

Version: V3.1

Level: Confidential

Shenzhen Concox Information Technology Co., Ltd

GPS Tracker

Communication Protocol

(JM-VL02,JM-VG03,JM-VG04,EG02,EG03,JM01,JV200,GT300,GT800,MT200,
OB22,X3,Q2,GT08,Wetrack lite,ET25,HVT001)

Writer	Date	Version	Description
	2019-4-28	V2.4	Add the alarm bit 19 in the alarm packet
	2019-9-27	V2.5	Add EG02 model
	2020-3-10	V2.6	Delete U20 model and add alarm code
	2020-5-8	V2.7	Add VL02 model Change the protocol number of EG02 heartbeat package to 23
	2020-6-11	V2.8	Add VG03 model
	2020-6-19	V2.9	Add EG03 model
	2021-1-26	V3.0	Add 0x5E Pulse signal line cut-off alarm of GT800
	2021-2-19	V3.1	Add VG04 model and 0X01 in the 94 00 packet

Content

目录

I. PROTOCOL PACKET FORMAT	4
1.1 Protocol Number	4
II. PROTOCOL PACKET	5
1. Login packet	5
1.1 Login message packet	5
1.2 Login packet response (server response)	6
2. Heartbeat Packet	7
2.1. Heartbeat packet sent by terminal	7
2.2 Server responds the heartbeat packet	8
3. GPS location packet	9
3.1 Location packet sent by terminal	9
3.2 Server location packet response	11
4 LBS Multiple Bases Extension Packet	12
4.1 Terminal sent LBS multiple bases extension packet	12
4.2 Server reply: No need to reply.	13
5 WIFI Information Protocol (Q2\HVT001)	13
5.1 WiFi packet sent by terminal	13
5.2 WIFI packet responded by sever	15
6 Alarm Packet	16
6.1 Alarm packet sent by terminal	16
6.2 Alarm packet response of server	20
7 Alarm Packet (LBS)	21
7.1 Alarm packet sent by terminal	21
8 Online command	23
8.1 Online command sent by server	23
8.2 Online command replied by terminal	23
9 Time calibration Packet	25
9.1 Time request sent by terminal	25
9.2 Server response time information	25
10 Information transmission packet	26
10.1 Information transmission packet sent by terminal	26
10.2 Server Response Information Transmission Packet	31
11 External device transfer protocol (apply X3)	31
11.1 Device send transparent data to server	31
11.2 Server Response transfer data Packet	31
12 Large File Transfer (apply to HVT001)	32
12.1 Terminal transfers the file to the server (8D)	32

III. APPENDIX	34
1. code fragment of the CRC-ITU lookup table algorithm implemented based on C language	34
2. Data Flow Diagram.....	35

ConcoX

I. Protocol Packet Format

Format	Length (Byte)	Description
Start Bit	2	0x780x78 (packet length : 1bit) or 0x79x79 (packet length 2 bits)
Packet Length	1(2)	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number	1	Transmission packet type (see the following diagram for details)
Information Content	N	The specific contents are determined by the protocol numbers corresponding to different applications.
Information Serial Number	2	The serial number of the first GPRS data (including status packet and data packet such as GPS, LBS) sent after booting is '1', and the serial number of data sent later at each time will be automatically added '1'.
Error Check	2	Serial Number (including "Packet Length" and "Information Serial Number"), are values of CRC-ITU. CRC error occurs when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit	2	Fixed value:0x0D0x0A

1.1 Protocol Number

Login Information	0x01
Positioning Data (UTC)	0x22
Heartbeat Packet	0x13
EG02\EG03 Heartbeat Packet	0x23
Online Command Response of Terminal	0x21 (0x15)
Alarm Data (UTC)	0x26
LBS Alarm	0x19
Alarm Data(UTC) apply to HVT001	0x27
Online Command	0x80
Time Check Packet	0x8A
WIFI Communication Protocol	0x2C
Information Transmission Packet	0x94
External device transfer Packet(apply X3)	0x9B
Server Response transfer data Packet	0x9B
External module transmission Packet	0x9C

II. Protocol Packet

1. Login packet

Description:

- Login packet is the information packet connecting the terminal and platform. It can send terminal information to platform.
- If a GPRS connection is established successfully, the terminal will send a first login message packet to the server and, within five seconds, if the terminal receives a data packet responded by the server, the connection is considered to be a normal connection; if not, the terminal will send login packet again.
- If no packet returned by server within 5 seconds, then the response of login packet is timeout.
- Terminal reboot automatically after 3 timeouts.

1.1 Login message packet

		Length	Description
Start Bit		2	0x78 0x78
Packet Length		1	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number		1	0x01
Information Content	Terminal ID	8	Example: IMEI number is 123456789123456, terminal ID is: 0x01 0x23 0x45 0x67 0x89 0x120x34 0x56
	Model Identification Code	2	Distinguish model of terminal by identification code.
	Time Zone Language	2	See the following chart for details of time zone language mark.
Information Serial Number		2	The serial number of the first GPRS data (including status packet and data packet such as GPS, LBS) sent after booting is '1', and the serial number of data sent later at each time will be automatically added '1'.
Error Check		2	Error check (From "Packet Length" to "Information Serial Number") , are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit		2	Fixed value:0x0D 0x0A

Example: 78 78 11 01 07 52 53 36 78 90 02 42 70 00 32 01 00 05 12 79 0D 0A

Time Zone Language

One and a half bits bit15—bit4	15	Time zone value expands 100 times	
	14		
	13		
	12		
	11		
	10		
	9		
	8		
	7		
	6		
	5		
	4		
Lower half bit4-bit0	3	GMT	
	2	No definition	
	1	Language Select Bit	Chinese
	0	Language Select Bit	English

Bit3 0-----Eastern time

1-----Western time

Example: Extended bit: 0x32 0x00 means GMT+8

Calculation method: $8 \times 100 = 800$ converts to HEX: 0X0320

Extended bit: 0x4D 0xD8 means GMT-12:45

Calculation method: $12.45 \times 100 = 1245$ converts to HEX: 0x04 0xDD

Here, to save 4 bytes, calculation result left shifted 4 bits and combined eastern time, western time and language bit.

