Event NO	Status	Associated Measurement
508	50N	04	01	50N Pickup	IN (A)
		12	02	50N Trip	IN (A)

Address	Description	Bit	Event NO	Status	Associated Measurement
510	50/51N	04	01	51N Pickup	IN (A)
		12	02	51N Trip	IN (A)

Address	Description	Bit	Event NO	Status	Associated Measurement
512	Inputs	00	17	Input 1	-

Address	Description	Bit	Event NO	Status	Associated Measurement
514	Outputs	03	01	Trip Output	-
		04	02	Output 2 (*)	-
		05	03	Output 3 (*)	-

Address	Description	Bit	Event NO	Status	Associated Measurement
516	Trip Block (*)	00	01	Phase A Block	IA (A)
		01	02	Phase B Block	IB (A)
		02	03	Phase C Block	IC (A)
		03	04	Phase Block	Imax (A)

Address	Description	Bit	Event NO	Status	Associated Measurement
520	Remote Modbus (*)	00	-	Remote communication	None
		25	08	Reset thermal image	None

Address	Description	Bit	Event NO	Status	Associated Measurement
522	49 (*)	04	01	49 Alarm	Thermal Image (%)
		12	02	49 Trip	Thermal Image (%)

Address	Description	Bit	Event NO	Status	Associated Measurement
538	Leds	00	-	Led 1	-
		01	-	Led 2	-
		02	-	Trip Bistable (*)	-

1.5.2. Criteria Map

CRITERIA	IDENTIFIER
GENERAL	51202
MEASUREMENT	65284
LOCAL	63745
50P	12805
51P	13061
50G	38405
51G	38661
INPUTS	64770
OUTPUTS	65027
TRIP BLOCK	51713
REMOTE MODBUS	63746
49	12545
SHB	51715
SIGNALLING	64259
OSCILLOGRAFY	64517

1.5.3. Measurements Map

The number of registries for all states is 2.

Address	Description	Format
300	Phase A current IA	FLOAT INVERSE
302	Phase B current IB	
304	Phase C current IC	
306	Neutral current IN	
308	Thermal Image TI	
310	Maximum phase current IMAX	

1.6. Settings Map

Settings	Address	Description	Format	Enumeration
General	600 **(*)**	Identification	ASCII20	-
	800 **(**)**			
	610 **(*)**	Frequency	DENUM	0 → 60 Hz 1 → 50 Hz
	810 **(**)**			
	612 **(*)**	Serial Number	LONG	-
	812 **(**)**			
	614 **(*)**	Language	DENUM	0 → English 1 → Spanish 2 → Depends on relay model
	814 **(**)**			
	616 **(*)**	Active Setting Group	LONG	-
	816 **(**)**			
	(#) 690 **(*)**	CT Accuracy	DENUM	0 → Epoxi 1 → Taped
	(#) 890 **(**)**			
	618 **(*)**	Trip Voltage Level	DENUM	0 → 12 VDC 1 → 17 VDC 2 → 22 VDC 3 → 24 VDC
	818 **(**)**			
	620 **(*)**	Nominal Current	FLOAT INVERSE	-
	820 **(**)**			
	622 **(*)**	CT Type	FLOAT INVERSE	-
	822 **(**)**			
	626 **(*)**	Password		-
	826 **(**)**			
	624 **(*)**	Local COM Address	LONG	-
	824 **(**)**			
	676 **(*)**	Remote COM Address	LONG	
	876 **(**)**			
	678 **(*)**	Remote Baud Rate	DENUM	0 → 4800 Bd 1 → 9600 Bd 2 → 19200 Bd 3 → 38400 Bd
	878 **(**)**			

(*) Read/Write Address (FC = 03 / 16).
(**) Address for Confirmation (FC = 16)
(#) Only for firmware versión 2.10 and above.

Settings	Address	Description	Format	Enumeration
50	630 **(*)**	Function Enable	DENUM	0 → Disable 1 → Enable 2 → SHB
	830 **(**)**			
	632 **(*)**	Tap	FLOAT INVERSE	-
	832 **(**)**			
	634 **(*)**	Time Delay	FLOAT INVERSE	-
	834 **(**)**			

