Send Orders for Reprints to reprints@benthamscience.ae

Research and Implementation of PLC Communication Network Based on CAN

Xiaoli Mei*

Chongqing College of Electronic Engineering, Chongqing 401331, China

Abstract: Field bus is an industrial data bus which has developed rapidly in recent years. It is mainly used to solve digital communications among field equipments, and message passing between field equipments and executive control systems. CAN bus is a kind of serial communication network supporting distributed control and real-time control effectively, and it applies double serial communication mode and has good error-detecting capacity, which makes it can work in high-noise or jammed environments and has higher reliability. The paper proposes PLC communication network scheme based on CAN bus. The scheme configures a RS232-CAN gateway on upper computer PC and each PLC to make upper computer PC and PLC have the ability of CAN bus communication for creating PLC communication network based on CAN bus. PLC network created by the scheme not only can realize centralized monitoring of PC on several PLCs and direct communication among PLCs, but also has higher cost and higher ability of system extension.

Keywords: CAN bus, communication, field bus, PLC.

1. INTRODUCTION

PLC (Programmable Logic Controller) applies figures to control specialized electronic computer. It uses the program memory which can be modified to store instruction, execute the functions such as logic, sequence, timing, enumeration and calculation, and controls various machineries or working procedures by simulation and function component including digital input and output. It is easy to understand and has the advantages of convenient operation and high reliability [1, 2].

The paper proposes the scheme of creating PLC communication network based on communication gateway of CAN bus. In the network, PC and each PLC have their own communication gateway [3]. In PLC network which is created with the above mode, the position of each PLC is equal, each PLC can send the communication to the other PLC actively, and can make centralized monitor on PLC in the network by PC. In the process of communication, CAN gateway is for hardware automatic arbitration to guarantee that the data of every communication is not lost [4, 5].

2. CAN BUS TECHNOLOGY

The full name of CAN is Controller Area Network. Because CAN has high performance, high reliability and unique design, it has been receiving more and more recognition [6].

*Address correspondence to this author at the Chongqing College of Electronic Engineering, Chongqing 401331, China;
E-mail: 2493617767@qq.com

2.1. Characteristics of CAN Bus

CAN belongs to bus-based serial communication network. Because CAN bus applies a lot of new techniques and unique design, the data of CAN bus has prominent reliability, real-time and flexibility compared with common communication bus. Its characteristics can be summarized as follows:

1) CAN is a kind of serial communication network supporting effectively distributed control and real-time control [7].

2) CAN protocol abide by the standard model of ISO/OSI in which physical layer and data link layer are adopted.

3) CAN can work in many ways, and is CSMA/CD in nature. Any node on the internet can send information to other nodes on internet actively regardless of master-slave at any time.

4) CAN adopts non-destructive bitwise arbitration technology. When multiple nodes send data to bus at the same time, the nodes with lower priority can quit sending initiatively, and the nodes with the highest priority can continue to send information insusceptibly, which saves conflict arbitration time of the bus. Especially, network paralysis doesn't appear in the situation of heavy network load.

5) CAN has flexible communication mode. CAN can realize the transmission and reception of data with several modes including point-to-point, point-to-multipoint and global broadcast without special scheduling.

6) Direct communication distance of CAN can reach as far as 10km, transmission rate is 5kbit/s, and the highest

1874-4443/15

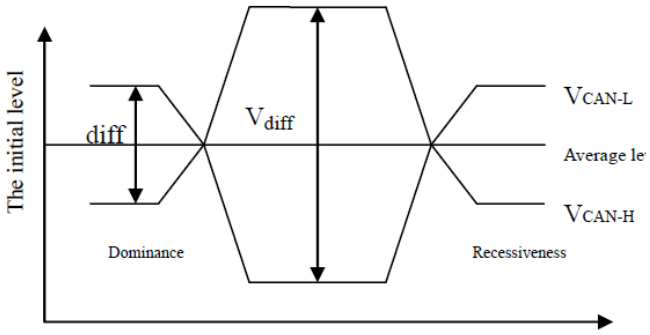

Fig. (1). Level of value logic of CAN bus.

