SmartHEMS
V100R024C00

MODBUS Interface Definitions

Issue	01
Date	2024-07-15

HUAWEI DIGITAL POWER TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Digital Power Technologies Co., Ltd. and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.
The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Digital Power Technologies Co., Ltd.

Address: Huawei Digital Power Antuoshan Headquarters
Futian, Shenzhen 518043
People's Republic of China

Website: https://digitalpower.huawei.com

Contents

1 Change History....1

2 Introduction....2

2.1 Terms and Abbreviations....2

2.2 System Requirements....3

3 Register Definitions....4

3.1 Register Definitions for the EMMA....4

3.2 Register Definitions for an External Smart Meter (If Connected)....18

3.3 Register Definitions for a Charger....20

3.4 Register Definitions for the SUN2000....21

3.5 Public Register Definitions....21

4 Overview of the Communications Protocol....23

4.1 Physical Layer....23

4.2 Data Link Layer....23

4.2.1 Addressing Mode....23

4.2.2 Frame Structure....23

4.2.3 Data Encoding....25

4.2.4 Interaction Process....25

4.3 Application Layer....25

4.3.1 Function Code List....25

4.3.2 Exception Code List....25

4.3.3 Reading Registers (0x03)....27

4.3.3.1 Frame Format of a Request from a Master Node....27

4.3.3.2 Frame Format of a Normal Response from a Slave Node....27

4.3.3.3 Frame Format of an Abnormal Response from a Slave Node....28

4.3.3.4 Examples....28

4.3.4 Writing into a Single Register (0x06)....29

4.3.4.1 Frame Format of a Request from a Master Node....29

4.3.4.2 Frame Format of a Normal Response from a Slave Node....29

4.3.4.3 Frame Format of an Abnormal Response from a Slave Node....29

4.3.4.4 Examples....29

4.3.5 Writing into Multiple Registers (0x10)....30

4.3.5.1 Frame Format of a Request from a Master Node....30

4.3.5.2 Frame Format of a Normal Response from a Slave Node........ 31
4.3.5.3 Frame Format of an Abnormal Response from a Slave Node........ 31
4.3.5.4 Examples........ 31
4.3.6 Reading Device Identifiers (0x2B)........ 33
4.3.6.1 Command for Querying Device Identifiers........ 34
4.3.6.2 Command for Querying a Device List........ 35
4.3.6.3 Device Description Definitions........ 36
5 Reference Documents........ 38

1 Change History

Issue	Date	Description
01	2024-07-15	The issue is the first official release.

2 Introduction

2.1 Terms and Abbreviations

Table 2-1 Terms and abbreviations

Name	Description
Master node	During master-slave communication, the party that initiates a communication request is referred to as the master node.
Slave node	During master-slave communication, the party that responds to a communication request is referred to as the slave node.
Broadcast address	Fixed to **0**.
Register address	Recorded in two bytes.
U16	16-bit unsigned integer
U32	32-bit unsigned integer
U64	64-bit unsigned integer
I16	16-bit signed integer
I32	32-bit signed integer
I64	64-bit signed integer
STR	Character string
MLD	Multiple bytes
N/A	Not applicable

2.2 System Requirements

Applicable model: EMMA

Firmware version:

SmartHEMS V100R024C00SPC100 or later

3 Register Definitions

3.1 Register Definitions for the EMMA

NOTE

The operation object of the following registers is the EMMA. In the communications protocol, the logical device ID is fixed to 0.

Table 3-1 Register definitions

Category	Signal Name	Read/Write (R/W)	Type	Unit	Gain	Register Address	Quantity	Default Value	Range
Characteristic data	Offering name	RO	STR	N/A	N/A	30000	15		
Characteristic data	SN	RO	STR	N/A	N/A	30015	10		
Characteristic data	Software version	RO	STR	N/A	N/A	30035	15		

Category	Signal Name	Read/Write (R/W)	Type	Unit	Gain	Register Address	Quantity	Default Value	Range
Characteristic data	Model	RO	STR	N/A	N/A	30222	20		
Sampled data	Inverter total absorbed energy	RO	U64	kWh	100	30302	4		
Sampled data	Energy charged today	RO	U32	kWh	100	30306	2		
Sampled data	Total charged energy	RO	U64	kWh	100	30308	4		
Sampled data	Energy discharged today	RO	U32	kWh	100	30312	2		
Sampled data	Total discharged energy	RO	U64	kWh	100	30314	4		
Sampled data	ESS chargeable energy	RO	U32	kWh	1000	30318	2		
Sampled data	ESS dischargeble energy	RO	U32	kWh	1000	30320	2		
Sampled data	Rated ESS capacity	RO	U32	kWh	1000	30322	2		
Sampled data	Consumption today	RO	U32	kWh	100	30324	2		
Sampled data	Total energy consumption	RO	U64	kWh	100	30326	4		
Sampled data	Feed-in to grid today	RO	U32	kWh	100	30330	2		