1.2 Login packet response (server response)

1.	Length	Description
Start Bit	2	0x78 0x78
Packet Length	1	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number	1	0x01
Information Serial Number	2	Serial number of data sent later each time will be automatically added '1'.
Error Check	2	Error check (From "Packet Length" to "Information Serial Number"), are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit	2	Fixed value: 0x0D 0x0A

Example: 78 78 05 01 00 05 9F F8 0D 0A

2. Heartbeat Packet

Description:

- Heartbeat packet is a data packet to maintain the connection between the terminal and the server.
- If a GPRS connection is established successfully, the terminal will send a first login message packet to the server and, within five seconds, if the terminal receives a data packet responded by the server, the connection is considered to be a normal connection; if not, the terminal will send login packet again.
- If no packet returned by server within 5 seconds, then the response of heartbeat packet is timeout.
- Terminal reboot automatically after 3 timeouts.

2.1. Heartbeat packet sent by terminal

Heartbeat Packet

		Length (Byte)	Description
Start Bit		2	0x78 0x78
Packet Length		1	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number		1	0x13(EG02\EG03: 0x23)
Information Content	Terminal Information Content	1	See the following diagram for details
	External voltage (Suitable for EG02\EG03 model)	2	Transformation method: To divide by 100 after convert hexadecimal decimal. Example: 0X0F,0X92, 0F92converted to decimal is 3986. Divide 3986 by 100 get 39.86. 39.86 is the external voltage value of the device
	Built-in battery voltage Level (EG02\EG03 without this byte)	1	0x00: No Power (shutdown) 0x01: Extremely Low Battery 0x02: Very Low Battery (Low Battery Alarm) 0x03: Low Battery (can be used normally) 0x04: Medium 0x05: High 0x06: Full
	GSM Signal Strength	1	0x00: no signal; 0x01: extremely weak signal; 0x02: weak signal; 0x03: good signal; 0x04: strong signal.
	Language/Extended Port Status	2	latter bit 0x01 Chinese 0x02 English
Serial Number		2	Serial number of data sent later each time will be automatically added '1'.
Error Check		2	Error check (From "Packet Length" to "Information Serial Number") , are values of CRC-ITU. CRC error occur when

		the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit	2	Fixed value: 0x0D 0x0A

Example: 78 78 0A 13 40 04 04 00 01 00 0F DC EE 0D 0A

Example: 78 78 0B 23 05 0F 92 04 00 02 00 08 8A 37 0D 0A (EG02\EG03 heartbeat Packet)

Terminal Information

One byte is consumed defining for various status information of the mobile phone.

Bit		Code Meaning
BYTE	Bit7	1: Oil and electricity disconnected
		0: Oil and electricity connected
	Bit6	1: GPS tracking is on
		0: GPS tracking is off
	Bit3~Bit5	Extended Bit
	Bit2	1: Charge On
		0: Charge Off
	Bit1	1: ACC high
		0: ACC Low
	Bit0	1: Defense Activated
		0: Defense Deactivated

2.2 Server responds the heartbeat packet

	Length (Byte)	Description
Start Bit	2	0x78 0x78
Packet Length	1	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number	1	0x13(EG02\EG03: 0x23)
Serial Number	2	Serial number of data sent later at each time will be automatically added '1'.
Error Check	2	Error check (From "Packet Length" to "Information Serial Number"), are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit	2	Fixed value: 0x0D0x0A

Example : 78 78 05 13 01 00 E1 A0 0D 0A

78 78 05 23 00 08 F2 9E 0D 0A(EG02\EG03 heartbeat packet reply)

3. GPS location packet

Description:

- Data packet used to transmit terminal location
- Upload locating data based on rule after successfully connected and positioned.
- Re-upload locating data after successfully connected.

3.1 Location packet sent by terminal

		Length	Description
Start Bit		2	0x78 0x78
Packet Length		1	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number		1	0x22 (UTC)/0x12
Information Content	Date Time	6	Year (1byte) Month (1byte) Day (1byte) Hour (1byte) Min (1byte) Second (1byte) (converted to decimal) (Date Time)
	Quantity of GPS satellites	1	The first character is GPS information length. The second character is positioning satellite number (converted to a decimal)
	Latitude	4	Convert to a decimal and divide 1800000
	Longitude	4	Convert to a decimal and divide 1800000
	Speed	1	Convert to a decimal
	Course, Status	2	Convert to binary number of 16 bits and calculate by bits (see the following diagram)
	MCC	2	Mobile Country Code(MCC) (converted to a decimal)
	MNC	1	Mobile Network Code(MNC)(converted to a decimal)
	LAC	2	Location Area Code (LAC) (converted to a decimal)
	Cell ID	3	Cell Tower ID(Cell ID)(converted to a decimal)
	ACC	1	ACC Status ACC low: 00, ACC high: 01 (not available for 06)
	Data Upload Mode	1	GPS data upload mode (06 series are excluded) 0x00 Upload by time interval 0x01 Upload by distance interval 0x02 Inflection point upload 0x03 ACC status upload 0x04 Re-upload the last GPS point when back to static. 0x05 Upload the last effective point when network recovers. 0x06 Update ephemeris and upload GPS data compulsorily

			0x07 Upload location when side key triggered 0x08 Upload location after power on 0x09 Unused 0x0A Upload the last longitude and latitude when device is static; time updated 0x0D Upload the last longitude and latitude when device is static 0x0E Gpsdup upload (Upload regularly in a static state.)
	GPS Real-Time Re-upload	1	0x00 Real time upload 0x01 Re-upload (06 series are excluded)
	Mileage	4	turn HEX into decimal. (Only available for devices with this function)
Serial Number		2	Serial number of data sent later at each time will be automatically added '1'.
Error Check		2	Error check (From "Packet Length" to "Information Serial Number"), are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit		2	Fixed value: 0x0D 0x0A

Example: 78 78 22 22 0F 0C 1D 02 33 05 C9 02 7A C8 18 0C 46 58 60 00 14 00 01 CC 00 28 7D 00 1F 71 00 00 01 00 08 20 86 0D 0A

i. Course & Status

Two bytes are consumed, defining the running direction of GPS. The value ranges from 0° to 360° measured clockwise from north of 0°.

