FOX commercial inverter
Modbus interface definition description

FoxESS Co., Ltd.

Document version V1.05.02.00
Release date 2024-08-15

Table of contents

1 Supported model list

This section describes the inverter models that use this protocol, and the minimum firmware version requirements required for these models. When the host computer connects to the inverter, please pay attention to the FW version.

1.1 Model description

Table 1-1 List of supported model series and firmware version requirements

Model series	Series ID	Minimum firmware version requirements

2 Introduction

The Modbus protocol is issued as a general device-level communication protocol standard. This document describes the Modbus protocol for FoxESS inverter, which is used to standardie subsequent third-party integrated development. Since the FoxESS inverter complies with the standard modbus specification, this document focuses on the information specific to the FoxESS inverter.

For additional information, please refer to the description in the ModBus standard specification document. For a detailed description of the standard protocols used by the FoxESS Inverter as well as customized sections and examples of interactions, please read **5 Communication Protocol Overview** .

2.1 Terms and abbreviations

Table 2-1 Terms and abbreviation definitions

Name	**Description**
master node	In master-slave communication, the party that actively initiates communication is called the master node.
slave node	In master-slave communication, the party that passively responds to commands is called a slave node.
broadcast address	Fixed to 0
Register address	The register address corresponds to a 2-byte message
U16	Unsigned 16-bit integer
U32	Unsigned 32-bit integer
I16	Signed 16-bit integer
I32	Signed 32-bit integer
STR	string
MLD	multibyte
Bitfield16	16-bit wide bitwise representation of data
Bitfield32	32-bit wide bitwise representation of data
-	not involving
s	Second
INV	inverter
BMS	battery management system
name	**describe**
RO	Read-only data
RW	Readable and writable data
WO	Write data only

3 Supported model list

Table 3-1 Inverter model definition table

Serial number	Signal name	Read and write	Type	Unit	Gain	Address	Number	Scope
1	Model name	RO	STR	N/A	1	30000	16	
2	SN	RO	STR	N/A	1	30016	16	
3	MFG ID	RO	STR	N/A	1	30032	16	

Table 3-2 Inverter version definition table

Serial number	Signal name	Read and write	Type	Unit	Gain	Address	Number	Scope
4	Master Version	RO	U16	N/A	N/A	36001	1	
5	Slave Version	RO	U16	N/A	N/A	36002	1	
6	Manager Version	RO	U16	N/A	N/A	36003	1	
7	Meter1 SN	RO	STR	N/A	N/A	36100	16	
8	Meter1 MFG ID	RO	STR	N/A	N/A	36116	16	
9	Meter1 TYPE	RO	STR	N/A	N/A	36132	16	
10	Meter1 Version	RO	STR	N/A	N/A	36148	1	
11	Meter2 SN	RO	STR	N/A	N/A	36200	16	
12	Meter2 MFG ID	RO	STR	N/A	N/A	36216	16	
13	Meter2 TYPE	RO	STR	N/A	N/A	36232	16	
14	Meter2 Version	RO	STR	N/A	N/A	36248	1	

Table 3-3 Battery version definition table

Serial number	Signal name	Read and write	Type	Unit	Gain	Address	Number	Scope
15	BMS1连接状态	RO	U16	N/A	N/A	37002	1	0：Offline 1：Online
16	BMS1Master version	RO	U16	N/A	N/A	37003	1	
17	BMS1主控类型	RO	U16	N/A	N/A	37004	1	
18	BMS1主控SN	RO	STR	N/A	N/A	37005	16	
19	BMS1从控个数	RO	U16	N/A	1	37032	1	范围：[0,32] 0:不存在
20	BMS1 Slave 1 version	RO	U16	N/A	N/A	37033	1	Maximum support for 32 channels of slave control. The number of channels actually read by the host computer is in accordance with the number of channels defined in "BMS1 Number of Slaves". The corresponding version of each battery: 37033 + (n - 1), where n is the number of slaves in the range of [1, 32].
21	BMS1 Slave 2 version	RO	U16	N/A	N/A	37034	1	
22	BMS1 从控1 SN	RO	STR	N/A	N/A	37097	16	最大支持32路从控。上位机实际读取路数按照“BMS1从控个数”定义的路数读取。每路电池对应的SN: 37097 +16* (n - 1)，其中n为从控个数范围是[1, 32]
23	BMS1 从控2 SN	RO	STR	N/A	N/A	37113	16	

24	BMS1 Voltage	RO	U16	V	10	37609	1	
25	BMS1 Current	RO	I16	A	10	37610	1	
26	BMS1 Ambient Temperature	RO	I16	℃	10	37611	1	
27	BMS1 SoC	RO	U16	%	1	37612	1	
28	BMS1 Max Temperature	RO	I16	℃	10	37617	1	
29	BMS1 Min Temperature	RO	I16	℃	10	37618	1	
30	BMS1 Max Cell Voltage	RO	U16	mV	1	37619	1	
31	BMS1 Min Cell Voltage	RO	U16	mV	1	37620	1	
32	BMS1 SOH	RO	U16	%	1	37624	1	
33	BMS1 Fault1	RO	Bitfield 16	N/A	N/A	37626	1	
34	BMS1 Fault2	RO	Bitfield 16	N/A	N/A	37627	1	
35	BMS1 Fault3	RO	Bitfield 16	N/A	N/A	37628	1	
36	BMS1 Fault4	RO	Bitfield 16	N/A	N/A	37629	1	
37	BMS1 Fault5	RO	Bitfield 16	N/A	N/A	37630	1	
38	BMS1 Fault6	RO	Bitfield 16	N/A	N/A	37631	1	
39	BMS1 Remain Energy	RO	U16	Wh	0.1	37632	1	
40	BMS1 FCC Capacity	RO	U16	Ah	10	37633	1	
41	reserve	RO	U16	N/A	N/A	37634	1	
42	BMS1 Design Energy	RO	U16	Wh	0.1	37635	1	
43	BMS1 Force to Change	RO	U16	N/A	N/A	37636	1	Range: [0, 1] 0: Reset

	battery Flag							1: Set Note: If set, pcs should charge the battery until the status is reset.
44	BMS2连接状态	RO	U16	N/A	N/A	37700	1	0：Offline 1：Online
45	BMS2 Master version	RO	U16	N/A	N/A	37701	1	
46	BMS2主控类型	RO	U16	N/A	N/A	37702	1	
47	BMS2主控SN	RO	STR	N/A	N/A	37703	16	
48	BMS2从控个数	RO	U16	N/A	1	37730	1	范围：[0,32] 0:不存在
49	BMS2 Slave 1 version	RO	U16	N/A	N/A	37731	1	Maximum support for 32 channels of slave control. The number of channels actually read by the host computer is in accordance with the number of channels defined in "BMS2 Number of Slaves". The corresponding version of each battery: 37033 + (n - 1), where n is the number of slaves in the range of [1, 32].
50	BMS2 Slave 2 version	RO	U16	N/A	N/A	37732	1	
51	BMS2从控1SN	RO	STR	N/A	N/A	37795	16	最大支持32路从控。上位机实际读取路数按照“BMS2从控个数”定义的路数读取。每
52	BMS2从控2SN	RO	STR	N/A	N/A	37811	16	