Settings	Address	Description	Format	Enumeration
51	636 **(*)**	Function Enable	DENUM	0 → Disable 1 → Enable 2 → SHB
	836 **(**)**			
	638 **(*)**	Curve Type	DENUM	0 → IEC Inverse 1 → IEC Very Inverse 2 → IEC Extremely Inverse 3 → Defined Time 4 → IEEE Inverse 5 → IEEE Very Inverse 6 → IEEE Extremely Inverse 7 → IEC Long Time Inverse
	838 **(**)**			
	640 **(*)**	Time Dial (TMS)	FLOAT INVERSE	-
	840 **(**)**			
	642 **(*)**	Tap	FLOAT INVERSE	-
	842 **(**)**			
	644 **(*)**	Time Delay	FLOAT INVERSE	-
	844 **(**)**			

Settings	Address	Description	Format	Enumeration
50N	646 **(*)**	Function Enable	DENUM	0 → Disable 1 → Enable 2 → SHB
	846 **(**)**			
	648 **(*)**	Tap	FLOAT INVERSE	-
	848 **(**)**			
	650 **(*)**	Time Delay	FLOAT INVERSE	-
	850 **(**)**			

(*) Read/Write Address (FC = 03 / 16).
(**) Address for Confirmation (FC = 16)

Settings	Address	Description	Format	Enumeration
51N	652 **(*)**	Function Enable	DENUM	0 → Disable 1 → Enable 2 → SHB
	852 **(**)**			
	654 **(*)**	Curve Type	DENUM	0 → IEC Inverse 1 → IEC Very Inverse 2 → IEC Extremely Inverse 3 → Defined Time 4 → IEEE Inverse 5 → IEEE Very Inverse 6 → IEEE Extremely Inverse 7 → IEC Long Time Inverse
	854 **(**)**			
	656 **(*)**	Time Dial (TMS)	FLOAT INVERSE	-
	856 **(**)**			
	658 **(*)**	Tap	FLOAT INVERSE	-
	858 **(**)**			
	660 **(*)**	Time Delay	FLOAT INVERSE	-
	860 **(**)**			

Settings	Address	Description	Format	Enumeration
49	662 **(*)**	Function Enable	DENUM	0 → Disable 1 → Enable
	862 **(**)**			
	664 **(*)**	Tap	FLOAT INVERSE	-
	864 **(**)**			
	666 **(*)**	Heating Constant τ	LONG	-
	866 **(**)**			
	668 **(*)**	Cooling Constant	LONG	-
	868 **(**)**			
	670 **(*)**	Alarm Level	LONG	-
	870 **(**)**			

Settings	Address	Description	Format	Enumeration
Trip Block	672 **(*)**	Function Enable	DENUM	0 → Disable 1 → Enable
	872 **(**)**			
	674 **(*)**	Tap	FLOAT INVERSE	-
	874 **(**)**			

(*) Read/Write Address (FC = 03 / 16).
(**) Address for Confirmation (FC = 16)

1.7. Commands Map

10	Reset thermal image

1.8. Examples

Each state is made up of 32 bits. The bits from 00 to 15 will be shown in the odd adrees and the bits from 16 to 32 in the even address.

The criterion is to show from the MSB to the LSB (BIGENDIAN criterion)

1.8.1. Modbus frame

Writing the access password “5555” to equipment no. 1

Address	Function	H Pickup Address	L Pickup Address	Number of H Registers	Number of L Registers	Number of Bytes	Password	Checksum H	Checksum L
0x01	0x10	0x00	0xA8	0x00	0x02	0x04	0x35 0x35 0x35 0x35	0x30	0xF4

And the SIA-B will reply OK:

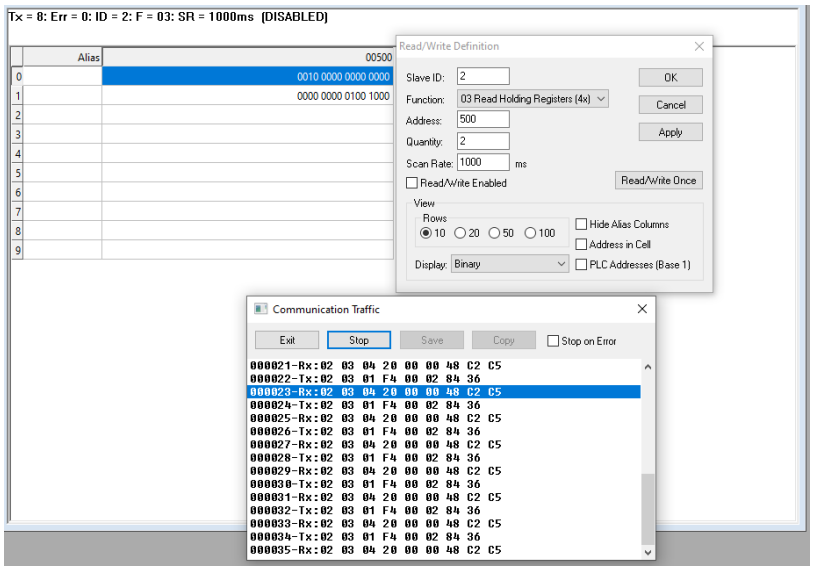
Address	Function	H Pickup Address	L Pickup Address	Number of H Registers	Number of L Registers	Checksum H	Checksum L
0x01	0x10	0x00	0xA8	0x00	0x02	0xC0	0x28