BYTE_1	Bit7	0
	Bit6	0
	Bit5	GPS real-time/differential positioning
	Bit4	GPS having been positioning or not
	Bit3	East Longitude, West Longitude
	Bit2	South Latitude, North Latitude
	Bit1	Course
	Bit0	
BYTE_2	Bit7	
	Bit6	
	Bit5	
	Bit4	
	Bit3	
	Bit2	
	Bit1	

	Bit0	
--	------	--

For example: the value is 0x15 0x4C, the corresponding binary is 00010101 01001100,

BYTE_1 Bit7	0	
BYTE_1 Bit6	0	
BYTE_1 Bit5	0 (real time GPS)	
BYTE_1 Bit4	1 (GPS has been positioned)	
BYTE_1 Bit3	0 (East Longitude)	
BYTE_1 Bit2	1 (North Latitude)	
BYTE_1 Bit1	0	
BYTE_1 Bit0	1	
BYTE_2 Bit7	0	
BYTE_2 Bit6	1	
BYTE_2 Bit5	0	→ Course 332 °(0101001100 in Binary, or 332 in decimal)
BYTE_2 Bit4	0	
BYTE_2 Bit3	1	
BYTE_2 Bit2	1	
BYTE_2 Bit1	0	
BYTE_2 Bit0	0	

which means GPS tracking is on, real time GPS, location at north latitude, east longitude and the course is 332 °.

3.2 Server location packet response

Location packet server no response

4 LBS Multiple Bases Extension Packet

Description: For transmission of data packet when device is not located

4.1 Terminal sent LBS multiple bases extension packet

		Length	Description
Start Bit		2	0x78 0x78
Packet Length		1	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number		1	0x28
Information Content	DATE(UTC)	6	Year (1byte) Month (1byte) Day (1byte) Hour (1byte) Min (1byte) Second (1byte) (converted to a decimal) (Date Time)
	MCC	2	Mobile Country Code(MCC) (converted to a decimal)
	MNC	1	Mobile Network Code(MNC)(converted to a decimal)
	LAC	2	Location Area Code (LAC) (converted to a decimal)
	CI	3	Cell Tower ID(Cell ID)(converted to a decimal)
	RSSI	1	Signal level of community, range 0x00~0xFF, 0x00 Weakest signal 0xFF Strongest signal
	NLAC1	2	Same as LAC
	NCI1	3	Same as CI
	NRSSI1	1	Same as RSSI
	NLAC2	2	Same as LAC
	NCI2	3	Same as CI
	NRSSI2	1	Same as RSSI
	NLAC3	2	Same as LAC
	NCI3	3	Same as CI
	NRSSI3	1	Same as RSSI
	NLAC4	2	Same as LAC
	NCI4	3	Same as CI
	NRSSI4	1	Same as RSSI
	NLAC5	2	Same as LAC
	NCI5	3	Same as CI
	NRSSI5	1	Same as RSSI
	NLAC6	2	Same as LAC
	NCI6	3	Same as CI
	NRSSI6	1	Same as RSSI
	Timing Advance	1	Value= “Actual time of signal from Mobile Station to Location base”- “Time of signal from Mobile Station to Location base supposed the distance is 0”
	LANGUAGE	2	0x00 0x01Chinese 0x00 0x02English
Serial Number		2	Serial number of data sent later at each time will be automatically added '1'.

Error Check	2	Error check (From “Packet Length” to “Information Serial Number”) , are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit	2	Fixed value:0x0D 0x0A

Example: 78 78 3B 28 10 01 0D 02 02 02 01 CC 00 28 7D 00 1F 71 3E 28 7D 00 1F 72 31 28 7D 00 1E 23
2D 28 7D 00 1F 40 18 00 00 00 00 00 00 00 00 00 00 00 00 00 FF 00 02 00 05 B1 4B 0D 0A

4.2 Server reply: No need to reply.

5 WIFI Information Protocol (Q2\HVT001)

WIFI information packet

Description: It is used for transmitting the WIFI data packet received by terminal.

5.1 WiFi packet sent by terminal

		Length (Byte)	Explain
Start Bit		2	0x78 0x78
Packet Length		1	Length= protocol number +information content+ serial number +error check
Protocol Number		1	0x2C
Info Content	Date and Time (UTC)	6	year (1byte) month (1byte) day (1byte) hour (1byte) minute (1byte) second (1byte) (convert to decimal)
	MCC	2	Mobile Country Code
	MNC	1	Mobile Network Code(MNC)
	LAC	2	Mobile Network Code(MNC)
	CI	3	Cell Tower ID(Cell ID)
	RSSI	1	Received Signal Strength Indicator , range from 0x00～0xFF, 0x00weak, 0xFF strongest。
	NLAC1	2	Same as LAC
	NCI1	3	Same as CI
	NRSSI1	1	Same as RSSI
	NLAC2	2	Same as LAC
	NCI2	3	Same as CI
	NRSSI2	1	Same as RSSI
	NLAC3	2	Same as LAC
	NCI3	3	Same as CI
	NRSSI3	1	Same as RSSI
NLAC4	2	Same as LAC	

	NCI4	3	Same as CI
	NRSSI4	1	Same as RSSI
	NLAC5	2	Same as LAC
	NCI5	3	Same as CI
	NRSSI5	1	Same as RSSI
	NLAC6	2	Same as LAC
	NCI6	3	Same as CI
	NRSSI6	1	Same as RSSI
	Time leads	1	Time difference between actual time of mobile station signal reaches to base station and time of mobile station signal reaches to base station when distance assumed 0
	WiFi quantity	1	Confirm WIFI quantity in the packet, 0: no WIFI detected
	WIFI MAC1	6	WIFI MAC of searched signal 1(transmit according to the actual number of searched WIFI. Search one, transmit one***; search none, then transmit 0)
Information Serial Number	WIFI strength 1	1	WIFI strength of signal 1
	WIFI MAC2	6	Same as above
	WIFI strength 2	1	Same as above
	...		
Information Serial Number		2	The serial number of the first GPRS data (including status packet and data packet such as GPS, LBS package) sent after booting is '1', and the serial number of data sent later at each time will be automatically added '1'.
Error Check		2	The check codes of data in the structure of the protocol, from the Packet Length to the Information Serial Number (including "Packet Length" and "Information Serial Number") , are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet.
Stop Bit		2	Fixed value: 0x0D 0x0A

WIFI packet server has no need to respond

6 Alarm Packet

Description:

- Transmit alarm content defined by terminal
- Server response and parse longitude and latitude into address and re-upload to terminal after receiving the alarm content
- Terminal send address to pre-set SOS number of device.