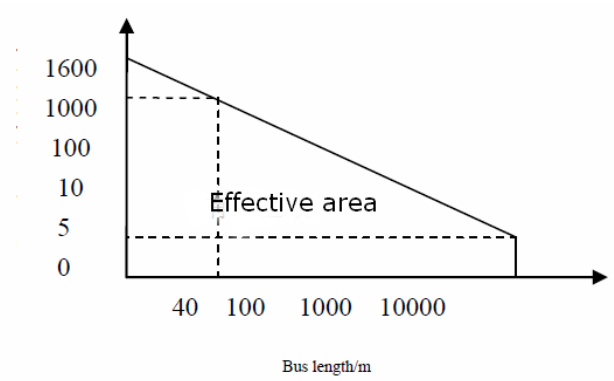

Fig. (2). The relationship between effective length and transmission rate of CAN bus.

Table 1. The maximum transmission distance between two nodes in CAN bus.

Bit Rate/(kbit/s)	Maximum Bus Length/m	Bus Timing	
		BTR0	BTR1
1000	40	00h	14h
500	130	00h	1Ch
250	270	01h	1Ch
125	530	03h	1Ch
100	620	43h	2Fh
50	1300	47h	2Fh
20	3300	53h	2Fh
10	6700	67h	2Fh
5	10000	7Fh	7Fh

communication rate could reach 1Mbit/s and transmission distance is 40m.

7) Data link layer of CAN adopts short frame structure which has short transmission time and is easy to correct, and the longest frame is 8 bytes. The information of each frame on CAN uses CRC-16 verification mode and other check measures, which effectively reduces the error rate of data, and bit error rate is only 3×10-5. The CAN node can close its output automatically for cutting off the connection between the node and bus in case of serious fault, which makes other nodes on the bus not to be effected, and CAN node has strong anti-jamming capacity.

8) The data bits has two pieces of logic; dominant bit 0 and recessive bit 1. And for time synchronization technology, which has the function of hardware self-locking and timing, automatic time tracking is applied [8-10].

2.2. Value Logic of The Bus

As shown in Fig. (**1**), total value of CAN is one of two pieces of complementary logic value, the dominance or the recessiveness. The dominant value represents logic 0 and the recessive value shows logic 1. When the dominance and the recessiveness send simultaneously, the last total value is dominant. In the recessive state, VCAN-H and VCAN-L are fixed at an average voltage level, and Vdiff is approximately 0. During the state of idle bus or dominance, bus sends the dominant state. Dominant status is represented by differential voltage more than the minimum threshold. And during the recessiveness, the dominant state is adapted to the recessive state and then is sent.

When the bus is idle, it presents recessive level. And any node can send a dominant level as the beginning of a frame. If there are two or more nodes sent simultaneously, bus contention will generate.

2.3. The Relationship Between Speed and Distances of CAN Bus

The maximum transmission distance between any two nodes in CAN system has a relation with bit rate. And the relationship between effective length of bus and transmission rate is displayed in Fig. (**2**). The maximum transmission distance between two nodes is shown in Table **1**.

Bosch Company formulated and launched CAN technical specification （Version 2.0）in September 1991. The technical specification includes two part, A and B. In November 1993, ISO officially promulgated international standard of Road traffic vehicles-digital switching- high speed communication controller LAN （CAN), which plays a role in promoting further standardization of CAN [8].

3. DESIGN AND REALIZATION OF GATEWAY PCB BOARD CIRCUIT

If the system only has microprocessor, it is unable to complete system function. And the performance of the microprocessor is also needed for designing peripheral circuit.

3.1. Reset Circuit of Atmega8 and Mcp2515

Reset circuit mainly has the function of completing power-on reset of the system and pushbutton reset of the users when the system is working. Reset circuit can use simple RC circuit and other complicated circuit. The paper adopts simple RC circuit, and the result shows that reset logic of RC circuit is reliable. IN5819 in RC circuit is schottky barrier diode whose role is to release electric charge on RC circuit when the capacitance discharges [10].

