

7-4 VS Series PLC Communication Protocol

A. The relevant communication parameters

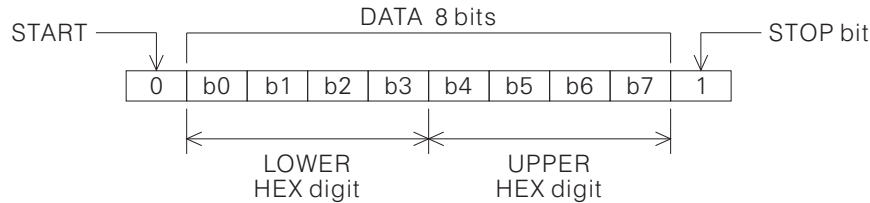
- Bits-per-character: 8 bits

Parity check: None

Stop bit: 1 bit

Baud rate: 300/600/1200/2400/4800/9600/19200/34800/57600/115200 bps. selectable (default: 19200 bps.)

- Syntax of a communication character



- This communication protocol adopted the mixed method of ASCII and the HEX code to transmit data. This protocol adopts a few ASCII codes, the conversion table below shows those characters and the corresponding ASCII codes.

Character	ASCII Code
STX	02H
ETX	03H
ACK	06H
DLE	10H

Character	ASCII Code
0	30H
1	31H
2	32H
3	33H
4	34H
5	35H
6	36H
7	37H

Character	ASCII Code
8	38H
9	39H
A	41H
B	42H
C	43H
D	44H
E	45H
F	46H

- Communication station number:

The available station number is between 0~254 (default: 0). If the communication command uses the station number 255, that is a broadcast command.

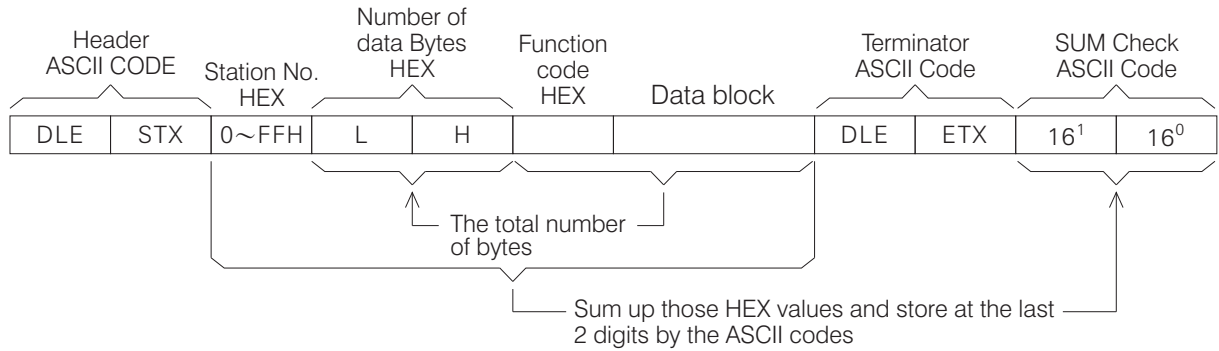
- Error code: When data string is feedback from a PLC, will include with an error code. The table lists the meaning of every error code.

Error Code	Description
00H	Communication is normal; no error
02H	Communication SUM Check Error
04H	The number of data bytes or the number of components is 0

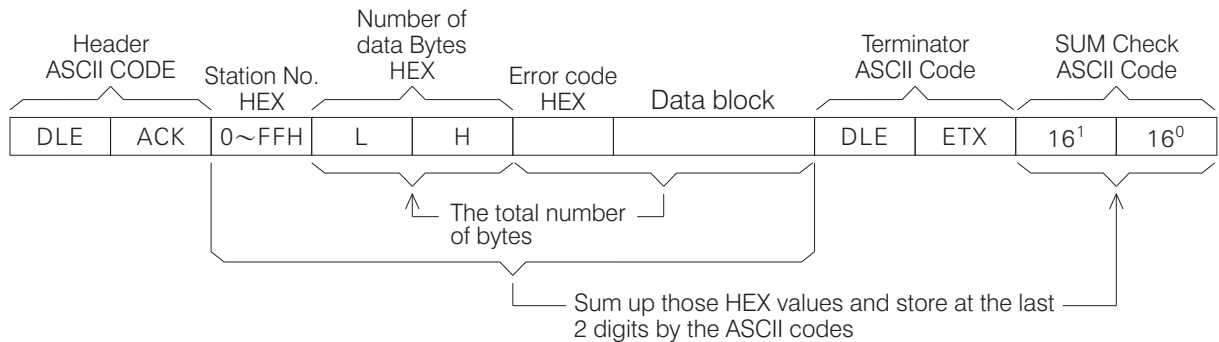
Error Code	Description
06H	The number of data bits exceeds the range
08H	Error ASCII conversion
31H	The command / function code is not existed