6.1 Alarm packet sent by terminal

Alarm packet (one fence)

		Length	Description
Start Bit		2	0x78 0x78
Packet Length		1	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number		1	0x26 (UTC)
Information Content	Date Time	6	Year (1byte) Month (1byte) Day (1byte) Hour (1byte) Min (1byte) Second (1byte) (converted to a decimal) (Date Time)
	Quantity of GPS information satellites	1	The first character is GPS information length, The second character is positioning satellite number (converted to a decimal)
	Latitude	4	Convert to a decimal and divide 1800000
	Longitude	4	Convert to a decimal and divide 1800000
	Speed	1	Convert to a decimal
	Course, Status	2	Convert to binary number of 16 bits and calculate by bits (see the following diagram) (same as GPS packet, see GPS packet for details)
	LBS length	1	LBS length in total (LBS length +MCC +MNC +Cell ID)
	MCC	2	Mobile Country Code(MCC) (converted to a decimal)
	MNC	1	Mobile Network Code(MNC)(converted to a decimal)
	LAC	2	Location Area Code (LAC) (converted to a decimal)
	Cell ID	3	Cell Tower ID(Cell ID)(converted to a decimal)
	Terminal Information	1	See the following diagram
	Build-in battery Voltage Level	1	0x00: No Power (shutdown) 0x01: Extremely Low Battery (not enough for calling or sending text messages, etc.) 0x02: Very Low Battery (Low Battery Alarm) 0x03: Low Battery (can be used normally) 0x04: Medium 0x05: High 0x06: Full
	GSM Signal Strength	1	0x00: no signal; 0x01: extremely weak signal;

			0x02: weak signal; 0x03: good signal; 0x04: strong signal.
	Alarm/Language	2	See the following diagram
	Mileage	4	Turn HEX into decimal. (Only available for devices with this function)
Serial Number		2	Serial number of data sent later at each time will be automatically added '1'.
Error Check		2	Error check (From "Packet Length" to "Information Serial Number"), are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit		2	Fixed value:0x0D 0x0A

Example: 78 78 25 26 12 03 0C 06 38 16 C3 02 6C 10 54 0C 38 C9 70 01 44 03 09 01 CC 00 28 66 00 0E EE
0C 06 04 03 02 00 0D A2 DB 0D 0A

Alarm packet (multiple fences)

		Length	Description
Start Bit		2	0x78 0x78
Packet Length		1	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number		1	0x27 (UTC)
Information Content	Date Time	6	Year (1byte) Month (1byte) Day (1byte) Hour (1byte) Min (1byte) Second (1byte) (converted to a decimal) (Date Time)
	Quantity of GPS information satellites	1	The first character is GPS information length, The second character is positioning satellite number (converted to a decimal)
	Latitude	4	Convert to a decimal and divide 1800000
	Longitude	4	Convert to a decimal and divide 1800000
	Speed	1	Convert to a decimal
	Course, Status	2	Convert to binary number of 16 bits and calculate by bits (see the following diagram) (same as GPS packet, see GPS packet for details)
	LBS length	1	LBS length in total (LBS length+ MCC+ MNC+ Cell ID)
	MCC	2	Mobile Country Code(MCC) (converted to a decimal)
	MNC	1	Mobile Network Code(MNC)(converted to a decimal)
	LAC	2	Location Area Code (LAC) (converted to a decimal)
	Cell ID	3	Cell Tower ID(Cell ID)(converted to a decimal)
	Terminal Information	1	See the following diagram

	Voltage Level	1	0x00: No Power (shutdown) 0x01: Extremely Low Battery (not enough for calling or sending text messages, etc.) 0x02: Very Low Battery (Low Battery Alarm) 0x03: Low Battery (can be used normally) 0x04: Medium 0x05: High 0x06: Full
	GSM Signal Strength	1	0x00: no signal; 0x01: extremely weak signal; 0x02: weak signal; 0x03: good signal; 0x04: strong signal.
	Alarm/Language	2	See the following diagram
	Fence No	1	Valid for geo-fence alarm, 1 means No.1, 2 means No.2....FF means invalid
	Mileage	1	Turn HEX into decimal. (Only available for devices with this function)
Serial Number		2	Serial number of data sent later at each time will be automatically added '1'.
Error Check		2	Error check (From "Packet Length" to "Information Serial Number"), are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit		2	Fixed value:0x0D 0x0A

Example: 78 78 25 26 11 0C 0D 13 37 36 CB 02 6C 15 A6 0C 38 CF 0A 00 54 B9 08 01 CC 00 28 66 00 0E EE D8 02 04 00 02 00 1D 76 F9 0D 0A

i. Terminal Information

Bit		Code Meaning
BYTE	Bit7	1:Oil and electricity disconnected
		0: Oil and electricity connected
	Bit6	1: GPS tracking is on
		0: GPS tracking is off
	Bit3~Bit5	100: SOS
		011: Low Battery Alarm
		010: Power Cut Alarm
		001: Vibration Alarm
		000: Normal
	Bit2	1: Charging
		0: Not Charge
	Bit1	1: ACC high

		0: ACC Low
	Bit0	1: Defense Activated
		0: Defense Deactivated

ii. Alarm language

Byte 1	0x00: normal
	0x01: SOS
	0x02: Power cut alarm
	0x03: Vibration alarm
	0x04: Enter fence alarm
	0x05: Exit fence alarm
	0x06 Over speed alarm
	0x09 Moving alarm
	0x0A Enter GPS dead zone alarm
	0x0B Exit GPS dead zone alarm
	0x0C Power on alarm
	0x0D GPS First fix notice
	0x0E External Low battery alarm
	0x0F External Low battery protection alarm
	0x10 SIM change notice
	0x11 Power off alarm
	0x12 Airplane mode alarm
	0x13 Disassemble alarm
	0x14 Door alarm
	0x15 Shutdown alarm due to low power
	0x16 Sound alarm
	0x17 Pseudo base-station alarm
	0x18 Open cover alarm
	0x19 Internal low Battery Alarm
	0x20 Sleep mode alarm
	0x21 Reserve
	0x22 Reserve
	0x23 Fall alarm
	0x24 Insert charger alarm(apply to asset tracker)
	0x29 Harsh acceleration alarm
	0x30 Harsh braking alarm
	0x2A Sharp Left Turn Alarm
	0x2B Sharp Right Turn Alarm