Category	Signal Name	Read/Write (R/W)	Type	Unit	Gain	Register Address	Quantity	Default Value	Range
Sampled data	Total feed-in to grid	RO	U64	kWh	100	30332	4		
Sampled data	Supply from grid today	RO	U32	kWh	100	30336	2		
Sampled data	Total supply from grid	RO	U64	kWh	100	30338	4		
Sampled data	Inverter energy yield today	RO	U32	kWh	100	30342	2		
Sampled data	Inverter total energy yield	RO	U32	kWh	100	30344	2		
Sampled data	PV yield today	RO	U32	kWh	100	30346	2		
Sampled data	Total PV energy yield	RO	U64	kWh	100	30348	4		
Sampled data	PV output power	RO	U32	kW	1000	30354	2		
Sampled data	Load power	RO	U32	kW	1000	30356	2		
Sampled data	Feed-in power	RO	I32	kW	1000	30358	2		
Sampled data	Battery charge/discharge power	RO	I32	kW	1000	30360	2		
Sampled data	Inverter rated power	RO	U32	kW	1000	30362	2		

Category	Signal Name	Read/Write (R/W)	Type	Unit	Gain	Register Address	Quantity	Default Value	Range
Sampled data	Inverter active power	RO	I32	kW	1000	30364	2		
Sampled data	SOC	RO	U16	%	100	30368	1		
Sampled data	ESS chargeable capacity	RO	U32	kWh	1000	30369	2		
Sampled data	ESS dischargeable capacity	RO	U32	kWh	1000	30371	2		
Sampled data	Backup power SOC	RO	U16	%	100	30373	1		
Sampled data	Yield this month	RO	U32	kWh	100	30380	2		
Sampled data	Monthly energy consumption	RO	U32	kWh	100	30382	2		
Sampled data	Monthly feed-in to grid	RO	U32	kWh	100	30384	2		
Sampled data	Yield this year	RO	U32	kWh	100	30386	2		
Sampled data	Annual energy consumption	RO	U32	kWh	100	30388	2		
Sampled data	Yearly feed-in to grid	RO	U32	kWh	100	30390	2		
Sampled data	Monthly supply from grid	RO	U32	kWh	100	30394	2		

Category	Signal Name	Read/Write (R/W)	Type	Unit	Gain	Register Address	Quantity	Default Value	Range
Sampled data	Yearly supply from grid	RO	U32	kWh	100	30396	2		
SmartGuard	Backup time notification threshold	RO	U16	min	1	30406	1		
Sampled data	Energy charged this month	RO	U32	kWh	100	30407	2		
Sampled data	Energy discharged this month	RO	U32	kWh	100	30409	2		
Device management	Number of inverters found	RO	U16	N/A	N/A	30801	1		
Device management	Number of chargers found	RO	U16	N/A	N/A	30804	1		
Device management	Subdevice presence flag	RO	Bitfield32	N/A	N/A	30811	2		Bit 0: SmartGuard
Time management	DST state	RO	U16	N/A	N/A	31002	1		0: DST not started 1: DST started

Category	Signal Name	Read/Write (R/W)	Type	Unit	Gain	Register Address	Quantity	Default Value	Range
Time management	Local time	RO	U32	N/A	N/A	31003	2		
WiFi management	WiFi-STA signal strength	RO	UINT 16	NA	NA	31135	1		[0,4] 0: no signal
Meter management	Phase A voltage of built-in electric energy sensor	RO	U32	V	100	31639	2		
Meter management	Phase B voltage of built-in electric energy sensor	RO	U32	V	100	31641	2		
Meter management	Phase C voltage of built-in electric energy sensor	RO	U32	V	100	31643	2		
Meter management	A-B line voltage of built-in electric energy sensor	RO	U32	V	100	31645	2		
Meter management	B-C line voltage of built-in electric energy sensor	RO	U32	V	100	31647	2		