1.8.2. States reading

GENERAL STATES→Address 500: BIT32 (2 registers):

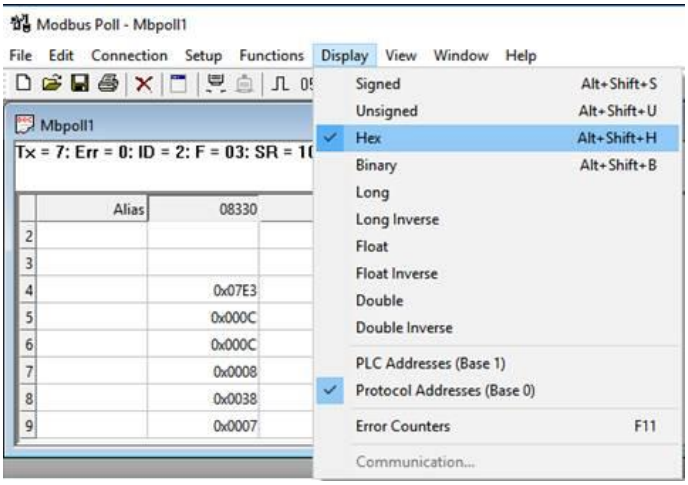
Address 501 will show the first 16 bits:

Address	Description	Bit	Event NO	Status	Associated Measurement
500	General	00	1	Trip	Imax (A)
		01	2	External Trip	-
		02	6	No Trip Power	-
		03	7	50 Hz	-
		04	8	Trip Block Enable	-
		05	16	Measure Error	-
		06	17	Ready	1: Vaux power 2: Self-powering 4: USB power
		07	19	Settings Changed	-
		08	21	Set Date/Time	-
		09	22	Local Communication	-
		10	23	Factory Settings	-
		11	24	EEPROM Error	-
		12	28	EEPROM Changed	-
		13	32	Events Error	-
		15	15	Reset	-
		16	49	Pickup (*)	Imax (A)
		-	30	New DFR	DFR number
		-	46	Identification	-
		-	48	Events Erased	-



1.8.3. Fault report reading

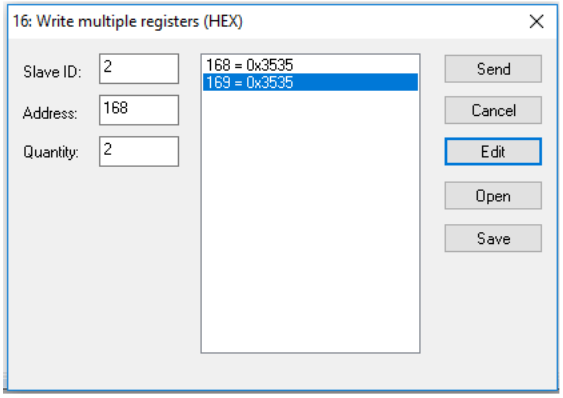
- First, it is important to select the correct format before proceeding. The format must be in HEX:



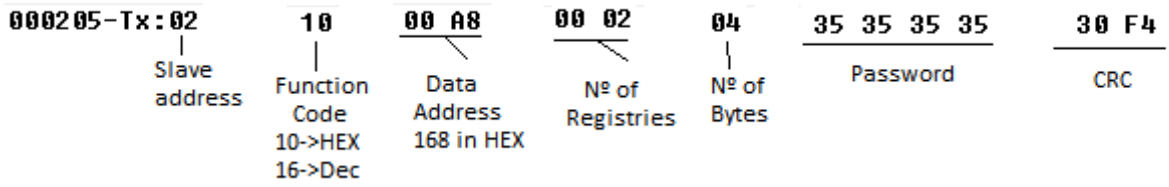
- Start the session: using the function 16 (write) enter the password, address 168 and 2 registers:

Function¤	Description¤	Start·address¤	Number·of·registries¤	Format¤	Reference¤
16¤	Write·the·Directory·of·Event¤	1¤	1¤	UINT¤	¤
16¤	Load·data·Profiling¤	2¤	1¤	¤	¤
16¤	Write·the·number·of·the·Setting·List¤	6¤	1¤	UINT¤	¤
03¤	Read·of·Model·and·Version¤	100¤	44¤	ASCII88¤	¤
16¤	Write·access·code¤	168¤	2¤	UCHAR4¤	See·Passwords·and·Access·Levels¤

The password “5555” must be entered in HEX → 0x3535 0x3535

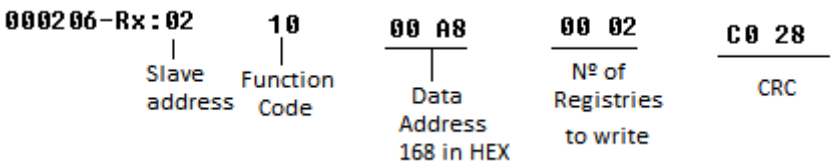


- **Request**



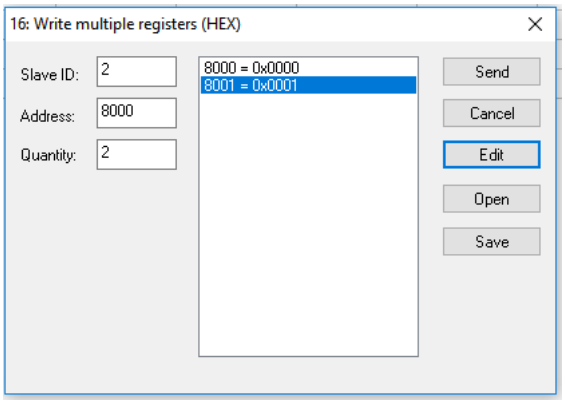
00 A8 is in HEX, so translated to DEC is 168.

- **Response:**

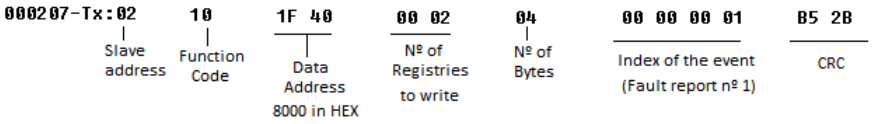


- rite the fault report index you want to read, (the newest fault report has the index number one):

Function	Description	Start address	Number of registries	Format	Reference
16	Write fault report index	8000	2		

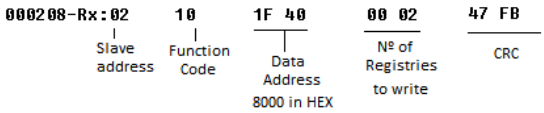


- **Request:**



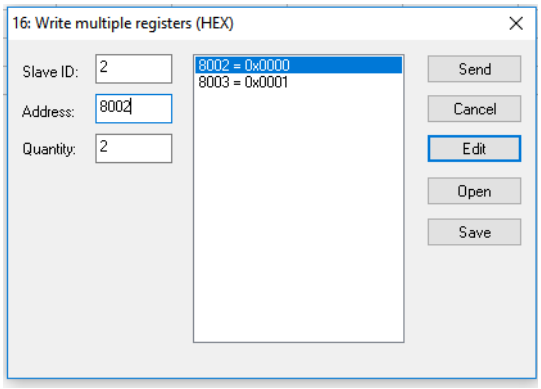
1F 40 is in HEX, so translated to DEC is 8000.

- **Response:**



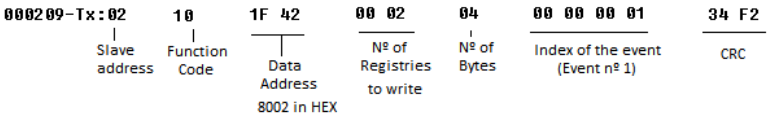
- Write the event index from which you want to start reading:

Function	Description	Start address	Number of registries	Format	Reference
16	Write event index from a fault report	8002	2		



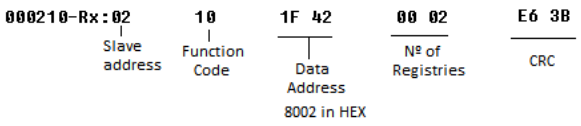
Here we will start reading from the first event

- **Request:**



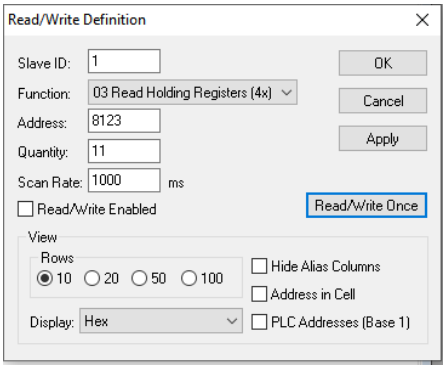
1F 42 is in HEX, so translated to DEC is 80002