	0x2C Sharp Crash Alarm
	0x2D Vehicle Rolling alarm
	0x4B Tilting alarm
	0x4C Sharp turn alarm
	0x4D Abrupt lane switching alarm
	0x4E Vehicle stability
	0x4F Vehicle angle abnormality
	0x32 Pull alarm
	0x3C Car theft alarm
	0x3D Illegal start of alarm
	0x3E Press the button to upload alarm
	0xFE ACC On alarm
	0xFF ACC Off alarm
	0x5E Pulse signal line cut-off alarm
Byte 2	0x01 Chinese 0x02 English 0x00 No need for reply

6.2 Alarm packet response of server

	Length	Description
Start Bit	2	0x78 0x78
Packet Length	1	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number	1	0x26 (UTC)
Information Serial Number	2	Serial number of data sent later at each time will be automatically added '1'.
Error Check	2	Error check (From "Packet Length" to "Information Serial Number"), are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit	2	Fixed value: 0x0D 0x0A

Example: 78 78 05 26 00 1C 9D 86 0D 0A

7 Alarm Packet (LBS)

Description:

- Transmit alarm content defined by terminal
- Server response and parse longitude and latitude into address and re-upload to terminal after receiving the alarm content
- Terminal send address to pre-set SOS number of device.

7.1 Alarm packet sent by terminal

ii.		Length	Description
Start Bit		2	0x78 0x78
Packet Length		1	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number		1	0x19 (UTC)
	MCC	2	Mobile Country Code(MCC) (converted to a decimal)
	MNC	1	Mobile Network Code(MNC)(converted to a decimal)
	LAC	2	Location Area Code (LAC) (converted to a decimal)
	Cell ID	3	Cell Tower ID(Cell ID)(converted to a decimal)
	Terminal Information	1	See the following diagram
	Voltage Level	1	0x00: No Power (shutdown) 0x01: Extremely Low Battery (not enough for calling or sending text messages, etc.) 0x02: Very Low Battery (Low Battery Alarm) 0x03: Low Battery (can be used normally) 0x04: Medium 0x05: High 0x06: Very High
	GSM Signal Strength	1	0x00: no signal; 0x01: extremely weak signal; 0x02: very weak signal; 0x03: good signal; 0x04: strong signal.
	Alarm/Language	2	See the following diagram
Serial Number		2	Serial number of data sent later at each time will be automatically added '1'.
Error Check		2	Error check (From "Packet Length" to "Information Serial Number"), are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit		2	Fixed value:0x0D 0x0A

Example: 78 78 12 19 01 CC 00 28 7D 00 1F 71 20 04 04 01 01 00 94 6C 89 0D 0A

iii. Terminal Information

Bit		Code Meaning
BYTE	Bit7	1:Oil and electricity disconnected
		0: Oil and electricity connected
	Bit6	1: GPS tracking is on
		0: GPS tracking is off
	Bit3~Bit5	100: SOS
		011: Low Battery Alarm
		010: Power Cut Alarm
		001:Vibration Alarm
	Bit2	000: Normal
		1: Charging
	Bit1	0: Not Charge
		1: ACC high
	Bit0	0: ACC Low
		1: Defense Activated
		0: Defense Deactivated

iv. Alarm language

Please refer to GPS alarm language

8 Online command

Description:

- Use server online command to control terminal to execute task.
- Terminal response results to server.

8.1 Online command sent by server

		Length	Description
Start Bit		2	0x78 0x78
Length of data bit		1	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number		1	0x80
Information Content	Length of Command	1	=Server flag bit + command content length
	Server Flag Bit	4	Leave for server identification. Terminal receives the original data in Binary in response packet
	Command Content	M	Character string replied in ASCII coding. Command content is compatible with SMS command.
	(Language)	2	Latter bit : 0x01 Chinese , 0x02 English (this bit is not mandatory)
Information Serial Number		2	Serial number of data sent later at each time will be automatically added '1'.
Check Bit		2	Error check (From "Packet Length" to "Information Serial Number"), are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit		2	Fixed value:0x0D 0x0A

Example :

The bellowing two both works :

Without language bit : 78 78 0E 80 08 00 00 00 00 73 6F 73 23 00 01 6D 6A 0D 0A

With language bit: 78 78 10 80 08 00 00 00 00 73 6F 73 23 00 02 00 01 9A 17 0D 0A

8.2 Online command replied by terminal

8.2.1 Terminal reply (general command: JV200/GT300/GT800/MT200)

		Length	Description
Start Bit		2	0x79 0x79
Length of data bit		2	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number		1	0x21
Information Content	Server Flag Bit	4	Leave for server identification. Terminal receives the original data in Binary in response packet
	Content Code	1	0x01 ASC II code 0x02 UTF16-BE code.
	Content	M	Data needed to be sent (according to content code format)

Information Serial Number	2	Serial number of data sent later at each time will be automatically added '1'.
Check Bit	2	Error check (From "Packet Length" to "Information Serial Number"), are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit	2	Fixed value:0x0D 0x0A

Example: 79 79 00 9D **21** 00 00 00 00 01 42 61 74 74 65 72 79 3A 34 2E 31 36 56 2C 4E 4F 52 4D 41 4C 3B 20 47 50 52 53 3A 4C 69 6E 6B 20 55 70 3B 20 47 53 4D 20 53 69 67 6E 61 6C 20 4C 65 76 65 6C 3A 53 74 72 6F 6E 67 3B 20 47 50 53 3A 53 65 61 72 63 68 69 6E 67 20 73 61 74 65 6C 6C 69 74 65 2C 20 53 56 53 20 55 73 65 64 20 69 6E 20 66 69 78 3A 30 28 30 29 2C 20 47 50 53 20 53 69 67 6E 61 6C 20 4C 65 76 65 6C 3A 3B 20 41 43 43 3A 4F 46 46 3B 20 44 65 66 65 6E 73 65 3A 4F 46 46 00 2E 26 DF 0D 0A

8.2.2 Terminal reply (APPLY to JM01)

		Length	Description
Start Bit		2	0x78 0x78
Length of data bit		1	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number		1	0x15
Information Content	Length of Command	1	=Server flag bit + command content length
	Server Flag Bit	4	Leave for server identification. Terminal receives the original data in Binary in response packet
	Command Content	M	Character string replied in ASCII coding.
	Language	2	Chinese:0x00 0x01 English:0x00 0x02
Information Serial Number		2	Serial number of data sent later at each time will be automatically added '1'.
Error Check		2	Error check (From "Packet Length" to "Information Serial Number"), are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit		2	Fixed value:0x0D 0x0A