Category	Signal Name	Read/Write (R/W)	Type	Unit	Gain	Register Address	Quantity	Default Value	Range
Meter management	C-A line voltage of built-in electric energy sensor	RO	U32	V	100	31649	2		
Meter management	Phase A current of built-in electric energy sensor	RO	I32	A	10	31651	2		
Meter management	Phase B current of built-in electric energy sensor	RO	I32	A	10	31653	2		
Meter management	Phase C current of built-in electric energy sensor	RO	I32	A	10	31655	2		
Meter management	Active power of built-in electric energy sensor	RO	I32	kW	1000	31657	2		
Meter management	Power factor of built-in electric energy sensor	RO	I32	N/A	1000	31661	2		

Category	Signal Name	Read/Write (R/W)	Type	Unit	Gain	Register Address	Quantity	Default Value	Range
Meter management	Apparent power of built-in electric energy sensor	RO	I32	kVA	1000	31663	2		
Meter management	Phase A active power of built-in electric energy sensor	RO	I32	kW	1000	31665	2		
Meter management	Phase B active power of built-in electric energy sensor	RO	I32	kW	1000	31667	2		
Meter management	Phase C active power of built-in electric energy sensor	RO	I32	kW	1000	31669	2		
Meter management	Total active energy of built-in electric energy sensor	RO	I64	kWh	100	31671	4		
Meter management	Total negative active energy of built-in electric energy sensor	RO	I64	kWh	100	31679	4		

Category	Signal Name	Read/Write (R/W)	Type	Unit	Gain	Register Address	Quantity	Default Value	Range
Meter management	Total positive active energy of built-in electric energy sensor	RO	I64	kWh	100	31687	4		
Meter management	Phase A voltage of external electric energy sensor	RO	U32	V	10	31895	2		
Meter management	Phase B voltage of external electric energy sensor	RO	U32	V	10	31897	2		
Meter management	Phase C voltage of external electric energy sensor	RO	U32	V	10	31899	2		
Meter management	A-B line voltage of external electric energy sensor	RO	U32	V	10	31901	2		
Meter management	B-C line voltage of external electric energy sensor	RO	U32	V	10	31903	2		

Category	Signal Name	Read/Write (R/W)	Type	Unit	Gain	Register Address	Quantity	Default Value	Range
Meter management	C-A line voltage of external electric energy sensor	RO	U32	V	10	31905	2		
Meter management	Phase A current of external electric energy sensor	RO	I32	A	100	31907	2		
Meter management	Phase B current of external electric energy sensor	RO	I32	A	100	31909	2		
Meter management	Phase C current of external electric energy sensor	RO	I32	A	100	31911	2		
Meter management	Active power of external electric energy sensor	RO	I32	kW	1000	31913	2		
Meter management	Power factor of external electric energy sensor	RO	I32	N/A	1000	31917	2		

Category	Signal Name	Read/Write (R/W)	Type	Unit	Gain	Register Address	Quantity	Default Value	Range
Meter management	Apparent power of external electric energy sensor	RO	I32	kVA	1000	31919	2		
Meter management	Phase A active power of external electric energy sensor	RO	I32	kW	1000	31921	2		
Meter management	Phase B active power of external electric energy sensor	RO	I32	kW	1000	31923	2		
Meter management	Phase C active power of external electric energy sensor	RO	I32	kW	1000	31925	2		
Meter management	Total active energy of external electric energy sensor	RO	I64	kWh	100	31927	4		
Meter management	Total negative active energy of external electric energy sensor	RO	I64	kWh	100	31935	4		

Category	Signal Name	Read/Write (R/W)	Type	Unit	Gain	Register Address	Quantity	Default Value	Range
Meter management	Total positive active energy of external electric energy sensor	RO	I64	kWh	100	31943	4		
Battery control	ESS control mode	RW	ENUM16	N/A	N/A	40000	1	2: maximum self-consumption	1: reserved 2: maximum self-consumption 3: reserved 4: fully fed to grid 5: time of use 6: Third-party dispatch
Battery control	[Time of Use mode] Preferred use of surplus PV power	RW	ENUM16	N/A	N/A	40001	1	1: charge	0: fed to grid 1: charge
Battery control	[Time of Use mode] Maximum power for charging batteries from grid	RW	U32	kW	1000	40002	2	5	[0, 50.000]
Battery control	[Time of Use mode] Charge/Discharge time window	RW	MLD	N/A	N/A	40004	43		