								路电池对应的SN：37795 +16* (n - 1)，其中n为从控个数范围是[1, 32]
53	BMS2 Voltage	RO	U16	V	10	38307	1	
54	BMS2 Current	RO	I16	A	10	38308	1	
55	BMS2 Ambient Temperature	RO	I16	℃	10	38309	1	
56	BMS2 SoC	RO	U16	%	1	38310	1	
57	BMS2 Max Temperature	RO	I16	℃	10	38315	1	
58	BMS2 Min Temperature	RO	I16	℃	10	38316	1	
59	BMS2 Max Cell Voltage	RO	U16	mV	1	38317	1	
60	BMS2 Min Cell Voltage	RO	U16	mV	1	38318	1	
61	BMS2 SOH	RO	U16	%	1	38322	1	
62	BMS2 Fault1	RO	Bitfield 16	N/A	N/A	38324	1	
63	BMS2 Fault2	RO	Bitfield 16	N/A	N/A	38325	1	
64	BMS2 Fault3	RO	Bitfield 16	N/A	N/A	38326	1	
65	BMS2 Fault4	RO	Bitfield 16	N/A	N/A	38327	1	
66	BMS2 Fault5	RO	Bitfield 16	N/A	N/A	38328	1	
67	BMS2 Fault6	RO	Bitfield 16	N/A	N/A	38329	1	
68	BMS2 Remain Energy	RO	U16	Wh	0.1	38330	1	
69	BMS2 FCC Capacity	RO	U16	Ah	10	38331	1	
70	reserve	RO	U16	N/A	N/A	38332	1	

71	BMS2 Design Energy	RO	U16	Wh	0.1	38333	1	
72	BMS2 Force to Change battery Flag	RO	U16	N/A	N/A	38334	1	Range: [0, 1] 0: Reset 1: Set Note: If set, pcs should charge the battery until the status is reset.

Table 3-4 Register definition table

Serial number	Signal name	Read and write	Type	Unit	Gain	Address	Number	Scope
73	Meter1/CT1 Connect State	RO	U16	N/A	N/A	38801	1	0 : Disconnect 1 : Connect
74	Meter1/CT1 R Phase Voltage	RO	I32	V	10	38802	2	
75	Meter1/CT1 S Phase Voltage	RO	I32	V	10	38804	2	
76	Meter1/CT1 T Phase Voltage	RO	I32	V	10	38806	2	
77	Meter1/CT1 R Phase Current	RO	I32	A	1000	38808	2	
78	Meter1/CT1 S Phase Current	RO	I32	A	1000	38810	2	
79	Meter1/CT1 T Phase Current	RO	I32	A	1000	38812	2	
80	Meter1/CT1 Combined Active Power	RO	I32	W	10	38814	2	
81	Meter1/CT1 R Phase Active Power	RO	I32	W	10	38816	2	
82	Meter1/CT1 S Phase Active Power	RO	I32	W	10	38818	2	

83	Meter1/CT1 T Phase Active Power	RO	I32	W	10	38820	2	
84	Meter1/CT1 Combined Reactive Power	RO	I32	Var	10	38822	2	
85	Meter1/CT1 R Phase Reactive Power	RO	I32	Var	10	38824	2	
86	Meter1/CT1 S Phase Reactive Power	RO	I32	Var	10	38826	2	
87	Meter1/CT1 T Phase Reactive Power	RO	I32	Var	10	38828	2	
88	Meter1/CT1 Combined Apparent Power	RO	I32	VA	10	38830	2	
89	Meter1/CT1 R Phase Apparent Power	RO	I32	VA	10	38832	2	
90	Meter1/CT1 S Phase Apparent Power	RO	I32	VA	10	38834	2	
91	Meter1/CT1 T Phase Apparent Power	RO	I32	VA	10	38836	2	
92	Meter1/CT1 Combined Power Factor	RO	I32	N/A	1000	38838	2	
93	Meter1/CT1 R Phase Power Factor	RO	I32	N/A	1000	38840	2	
94	Meter1/CT1 S Phase Power Factor	RO	I32	N/A	1000	38842	2	
95	Meter1/CT1 T Phase Power Factor	RO	I32	N/A	1000	38844	2	

96	Meter1/CT1 Freq	RO	I32	Hz	100	38846	2	
97	Meter2/CT2 Connect State	RO	U16	N/A	N/A	38901	1	0 : Disconnect 1 : Connect
98	Meter2/CT2 R Phase Voltage	RO	I32	V	10	38902	2	
99	Meter2/CT2 S Phase Voltage	RO	I32	V	10	38904	2	
100	Meter2/CT2 T Phase Voltage	RO	I32	V	10	38906	2	
101	Meter2/CT2 R Phase Current	RO	I32	A	1000	38908	2	
102	Meter2/CT2 S Phase Current	RO	I32	A	1000	38910	2	
103	Meter2/CT2 T Phase Current	RO	I32	A	1000	38912	2	
104	Meter2/CT2 Combined Active Power	RO	I32	W	10	38914	2	
105	Meter2/CT2 R Phase Active Power	RO	I32	W	10	38916	2	
106	Meter2/CT2 S Phase Active Power	RO	I32	W	10	38918	2	
107	Meter2/CT2 T Phase Active Power	RO	I32	W	10	38920	2	
108	Meter2/CT2 Combined Reactive Power	RO	I32	Var	10	38922	2	
109	Meter2/CT2 R Phase Reactive Power	RO	I32	Var	10	38924	2	
110	Meter2/CT2 S Phase Reactive Power	RO	I32	Var	10	38926	2	

111	Meter2/CT2 T Phase Reactive Power	RO	I32	Var	10	38928	2	
112	Meter2/CT2 Combined Apparent Power	RO	I32	VA	10	38930	2	
113	Meter2/CT2 R Phase Apparent Power	RO	I32	VA	10	38932	2	
114	Meter2/CT2 S Phase Apparent Power	RO	I32	VA	10	38934	2	
115	Meter2/CT2 T Phase Apparent Power	RO	I32	VA	10	38936	2	
116	Meter2/CT2 Combined Power Factor	RO	I32	N/A	1000	38938	2	
117	Meter2/CT2 R Phase Power Factor	RO	I32	N/A	1000	38940	2	
118	Meter2/CT2 S Phase Power Factor	RO	I32	N/A	1000	38942	2	
119	Meter2/CT2 T Phase Power Factor	RO	I32	N/A	1000	38944	2	
120	Meter2/CT2 Freq	RO	I32	Hz	100	38946	2	

Table 3-5

Serial number	Signal name	Read and write	Type	Unit	Gain	Address	Number	Scope
121	Protocol version	RO	U32	N/A	N/A	39000	2	For example, 0x01020304 indicates version V1.02.03.04, and the initial version is V1.01.00.00

122	Model name	RO	STR	N/A	1	39002	16	
123	SN	RO	STR	N/A	1	39018	16	
124	PN	RO	STR	N/A	1	39034	16	
125	Model ID	RO	U16	N/A	1	39050	1	
126	Number of strings	RO	U16	N/A	1	39051	1	
127	Number of MPPTs	RO	U16	N/A	1	39052	1	
128	Rated power (Pn)	RO	I 32	kW	1000	39053	2	
129	Maximum active power (Pmax)	RO	I32	kW	1000	39055	2	
130	Maximum apparent value (Smax)	RO	I32	kVA	1000	39057	2	
131	Maximum reactive power (Qmax, fed into the grid)	RO	I32	kVar	1000	39059	2	
132	Maximum reactive power (Qmax, absorbed from the grid)	RO	I32	kVar	1000	39061	2	
133	Status 1	RO	Bitfield16	N/A	1	39063	1	Bit0: Standby Bit1: Reserved Bit2: Operation Bit3: Reserved Bit4: Reserved Bit5: Reserved Bit6: Fault Bit7: Reserved
134	reserve	RO	Bitfield16			39064	1	
135	Status 3	RO	Bitfield32	N/A	1	39065	2	Bit0: Off-grid or not