B. Communication protocol data format

- The communication command string is sent to the Slave PLC



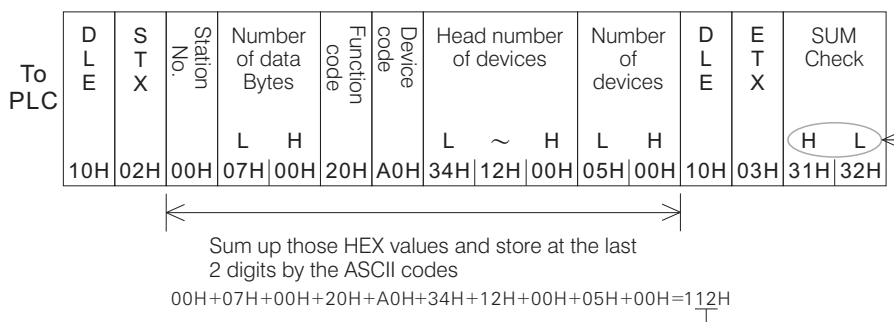
- The communication feedback string from the Slave PLC



- Header:** The starting characters of the data string to be transferred.
The characters of the header for command string sent to the Slave is DLE(10H) + STX(02H) by the ASCII code; the header of feedback string from the Slave is DLE(10H) + ACK(06H) by the ASCII code.
- Station No.:** The Slave's identification number.
Every Slave PLC at the same communication circuit must have a unique station number, the Slave will respond to the command if its station number matches with the number in the command. Thus, the Master (computer) can use the station number to make a command for the particular Slave PLC.
- Number of data Bytes:** Counting the number of bytes from the function or error code to the end of the data block.
- Function code:** The Master PLC or computer commands the Slave PLC to do the appointed task.

Command	Function Code	Object of Device
Word Device Read	20H	D, SD, R, T, C
Word Device Write	28H	D, SD, R, T, C
Bit Device Read	21H	the coil or contact of X, Y, M, SM, S, T and C
Bit Device Write	29H	the coil or contact of X, Y, M, SM, S, T and C

- Data block:** The contents in the data block may include the head number of devices, the number of devices, the content values of sending data and so forth.
- Terminator:** The last characters of the data string to be transferred.
The characters of the terminator for command string is DLE(10H) + ETX(03H) by the ASCII code.
- SUM Check:** Sum up the content values of HEX data from the beginning of station No. to the end of the data block. Use the accumulated last two digits (by the HEX format) and convert that into two ASCII codes to be the check code.
To operate the same code-checking procedures at both data sending and receiving ends can ensure the data transmission is correct.