Category	Signal Name	Read/Write (R/W)	Type	Unit	Gain	Register Address	Quantity	Default Value	Range
Limited feed-in	Power control mode at grid connection point	RW	ENUM16	NA	NA	40100	1	0: unlimited	0: unlimited 5: grid connected with zero power 6: limited feed-in (kW) 7: power-limited grid connected (%)
Limited feed-in	Limitation mode	RW	ENUM16	NA	NA	40101	1	0: total power	0: total power 1: single-phase power
Limited feed-in	Maximum grid feed-in power (kW)	RW	I32	kW	1000	40107	2	0	[–1, Pmax]
Limited feed-in	Maximum grid feed-in power (%)	RW	U16	%	10	40109	1	0	[0, 100.0]
Limited feed-in	Three-phase imbalance control	RW	ENUM16	NA	NA	40110	1	0	0: disabled; 1: enabled
Time management	System time	RW	U32	N/A	1	40470	2		

Category	Signal Name	Read/Write (R/W)	Type	Unit	Gain	Register Address	Quantity	Default Value	Range
Time management	Local time - year	RW	U16	N/A	1	40490	1		[2000,2068]
Time management	Local time - month	RW	U16	N/A	1	40491	1		[1,12]
Time management	Local time - day	RW	U16	N/A	1	40492	1		[1,31]
Time management	Local time - hour	RW	U16	N/A	1	40493	1		[0,23]
Time management	Local time - minute	RW	U16	N/A	1	40494	1		[0,59]
Time management	Local time - second	RW	U16	N/A	1	40495	1		[0,59]

Category	Signal Name	Read/Write (R/W)	Type	Unit	Gain	Register Address	Quantity	Default Value	Range
SmartGuard	Power supply configuration	RW	ENUM16	N/A	N/A	41214	1	0	0: none 1: mains only 2: mains + generator 3: generator only
SmartGuard	Consider mains to be faulty if	RW	ENUM16	N/A	N/A	41215	1	0	0: open 1: closed

3.2 Register Definitions for an External Smart Meter (If Connected)

NOTE

The operation object of the following registers is an external smart meter. If a built-in meter is used, the built-in registers of the EMMA are used.

The logical device ID in the communications protocol is set to the logical address of the device and can be queried by running the 2B command.

On the smart meter connected to the EMMA, a positive value indicates the power fed to the grid, and a negative value indicates the power supplied from the grid.

Table 3-2 Register definitions

Signal Name	Status	Read/Write (R/W)	Type	Unit	Gain	Register Address	Quantity	Default Value	Range
Running status	Valid	RO	ENUM16	N/A	N/A	30500	1		0: online 1: offline

Signal Name	Status	Read/Write (R/W)	Type	Unit	Gain	Register Address	Quantity	Default Value	Range
Phase A voltage	Valid	RO	U32	V	100	30502	2		
Phase B voltage	Valid	RO	U32	V	100	30504	2		
Phase C voltage	Valid	RO	U32	V	100	30506	2		
A-B line voltage	Valid	RO	U32	V	100	30508	2		
B-C line voltage	Valid	RO	U32	V	100	30510	2		
C-A line voltage	Valid	RO	U32	V	100	30512	2		
Phase A current	Valid	RO	I32	A	10	30514	2		
Phase B current	Valid	RO	I32	A	10	30516	2		
Phase C current	Valid	RO	I32	A	10	30518	2		
Active power	Valid	RO	I32	kW	1000	30520	2		
Power factor	Valid	RO	I32	N/A	1000	30524	2		
Apparent power	Valid	RO	I32	kVA	1000	30526	2		
Phase A active power	Valid	RO	I32	kW	1000	30528	2		
Phase B active power	Valid	RO	I32	kW	1000	30530	2		
Phase C active power	Valid	RO	I32	kW	1000	30532	2		
Total active energy	Valid	RO	I64	kWh	100	30534	4		

Signal Name	Status	Read/Write (R/W)	Type	Unit	Gain	Register Address	Quantity	Default Value	Range
Total negative active energy	Valid	RO	I64	kWh	100	30542	4		
Total positive active energy	Valid	RO	I64	kWh	100	30550	4		

3.3 Register Definitions for a Charger

NOTE

The operation object of the following registers is a Huawei's charger. The logical device ID in the communications protocol is set to the logical address of the device and can be queried by running the 2B command.

