# KinCony KCSv3 protocol – Modbus

Note: This protocol document use for KinCony ESP32-S3 smart controller:

you need to download KCS v3 firmware to ESP32-S3 firstly.

Different board will have different channel of digital output, digital input , ADC, DAC,IR, RF. So the protocol is same , just according to the hardware resource to set channel number.

## Modbus send command format:

| Data | byte | description | remark |
|---|---|---|---|
| 01 | 1 | Modbus Address | range 01-FE |
| 01 | 1 | Function code | 01: read digital output state |
| 0000 | 2 | register address | 0000-starting register address |
| 0040 | 2 | register number | if KC868-A64 read 64 output state, will receive 8 bytes. 0x40 means 64 channel |
| 3DFA | 2 | CRC | Modbus CRC |

## Modbus receive command format:

| Data | byte | description | remark |
|---|---|---|---|
| 01 | 1 | Modbus Address | range 01-FE |
| 01 | 1 | Function code | 01: read digital output state |
| 08 | 1 | Data length | Read 8 bytes |
| 8000000000000000 | 8 | Read data | 8byte: 64 channel output |
| 3C7D | 2 | CRC | Modbus CRC |

The above is an example of the structure of the Modbus communication

(read digital output state)

1. read digital output state function code : 01

send：01 01 00 00 00 40 FA 3D
receive：01 01 08 00 00 00 00 00 00 00 80 BD 35

Send message: register address 0x0000 register number:0x40 = 64 channel digital output
Receive message: data length=8 bytes, D7,D6,D5,D4,D3,D2,D1,D0

D0=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=output8-1 bit7=output8 …… bit0=output1
D1=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=output16-9 bit7=output16 …… bit0=output9
D2=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=output24-17 bit7=output16 …… bit0=output17
D3=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=output32-25 bit7=output32 …… bit0=output25
D4=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=output40-33 bit7=output40 …… bit0=output33
D5=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=output48-41 bit7=output48 …… bit0=output41
D6=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=output56-49 bit7=output49 …… bit0=output49
D7=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=output64-57 bit7=output64 …… bit0=output57

Every bit=1: ON bit=0: OFF

For example:
Feedback: 01 01 08 00 00 00 00 00 00 00 80 BD 35
D7=0x00
D6=0x00
D5=0x00
D4=0x00
D3=0x00
D2=0x00
D1=0x00
D0=0x80=(10000000)binary means: output8:ON output1-7:OFF
---

Note: you can read any register address and number. For example , you can send “01 01 00 01 00 07 08 2C” that means read total 7 channels data begin with channel-2’s address. It will feedback “01 01 01 40 50 78”, read the data is 0x40=(01000000)binary, only the lower 7 bits are valid, it’s the value of the output8-2, the highest bit 0 is meaningless, not the value of the output9.

2. Read all digital input state function code: 02

send：01 02 00 00 00 40 FA 79
receive：01 02 08 00 00 00 00 00 00 00 02 D3 45

Send message: register address 0x0000 register number:0x40 = 64 channel digital input
Receive message: data length=8 bytes, D7,D6,D5,D4,D3,D2,D1,D0

D0=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=input8-1 bit7=input8 …… bit0=input1
D1=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=input16-9 bit7=input16 …… bit0=input9
D2=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=input24-17 bit7=input16 …… bit0=input17
D3=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=input32-25 bit7=input32 …… bit0=input25
D4=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=input40-33 bit7=input40 …… bit0=input33
D5=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=input48-41 bit7=input48 …… bit0=input41
D6=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=input56-49 bit7=input49 …… bit0=input49
D7=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=input64-57 bit7=input64 …… bit0=input57

Every bit=1: trigger bit=0: not trigger

For example:
Feedback: 01 01 08 00 00 00 00 00 00 00 80 BD 35
D7=0x00
D6=0x00
D5=0x00
D4=0x00
D3=0x00
D2=0x00
D1=0x00
D0=0x02=(00000010)binary means: input2: trigger input1-7: not trigger
---
Note: you can read any register address and number.

3. Read ADC (analog input) state Function code: 03
send：01 03 00 00 00 04 09 44
receive：01 03 08 0A 32 00 00 00 00 00 00 06 6B

Send message: register address 0x0000 register number:0x04 = 4 channel ADC
If register number>ADC channel number, just feedback until MAX number's ADC data.

Receive message: data length=8 bytes for 4 channel ADC data, because 10-bit ADC precision, every 2 bytes is one channel's data . "08 0A" = 0x80A=(2058)decimal= ADC1 original acquisition value, others ADC channel all are 0.

4. Read DAC (analog output) state Function code: 04
send：01 04 00 00 00 02 09 44
receive：01 04 02 00 32 E5 38

Send message: register address 0x0000 register number:0x02 = 2 channel DAC
If register number>DAC channel number, just feedback until MAX number's DAC data.