Example: 78 78 28 **15** 20 **00 00 00 00** 53 4F 53 31 3A 31 33 34 32 31 36 33 32 36 39 39 20 53 4F 53 32 3A 20 53 4F 53 33 3A **00 01** 00 2A C3 9C 0D 0A

9 Time calibration Packet

Description:

Used for checking time request sent by terminal to server

Generally, it is not mandatory to response as the device can calibrate the time by GPS :

Server can response with a UTC time if needed

9.1 Time request sent by terminal

	Length (Byte)	Description
Start Bit	2	0x78 0x78
Packet Length	1	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number	1	0x8A
Serial Number	2	Serial number of data sent later at each time will be automatically added '1'.
Error Check	2	Error check (From "Packet Length" to "Information Serial Number"), are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit	2	Fixed value: 0x0D0x0A

Example: 78 78 05 8A 00 06 88 29 0D 0A

9.2 Server response time information

	Length	Description
Start Bit	2	0x78 0x78
Packet Length	1	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number	1	0x8A (UTC)
Information Content Date Time	6	Year (1byte) Month (1byte) Day (1byte) Hour (1byte) Min (1byte) Second (1byte) (converted to a decimal)
Serial Number	2	Serial number of data sent later at each time will be automatically added '1'.
Error Check	2	Error check (From "Packet Length" to "Information Serial Number"), are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit	2	Fixed value: 0x0D0x0A

Example: 78 78 0B 8A 0F 0C 1D 00 00 15 00 06 F0 86 0D 0A

10 Information transmission packet

Description:

Terminal transmits all types of non-position data.

10.1 Information transmission packet sent by terminal

		Length	Description
Start Bit		2	0x79 0x79
Length of data bit		2	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number		1	0x94
Information Content	Information Type (Sub-protocol Number)	1	00 External power voltage 01~03 (custom) 04 Terminal status synchronization 05 Door status 06 Voltage mileage 08 Self-detection parameters 0A ICCID 0D Fuel sensor data 21 Terminal bluetooth address 23 Transmission terminal Bluetooth keyto add
	Data Content	N	Different information type results in different transmission content. See the following for details.
Information Serial Number		2	Serial number of data sent later at each time will be automatically added '1'.
Check Bit		2	Error check (From "Packet Length" to "Information Serial Number"), are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit		2	Fixed value:0x0D0x0A

Example: 79 79 00 7F 94 04 41 4C 4D 31 3D 43 34 3B 41 4C 4D 32 3D 43 43 3B 41 4C 4D 33 3D 34 43 3B 53 54 41 31 3D 43 30 3B 44 59 44 3D 30 31 3B 53 4F 53 3D 2C 2C 3B 43 45 4E 54 45 52 3D 3B 46 45 4E 43 45 3D 46 65 6E 63 65 2C 4F 4E 2C 30 2C 32 33 2E 31 31 31 38 30 39 2C 31 31 34 2E 34 30 39 32 36 34 2C 34 30 30 2C 49 4E 20 6F 72 20 4F 55 54 2C 30 3B 4D 49 46 49 3D 4D 49 46 49 2C 4F 46 46 00 0A 06 1E 0D 0A

Transmitted information content

When type is 00, the bit transmit external battery. This bit is two-digit hexadecimal value. Hexadecimal value converted to decimal value and divide 100. If device with two ADC port, ADC2 will add 0X01 as a distinction.(VG04)

Example: 0X04,0X9F, 049F converted to decimal is 1183, then divide 100 is 11.83, which means external voltage is 11.83V

ADC2: 0X05 0X36 0X01, 0X05 0X36 converted to decimal is 1334, then divide 100 is 13.34, which means

external voltage is 13.34V

When type is 04, the bit transmits information of terminal status synchronization. The bit length extended. Transmission is ASCII code.

Definition of content identifier

Definition	Identifier
Alarm Bit1	ALM1
Alarm Bit 2	ALM2
Alarm Bit 3	ALM3
Status Bit 1	STA1
SOS Number	SOS
Centre Number	CENTER
Fence	FENCE
Fuel/Electricity Cutoff Status	DYD
Mode	MODE

✧ ALM1 Definition (Status)

Bit	Definition	Mark
bit7	Vibration Alarm	1 ON 0 OFF
bit6	Network Alarm	1 ON 0 OFF
bit5	Phone Alarm	1 ON 0 OFF
bit4	SMS Alarm	1 ON 0 OFF
bit3	Displacement Alarm	1 ON 0 OFF
bit2	Network Alarm	1 ON 0 OFF
bit1	Phone Alarm	1 ON 0 OFF
bit0	SMS Alarm	1 ON 0 OFF

✧ ALM2 Definition (Status)

Bit	Definition	Mark
bit7	Low Internal Battery Alarm	1 ON 0 OFF
bit6	Network Alarm	1 ON 0 OFF
bit5	Phone Alarm	1 ON 0 OFF
bit4	SMS Alarm	1 ON 0 OFF
bit3	Low External Battery Alarm	1 ON 0 OFF
bit2	Network Alarm	1 ON 0 OFF
bit1	Phone Alarm	1 ON 0 OFF
bit0	SMS Alarm	1 ON 0 OFF

✧ ALM3 Definition (Status)

Bit	Definition	Mark
bit7	Overspeed Alarm	1 ON 0 OFF
bit6	Network Alarm	1 ON 0 OFF
bit5	Phone Alarm	1 ON 0 OFF
bit4	SMSAlarm	1 ON 0 OFF
bit3	Power Off Alarm	1 ON 0 OFF

bit2	Network Alarm	1 ON 0 OFF
bit1	Phone Alarm	1 ON 0 OFF
bit0	SMS Alarm	1 ON 0 OFF

✧ **STA1 Definition (Status)**

Bit	Definition	Mark
bit7	Arm Status	1 Arm 0 Disarm
bit6	Automatically Arm	1 ON 0 OFF
bit5	Manually Arm	1 ON 0 OFF
bit4	Remotely Disarm	1 ON 0 OFF
bit3	Remotely lock car	1 Remotely lock car 0 Non-remote lock car
bit2	To Be Defined	
bit1	Disassembly OFF	1 ON 0 OFF
bit0	Disassembly Alarm Status	1 ON 0 OFF