								0: Not off-grid 1: Off-grid
136	Alarm 1	RO	Bitfield16	N/A	1	39067	1	Refer to 4.1 Alarm information
137	Alarm 2	RO	Bitfield16	N/A	1	39068	1	Refer to 4.1 Alarm information
138	Alarm 3	RO	Bitfield16	N/A	1	39069	1	Refer to 4.1 Alarm information
139	PV1 voltage	RO	I16	V	10	39070	1	Supports up to 24 channels of string information. The actual number of reading channels of the host computer is based on the number of channels defined by "number of strings". The actual corresponding voltage and current register addresses of each string are PVn voltage: 39070 + 2*(n - 1), PVn current: 39071 + 2*(n – 1). Where n is the string number range is [1, 24]
140	PV1 current	RO	I16	A	100	39071	1	
141	PV2 voltage	RO	I16	V	10	39072	1	
142	PV2 current	RO	I16	A	100	39073	1	
143	PV3 voltage	RO	I16	V	10	39074	1	
144	PV3 current	RO	I16	A	100	39075	1	
145	PV4 voltage	RO	I16	V	10	39076	1	
146	PV4 current	RO	I16	A	100	39077	1	
147	Total PV input power	RO	I32	kW	1000	39118	2	-
148	reserve	RO	U16			39120	1	-
149	reserve	RO	U16			39121	1	-
150	reserve	RO	U16			39122	1	-

151	Grid R phase voltage	RO	I16	V	10	39123	1	
152	Grid S-phase voltage	RO	I16	V	10	39124	1	
153	Grid T-phase voltage	RO	I16	V	10	39125	1	
154	Inverter R phase current	RO	I32	A	1000	39126	2	
155	Inverter S phase current	RO	I32	A	1000	39128	2	
156	Inverter T phase current	RO	I32	A	1000	39130	2	
157	reserve	RO	U 32			39132	2	
158	Active power	RO	I32	kW	1000	39134	2	
159	Reactive power	RO	I32	kVar	1000	39136	2	
160	power factor	RO	I16	N/A	1000	39138	1	
161	Grid frequency	RO	I16	Hz	100	39139	1	
162	reserve	RO	U16			39140	1	
163	internal temperature	RO	I16	℃	10	39141	1	
164	reserve	RO	U16			39142	1	
165	reserve	RO	U16			39143	1	
166	reserve	RO	U16			39144	1	
167	reserve	RO	U32			39145	2	
168	reserve	RO	U32			39147	2	
169	Cumulative power generation	RO	U 32	kWh	100	39149	2	

170	Power generation on the day	RO	U 32	kWh	100	39151	2	
171	reserve	RO	U16			39153	1	
172	reserve	RO	U32			39154	2	
173	reserve	RO	U16			39156	1	
174	reserve	RO	U16			39157	1	
175	reserve	RO	U32			39158	2	
176	reserve	RO	U16			39160	1	
177	reserve	RO	U16			39161	1	
178	[Energy storage module 1] Charge and discharge power *	RO	I32	W	1	39162	2	> 0: charging < 0: discharging
179	reserve	RO	U32			39164	2	
180	reserve	RO	U32			39166	2	
181	[Meter collection] Active power *	RO	I32	W	1	39168	2	> 0: Feed power to the grid < 0: Take power from the grid
182	reserve	RO	U16			39170	1	
183	reserve	RO	U16			39171	1	
184	reserve	RO	U16			39172	1	
185	reserve	RO	U16			39200	1	
186	E PS R Phase Voltage	RO	U16	V	10	39201	1	

187	E PS S Phase Voltage	RO	U16	V	10	39202	1	
188	E PS T Phase Voltage	RO	U16	V	10	39203	1	
189	E PS RPhaseCurrent _	RO	I32	A	10 00	39204	2	
190	E PS S Phase Current	RO	I32	A	10 00	39206	2	
191	E PS TPhaseCurrent _	RO	I32	A	10 00	39208	2	
192	E PS R Phase Power	RO	I32	W	1	39210	2	
193	EPS S Phase Power	RO	I32	W	1	39212	2	
194	EPS T Phase Power	RO	I32	W	1	39214	2	
195	EPS Combined Power	RO	I32	W	1	39216	2	
196	EPS Frequency	RO	I16	Hz	100	39218	1	
197	Load R Phase Power	RO	I32	W	1	39219	2	
198	Load S Phase Power	RO	I32	W	1	39221	2	
199	Load T Phase Power	RO	I32	W	1	39223	2	
200	Load Combined Power	RO	I32	W	1	39225	2	
201	Battery1 Voltage _	RO	I16	V	10	39227	1	
202	Battery1 Current _	RO	I32	A	10 00	39228	2	
203	Battery 1 Power _	RO	I32	W	1	39230	2	

204	Battery 2 Voltage _	RO	I16	V	10	39232	1	
205	Battery 2 Current _	RO	I32	A	10 00	39233	2	
206	Battery 2 Power _	RO	I32	W	1	39235	2	
207	Battery Combined Power	RO	I32	W	1	39237	2	
208	reserve	RO	I16			39239	1	
209	reserve	RO	I16			39240	1	
210	reserve	RO	I16			39241	1	
211 k	reserve	RO	I32			39242	2	
212	reserve	RO	I32			39244	2	
213	reserve	RO	I32			39246	2	
214 k	INV R Phase Active Power	RO	I32	W	1	39248	2	
215	INV S Phase Active Power	RO	I32	W	1	39250	2	
216	INV T Phase Active Power	RO	I32	W	1	39252	2	
217	reserve	RO	I32			39254	2	
218	INV R Phase Reactive Power	RO	I32	Var	1	39256	2	
219	INV S Phase Reactive Power	RO	I32	Var	1	39258	2	
220	INV T Phase Reactive Power	RO	I32	Var	1	39260	2	
221	reserve	RO	I32			39262	2	
222	INV R Phase A transparent Power	RO	I32	VA	1	39264	2	

223	INV S Phase A transparent Power	RO	I32	VA	1	39266	2	
224	INV T Phase A transparent Power	RO	I32	VA	1	39268	2	
225	INV Combined A parent Power	RO	I32	VA	1	39270	2	
226	INV Frequency R	RO	I16	Hz	100	39272	1	
227	INV Frequency S	RO	I16	Hz	100	39273	1	
228	INV Frequency T	RO	I16	Hz	100	39274	1	
229	Available Import Power	RO	I32	W	1	39275	2	
230	Available Export Power	RO	I32	W	1	39277	2	
231	PV1 Power	RO	I32	W	1	39279	2	Maximum support for 24 channels of string information. The number of channels actually read by the host computer is in accordance with the number of channels defined in "Number of strings". The voltage and current registers corresponding to each string are as follows PVn Power: 39279 + 2*(n - 1) Where n is the string number, the range is [1, 24].
232	PV2 Power	RO	I32	W	1	39281	2	
233	PV3 Power	RO	I32	W	1	39283	2	
234	PV4 Power	RO	I32	W	1	39285	2	

235	MPPT1 Voltage	RO	I16	V	10	39327	1	最大支持24路组串信息。上位机实际读取路数按照“组串个数”定义的路数读取。每路组串实际对应的电压和电流寄存器地址为 MPPTn Volt：39327 + 4*(n - 1) MPPTn Curr：39328 + 4*(n - 1) MPPTn Power：39329 + 4*(n - 1) 其中n为组串编号范围是[1, 24]
236	MPPT1 Current	RO	I16	A	100	39328	1	
237	MPPT1 Power	RO	I32	W	1	39329	2	
238	MPPT2 Voltage	RO	I16	V	10	39331	1	
239	MPPT2 Current	RO	I16	A	100	39332	1	
240	MPPT2 Power	RO	I32	W	1	39333	2	
241	MPPT3 Voltage	RO	I16	V	10	39335	1	
242	MPPT3 Current	RO	I16	A	100	39336	1	
243	MPPT3 Power	RO	I32	W	1	39337	2	