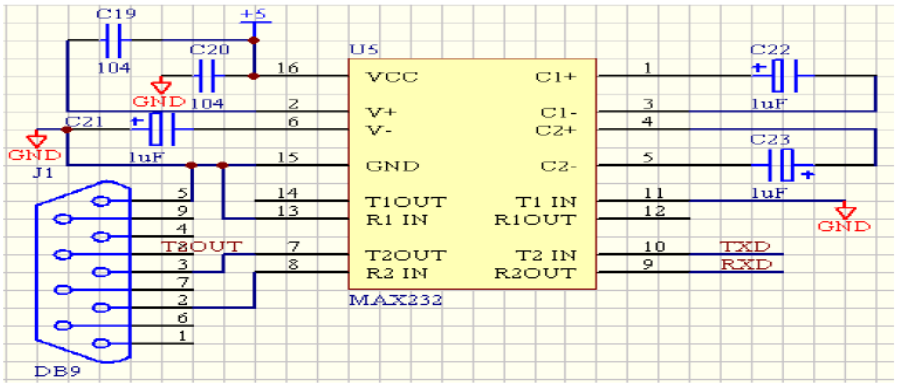

Fig. (3) Serial interface circuit.

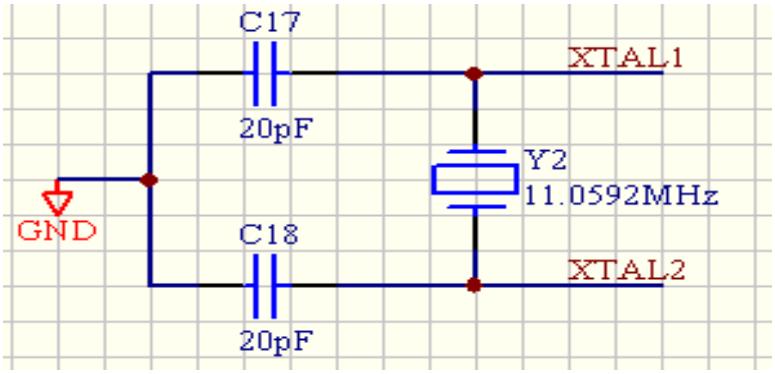

Fig. (4). Crystal circuit of Atmega8.

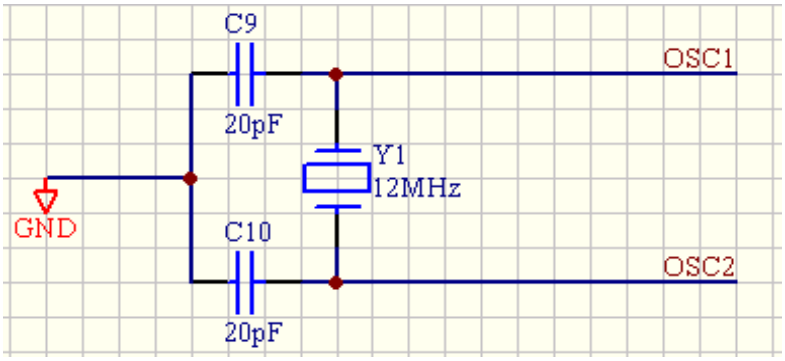

Fig. (5). Crystal circuit of Mcp2515.

3.2. Serial Interface Circuit

The paper adopts special level conversion chip, chip MAX232 of Maxim corporation.

In chip MAX232, there is a mains voltage converter which can transform the input mains voltage of +5V into the voltage of ±10V needed by the output level of RS-232C. So serial communication system of chip interface only needs single +-5V power supply.

Serial interface circuit is shown in Fig. (**3**). In Fig. (**3**), the transformation portion of mains voltage is C19, C21, C22 and C23. The device is very sensitive to power supply noise. Therefore, VCC must add decoupling capacitor C20 whose value is 0.1uF. The capacitors including C19, C21, C22 and C23 take polar capacitor C20 with the same value for improving anti-jamming capability, and they must be close to the device to the greatest extent on connection. T1IN and T2IN can connected to the TXD pin of Atmega8 MCU directly. R1OUT and R2OUT also can connected to the TXD pin of Atmega8 MCU directly. T1OUT and T1OUT can connected directly to the receiving end of PC or PLC, and R1INand and R2IN can connected directly to the transmitting end of serial interface in PC or PLC.

3.3. Clock Circuit

In the circuit of the gateway, Atmega8 MCU and CAN controller Mcp2515 all have their own external crystal circuit.

External crystal used by Atmega8 and Mcp2515 are respectively 11.0592MHz and 12MHz. Their clock circuits are shown in Figs. (**4** and **5**).