Receive message: data length=2 bytes for 2 channel DAC data, DAC1=0x00, DAC2=0x32

5. Set ON/OFF one channel of digital output Function code: 05
send：01 05 00 00 FF 00 8C 3A
receive：01 05 02 FF 00 F9 3C

Send message: register address 0x0000 (FF 00): ON (00 00): OFF
For example:
01 05 00 00 FF 00 8C 3A turn ON output1
01 05 00 00 00 00 CD CA turn OFF output1

6. Set DAC Function code: 06
send：01 06 00 00 00 25 11 48
receive：01 06 02 00 25 F9 3C

Send message: register address 0x0000 fifth byte 0x00 is always fixed, never change it. Sixth byte is DAC set value. This command is set DAC1=0x25

7. Set ON/OFF multi channel of digital output Function code: 0F

send：01 0F 00 00 00 40 00 00 00 00 00 00 00 05 0F 4E
receive：01 0F 02 00 00 BB 14

Send message: register address 0x0000 register number:0x40 = 64 channel digital output

data length=8 bytes, D7,D6,D5,D4,D3,D2,D1,D0

D0=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=output8-1 bit7=output8 …… bit0=output1
D1=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=output16-9 bit7=output16 …… bit0=output9
D2=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=output24-17 bit7=output16 …… bit0=output17
D3=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=output32-25 bit7=output32 …… bit0=output25
D4=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=output40-33 bit7=output40 …… bit0=output33
D5=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=output48-41 bit7=output48 …… bit0=output41
D6=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=output56-49 bit7=output49 …… bit0=output49
D7=(bit7 bit6 bit5 bit4 bit3 bit2 bit1 bit0)b=output64-57 bit7=output64 …… bit0=output57

Every bit=1: ON bit=0: OFF

D7=0x00=(00000000)binary means: output64-57:OFF
D6=0x00=(00000000)binary means: output56-49:OFF
D5=0x00=(00000000)binary means: output48-41:OFF
D4=0x00=(00000000)binary means: output40-33:OFF
D3=0x00=(00000000)binary means: output32-25:OFF
D2=0x00=(00000000)binary means: output24-17:OFF
D1=0x00=(00000000)binary means: output16-9:OFF
D0=0x05=(00000101)binary means: output1,3:ON others:OFF

Receive message: data length=2 bytes “00 00” means successful control.

8. Set ON/OFF/TOGGLE for any multi channel of digital output Function code: 0E
send：01 0E 00 00 00 40 00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 20 33 78
receive：01 0E 02 00 00 BA E8

Send message: register address 0x0000 register number:0x40 = 64 channel digital output. In fact, these two parameters do not matter.

if use KC868-A64 , it have 64 digital output, every byte have 8 bit, every bit mean every digital output state, so KC868-A64 have 8 bytes. We will use ON/OFF/TOGGLE for these, so total need 8*3=24 bytes.

(D23,D22,D21,D20,D19,D18,D17,D16) use for ON command
(D15,D14,D13,D12,D11,D10,D9,D8) use for OFF command
(D7,D6,D5,D4,D3,D2,D1,D0) use for TOGGLE command
D23,D22,D21,D20,D19,D18,D17,D16,D15,D14,D13,D12,D11,D10,D9,D8,D7,D6,D5,D4,D3,D2,D1,D0
are “decimal” number, every data convert to binary, bit ”1” is effective , bit “0” is ineffective.

For example:
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 20
D24 D23 D22 …… D2 D1 D0
D16=0x80=(10000000)b means: turn ON output-8
D8=0x40=(01000000)b means: turn OFF output-7

D0=0x20=(00100000)b  means: TOGGLE output-6

So send this command, will turn ON output-8,turn OFF output-7, TOGGLE output-6 simultaneously.

---

9. For IR sender / receiver function

// 01: Address
// 08: Function code - Learn IR
// 00 05: Register address, 05 means ID=6 because ID begin with 0
// 00 04: Send IR tube, values range from 1-8. 04 means the 4th channel
// F1 C9: CRC
send：01 08 00 05 00 04 F1 C9

// 01: Address
// 08: Function code - Learn IR
// 02: Data length
// 00 05: Data value, corresponding to the register address when transmitting
// 7A 63: CRC
receive：01 08 02 00 05 7A 63

---

// 01: Address
// 07: Function code - Send IR
// 00 02: Register address, send IR at index 2, which ID=3
// 00 01: Register count, fixed value 1, only one infrared can be controlled at a time
// D4 0A: CRC
send：01 07 00 02 00 01 D4 0A

// 01: Address
// 07: Function code - Send IR
// 02: Data length
// 00 02: Data value, corresponding to the register address when transmitting
// 38 B5: CRC
receive：01 07 02 00 02 38 B5

---

// 01: Address
// 09: Function code - Delete IR
// 00 07: Register address, 07 means ID=8
// 00 01: Register count, fixed value 1, only one infrared can be deleted at a time
// AD CA: CRC
send：01 09 00 07 00 01 AD CA

// 01: Address
// 09: Function code - Delete IR
// 02: Data length
// 00 07: Data value, corresponding to the register address when transmitting
// FA 5E: CRC
receive：01 09 02 00 07 FA 5E