Table 3-6

Serial number	Signal name	Read and write	Type	Unit	Gain	Address	Number	Scope
244	reserve	RO	U16			39600	1	
245	PV total power	RO	U 32	kWh	10 0	39601	2	
246	Total PV power today	RO	U32	kWh	10 0	39603	2	
247	Total charging capacity	RO	U 32	kWh	10 0	39605	2	
248	Today’s total charging capacity	RO	U32	kWh	10 0	39607	2	
249	Total discharge power	RO	U 32	kWh	10 0	39609	2	
250	Today’s total discharge power	RO	U32	kWh	10 0	39611	2	
251	Total power of feeder network	RO	U 32	kWh	10 0	39613	2	

252	Today's total feeder power	RO	U32	kWh	10 0	39615	2	
253	Total power taken	RO	U 32	kWh	10 0	39617	2	
254	Today's total electricity consumption	RO	U32	kWh	10 0	39619	2	
255	Output total power	RO	U 32	kWh	10 0	39621	2	
256	Total power output today	RO	U32	kWh	10 0	39623	2	
257	Enter total power	RO	U 32	kWh	10 0	39625	2	
258	Enter total power today	RO	U32	kWh	10 0	39627	2	
259	Total load power	RO	U 32	kWh	10 0	39629	2	
260	Total load power today	RO	U32	kWh	10 0	39631	2	

Table 3-7

Serial number	Signal name	Read and write	Type	Unit	Gain	Address	Number	Scope
261	reserve	WO	U16	N/A	N/A	45000	1	
262	reserve	WO	U16	N/A	N/A	45001	1	
263	Factory Reset	WO	U16	N/A	N/A	45002	1	Range: [0,1] 0: Invalid; 1: Active
264	Battery power active	WO	U16	N/A	N/A	45003	1	Range: [0, 1] 0:Invalid; 1: Active Note: Only the H3 Smart series is supported.
265	reserve	WO	U16	N/A	N/A	45004	1	
266	Battery power shut-dowm	WO	U16	N/A	N/A	45005	1	Range: [0, 1] 0:Invalid; 1: Active Note: Only the H3

								Smart series is supported.
267	Battery power ON/OFF	RO	U16	N/A	N/A	45006	1	Range: [0, 1] 0: OFF 1: ON
268	Battery Connect Enable	RW	U16	N/A	N/A	45007	1	Range: [0, 1] 0: Disable 1: Enable Note: Only the H3 Smart series is supported.

Table 3-8

Serial number	Signal name	Read and write	Type	Unit	Gain	Address	Number	Scope
269	reserve	RO	U16			46000	1	
270	Remote Control	RW	Bitfield 16	N/A	1	46001	1	Bit 0: Remote Control enable 0: Disable 1: Enable Bit 1: Definition for positive direction 0: power-generation system 1: power-consumption system Bits 3:2 : Controlled target 00: AC 01: Battery 10: Grid (CT/Meter) 11: AC (Grid first) Bits 15:4 Reserved
271	Remote Timeout_Set	RW	U16	s	1	46002	1	
272	Remote Control Active Power Command	RW	I32	W	1	46003	2	
273	Remote Control Reactive	RW	I32	Var	1	46005	2	

	Power Command							
274	Remote Timeout Countdown	RO	U16	s	1	46007	1	
275	Pwr_limit Bat_Up	RO	I32	W	1	46018	2	
276	Pwr_limit Bat_Dn	RO	I32	W	1	46020	2	

Table 3-9

Serial number	Signal name	Read and write	Type	Unit	Gain	Address	Number	Scope
277	reserve	RW	U16			46500	1	
278	Import Power Limit *	RW	I32	W	1	46501	2	
279	Threshold SOC *	RW	U16	%	1	46503	1	
280	Export P eak L imit *	RW	I 32	W	1	46504	2	
281	ChrInLowImport *	RW	U16	N/A	1	46506	1	
282	ChrInLowTime1-StartHour *	RW	U16	N/A	1	46507	1	
283	ChrInLowTime1-StartMinute *	RW	U16	N/A	1	46508	1	
284	ChrInLowTime1-EndHour *	RW	U16	N/A	1	46509	1	
285	ChrInLowTime1-EndMinute *	RW	U16	N/A	1	46510	1	
286	ChrInLowTime2-StartHour *	RW	U16	N/A	1	46511	1	
287	ChrInLowTime2-StartMinute *	RW	U16	N/A	1	46512	1	
288	ChrInLowTime2 - EndHour *	RW	U16	N/A	1	46513	1	

289	ChrInLowTime2-EndMinute *	RW	U16	N/A	1	46514	1	

Table 3-10

Serial number	Signal name	Read and write	Type	Unit	Gain	Address	Number	Scope
290	reserve	RW	U16			46601	1	
291	reserve	RW	U16			46602	1	
292	reserve	RW	U16			46603	1	
293	reserve	RW	U16			46604	1	
294	reserve	RW	U16			46605	1	
295	reserve	RW	U16			46606	1	
296	Battery maximum charging current *	RW	I16	A	10	46607	1	H3:[0,26] H3Pro:[0,50] KH:[0,50] H1:[0 , 40] H1-G2:[0 ,40]
297	Battery maximum discharge current *	RW	I16	A	10	46608	1	H3:[0,26] H3Pro:[0,50] KH:[0,50] H1:[0 , 50] H1-G2:[0 ,40]
298	Minimum SoC *	RW	U16	%	1	46609	1	[10,100]
299	Maximum SoC *	RW	U16	%	1	46610	1	[10,100]
300	Minimum SoC OnGrid *	RW	U16	%	1	46611	1	[10,100]
301	EPS Frequency Select * _	RW	U16	N/A	N/A	46612	1	0: invalid 1:50Hz 2: 60Hz

302	EPS Oput * _	RW	U16	N/A	N/A	46613	1	0:Disable 2:EPS Mode 3:Ups Mode
303	Balance Load *	RW	U16	N/A	N/A	46614	1	0:Disable 1:Enable
304	Balance Logic First *	RW	U16	N/A	N/A	46615	1	0:Disable 1:Enable
305	Export Power L imit	RW	I32	W	1	46616	2	[0,Pmax]
306	Import Current Limit	RW	I 16	A	1 0	46618	1	
307	E xport Current Limit	RW	I 16	A	1 0	46619	1	

Table 3-11

Serial number	Signal name	Read and write	Type	Unit	Gain	Address	Number	Scope
308	system time	RW	U32	N/A	N/A	49000	2	[946684800,3155759999] local time
309	reserve	RW	U16			49002	1	
310	reserve	RW	U16			49003	1	
311	reserve	RW	U16			49004	1	
312	[Power Grid Scheduling] None Power compensation (PF)	RW	I16	N/A	1000	49005	1	(-1, -0.8] U [0.8, 1]
313	[Power Grid Scheduling] None Power compensation (Q/S)	RW	I16	N/A	1000	49006	1	[-1.000,+1.000] The equipment end converts this value into a fixed value of Q for reactive power control; where S is Smax

