RD6006 Protocol USB-serial: reverse engineering

This is from a reverse engineering of data protocol between the Riden Window 10 SW and a RD6006-W.
This is not complete: it is a work in progress, open to all contributions.
Riden assured me that he would like to make the protocol public in the near future ... For now you can use this.

Used tools:

- ***Termite***, HEX terminal COM, free https://www.compuphase.com/products_en.htm
- ***Serialmon***, COM sniffer test-mode https://www.dunovo.com/
- ***Online CRC Calculator*** https://crccalc.com/

MODBUS Protocol

Set bits: 8N1
Set baudrate: 115200
DTR/DSR

Frame description :

Slave Address	Function Code	Data	CRC
1 byte	1 byte	0 up to 252 byte(s)	2 bytes CRC Low, CRC Hi

Figure 12: RTU Message Frame

Slave Address: 1..247 (0: broadcast)
Function code: see later
Data: 0..252 byte(s)
CRC16-MODBUS: see https://crccalc.com/ for code.

Function descriptions

0x03: read registers (WORD16)

Master: (read DATA0 values)

ADDR	FUNC	DATA start Addr HI	DATA start Addr LO	DATA Word# HI	DATA Word# LO	CRC HI	CRC LO
0x01	0x03	0x00	0x50	0x00	0x04	0x44	0x18

Slave: (get DATA0 values: V-SET I-SET S-OVP S-OCP)

ADDR	FUNC	DATA byte count	DATA byte [50] HI	DATA byte [50] LO	DATA byte [51] HI	DATA byte [51] LO	DATA byte [52] HI	DATA byte [52] LO	DATA byte [53] HI	DATA byte [53] LO	CRC HI	CRC LO
0x01	0x03	0x08	0x01	0xF4	0x0B	0xC2	0x02	0xBB	0x0F	0x96	0x6D	0x7D

0x06: Set single register (WORD16)

Master: (set OUTPUT ON)

ADDR	FUNC	DATA start Addr HI	DATA start Addr LO	DATA Word HI	DATA Word LO	CRC HI	CRC LO
0x01	0x06	0x00	0x08	0x00	0x01	0xC9	0xC8

Slave: echo

ADDR	FUNC	DATA start Addr HI	DATA start Addr LO	DATA Word HI	DATA Word LO	CRC HI	CRC LO
0x01	0x06	0x00	0x08	0x00	0x01	0xC9	0xC8

0x10 Set multiple registers (WORD16)

Master: (set DATA0 values: V-SET I-SET S-OVP S-OCP)

ADDR	FUNC	DATA start Addr HI	DATA start Addr LO	DATA Word count # HI	DATA Word count # LO	DATA bytes count	DATA byte [50] HI	DATA byte [50] LO	DATA byte [51] HI	DATA byte [51] LO	DATA byte [52] HI	DATA byte [52] LO	DATA byte [53] HI	DATA byte [53] LO	CRC HI	CRC LO
0x01	0x10	0x00	0x50	0x00	0x04	0x08	0x00	0xF4	0x0B	0xC2	0x02	0xBB	0x0F	0x96	0x55	0xAA

Slave: ok

ADDR	FUNC	DATA start Addr HI	DATA start Addr LO	DATA Word count# HI	DATA Word count# LO	CRC HI	CRC LO
0x01	0x10	0x00	0x50	0x00	0x04	0xDB	0x50

MODBUS also defines other functions, but they do not seem to be used by RD6006

NOTE on RD6006 Protocol

At startup the WIN program (Master):

1) sends: “queryd” + 0x0D + 0x0A

2) reads 0000 – 0003 registers

3) sets 000F (CONNECTED) register to 1

4) Reads 0048 (backliught) register

….. more user operations

…. polling loop using: 0x01 0x03 0x00 0x04 0x00 0x26 0x85 0xD1

to get registers 0x0004 …0x0029

-2) sets 0012 (OUTPUT) register to OFF

-1) sets 000F (CONNECTED) register to 0

RD6006 registers

Thi is the current list (incomplete) of registers I found.

0000	0xEA 0x9E	Signature = 60062
0001	0x00 0x00 ??	??
0002	0x19 0x40	Serial number (6464)
0003	0x00 0x80	Firmware version (1.28) x 100
0004	0x00 0x00 ??	??
0005	TEMP SYS C	
0006	0x00 0x00 ??	??
0007	TEMP SYS F	
0008	V-SET	V value x 100
0009	I-SET	I value x 1000
000A	V-OUT	V value x 100
000B	I-OUT	I value x 1000
000C		
000D		
000E	V-INPUT	V value x 100
000F	CONNECTED	0 = local, 1 = connected
0010		
0011		
0012	OUTPUT ON/OFF	0= OFF, 1=ON
0013		
0014		
0015		
0016		
0017		
0018		
0019		
001A		
001B		
001C		
001D		
001E		
001F		
0020		
0021		
0022	00 ??	??
0023	TEMP PROBE C	
0024	00 ??	??
0025	TEMP PROBE F	
0026	AMPEREH HI	Ah value x 1000
0027	AMPEREH LO	
0028	WATTH HI	Wh value x 1000
0029	WATTH LO	
002A		
002B		
002C		
002D		
002E		
002F		

0030	CLOCK YY	
0031	CLOCK MM	
0032	CLOCK DD	
0033	CLOCK hh	
0034	CLOCK mm	
0035	CLOCK ss	
0036		
0037		
0038		
0039		
003A		
003B		
003C		
003D		
003E		
003F		
0040		
0041		
0042		
0043		
0044		
0045		
0046		
0047		
0048	BACKLIGHT	Values: 0..5
0049		
004A		
004B		
004C		
004D		
004E		
004F		
0050	DATA0 V-SET	
0051	DATA0 I-SET	
0052	DATA0 S-VOP	
0053	DATA0 S-OCP	
0054	DATA1 V-SET	
0055	DATA1 I-SET	
0056	DATA1 S-VOP	
0057	DATA1 S-OCP	
0058	DATA2 V-SET	
0059	DATA2 I-SET	
005A	DATA2 S-VOP	
005B	DATA2 S-OCP	
005C	DATA3 V-SET	
005D	DATA3 I-SET	
005E	DATA3 S-VOP	
005F	DATA3 S-OCP	
0060	DATA4 V-SET	
0061	DATA4 I-SET	
0062	DATA4 S-VOP	
0063	DATA4 S-OCP	

0064	DATA5 V-SET	
0065	DATA5 I-SET	
0066	DATA5 S-VOP	
0067	DATA5 S-OCP	
0068	DATA6 V-SET	
0069	DATA6 I-SET	
006A	DATA6 S-VOP	
006B	DATA6 S-OCP	
006C	DATA7 V-SET	
006D	DATA7 I-SET	
006E	DATA7 S-VOP	
006F	DATA7 S-OCP	
0070	DATA8 V-SET	
0071	DATA8 I-SET	
0072	DATA8 S-VOP	
0073	DATA8 S-OCP	
0074	DATA9 V-SET	
0075	DATA9 I-SET	
0076	DATA9 S-VOP	
0077	DATA9 S-OCP	
0078		
0079		
007A		
007B		
007C		
007D		
007E		
007F		
0080		