Table 3-3 Register definitions

Signal Name	Status	Read/Write (R/W)	Type	Unit	Gain	Register Address	Quantity	Default Value	Range
Offering name	Valid	RO	STR	NA	NA	30000	15		
ESN	Valid	RO	STR	NA	NA	30015	16		
Software version	Valid	RO	STR	NA	NA	30031	16		
Rated power	Valid	RO	U32	kW	10	30076	2		[0,100]
Charger model	Valid	RO	STR	NA	NA	30078	14		
Bluetooth name	Valid	RO	STR	NA	NA	30094	16		
Phase A voltage	Valid	RO	U32	V	10	30500	2		[0,800]

Signal Name	Status	Read/Write (R/W)	Type	Unit	Gain	Register Address	Quantity	Default Value	Range
Phase B voltage	Valid	RO	U32	V	10	30502	2		[0,800]
Phase C voltage	Valid	RO	U32	V	10	30504	2		[0,800]
Total energy charged	Valid	RO	U32	kWh	1000	30506	2		
Charger temperature	Valid	RO	I32	°C	10	30508	2		[–100,+200]

3.4 Register Definitions for the SUN2000

NOTE

Note: The operation object of the following registers is the SUN2000 inverter. In the communications protocol, the logical device ID is set to the RS485 address of the inverter.

For details about the register definitions, see the description of the SUN2000 VXXXRXXXCXX Modbus interface definitions.

3.5 Public Register Definitions

All types of devices connected to the EMMA must support public registers provided by the EMMA.

Table 3-4 Register definitions

Signal Name	Read/Write (R/W)	Type	Register Address	Quantity	Description
Active alarm SN	RO	U32	65500	2	Specifies the sequence number of an active alarm of the device; used for alarm synchronization on the management system.

Historical alarm SN	RO	U32	65502	2	Specifies the sequence number of a historical alarm of the device; used for alarm synchronization on the management system.
Device SN	RO	STR	65510	10	A unified top-level interface is provided for querying device ESNs. -- For a Huawei-developed device (such as inverter) that has an ESN, the HEMS reads the ESN of the inverter and copies it to the common register. -- For a third-party device (such as Shelly circuit breaker), that does not have an ESN, the HEMS automatically generates an ESN for the device.
Device alias	RW	STR	65524	10	Specifies the device name to be displayed to the user. -- The model information on the nameplates of the SmartGuard, HEMS, and inverter as the default values for these devices. -- The default value is **My Charging Pile** for a charger.
Device connection status	RO	U16	65534	1	A unified interface for device status query is provided to query the online and offline status of devices.

4 Overview of the Communications Protocol

4.1 Physical Layer

Communication through the Ethernet

Port number: 502

4.2 Data Link Layer

4.2.1 Addressing Mode

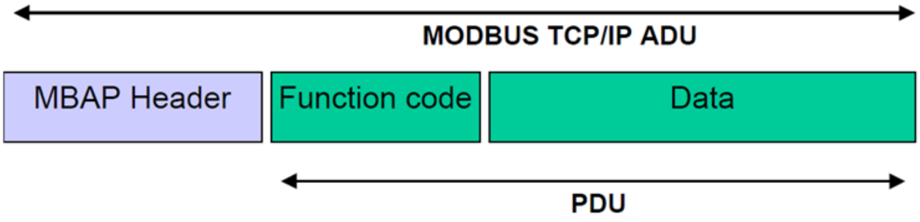
Logical addresses are used in Modbus-TCP data frames to distinguish devices. The following table describes the rules for allocating logical addresses.

NOTE

The address for device access is the RS485 address of the device, which can be read by running the 2B command on the EMMA.

EMMA Local Address	Slave Node Address	Reserved
0	1–247	248–255

4.2.2 Frame Structure



NOTE

A frame can contain a maximum of 256 bytes.

Frame structure definitions in this document include only the function code and data.

Table 4-1 MBAP definitions

Data Field	Length (Bytes)	Description	Client	Server
Transmission identifier	2	Identifier for matching between a request frame and a response frame	Assigned by the client. It is recommended that each frame be assigned a unique identifier.	The identifier of the response frame from the server must be the same as that of the corresponding request frame.
Protocol type	2	0 = Modbus protocol	Assigned by the client; 0 by default.	The identifier of the response frame from the server must be the same as that of the corresponding request frame.
Data length	2	Identifies the number of bytes in the message to follow.	Assigned by the client based on the actual data frame.	Assigned by the server based on the actual frame length.
Logical device ID	1	Identifies the EMMA or a device connected to the EMMA. 0: EMMA 1–247: inverter or other devices	Assigned by the client based on the actual data frame request.	The identifier of the response frame from the server must be the same as that of the corresponding request frame.