314	[Power grid dispatch] Active power percentage derating (0.1%)	RW	I 16	%	10	49007	1	Range: [0, 100.0] Active power fine adjustment interface
315	reserve	RW	U32			49008	2	
316	reserve	RW	U 32			49010	2	
317	reserve	RW	MLD			49012	twenty one	
318	reserve	RW	MLD			49033	twenty one	
319	reserve	RW	MLD			49054	twenty one	
320	reserve	RW	U16			49075	1	
321	reserve	RW	U16			49076	1	
322	Power on	RW	U16	N/A	N/A	49077	1	Range: [0,1] 0: invalid 1: valid 读取开关机状态请查询49228地址的寄存器
323	Shut down	RW	U16	N/A	N/A	49078	1	Range: [0,1] 0: invalid 1: valid 读取开关机状态请查询49228地址的寄存器
324	Grid standard code	RW	U16	N / A	N/A	49079	1	Reference 4.2 Power Grid Standard Code
325	reserve	RW	U32			49080	2	
326	reserve	RW	U32			49082	2	
327	reserve	RW	U32			49084	2	
328	reserve	RW	U 16			49086	1	
329	reserve	RW	U16			49087	1	

330	reserve	RW	U16			49088	1	
331	reserve	RW	MLD			49089	41	
332	reserve	RW	U32			49130	2	
333	reserve	RW	U32			49132	2	
334	reserve	RW	U32			49134	2	
335	Grid point power limit	RW	I32	W	1	49136	2	[0, Pmax] Default value: Pmax
336	reserve	RW	U16			49138	1	
337	reserve	RW	U16			49139	1	
338	reserve	RW	U16			49140	1	
339	reserve	RW	U 32			49141	2	
340	reserve	RW	MLD			49143	41	
341	Work mode	RW	U16	N/A	N/A	49203	1	1:Self Use 2:Feedin Priority 3:BackUp 4:Peak Shaving 6:Force Charge 7:Force Discharge
342	DRM	RW	U16	N / A	N/A	49206	1	0: Disable 1: Enable (Only valid under Australian safety regulations)
343	Meter1 /CT1	RW	U16	N / A	N/A	49207	1	0: OFF 1: Meter 1-PHASE 2:CT 3:Meter 3-PHASE
344	Meter2 /CT2 *	RW	U16	N / A	N/A	49208	1	0: OFF

								1: Meter 1-PHASE 2: CT 3: Meter 3-PHASE
345	BUZZ ER	RW	U16	N / A	N/A	49209	1	0: Disable 1: Enable
346	MPPT Switch	RW	U16	N / A	N/A	49210	1	0: Disable 1: Enable
347	Relay1 Switch	RW	U16	N/A	N/A	49211	1	0:Disable 1:Enable
348	Relay2 Switch	RW	U16	N/A	N/A	49212	1	0:Disable 1:Enable
349	Brightness Level	RW	U16	%	1	49221	1	0-100%
350	Year	RW	U16	N/A	1	49222	1	2000-2099
351	Month	RW	U16	N/A	1	49223	1	1-12
352	Day	RW	U16	N/A	1	49224	1	1-31
353	Hour	RW	U16	N/A	1	49225	1	0-23
354	Minute	RW	U16	N/A	1	49226	1	0-59
355	Second	RW	U16	N/A	1	49227	1	0-59
356	System Power State	RO	U16	N/A	1	49228	1	0: Turn OFF 1: Turn ON
357	Idle State	RW	U16	N/A	1	49229	1	0: Disable 1: Enable
358	Idle Loadpower Threshold	RW	U16	W	1	49230	1	Range: H3: 100~200 H3Pro: 100~600
359	Clear Idle Count	WO	U16	N/A	1	49231	1	0: Clear Idle Count
360	Key Password	RW	STR	N/A	1	49232	8	
361	Network status	RO	U16	N/A	1	49240	1	0: Not connected 1: Disconnection 2: Connection

362	Ripple Control Enable	RW	U16	N/A	1	49241	1	0: Disable 1: Enable
363	Trigger Signal	RO	U16	N/A	1	49242	1	Bit0: K1 status Bit1: K2 status Bit2: K3 status Bit3: K4 status
364	K1 Power Ratio	RW	U16	%	1	49243	1	Range: [0, 100]
365	K2 Power Ratio	RW	U16	%	1	49244	1	Range: [0, 100]
366	K3 Power Ratio	RW	U16	%	1	49245	1	Range: [0, 100]

Notice

marked * are only supported by some models or standard codes.

4 Interface usage instructions

4.1 Alarm information

Table 4-1 Alarm information

Number	Alarm	Bit	Alarm name	Level
1	Alarm 1	0	Input string voltage is high	important
2	Alarm 1	1	DC arc fault *	important
3	Alarm 1	2	String reverse connection	important
4	Alarm 1	3	reserve	
5	Alarm 1	4	reserve	
6	Alarm 1	5	reserve	
7	Alarm 1	6	reserve	
8	Alarm 1	7	Grid power outage	important
9	Alarm 1	8	Abnormal power grid voltage	important
10	Alarm 1	9	reserve	
11	Alarm 1	10	reserve	
12	Alarm 1	11	Abnormal power grid frequency	important
13	Alarm 1	12	reserve	
14	Alarm 1	13	reserve	
15	Alarm 1	14	Output overcurrent	important
16	Alarm 1	15	The DC component of the output current is too large	important

Number	Alarm	Bit	Alarm name	Level
17	Alarm 2	0	Abnormal residual current	important
18	Alarm 2	1	System grounding abnormality	important
19	Alarm 2	2	Low insulation resistance	important
20	Alarm 2	3	Temperature is too high	important
21	Alarm 2	4	reserve	
22	Alarm 2	5	reserve	
23	Alarm 2	6	reserve	
24	Alarm 2	7	reserve	
25	Alarm 2	8	reserve	

26	Alarm 2	9	Energy storage equipment abnormality	important
27	Alarm 2	10	isolated island	important
28	Alarm 2	11	reserve	
29	Alarm 2	12	reserve	
30	Alarm 2	13	reserve	
31	Alarm 2	14	Off-grid output overload *	important
32	Alarm 2	15	reserve	

Number	Alarm	Bit	Alarm name	Level
33	Alarm 3	0	reserve	
34	Alarm 3	1	reserve	
35	Alarm 3	2	reserve	
36	Alarm 3	3	External fan abnormality	important
37	Alarm 3	4	Energy storage reverse connection *	important
38	Alarm 3	5	reserve	
39	Alarm 3	6	reserve	
40	Alarm 3	7	reserve	
41	Alarm 3	8	reserve	
42	Alarm 3	9	Meter Lost	
43	Alarm 3	10	BMS Lost	
44	Alarm 3	11	reserve	
45	Alarm 3	12	reserve	
46	Alarm 3	13	reserve	
47	Alarm 3	14	reserve	
48	Alarm 3	15	reserve	

Notice

The above table is a summary of F OX inverter alarm information. Some alarms need to be equipped with corresponding function modules before they can be detected.