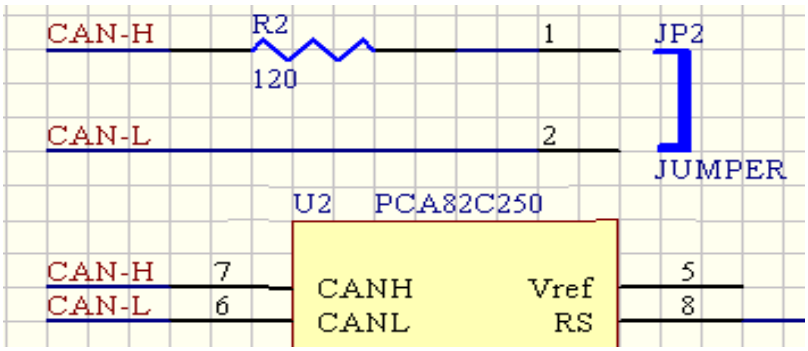

Fig. (6). Resistive circuit loaded in terminal of CAN bus.

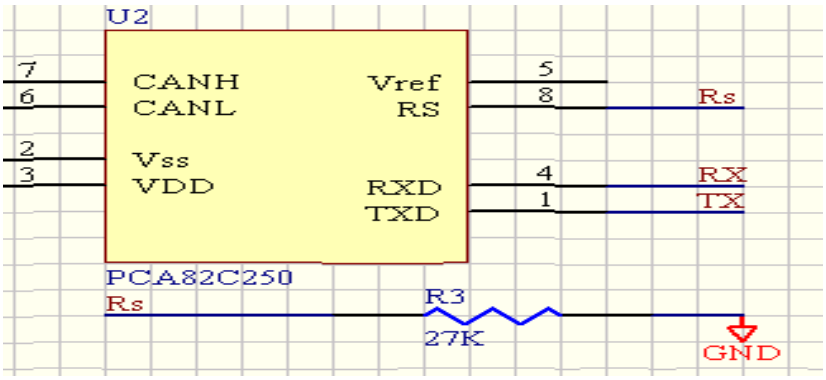

Fig. (7). Circuit diagram of slope controlling mode.

In the crystal circuit of Atmega8, the pin of XTAL1 and XTAL2 is respectively input end and output end of inverting amplifier of oscillator in chip. Oscillator Y2 can use quartz crystal oscillator and ceramic resonator. The clock needs to be set as the external clock for input without frequency in developing.

3.4. Resistive Circuit Loaded in the Terminal of CAN Bus

In Figs. (**2-6**), each end of CAN bus connected to terminal resistance RL, has the function of inhibiting reflex. There are terminal resistances RL in the network. If there is one CAN node being connected to the network, the dominant will be sent to the bus to generate current flowing terminal resistance, which generates voltage difference between two lines of bus.

Each gateway is designed with a terminal resistance R2 passing jumper connection in PLC network, as shown in Fig. (**6**). The users can choose if R2 of every gateway is connected to the network according to their needs. In the network of CAN bus, there are terminal resistance of 2 gateways connected to the network.

3.5. Selection of PCA82C250 Working Mode

In the network design of the paper, because the bus cable is unshielded and electromagnetic compatibility is considered, switching speed of bus signals for PCA82C250 must be reduced. Switching speed could be adjusted by controlling series resistance R3 of pin RS, as shown in Fig. (**7**).

Because this study is still at the experimental stage, the resistivity of resistance R3 selected here is tentatively scheduled for 27k Ω . The resistivity is between 16.5 k Ω and 140 k Ω , so PCA82C250 is in slope of controlling mode, and output voltage of Rs pin is about 0.5*Vcc.

4. DESIGNING GATEWAY PROTOCOL PROCEDURES OF DIRECT COMMUNICATION AMONG PLC BASED ON CAN BUS

4.1. Write Command Communication Among PLC

This chapter takes write command "@02EX01100000FF0A2E*" as an example to describe write command communication among PLC. The process of write command "@02EX01100000FF0A2E*" initiating communication is as follows:

PLC2 initiates write command "@02EX0110000-0FF0A2E*"by the internal TXD command.

Gateway A2 receives the data of the above-mentioned command.