- **Response:**

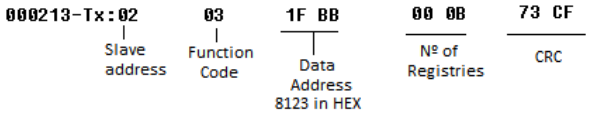


- Read the event you have selected in the previous step with function 3 (read holding register), address 8123 and 11 registers:

Function	Description	Start address	Number of registries	Format	Reference
03	Read event from a fault report	8123	11	EVENTO2	

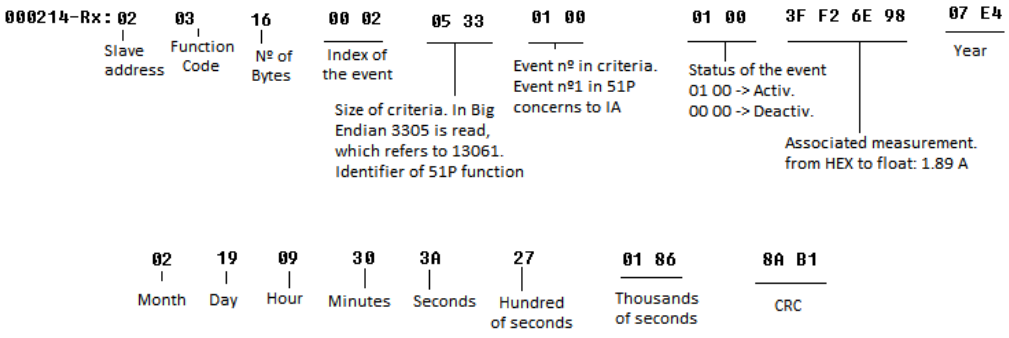


Request:



1F BB in HEX translated to DEC is 8123.

- **Response:**



*To check which value refers to event nº 1 inside the 51P, check the data in states map:

Address¤	Description¤	Bit¤	Event·NO¤	Status¤	Associated·Measurement¤	Format¤
506¤	51¤	00¤	01¤	51·Phase·A·Pickup¤	IA·(A)¤	BIT32¤
		01¤	02¤	51·Phase·B·Pickup¤	IB·(A)¤	
		02¤	03¤	51·Phase·C·Pickup¤	IC·(A)¤	
		03¤	04¤	51·Pickup¤	Imax·(A)¤	
		08¤	05¤	51·Phase·A·Trip¤	IA·(A)¤	
		09¤	06¤	51·Phase·B·Trip¤	IB·(A¤	
		10¤	07¤	51·Phase·C·Trip¤	IC·(A)¤	
		11¤	08¤	51·Trip¤	Imax·(A)¤	

1.8.4. Time and Date synchronization

The relay has two addresses available for synchronizing the date and time. The following considerations must be considered before synchronizing:

- Only dates from 1 January 2000 00:00:01 onwards are accepted.
- When synchronizing from rear communications, the relay must be on remote mode. Touching the HMI or communicating from the local port will put the relay on local mode for 5 minutes.
- to perform the synchronization it is necessary to log in (address 168)

Address 170 (FH Type)

Address 170 accepts date and time without translating to UNIX.

The FH type contains the following data:

Year(UINT).*month*(UCHAR).*day*(UCHAR).*hour*(UCHAR).*minutes*(UCHAR).*seconds*(UCHAR).*hundredth*(UCHAR).*thousandth*(UINT)

Example:

09/02/2021 09:57:10 am (UTC)

Address 170 to 175 allows big endian format, as follows:

	Value	HEX	REGISTER ADDRESS	REGISTER VALUE (HEX)	REGISTER VALUE (DEC)
Year (2 bytes)	2021	07E5	170	0x07E5	2021
Month (1 byte)	09	09	171	0x0902	2306
Day (1 byte)	02	02			
Hour (1 byte)	09	09	172	0x0939	2361
Minutes (1 byte)	57	39			
Seconds (1 byte)	10	0A	173	0x0A00	2560
hundredths of a second (1 byte)	00	00			
thousandths of a second (2 bytes)	0000	0000	174	0x0000	0000

Bizkaia Technology Park

Building, 604

Derio, 48160 Bizkaia SPAIN

T. +34 94 471 14 09

fanox@fanox.com

www.fanox.com

www.fanox.com