4.2 Grid standard code

Table 4-2 List of power grid standard codes

Enumeration value	Standard name	Applicable countries or regions
0	AS4777_AU	Australia
1	AS4777_NZ	New Zealand
2	G98_UK	U.K.
3	G99_UK	U.K.
4	EN50549_NL	Netherlands
5	CEI021_A	Italy
6	VDE0126	Germany
7	VDE4105_DE	Germany
8	NBR-220_BR	Brazil
9	NBR-240_BR	Brazil
10	IEC61727	India
11	Philippines	the Philippines
12	NRS_SA	South Africa
13	Vietnam	Vietnam
14	EN50549_PL	Poland
15	EN50549_PT	Portugal
16	PPDS_CR	Czech Republic
17	UNE-206_SP	Spain
18	RD1699_SP	Spain
19	Belgium	Belgium
20	VFR2019_FR	France
21	UTE_FR	France
22	Singapore	Singapore
23	Indonesia	Indonesia
24	Malaysia	Malaysia
25	Cambodia	Cambodia
26	PEA_TH	Thailand
27	MEA_TH	Thailand

Enumeration value	Standard name	Applicable countries or regions
28	Sri Lanka	Sri Lanka
29	Pakistan	Pakistan
30	Ireland	Ireland
31	Denmark 3.2.1	Denmark
32	Slovakia	Slovakia
33	Austria	Austria
34	Switzerland	Switzerland
35	Slovenia	slovenia
36	Hungary	Hungary
3 7	Serbia	Serbia
3 8	Croatia	Croatia
39	Turkey	Türkiye
40	Cyprus	Cyprus
41	Bulgaria	Bulgaria
42	Romania	Romania
43	Greece	Greece
44	Latvia	Latvia
45	Lithuania	Lithuania
46	Estonia	Estonia
47	Sweden	Sweden
48	Norway	Norway
49	Finland	Finland
50	Argentina	Argentina
51	Chile BT	Chile
52	Mexico	Mexico
53	USA	USA
54	Hawaii	Canada
55	CQC_CN	China
56	Japan	Japan
57	CQC_CN-1	China (wide range)
58	Local	India (wide range)

Enumeration value	Standard name	Applicable countries or regions
59	Saudi Arabia	Saudi Arabia
60	AS4777_AU-2020A	Australia(A)
61	AS4777_AU-2020B	Australia(B)
62	AS4777_AU-2020C	Australia(C)
63	AS4777_NZ-2020	New Zealand
64	CQC_CN-2	China (wide range 2)
65	CEI021_B	Italy
6 6	CEI021_Areti_A	Italy
6 7	CEI021_Areti_B	Italy
6 8	NBR-220_BR2022	Brazil
6 9	Spain	Spain
70	CQC_CN-3	China
71	Puerto Rico	Puerto Rico
72	G98_NI	Northern Ireland
73	G99_NI	Northern Ireland
74	USA-208	USA
75	VDE4110_DE	Germany
76	KSC8564	South Korea
77	KSC8565	South Korea
78	PR-LUMA	Puerto Rico
79	CEI016	Italy
80	DUBAI	Dubai
81	Denmark3.2.2	Denmark
82	TR 3.3.1-DK1	Denmark
83	TR 3.3.1-DK2	Denmark
84	Chile MT-A	Chile
85	Chile MT- B	Chile

Notice

The setting of the power grid standard code needs to be selected according to local regulatory requirements.

5 Communication protocol overview

The Modbus communication protocol is divided into the following layers (Physical layer, Data link layer, and Application layer), which are described layer by layer:

Application layer
Data link layer
Physical layer

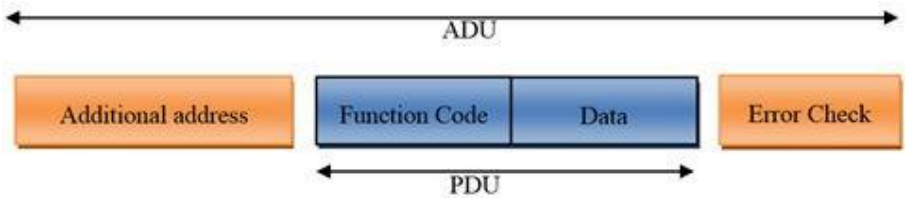
5.1 Physical layer

FoxESS inverter provides Modbus communication based on RS485 physical layer medium. Comply with Modbus-RTU format convention.

5.2 Data link layer

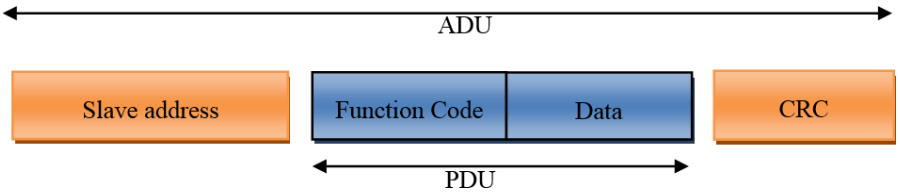
The general frame structure of the Modbus protocol is as follows:

Figure 5-2 Modbus general frame format



5.2.1 Modbus-RTU

Figure 5-3 Modbus-RTU frame format



5.2.1.1 ADU length

Based on the serial bus ADU is designed according to 256 bytes, where:

Slave address : 1 byte

CRC : 2 bytes

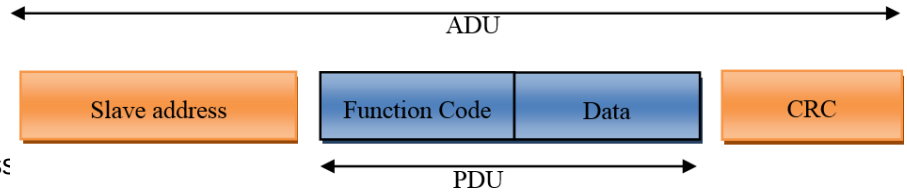
PDU: : 253 bytes

5.2.1.2 Mailing address

Modbus-RTU communication is commonly used in serial communication . Slave address represents the

slave address.

Figure 5-4 Modbus general frame format



The address

Table 5-1 Serial link address allocation

Broadcast address	Slave node address	Reserve
0	1 ~ 247	248 ～ 255

The address is reserved for use as a control access to the communication extension module object. FoxESS reserves the right to distribute and use it uniformly.