After A2 receives the above-mentioned command, firstly, the fourth character 'E' is judged to determine the string data through PLC command initiated by PLC2 rather than the response frame data of Hostlink protocol. Secondly, the eighth character '1' is judged to determine the string data through PLC command. The fifth and sixth characters can be judged to determine the node ID of the read and written PLC, and node identifier of the gateway to which the read and written PLC belongs can be calculated by the node

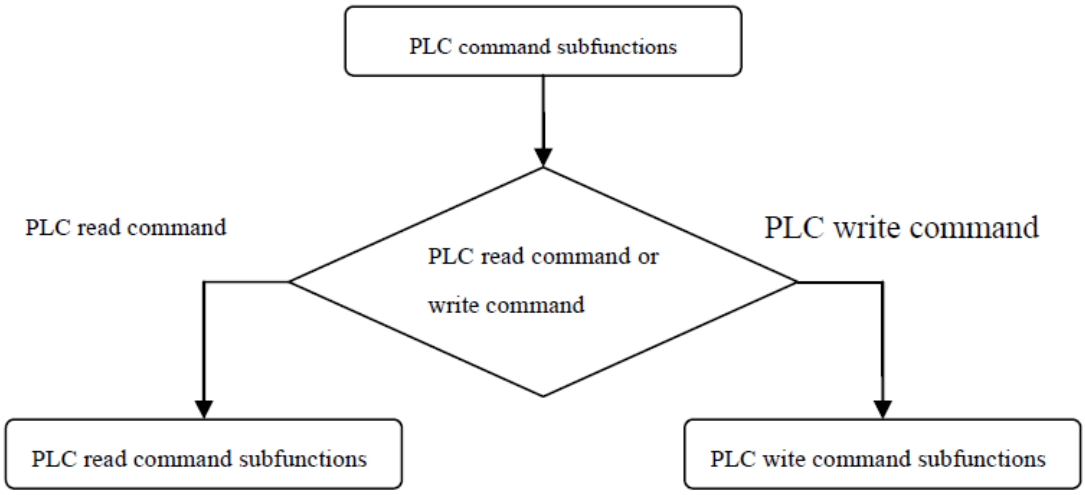

Fig. (8). Flow chart of PLC command subfunctions.

ID. Lastly, PLC command data which has been managed, is transmitted to the gateway to which the read and written PLC belongs [5].

The process of calculating the gateway to which the read and written PLC belongs, is realized by the node ID with function read_receive_plc_command_id which is displayed as follows:

```
void read_receive_plc_command_id(void)
{
    uint16_t temp;
    uint16_t can_lid=0;
    uint16_t can_hid=0;
    uint16_t can_hidx=0;
    can_hidx=(uint16_t)(uart_tx[5]-0x30); //ID of high-order CAN
    can_hid=(can_hidx<<8);
    can_lid=(uint16_t)(uart_tx[6]-0x30); //ID of low-order CAN
    temp=((can_hid | can_lid)<<5);
    pc_2515_tx_id_dlc[0]=(temp>>8); // Writing standard frame high order ID
    pc_2515_tx_id_dlc[1]=(temp); // Writing standard frame low order ID
}
```

PLC command "@02EX01100000FF0A2E" of the chapter is taken as an example. A2 will process the command into the following format and transmits to A1 for two times.

Write command:

0xC0	'0'	'2'	'0'	'1'	'1'	'0'	'0'

0xC0	'0'	'0'	'0'	'F'	'F'	'0'	'A'

In the write command, ASCII character of the character '@' adds 128 to get 0xC0. After A1 receives the two strings data, ASCII character of the first character for every data string becomes 0xC0, that is, the data is from one PLC in the network rather than PC.

(3) After A1 receives the above-mentioned write command data which is managed by A2, it needs to be managed into write command frame according to Hostlink protocol. And the process is as follows:

1) Determining command code. Command code is determined by the sixth and seventh character of the first string data. The sixth character determines read-write property, that is if the sixth character is '1', it is write command, and the character '1'will be transferred into 'R'. If the sixth character is '0', it is read command, and the character '0'will be transferred into 'W'. The seventh character determines storage area to read and write. If the seventh character is '1', the storage area is IR, and the character '1'will be transferred into 'R'. If the seventh character is '0', the storage area is DM, and the character '0'will be transferred into 'D'. We can see from equation (2) that the sixth and seventh character of the first string data is respectively '1'and '0', so the command code is WD and the property of command is write DM storage area command.