4.2.3 Data Encoding

Modbus uses a big-Endian representation for addresses and data elements. This means that when multiple bytes are sent, the most significant byte is sent first.

Example:

Register Size	Value
16 bits	0x1234

The first byte sent is 0x12, followed by 0x34.

4.2.4 Interaction Process

A communication process is always initiated by the master node. Slave nodes do not initiate communication processes.

In unicast mode, a slave node returns one response for each request from the master node. If the master node does not receive any response from the slave node within 5 seconds, the communication process is regarded as timed out.

In broadcast mode, slave nodes receive but do not respond to the requests from the master node.

4.3 Application Layer

4.3.1 Function Code List

Table 4-2 Function code list

Function Code	Meaning	Remarks
0x03	Reading registers	Reads a single register or a block of contiguous registers.
0x06	Writing into a single register	Writes into a single register.
0x10	Writing into multiple registers	Writes into a block of contiguous registers.
0x2B	Reading device identifiers	Obtains the device type and version number.

4.3.2 Exception Code List

Exception codes must be unique for each network element (NE) type. The names and descriptions should be provided in the NE interface document. Different versions of the same NE type must be backward compatible. Exception codes in use cannot be assigned to other exceptions.

Table 4-3 Exception codes returned by an NE (0x00–0x8F used for common exception codes)

Code	Name	Meaning
0x01	Invalid function	The function code received in the query is not allowable for the server (or slave node). This may be because the function code is only applicable to newer devices, and was not implemented in the unit selected. It also indicates that the server (or slave node) is in the wrong state to process a request of this type, for example because it is not configured and is being asked to return register values.
0x02	Invalid data address	The data address received in the query is not an allowable address for the server (or slave). More specifically, the combination of the reference number and transfer length is invalid. For a controller with 100 registers, a request with an offset of 96 and a length of 4 is successfully executed, and a request with an offset of 96 and a length of 5 is responded with the error code 02.
0x03	Invalid data value	The value contained in the query is not an allowable value for the server (or slave node). This indicates a fault in the structure of the remainder of a complex request, such as an incorrectly implied length. It specifically does not mean that a data item submitted for storage in a register has a value outside the expectation of the application program since the Modbus protocol is unaware of the significance of any particular value of any particular register.
0x04	Slave device failure	An error occurred while the server was attempting to perform the requested action.
0x05	Acknowledge	The server has accepted the request and is processing it, but a long duration of time will be required to do so. This response is returned to confirm the acceptance of the request.
0x06	Slave device busy	The server cannot accept a Modbus request PDU. The client application determines whether and when to retransmit the request.

0x08	Memory parity error	Used in conjunction with function codes 20 and 21 and reference type 6 to indicate that the extended file area failed to pass a consistency check. The server (or slave node) attempted to read a record file, but detected a parity error in the memory. The client (master node) can retry the request, but a service may be required on the server (or slave node).
0x0A	Gateway path unavailable	Applies to the TCP/IP protocol.
0x0B	Gateway target device failed to respond	Applies to the TCP/IP protocol.
0x80	No permission	An operation is not allowed because of a permission authentication failure or permission expiration.
0x81	Parameter verification failed	For register parameters (such as WiFi passwords) with specific functions, the slave device requires that the parameter values comply with certain specifications (for example, the secret values meet the weak password verification rules). Otherwise, this exception code is returned.

4.3.3 Reading Registers (0x03)

4.3.3.1 Frame Format of a Request from a Master Node

Data Field	Length	Description
Function code	1 byte	0x03
Register start address	2 bytes	0x0000–0xFFFF
Number of registers	2 bytes	1–125

4.3.3.2 Frame Format of a Normal Response from a Slave Node

Data Field	Length	Description
Function code	1 byte	0x03
Byte count	1 byte	2 x *N*
Register value	2 x *N* bytes	N/A

NOTE

N refers to the number of registers.

4.3.3.3 Frame Format of an Abnormal Response from a Slave Node

Data Field	Length	Description
Function code	1 byte	0x83
Exception code	1 byte	For details, see **Exception Code List**.

4.3.3.4 Examples

The master node sends a query request (register address: 32306/0X7E32) to the slave node (logical device ID: 01).