5.2.1.3 CRC check

The CRC check range is the check of all bytes before the CRC field, using 16-bit CRC check. The implemented reference code is as follows:

```
  static unsigned char auchCRCHi[] = {
  0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0, 0x80, 0x41, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81,
  0x40, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81, 0x40, 0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0,
  0x80, 0x41, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81, 0x40, 0x00, 0xC1, 0x81, 0x40, 0x01,
  0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0, 0x80, 0x41, 0x01, 0xC0, 0x80, 0x41,

0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81, 0x40, 0x00, 0xC1, 0x81,
0x40, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0, 0x80, 0x41, 0x01, 0xC0,
0x80, 0x41, 0x00, 0xC1, 0x81, 0x40, 0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0, 0x80, 0x41, 0x01,
0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81, 0x40,
0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0, 0x80, 0x41, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81,
0x40, 0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0,
0x80, 0x41, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81, 0x40, 0x00, 0xC1, 0x81, 0x40, 0x01,
0xC0, 0x80, 0x41, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0, 0x80, 0x41,
0x00, 0xC1, 0x81, 0x40, 0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81,
0x40, 0x01, 0xC0, 0x80, 0x41, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0,
0x80, 0x41, 0x00, 0xC1, 0x81, 0x40, 0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0, 0x80, 0x41, 0x01,
0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81, 0x40, 0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0, 0x80, 0x41,
0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0, 0x80, 0x41, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81,
0x40
} ;

/* CRC value of low byte */ static char auchCRCLo[] =
{
0x00, 0xC0, 0xC1, 0x01, 0xC3, 0x03, 0x02, 0xC2, 0xC6, 0x06, 0x07, 0xC7, 0x05, 0xC5, 0xC4,
0x04, 0xCC, 0x0C, 0x0D, 0xCD, 0x0F, 0xCF, 0xCE, 0x0E, 0x0A, 0xCA, 0xCB, 0x0B, 0xC9, 0x09,
0x08, 0xC8, 0xD8, 0x18, 0x19, 0xD9, 0x1B, 0xDB, 0xDA, 0x1A, 0x1E, 0xDE, 0xDF, 0x1F, 0xDD,
0x1D, 0x1C, 0xDC, 0x14, 0xD4, 0xD5, 0x15, 0xD7, 0x17, 0x16, 0xD6, 0xD2, 0x12, 0x13, 0xD3,
0x11, 0xD1, 0xD0, 0x10, 0xF0, 0x30, 0x31, 0xF1, 0x33, 0xF3, 0xF2, 0x32, 0x36, 0xF6, 0xF7,
0x37, 0xF5, 0x35, 0x34, 0xF4, 0x3C, 0xFC, 0xFD, 0x3D, 0xFF, 0x3F, 0x3E, 0xFE, 0xFA, 0x3A,
0x3B, 0xFB, 0x39, 0xF9, 0xF8, 0x38, 0x28, 0xE8, 0xE9, 0x29, 0xEB, 0x2B, 0x2A, 0xEA, 0xEE,
0x2E, 0x2F, 0xEF, 0x2D, 0xED, 0xEC, 0x2C, 0xE4, 0x24, 0x25, 0xE5, 0x27, 0xE7, 0xE6, 0x26,
0x22, 0xE2, 0xE3, 0x23, 0xE1, 0x21, 0x20, 0xE0, 0xA0, 0x60, 0x61, 0xA1, 0x63, 0xA3, 0xA2,
0x62, 0x66, 0xA6, 0xA7, 0x67, 0xA5, 0x65, 0x64, 0xA4, 0x6C, 0xAC, 0xAD, 0x6D, 0xAF, 0x6F,
0x6E, 0xAE, 0xAA, 0x6A, 0x6B, 0xAB, 0x69, 0xA9, 0xA8, 0x68, 0x78, 0xB8, 0xB9, 0x79, 0xBB,
0x7B, 0x7A, 0xBA, 0xBE, 0x7E, 0x7F, 0xBF, 0x7D, 0xBD, 0xBC, 0x7C, 0xB4, 0x74, 0x75, 0xB5,
0x77, 0xB7, 0xB6, 0x76, 0x72, 0xB2, 0xB3, 0x73, 0xB1, 0x71, 0x70, 0xB0, 0x50, 0x90, 0x91,
0x51, 0x93, 0x53, 0x52, 0x92, 0x96, 0x56, 0x57, 0x97, 0x55, 0x95, 0x94, 0x54, 0x9C, 0x5C,
0x5D, 0x9D, 0x5F, 0x9F, 0x9E, 0x5E, 0x5A, 0x9A, 0x9B, 0x5B, 0x99, 0x59, 0x58, 0x98, 0x88,
0x48, 0x49, 0x89, 0x4B, 0x8B, 0x8A, 0x4A, 0x4E, 0x8E, 0x8F, 0x4F, 0x8D, 0x4D, 0x4C, 0x8C,
```

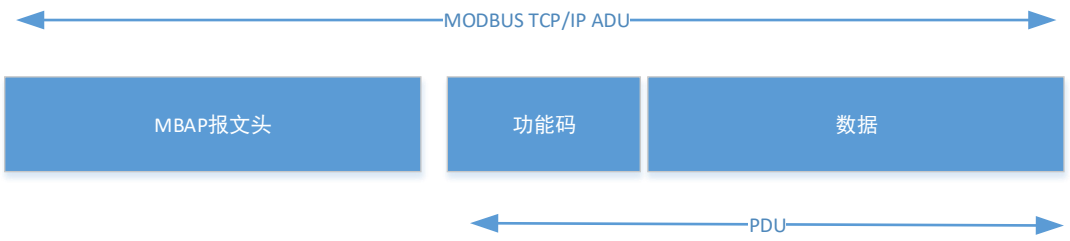
```
0x44, 0x84, 0x85, 0x45, 0x87, 0x47, 0x46, 0x86, 0x82, 0x42, 0x43, 0x83, 0x41, 0x81, 0x80,
0x40
};

unsigned short CRC16 ( puchMsg, usDataLen ) /* The function returns the CRC as an unsigned short type */ unsigned char *puchMsg ; /*
message to calculate CRC upon */
unsigned short usDataLen; /* quantity of bytes in message */
{
unsigned char uchCRCHi = 0xFF ; /* high byte of CRC initialized */ unsigned char uchCRCLo
= 0xFF ; /* low byte of CRC initialized */ unsigned uIndex ; /* will index into CRC lookup table
*/
while (usDataLen--) /* pass through message buffer */
{
uIndex = uchCRCLo ^ *puchMsg++ ; /* calculate the CRC */ uchCRCLo = uchCRCHi ^
auchCRCHi[uIndex] ;
uchCRCHi = auchCRCLo[uIndex];
}
return (uchCRCHi << 8 | uchCRCLo) ;
}
```

Code source: "MODBUS over Serial Line Specification and Implementation Guide V1.02"

5.2.2 Modbus- TCP

Figure 5-5 Modbus- TCP frame



5.2.2.1 ADU length

The standards-based recommended frame length is 260 bytes. When applying some extended functions, the data can extend the ADU to an appropriate length according to its own resource conditions to improve network transmission efficiency. The actual ADU length is reflected in the MBAP header length field.

5.2.2.2 MBAP message header

When Modbus is applied on TCP/IP, a special MBAP header (Modbus application protocol header) will be used to identify the Modbus application data unit (ADU). The MBAP header is divided into 4 fields and a total of 7 words. section, defined as follows:

Table 5-2 MBAP definition table

Data field	Length (Byte)	Description	Client	Server
Transport identifier	2	Request frame and response frame matching identifier	Client allocation, it is recommended that each frame of data request transmission identifier be different	The identifier in the server-side response frame must be consistent with the request frame
Agreement type	2	0 = MODBUS protocol	Client allocation, default is 0	The identifier in the server-side response frame must be consistent with the request frame

Data length	2	Subsequent data length	The client allocates based on actual frames	Server allocates based on actual frame length
Logical device ID	1	0	Client requests allocation based on actual frames	The identifier in the server-side response frame must be consistent with the request frame