2) Calculating FCS Check Code

Firstly, the information in front of FCS check code in write command frame which accords with Hostlink protocol, must be obtained before calculation. We can get from equations ① and ② that the previous part of FCS check code in write command frame is "@01WD0000FF0A" by which FCS can be calculated as "23".

3) After processing the write command data into the format of write command frame of Hostlink protocol, it is sent to PLC1.

Write command frame which is managed at last is shown as follows:

Write command frame:

'@'	'0'	'1'	'W'	'D'	'0'	'0'	'0'
'0'	'F'	'F'	'0'	'A'	'2'	'3'	'*'
0x0D	0x0A						

(4) After receiving write command frame, PLC1 will send write response frame to A1. Because it is the communication among PLC, there is no sense for the response frame data. Therefore, A1 will delete it after receiving response frame data. And the write command communication of PLC is over.

4.2. Read Command Communication Among PLC

The chapter takes the transmission process in the network of read command "@02EX010000005E*"as an example to describe read command communication among PLC. The communication process is as follows:

PLC2 transmits read command "@02EX010000-005E*"by the internal TXD command.

Gateway A2 receives the data coming from PLC2.

After A2 receives the above-mentioned command, firstly, the fourth character 'E' is judged to determine the string data through PLC command initiated by PLC2 rather than the response frame data of Hostlink protocol. Secondly, the eighth character '0' is judged to determine the string data through PLC read command. The fifth and sixth characters can be judged to determine the node ID of the read-write PLC, and the node identifier of the gateway to which the read-write PLC belongs, can be calculated by the node ID. After A2 receives PLC command, node identifier of gateway A1 can be calculated by node ID of PLC1 in command, which is realized by function read_receive_plc_command_id(void).

PLC command "@02EX01100000FF0A2E" of the chapter is taken as an example. And A2 will process the command into the following format and transmits to A1 for two times.

Read command:

0xC0	'0'	'2'	'0'	'1'	'0'	'0'	'0'

0xC0	'0'	'0'	'0'	'*'	0x0D

(3) After A1 receives the above-mentioned write command data which is managed by A2, it needs to be managed into write command frame according to Hostlink protocol. And the process is as follows:

1) Determining command code. Command code is determined by the sixth and seventh characters of the first string data. The sixth character determines read-write property, if the sixth character is '1', it is read command, and the character '1'will be transferred into 'W'. If the sixth character is '0', it is read command, and the character '0' will be transferred into 'R'. The seventh character determines storage area to read and write. If the seventh character is '1', the storage area is IR, and the character '1' will be transferred into 'R'. If the seventh character is '0', the storage area is DM, and the character '0' will be transferred into 'D'.

2) Calculating FCS check code

Firstly, the information in front of FCS check code in read command frame must be obtained firstly and then be calculated. We can get from 1) and (2)that the previous part of FCS check code in read command frame is "@01WD0000FF0A" by which FCS can be calculated as "56".

3) After processing the read command data into the format of read command frame of Hostlink protocol, it is sent to PLC1.

Read command frame which is managed at last is shown as follows:

Read command frame:

'@'	'0'	'1'	'R'	'D'	'0'	'0'	'0'
'0'	'0'	'0'	'0'	'1'	'5'	'6'	'*'
0x0D	0x0A						

(3) A1 will receive read response frame of PLC1 after transmitting read command frame to PLC1. Because read response frame of PLC1 has the read channel data of PLC2, the relevant data needs to be fed back to PLC2.

After A1 receives read command frame of PLC1, the read channel data needs to be fed back to PLC2. But RXD command received in PLC under Hostlink protocol, is not available, so read response frame needs to be processed into the format of write command frame and then be transmitted to PLC2. The final write response frame which is processed by gateways A1 and A2 is defined as write command.

If the read data is 5555, read response frame of PLC1 received by A1 is as follows:

'@'	'0'	'1'	'R'	'D'	'0'	'0'	'5'
'5'	'5'	'5'	'5'	'7'	'*'	0x0D	

Because only data "5555" is the available information in the above-mentioned data, these data need to be processed into write command frame format of Hostlink protocol in A1 and A2, and "5555" will be fed back to PLC2.