✧ **Fuel/Electricity Status Definition**

Bit	Definition	Mark
bit7	Undefined	
bit6	Undefined	
bit5	Undefined	
bit4	Undefined	
bit3	Deferred execution caused by overspeed	1Valid bit 0 Invalid bit
bit2	Deferred execution caused by GPS unlocated	1Valid bit 0 Invalid bit
bit1	Oil/Electricity cutoff	1Valid bit 0 Invalid bit
bit0	Oil/Electricity connection	1Valid bit 0 Invalid bit

- ✧ SOS definition: adopt ASCII to transmit (use “,” to separate if multiple SOS numbers)
- ✧ Center number definition: adopt ASCII to transmit
- ✧ Fence definition: adopt ASCII to transmit
- ✧ Mode: adopt ASCII to transmit(separate parameters by “ , ”)

Example : ALM1=FF;ALM2=FF;ALM3=FF;STA1=CO ; DYD=01 ; SOS=12345 , 2345 , 5678 ;
CENTER=987654;FENCE=FENCE,ON,0,-22.277120,-113.516763,5,IN,1; MODE=MODE,1,20,500

Notice: Not all contents are transmitted and please parse based on bits. Different products upload different contents.

When type is 05, this bit transmit external IO detection(door checking). Transmission is hexadecimal.

Bit	Definition	Mark
bit7	To Be Defined	
bit6	To Be Defined	
bit5	To Be Defined	
bit4	To Be Defined	
bit3	To Be Defined	
bit2	IO Status	1 High 0 Low

bit1	Triggering Status	1High triggering 0 Low triggering
bit0	Door Status	1ON 0 OFF

When type is 08, the bit will transmit terminal Self-checking parameters information. The position length is extended and ASCII code transmitted

When the type is 0A, this bit transmits ICCID, which is hexadecimal

IMEI	8	eg: If IMEI is 123456789123456, the terminal ID is: 0x01 0x23 0x45 0x67 0x89 0x12 0x34 0x56
IMSI	8	eg: If IMSI is 123456789123456, the terminal ID is: 0x01 0x23 0x45 0x67 0x89 0x12 0x34 0x56
ICCID	10	eg: If ICCID is 12345123456789123456, the terminal ID is: 0x12 0x34 0x51 0x23 0x45 0x67 0x89 0x12 0x34 0x56

When the type is OD, this bit transmits fuel data

fuel sensor sample:

79 79 00 3F 94 0D 11 09 07 08 0C 03 21 41 49 4F 49 4C 2C 30 32 2C 30 32 35 2E 39 30 30 2C 30 32 35
2E 34 30 30 2C 35 31 39 4A 2C 30 32 30 30 2C 30 32 37 2E 31 34 30 2C 30 2C 30 30 2C 39 46 83 A7
0D 12 0D 0A

Packet Type: General Packet data transmission (94)

CRC: CRC is correct, 0D12

Package length = 63 (003F)

Transmission type: fuel sensor (0D), transmission information: time and sensor information (11 09 07 08
0C 03 21 41 49 4F 49 4C 2C 30 32 2C 30 32 35 2E 39 30 30 2C 30 32 35 2E 34 30 30 2C 35 31 39 4A
2C 30 32 30 30 2C 30 32 37 2E 31 34 30 2C 30 2C 30 30 2C 39 46)

Time: 11 09 07 08 0C 03 21

Sensor information:

21 41 49 4F 49 4C 2C 30 32 2C 30 32 35 2E 39 30 30 2C 30 32 35 2E 34 30 30 2C 35 31 39 4A 2C 30 3
2 30 30 2C 30 32 37 2E 31 34 30 2C 30 2C 30 30 2C 39 46

Transfer ASCII:

!AIOIL,02,025.900,025.400,519J,0200,027.140,0,00,9F

ASCII	Description
!AIOIL	Head of Protocol
02	Device address
025.900	Liquid level output value (Unit: cm)
025.400	Temperature
4	protocol version number
12	Software version number
z	Hardware version number
02	Echo signal number (signal level)
0	Software status code
0	Hardware status code
027.140	Liquid level measurement value (Unit: cm)
0	Motion status code, 0: move. 1: static
00	Multiples of excitation waveform
9F	Check code(Sum Check Bit) (capital letter)

When the type is 21,this bit is terminal Bluetooth address

Data content: Bluetooth address [6] bytes

When the type is 23,this bit is transmission terminal Bluetooth key

Data content: 01 10 +16 byte key

10.2 Server Response Information Transmission Packet

Server no Response

11 External device transfer protocol (apply X3)

11.1 Device send transparent data to server

		Length	Description
Start Bit		2	0x79 0x79
Length of data bit		2	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number		1	0x9B
Information Content	Module type code	1	03
	Transparent content	N	
Information Serial Number		2	Serial number of data sent later at each time will be automatically added '1'.
Check Bit		2	Error check (From "Packet Length" to "Information Serial Number"), are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit		2	Fixed value:0x0D0x0A

Example:

79 79 00 14 9B 03 02 31 42 30 30 31 33 46 37 37 37 38 38 03 00 0B E8 E9 0D 0A

11.2 Server Response transfer data Packet

		Length	Description
Start Bit		2	0x79 0x79
Length of data bit		2	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number		1	0x9B
Information Content	Module type code	1	02
	Transparent	N	01: Identify successful 00: fail

	content		
Information Serial Number	2	Serial number of data sent later at each time will be automatically added ‘1’.	
Check Bit	2	Error check (From “Packet Length” to “Information Serial Number”) , are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)	
Stop Bit	2	Fixed value:0x0D0x0A	

Example:

79 79 00 07 9B 02 01 00 1E 73 0D 0D 0A

12 Large File Transfer (apply to HVT001)

- Used to transfer large files, such as voice files
- Terminal send data to server by adopting the 8D protocol; server send data to terminal by adopting the 90 protocol. Both protocols' format are the same.
- Terminal space is limited, therefore, free space needs to be check before data sent to terminal by server.