Description	MBAP							Function code	Data			
	Protocol identifier		Protocol type		Data length		Logical device ID		Register address		Number of registers	
Frame Data	00	01	00	00	00	06	00	03	7E	32	00	02

Normal response from a slave node:

Description	MBAP Header							Function code	Data				
	Protocol identifier		Protocol type		Data length		Logical device ID		Byte count	Register data			
Frame Data	00	01	00	00	00	07	00	03	04	00	00	00	01

Abnormal response from a slave node:

Description	MBAP Header							Function code	Data
	Protocol identifier		Protocol type		Data length		Logical device ID		Error code
Frame Data	00	01	00	00	00	03	00	83	03

4.3.4 Writing into a Single Register (0x06)

4.3.4.1 Frame Format of a Request from a Master Node

Data Field	Length	Description
Function code	1 byte	0x06
Register address	2 bytes	0x0000–0xFFFF
Register value	2 bytes	0x0000–0xFFFF

4.3.4.2 Frame Format of a Normal Response from a Slave Node

Data Field	Length	Description
Function code	1 byte	0x06
Register address	2 bytes	0x0000–0xFFFF
Register value	2 bytes	0x0000–0xFFFF

4.3.4.3 Frame Format of an Abnormal Response from a Slave Node

Data Field	Length	Description
Function code	1 byte	0x86
Exception code	1 byte	For details, see **Exception Code List**.

4.3.4.4 Examples

The master node sends a command (register address: 40200/0X9D08) to a slave node (address: 01).

Description	MBAP							Function code	Data			
	Protocol identifier		Protocol type		Data length		Logical device ID		Register address		Register data	
Frame Data	00	01	00	00	00	06	00	06	9D	08	00	00

Normal response from a slave node:

Description	MBAP							Function code	Data			
	Protocol identifier		Protocol type		Data length		Logical device ID		Register address		Register data	
Frame Data	00	01	00	00	00	06	00	06	9D	08	00	00

Abnormal response from a slave node:

Description	MBAP							Function code	Data
	Protocol identifier		Protocol type		Data length		Logical device ID		Error code
Frame Data	00	01	00	00	00	03	00	86	04

4.3.5 Writing into Multiple Registers (0x10)

4.3.5.1 Frame Format of a Request from a Master Node

Data Field	Length	Description

Function code	1 byte	0x10
Register start address	2 bytes	0x0000–0xFFFF
Number of registers	2 bytes	0x0000–0x007b
Byte count	1 byte	2 x *N*
Register value	2 x *N* bytes	Value

NOTE

N refers to the number of registers.

4.3.5.2 Frame Format of a Normal Response from a Slave Node

Data Field	Length	Description
Function code	1 byte	0x10
Register address	2 bytes	0x0000–0xFFFF
Number of registers	2 bytes	0x0000–0x007b

4.3.5.3 Frame Format of an Abnormal Response from a Slave Node

Data Field	Length	Description
Function code	1 byte	0x90
Exception code	1 byte	For details, see **Exception Code List**.

4.3.5.4 Examples

The master node sets the register address 40118/0X9CB6 to 2 and the register address 40119/0X9CB7 to 50 for the slave node (address: 01). The request frame format is as follows.

Description	MBAP							Function code	Data								
	Protocol identifier		Protocol type		Data length		Logical device ID		Register address		Number of registers		Byte count	Register data			
Frame Data	00	01	00	00	00	0B	00	10	9C	B6	00	02	04	00	02	00	32

Normal response from a slave node:

Description	MBAP							Function code	Data			
	Protocol identifier		Protocol type		Data length		Logical device ID		Register address		Number of registers	
Frame Data	00	01	00	00	00	06	00	10	9C	B6	00	02

Abnormal response from a slave node:

Description	MBAP				Function code	Data
	Protocol identifier	Protocol type	Data length	Logical device ID		Error code

Frame Data	00	01	00	00	00	06	00	90	04

4.3.6 Reading Device Identifiers (0x2B)

This function code allows reading identifiers and added packets that are relevant to the physical and function description of the remote devices.

The interface for reading device identifiers is simulated as an address space composed of a set of addressable data elements. Data elements are objects to be read, and object IDs identify them.

A data element consists of three objects:

1. Basic device identifier: All objects of this type are mandatory, such as the vendor name, product code, and revision version.
2. Regular device identifier: In addition to the basic data objects, the device provides additional and optional identifiers and data object description. All of the objects of this type are defined according to the standard but their execution is optional.
3. Extended device identifier: In addition to regular data objects, the device provides additional and optional identifiers and private data object description. All the data is related to the device.