A1 will be processed into the following format after receiving "@01RD00555557*"and then be transmitted to A2.

'0'	'2'	'W'	'L'	'5'	'5'	'5'	'5'
(5) After A2 receives "02WL5555" which comes from A1, the first character is judged to determine if it is write command data, and then it is processed into write command frame format of Hostlink protocol and transmitted to PLC2. The final write command frame format is as follows: '@'	'0'	'2'	'W'	'L'	'0'	'0'	'0'
'0'	'5'	'5'	'5'	'5'	'5'	'9'	'*'
0x0D	0x0A						

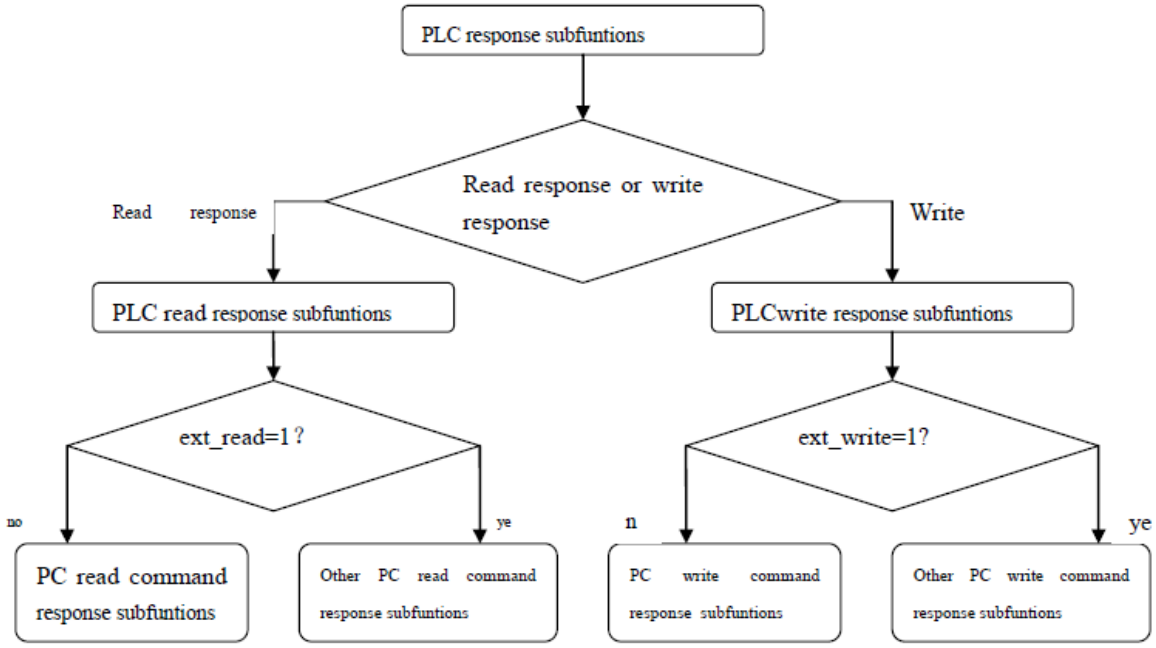

Fig. (9). Flow chart of PLC response subfunctions.

After receiving write response data of PLC2, A2 will be deleted. And read command communication of PLC is over.

5. REALIZATION OF SOFTWARE FOR GATEWAY PROTOWAY PROTOCOL PROCEDURES

5.1. Design Flow of PC Gateway Software

In the process of designing a software, the communication between PC gateway and PC is through the interface RS-232C of gateway, and the communication between PC gateway and PLC gateway is through CAN bus. The software of PC gateway consists of main program and interrupt service routine.

The process of the main program for PC gateway is as follow. Firstly, the main program for PC gateway initializes Atmega8 single chip and CAN controller Mcp2515, and then it receives command frame data from PC by serial interface. If there is no serial interface, the program will inquire the serial interface all the time and wait for the data from serial interface. After gateway receives the serial interface, the program will check if it accords with the command frame format of serial interface, And if it doesn't conform to it, it will be deserted and the program continues to wait for new data from serial interface, and if it conforms, command frame data can be processed.