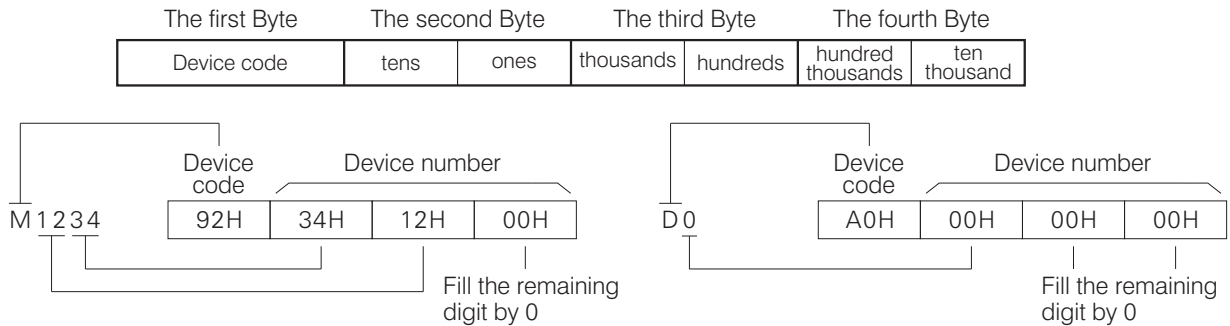


C. Statement of the Device code

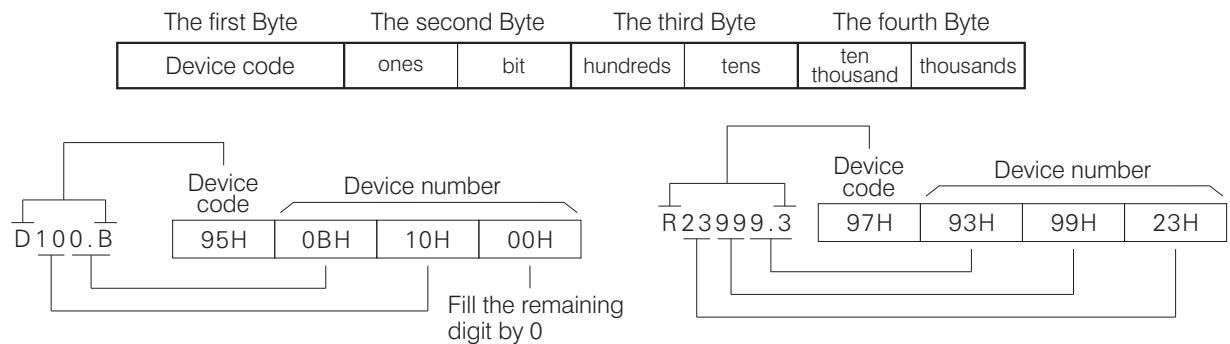
Mapping the head device's "Device code" is often needed for the data block access, following describes the coding rules.

The Device code takes four Bytes. The first Byte represents the device type and the second to fourth Bytes represent the number of the device.

- General the bit devices and word devices follow the coding rule below:



- The bit at a register (D.b or R.b) follows the coding rule below:



Device	Device ID	Device Code	Range of Device No.	Examples of Device Code	
				Device ID	Code L → H
External Input X	X0~X377 (Octal)	90H	0~377	X15	90H,15H,00H,00H
External Output Y	Y0~Y377 (Octal)	91H	0~377	Y123	91H,23H,01H,00H
Auxiliary Relay M	M0~M8191	92H	0~8191	M1234	92H,34H,12H,00H
Step Relay S	S0~S4095	93H	0~4095	S100	93H,00H,01H,00H
Special Relay M	M9000~M9511	94H	0~511	M9012	94H,12H,00H,00H
Register D's Bit D.b	D0~D8999 at D.0~D.F	95H	0~8999 0~F	D123.F	95H,3FH,12H,00H
Register R's Bit R.b	R0~R23999 at R.0~R.F	97H	0~23999 0~F	R23999.3	97H,93H,99H,23H
Coil of a timer T	T0~T511	98H	0~511	T25	98H,25H,00H,00H
Contact of a timer T	T0~T511	99H	0~511	T123	99H,23H,01H,00H
Coil of a counter C	C0~C255	9CH	0~255	C0	9CH,00H,00H,00H
Contact of a counter C	C0~C255	9DH	0~255	C200	9DH,00H,02H,00H
Register D (content value)	D0~D8999	A0H	0~8999	D1000	A0H,00H,10H,00H
Special Register SD (content value)	D9000~D9511	A1H	0~511	D9001	A1H,01H,00H,00H
Register R (content value)	R0~R23999	A2H	0~23999	R12345	A2H,45H,23H,01H
Timer T (present value)	T0~T511	A8H	0~511	T255	A8H,55H,02H,00H
16-bit Counter C (current value)	C0~C199	ACH	0~199	C0	ACH,00H,00H,00H
32-bit Counter C (current value)	C200~C255	ADH	200~255	C235	ADH,35H,02H,00H

D. Statement of the communication command

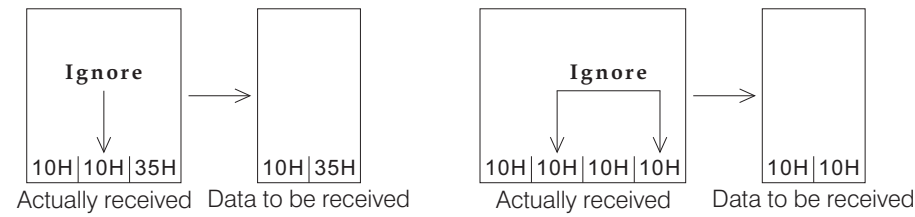
- The sending equipment will bind the codes together that includes the header, terminator and check code in a communication command string. Except those three special purpose codes, if the content data include with the code 10H in the string, the code 10H should be repeated once.

For example:



- When a receiving equipment gets two consecutive 10H codes, the second 10H code needs to be ignored.