12.1 Terminal transfers the file to the server (8D)

Terminal send to the server

		Length (Byte)	Explain
	Start Bit	2	0x79 0x79
	Packet length	2	Length= protocol number +information content+ serial number +error check
	Protocol Number	1	0x8D
Info Content	File Type	1	0x00 voice file(monitored) 0x01 voice file(SOS) 0x02 intercom voice file
	File Length	4	Length of transferred file
	File Error Check Type	1	when error check type is "00", use CRC check to transfer file when error check type is "01", use MD5check to transfer file
	File Error Check	N	when error check type is "00", use CRC check to transfer file. The length is 2 bytes. when error check type is "01", use MD5check to transfer file. The length is 16 bytes.
	Start Bit	4	start position bytes number of split-transmitting

	Current Content Length	2	Data length behind start position of split-transmitting
	Content	M	Data packet after split
	Flag Bit	N	File type is the type of transferred file when file type is 00 voice file (monitoring), the position length is 6 bytes. Start date and coding method of monitoring is the same as location packet. when file type is 01 voice file (SOS), the position length is 2 bytes. Bytes are the same with the corresponding SOS alarm packet serial number. when file type is 02 voice file (income), the position length is 6 bytes. Start date and coding method of monitoring is the same as location packet.
Information Serial Number		2	The serial number of the first GPRS data (including status packet and data packet such as GPS, LBS package) sent after booting is '1', and the serial number of data sent later at each time will be automatically added '1'.
Error Check		2	The check codes of data in the structure of the protocol, from the Packet Length to the Information Serial Number (including "Packet Length" and "Information Serial Number") , are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet.
Stop Bit		2	Fixed value: 0x0D 0x0A

iii. Appendix

1. code fragment of the CRC-ITU lookup table algorithm implemented based on C language

```
static const U16 crctab16[] =
{
    0X0000, 0X1189, 0X2312, 0X329B, 0X4624, 0X57AD, 0X6536, 0X74BF,
    0X8C48, 0X9DC1, 0XAF5A, 0XBED3, 0XCA6C, 0XDBE5, 0XE97E, 0XF8F7,
    0X1081, 0X0108, 0X3393, 0X221A, 0X56A5, 0X472C, 0X75B7, 0X643E,
    0X9CC9, 0X8D40, 0XBFDB, 0XAE52, 0XDAED, 0XCB64, 0XF9FF, 0XE876,
    0X2102, 0X308B, 0X0210, 0X1399, 0X6726, 0X76AF, 0X4434, 0X55BD,
    0XAD4A, 0XBCC3, 0X8E58, 0X9FD1, 0XEB6E, 0XFAE7, 0XC87C, 0XD9F5,
    0X3183, 0X200A, 0X1291, 0X0318, 0X77A7, 0X662E, 0X54B5, 0X453C,
    0XBDCB, 0XAC42, 0X9ED9, 0X8F50, 0XFBF7, 0XEA66, 0XD8FD, 0XC974,
    0X4204, 0X538D, 0X6116, 0X709F, 0X0420, 0X15A9, 0X2732, 0X36BB,
    0XCE4C, 0XDFC5, 0XED5E, 0XFCDD, 0X8868, 0X99E1, 0XAB7A, 0XBAF3,
    0X5285, 0X430C, 0X7197, 0X601E, 0X14A1, 0X0528, 0X37B3, 0X263A,
    0XDECD, 0XCF44, 0XFDDE, 0XEC56, 0X98E9, 0X8960, 0XBBFB, 0XAA72,
    0X6306, 0X728F, 0X4014, 0X519D, 0X2522, 0X34AB, 0X0630, 0X17B9,
    0XEF4E, 0XFEC7, 0XCC5C, 0XDDD5, 0XA96A, 0XB8E3, 0X8A78, 0X9BF1,
    0X7387, 0X620E, 0X5095, 0X411C, 0X35A3, 0X242A, 0X16B1, 0X0738,
    0XFFCF, 0XEE46, 0XDCDD, 0XCD54, 0XB9EB, 0XA862, 0X9AF9, 0X8B70,
    0X8408, 0X9581, 0XA71A, 0XB693, 0XC22C, 0XD3A5, 0XE13E, 0XF0B7,
    0X0840, 0X19C9, 0X2B52, 0X3ADB, 0X4E64, 0X5FED, 0X6D76, 0X7CFF,
    0X9489, 0X8500, 0XB79B, 0XA612, 0XD2AD, 0XC324, 0XF1BF, 0XE036,
    0X18C1, 0X0948, 0X3BD3, 0X2A5A, 0X5EE5, 0X4F6C, 0X7DF7, 0X6C7E,
    0XA50A, 0XB483, 0X8618, 0X9791, 0XE32E, 0XF2A7, 0XC03C, 0XD1B5,
    0X2942, 0X38CB, 0X0A50, 0X1BD9, 0X6F66, 0X7EEF, 0X4C74, 0X5DFD,
    0XB58B, 0XA402, 0X9699, 0X8710, 0XF3AF, 0XE226, 0XD0BD, 0XC134,
    0X39C3, 0X284A, 0X1AD1, 0X0B58, 0X7FE7, 0X6E6E, 0X5CF5, 0X4D7C,
    0XC60C, 0XD785, 0XE51E, 0XF497, 0X8028, 0X91A1, 0XA33A, 0XB2B3,
    0X4A44, 0X5BCD, 0X6956, 0X78DF, 0X0C60, 0X1DE9, 0X2F72, 0X3EFB,
    0XD68D, 0XC704, 0XF59F, 0XE416, 0X90A9, 0X8120, 0XB3BB, 0XA232,
    0X5AC5, 0X4B4C, 0X79D7, 0X685E, 0X1CE1, 0X0D68, 0X3FF3, 0X2E7A,
    0XE70E, 0XF687, 0XC41C, 0XD595, 0XA12A, 0XB0A3, 0X8238, 0X93B1,
    0X6B46, 0X7ACF, 0X4854, 0X59DD, 0X2D62, 0X3CEB, 0X0E70, 0X1FF9,
    0XF78F, 0XE606, 0XD49D, 0XC514, 0XB1AB, 0XA022, 0X92B9, 0X8330,
    0X7BC7, 0X6A4E, 0X58D5, 0X495C, 0X3DE3, 0X2C6A, 0X1EF1, 0X0F78,
};

//calculate the 16-bit CRC of data with predetermined length.
U16 GetCrc16(const U8* pData, int nLength)
{
    U16 fcs = 0xffff; //initialization
    while (nLength > 0) {
        fcs = (fcs >> 8) ^ crctab16[(fcs ^ *pData) & 0xff];
        nLength--;
        pData++;
    }
    return ~fcs; //negated
}
```

2. Data Flow Diagram