Table 4-4 Device identification information

Object ID	Object Name/ Description	Type	Mandatory/ Optional	Category
0x00	Vendor name	ASCII character string	Mandatory	Basic
0x01	Product code	ASCII character string	Mandatory	
0x02	Main revision version	ASCII character string	Mandatory	
0x03–0x7F	N/A	N/A	N/A	Normal
0x80–0xFF	N/A	N/A	N/A	Extended

4.3.6.1 Command for Querying Device Identifiers

Table 4-5 Request frame format

Data Field	Length	Description
Function code	1 byte	0x2B
MEI type	1 byte	0x0E
ReadDevId code	1 byte	01
Object ID	1 byte	0x00

Table 4-6 Frame format of a normal response

Data Field			Length	Description
Slave node address			1 byte	1–247
Function code			1 byte	0x2B
MEI type			1 byte	0x0E
ReadDevId code			1 byte	01
Consistency level			1 byte	01
More			1 byte	N/A
Next object ID			1 byte	N/A
Number of objects			1 byte	N/A
Object list	First object	Object ID	1 byte	0x00
		Object length	1 byte	N
		Object value	N byte	N/A

Table 4-7 Object list

Object ID	Object Name/ Description	Description	Category
0x00	Vendor name	"HUAWEI"	Basic
0x01	Product code	"SUN2000"	
0x02	Main revision version	ASCII character string, software version	

Table 4-8 Frame format of an abnormal response

Data Field	Length	Description
Function code	1 byte	0xAB
Exception code	1 byte	For details, see **Exception Code List**.

4.3.6.2 Command for Querying a Device List

Table 4-9 Request frame format

Data Field	Length	Description
Function code	1 byte	0x2B
MEI type	1 byte	0x0E
ReadDevId code	1 byte	03
Object ID	1 byte	0x87

Table 4-10 Frame format of a normal response

Data Field			Length	Description
Function code			1 byte	0x2B
MEI type			1 byte	0x0E
ReadDevId code			1 byte	03
Consistency level			1 byte	03
More			1 byte	N/A
Next object ID			1 byte	N/A
Number of objects			1 byte	N/A
Object list	First object	Object ID	1 byte	0x87
		Object length	1 byte	N
		Object value	N byte	N/A
	…	…	…	…

Table 4-11 Object list

Object ID	Object Name	Type	Description
0x80–0x86	Reserved		Returns a null object with a length of 0.
0x87	Number of devices	int	Returns the number of devices connected to the RS485 address.
0x88	Description about the first device	ASCII character string See the following device description definitions.	Returns only description about the first device if an NE allows only one device to be connected to each RS485 address.
0x89	Description about the second device	Same as above	Same as above
...	...	...	..
0xFF	Description about the 120th device	Same as above	Same as above
0x00	Description about the 121th device	Same as above	Same as above
0x01	Description about the 122th device	Same as above	Same as above
...	...	...	...

4.3.6.3 Device Description Definitions

Each device description consists of all "attribute=value" character strings.

"Attribute ID=%s;attribute ID=%s; ... attribute ID=%s"

Example:

- EMMA information example (8=HEMS): 1=EMMA-A02;2=V100R024C00B030;3=P1.15-D1.0;4=NS123456789;5=0;6=1.0;8=HEMS;9=0

Description about key parameters:

Device model 1: EMMA-A02

Version 2: V100R024C00B030

ESN 4: NS123456789

Communication address 5: 0

- Inverter information example (8=SUN2000):
  1=xx;2=V100R024C10SPC120;3=P1.15-D5.0;4=123232323;5=2;6=1;8=SUN2000

Description about key parameters:

Device model 1: xx

Version 2: V100R024C10SPC120

ESN 4: 123232323

Communication address 5: 2

Table 4-12 Attribute definitions

Attribute ID	Attribute Name	Type	Description
1	Device model	ASCII character string	Product nameplate
2	Device software version	ASCII character string	Software version
3	Interface protocol version	ASCII character string	See the interface protocol version definitions.
4	ESN	ASCII character string	N/A
5	Device ID	int	0, 1, 2, 3, ... (assigned by NEs; 0 indicates the master device into which the Modbus card is inserted)
6=	Feature version	String	
7=	Unknown		
8=	Product type	String	

Table 4-13 Frame format of an abnormal response

Data Field	Length	Description
Function code	1 byte	0xAB
Exception code	1 byte	For details, see **Exception Code List**.

5 Reference Documents

Modbus_Application_Protocol_V1_1b3

Modbus over serial line specification and implementation guide V1.02

Modbus_Messaging_Implementation_Guide_V1_0b