For example:



- Function code 20H: to read word devices (up to 64 words can be read at one command).

Command to PLC	D L E	S T X	Station No. 00H }	Number of data Bytes		Function code	Device code	Head number of devices			Number of devices		D L E	E T X	SUM Check
	10H	02H	FFH	L	H	20H	XXH	L	~	H	L	H	10H	03H	H L

Feedback from PLC (complete)	D L E	A C K	Station No. As above	Number of data Bytes		Error code	Data block			Data block	D L E	E T X	SUM Check
	10H	06H		L	H	00H	L H				L H	10H	03H	H L

Feedback from PLC (error)	D L E	A C K	Station No. As above	Number of data Bytes		Error code	D L E	E T X	SUM Check
	10H	06H		01H	00H	XXH	10H	03H	H L

Example 1: Read the content values of D1234~D1238 at the Salve #0. (five 16-bit word devices)
 Suppose D1234 = 89ABH, D1235 = 1000H, D1236 = 2345H, D1237 = 0H and D1238 = 3FH at the Salve #0.

Command to PLC	D L E	S T X	Station No.	Number of data Bytes		Function code	Device code	Head number of devices			Number of devices		D L E	E T X	SUM Check
	10H	02H	00H	L	H	20H	A0H	L	~	H	L	H	10H	03H	H L

Feedback from PLC (complete)	D L E	A C K	Station No.	Number of data Bytes		Error code	Value at D1234		Value at D1235		Value at D1236		Value at D1237		Value at D1238		D L E	E T X	SUM Check
	10H	06H	00H	L	H	00H	L	H	L	H	L	H	L	H	L	H	10H	03H	H L

Example 2: Read the present values of C235 and C236 at the Salve #0. (two 32-bit double word devices)
 Suppose C235 = 236B9H and C236 = 11253648H at the Salve #0.
 Since the C235 and C236 are 32-bit devices, their current value will be consisted of two words (Low word and High word).

Command to PLC	D L E	S T X	Station No.	Number of data Bytes		Function code	Device code	Head number of devices			Number of devices		D L E	E T X	SUM Check
	10H	02H	00H	L	H	20H	ADH	L	~	H	L	H	10H	03H	H L

Feedback from PLC (complete)	D L E	A C K	Station No.	Number of data Bytes		Error code	Present value at C235				Present value at C236				D L E	E T X	SUM Check
	10H	06H	00H	L	H	00H	LL	LH	HL	HH	LL	LH	HL	HH	10H	03H	H L

- Function code 21H: to read bit devices (up to 1024 bits can be read at one command).

Command to PLC	D L E	S T X	Station No. 00H ~ FFH	Number of data Bytes		Function code 21H	Device code XXH	Head number of devices			Number of devices		D L E	E T X	SUM Check	
	10H	02H		L	H			L	~	H	L	H	10H	03H	H	L

Feedback from PLC (complete)	D L E	A C K	Station No.	Number of data Bytes		Error code	Data block (Transmit unit: Byte)							D L E	E T X	SUM Check	
	10H	06H	As above	L	H	00H	B0	B1					Bn	10H	03H	H	L

Feedback from PLC (error)	D L E	A C K	Station No.	Number of data Bytes	Error code	D L E	E T X	SUM Check	
	10H	06H	As above	01H 00H	XXH	10H	03H	H	L

Example 1: Read the states of M10~M63 at the Salve #0 (total 54 bit devices)
 Suppose the states of M10~M63 at the Salve #0 are as below: (composed to Byte values)

	8 bits								
55H	0	1	0	1	0	1	0	1	M10 (B0)
AAH	1	0	1	0	1	0	1	0	M18 (B1)
00H	0	0	0	0	0	0	0	0	M26 (B2)
FFH	1	1	1	1	1	1	1	1	M34 (B3)
ABH	1	0	1	0	1	0	1	1	M42 (B4)
12H	0	0	0	1	0	0	1	0	M50 (B5)
2EH	0	0	1	0	1	1	1	0	M58 (B6)

※ 54 bits in total, 54 = 36H (the number of devices)

Fill the unused devices as "0"

Command to PLC	D L E	S T X	Station No.	Number of data Bytes		Function code	Device code	Head number of devices			Number of devices		D L E	E T X	SUM Check	
				L	H			L	~	H	L	H			H	L
	10H	02H	00H	07H	00H	21H	92H	10H	00H	00H	36H	00H	10H	03H	30H	30H

Feedback from PLC (complete)	D L E	A C K	Station No.	Number of data Bytes		Error code	Status (by Byte values) at M10–M63						D L E	E T X	SUM Check		
				L	H		B0	B1	B2	B3	B4	B5	B6			H	L
	10H	06H	00H	08H	00H	00H	55H	AAH	00H	FFH	ABH	12H	2EH	10H	03H	46H	31H

- Function code 28H: to write word devices (up to 64 words can be write at one command).