5.2. Design Flow of PLC Gateway Software

On the one hand, PLC gateway receives and processes the data of PLC, and transmits the data to PC gateway or other PLC gateways. Similarly, the main program of PLC gateway receives the data belonging to PLC by the way of inquiring. After PLC gateway receives the data, firstly, the data should be judged if they are PLC command data or response frame data, before processing with the corresponding subfunctions.

Flow chart of PLC command subfunction is shown in Fig. (**8**). In PLC command subfunctions, firstly, the program differentiates if the PLC command initiated by PLC which the gateway belongs to, is read command or write command. Secondly, the corresponding subfunctions are adjusted to the process. Lastly, the processed PLC command is transmitted to the gateway to which the read-write PLC belongs in the network.

Flow chart of PLC response subfunctions is shown in Fig. (**9**). In the response frame initiated by PLC to which the gateway belongs, firstly, PLC response subfunctions differ-

entiate if they are read response frame or write response frame. Secondly, the subfunctions differentiate if they are PC response command frame initiated by PLC or PLC command response initiated by other PLC.

Flow chart of PLC gateway interrupt program is shown in Fig. (**9**). PLC receives and processes communication data from PC gateway or other PLC gateways by interrupt service program. Communication data from PC gateway or other PLC gateways may be PC command data, PLC command initiated by PLC, and response write command data from other PLC after PLC transmitting PLC read command. The above-mentioned communication data adjust respectively on receiving PC command subfunctions, receiving other PLC command subfunctions and receiving PLC response write subfunctions for processing.

CONCLUSION

The paper summarizes the existing deficiency based on the analysis of common PLC communication network. And the paper develops PLC network based on CAN bus with PC gateway and PLC gateway as the medium which makes CAN bus protocol as the basis, Atmega8 single chip as controller and Mcp2515 as CAN controller. Gateway communication protocol not only makes use of the existing PLC communication protocol, but also expands the existing communication protocol, which satisfies the needs of new communication and makes the new PLC network have the great advantages in cost-effectiveness and functions reliability.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

[1] X. Liu, X. Zhou, Z. Zhao, and N. Yu, "Distributed I/O monitoring system updating the program online based on CAN bus," *Coal Technology*, vol. 28, no. 3, pp. 34-37, 2010.

[2] Y. Lv, H. Yuan, and J. Xing, "Design of a distributed position servo system based on CAN bus", *Application of Electronic Technique*, vol. 35, no. 3, pp. 136-139, 2010.

[3] W. Li, L. Duan, M. Zhao, S. Wang, and Y. Yu, "A Control System of Flexible Fixture Based on EtherCAT and CAN Bus", *Electronics Optics and Control*, vol. 40, no. 11, pp. 89-92, 2012.

[4] L. Li, A. Wang, F. Cao, and Z. Li, "Design and realization of expand embedded PLC I/O for SPT bus", *Computer Measurement & Control*, pp. 75-76, 2012.

[5] J. Wu, "Monitoring System of PLC Controlling Production System Based on Field Bus". *Machine and Hydraulic*, pp. 72-73, 2010.

[6] S.H. Yu, C.H. Hyun, W. H. Kim, and M. Park, "Secure communication *via* active backstepping control and synchronization for new hyperchaotic systems", *JDCTA*, vol. 6, no. 10, pp. 276- 286, 2012.

[7] C. Duanmu, and Y. Yang, "A new algorithm for optimal power allocation in cooperative communications by using the differential evolution scheme", *AISS*, vol. 4, no. 8, pp. 229 -236, 2012.

[8] H. Li, L. Pang, and Y. Wang, "A domain-based secure communication scheme with fault-tolerant capacity", *AISS*, vol. 4, no. 5, pp. 44-52, 2012.

[9] Y. Shi, and Q. Wen, "An ID-based secure communication scheme for control system", *IJACT*, vol. 4, no. 15, pp. 98-104, 2012.

[10] Y. Yue, C. Sha, and X. Zhang, "Implementation of serial communication between host computer and PLC based on host link protocol", *IJACT*, vol. 4, no. 18, pp. 80-88, 2012.

Received: June 16, 2015 Revised: August 10, 2015 Accepted: September 19, 2015