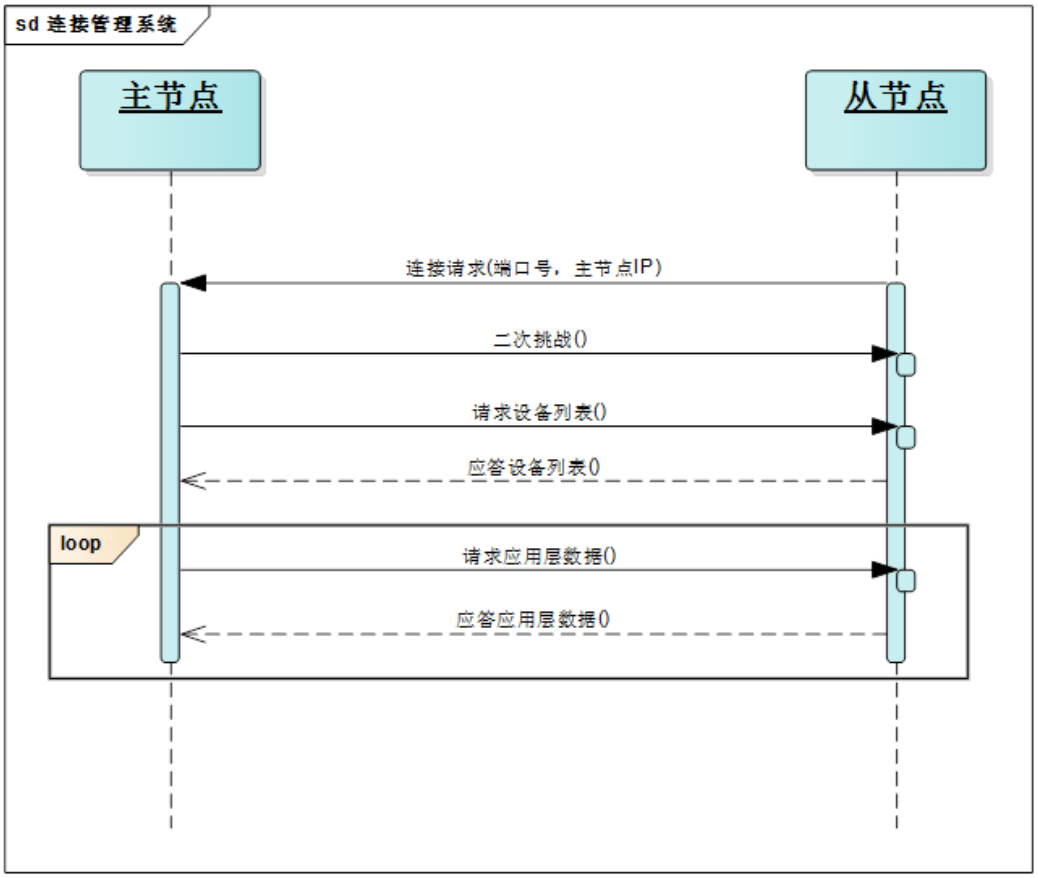
5.2.2.3 TCP port

In a LAN or VPN environment, the master node can actively initiate TCP socket link establishment to the slave node. The master node can use port 502 to request data services from the slave node.
In a cross-public network non-VPN environment, the device deployed on the internal network side needs to initiate a TCP socket link establishment to the master node exposed on the public network side. At this time, you need to preset the fixed access port number of the master node on the slave node side. Based on security and traffic streamlining considerations, the master node is required to provide at least 1 encrypted port and 1 non-encrypted port.

5.2.2.4 TCP link building process

Considering the particularity of cross-public network applications, this section only focuses on describing this scenario. The following figure describes the slave node access process:

Figure 5-7 TCP secure link establishment process



5.3 Application layer

5.3.1 Function code list

Table 5-2 Function code list

Function code	Meaning	Remark
0x03	Read register	Supports single and multiple register sequential reads
0x06	Write to a single register	Support single register write action
0x10	Write multiple registers	Supports continuous writing of multiple registers

5.3.2 Exception code list

Each network element type needs to ensure that the exception code of its product is unique, and the name and description are provided uniformly (Chinese and English description information needs to be provided in the network element interface document). Multiple versions of the same network element type must be forward compatible, and the encoding that has been used cannot be reused for others.

Table 5-3 Summary table of exception codes returned by network elements (0x00-0x8F is the public exception code segment)

Code	Name	Meaning
0x01	illegal function	For the server (or slave), the function code received in the query is an impermissible operation. This may be because the function code only applies to new equipment and is not available in the selected unit. It is also indicated that the server (or slave) handles this request in an error state, for example because it is unconfigured and requires a return register value.
0x02	Illegal data address	The query request received by the server contains a disallowed register address. More specifically, the combination of register starting address and register number is invalid. For a controller with 100 registers, the first PDU address is 0, and the last one is 99. If the starting register address in a request is 96 and the number of registers is 4, then this request can get the return value of registers 96, 97, 98, 99. If a request is submitted with a starting register address of 96 and the number of registers is 5, then the request will fail and the exception code 0x02 "illegal data address" returned, because it is trying to read registers 96, 97, 98, 99, 100, But 100 is an address that has no actual definition .
0x03	illegal data value	The value included in the query is not allowed for the server (or slave). This value indicates a failure in the remaining structure of the combined request, for example: the implicit length is incorrect. It does not mean that, because the MODBUS protocol is not aware of the significance of any special value in any special register, the data item submitted for storage in the register has a value other than that expected by the application.
0x04	Slave node device failure	During execution, the server failed.
0x06	slave device busy	The server cannot accept the MODBUS request PDU. It is the client application's responsibility to decide if and when to resend the request.
0x80	No permission	Authentication fails or permissions expire after timeout, and operation is prohibited.

5.3.3 Read register (0x03)

5.3.3.1 Master node request frame format

Table 5-4 Master node request frame format

Data field	Length	Description
Function code	1 byte	0x03
Register starting address	2 bytes	0x0000~0xFFFF
Number of registers	2 bytes	1~125

5.3.3.2 Normal response frame format from the node

Table 5-5 Normal response frame format of the slave node

Data field	Length	Description
Function code	1 byte	0x03
Number of bytes	1 byte	2×N
Register value	2×N bytes	NA

illustrate

N is the number of registers.

5.3.3.3 Slave node exception response frame format

Table 5-6 Slave node exception response frame format

Data field	Length	Description
Function code	1 byte	0x83
Exception code	1 byte	See **exception code list**

5.3.4 Write a single register (0x06)

5.3.4.1 Master node request frame format

Table 5-7 Master node request frame format

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

5.3.4.2 Normal response frame format from the node

Table 5-8 Normal response frame format of the slave node

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

5.3.4.3 Slave node exception response frame format

Table 5-9 Slave node exception response frame format

Data field	Length	Description
Function code	1 byte	0x86
Exception code	1 byte	See **exception code list**

5.3.5 Write multiple registers (0x10)

5.3.5.1 Master node request frame format

Table 5-10 Master node request frame format

Data field	Length	Description
Function code	1 byte	0x10
Register starting address	2 bytes	0x0000~0xFFFF
Number of registers	2 bytes	0x0000~0x007B
Number of bytes	1 byte	2×N
Register value	2×N bytes	Value

illustrate

N is the number of registers.

5.3.5.2 Normal response frame format from the node

Table 5-11 Normal response frame format of the slave node

Data field	Length	Description
Function code	1 byte	0x10
Register address	2 bytes	0x0000~0xFFFF
Number of registers	2 bytes	0x0000~0x007B

5.3.5.3 Slave node exception response frame format

Table 5-12 Slave node exception response frame format

Data field	Length	Description
Function code	1 byte	0x90
Exception code	1 byte	See **exception code list**

5.3.6 Configure slave address

This function is used to configure the M OSBUS address .

The data frame is composed as follows :

Data field	Value	Description
Slave address	0xF9	Configure the slave address exclusively
Function code	0x06	Write to a single register
Register address	0x5A5A	special address
Register value	2 bytes	Write slave address Range: 10 - 99
CRC 16	2 bytes	

Change record table

version number	change log	time
V1.0	First edition	2023.07.18
V1.01.00.00	Add register definition and Modbus-TCP definition	2023.11.08
V1.02.00.00	Add some registers to optimise document formatting	2023.12.06
V1.03.00.00	Add some registers	2023.12.29
V1.04.00.00	Add some registers, and the meter lost information.	2024.03.20
V1.05.00.00	1. Add register 30032, 36100, 36116, 36132, 36148, 36200, 36216, 36232, 36248, 37635, 38333, and 45002, etc. 2. Modify the definition information for registers 37632, 38330, 39118, etc. 3. Add Alarm 43 information.	2024.05.16
V1.05.01.00	1. Modify the defined Bits 3:2 for reguster 46001.	2024.05.17
V1.05.02.00	1. Add register 37636, 38334, 45003, 45005, 45006, 45007, 49232, 49240, 49241, 49242, 49243, 49244, 49245, etc. 2. Modfiy the definition information for registers 37619, 37620, 38317, 38318, 46001, etc.	2024.08.15