Command to PLC	D L E	S T X	Station No. 00H }	Number of data Bytes		Function code 28H	Device code XXH	Head number of devices			Number of devices		Data to be written		Data to be written		D L E	E T X	SUM Check
	10H	02H	FFH	L	H	28H	XXH	L	~	H	L	H	L	H		L	H	10H	03H	H L

Feedback from PLC (complete)	D L E	A C K	Station No. As above	Number of data Bytes		Error code 00H	D L E	E T X	SUM Check
	10H	06H	As above	01H	00H	00H	10H	03H	H L

The error code in feedback string at a successful communication is 00H; but if the error code is not 00H, that means error happened (refer to the list at the beginning of this section).

Feedback from PLC (error)	D L E	A C K	Station No. As above	Number of data Bytes		Error code XXH	D L E	E T X	SUM Check
	10H	06H	As above	01H	00H	XXH	10H	03H	H L

Example 1: Write the values 2048H and 300H into the D7000 and D7001 at the Salve #0 (two 16-bit word devices)

Command to PLC	D L E	S T X	Station No.	Number of data Bytes		Function code	Device code	Head number of devices			Number of devices		Data write to D7000		Data write to D7001		D L E	E T X	SUM Check
	10H	02H	00H	L	H	28H	A0H	L	~	H	L	H	L	H	L	H	10H	03H	H L

Feedback from PLC (complete)	D L E	A C K	Station No.	Number of data Bytes		Error code	D L E	E T X	SUM Check
	10H	06H	00H	L	H	00H	10H	03H	H L

Example 2: Write the value 89AB1234H into the C210 at the Salve #0 (a 32-bit double word device)

Command to PLC	D L E	S T X	Station No.	Number of data Bytes		Function code	Device code	Head number of devices			Number of devices		Data write to C210				D L E	E T X	SUM Check
	10H	02H	00H	L	H	28H	ADH	L	~	H	L	H	LL	LH	HL	HH	10H	03H	H L

Feedback from PLC (complete)	D L E	A C K	Station No.	Number of data Bytes		Error code	D L E	E T X	SUM Check
	10H	06H	00H	L	H	00H	10H	03H	H L

- Function code 29H: to write bit devices (up to 1024 bits can be write at one command).

Command to PLC	D L E	S T X	Station No.	Number of data Bytes		Function code	Device code	Head number of devices			Number of devices		Data block (Transmit unit: Byte)				D L E	E T X	SUM Check
	10H	02H	00H }	L	H	29H	XXH	L	~	H	L	H	B0	B1		Bn	10H	03H	H L

Feedback from PLC (complete)	D L E	A C K	Station No.	Number of data Bytes		Error code	D L E	E T X	SUM Check
	10H	06H	As above	01H	00H	00H	10H	03H	H L

The error code in feedback string at a successful communication is 00H; but if the error code is not 00H, that means error happened (refer to the list at the beginning of this section).

Feedback from PLC (error)	D L E	A C K	Station No.	Number of data Bytes		Error code	D L E	E T X	SUM Check
	10H	06H	As above	01H	00H	XXH	10H	03H	H L

Example 1: Write the status below into the M100~M127 at the Salve #0 (total 28 bit devices)

8 bits								
EFH	1	1	1	0	1	1	1	M100 (B0)
CDH	1	1	0	0	1	1	0	M108 (B1)
35H	0	0	1	1	0	1	0	M116 (B2)
00H	0	0	0	0	0	0	0	M124 (B3)

Fill the unused devices as "0" M127

※ 28 bits in total, 28 = 1CH (the number of devices)

Command to PLC	D L E	S T X	Station No.	Number of data Bytes		Function code	Device code	Head number of devices			Number of devices		Data write to M100~M127				D L E	E T X	SUM Check
	10H	02H	00H	L	H	29H	92H	L	~	H	L	H	B0	B1	B2	B3	10H	03H	H L

Feedback from PLC (complete)	D L E	A C K	Station No.	Number of data Bytes		Error code	D L E	E T X	SUM Check
	10H	06H	00H	L	H	00H	10H	03H	30H 31H