Communication PLC with Embedded systems

DUSAN HAVLIK
Department of Control Engineering
CTU in Prague, FEE
Karlovo namesti 13, 121 35 Prague 2
CZECH REPUBLIC

Abstract: This paper presents communication PLC and embedded systems. The paper presents centralized and decentralized network between PLC and embedded systems. Communication PLC and embedded systems is dependent on structure of network and is type master - slave. In the end of the paper is connection between PLC and embedded systems.

Key-Words: PLC, embedded systems, communication, network

1.0 Introduction

Development new technology ables to existing new way of solution technology process. One of partial solution in control of a technology process is using of embedded systems collaboration with PLC. This paper presents communication between embedded systems and PLC.

2.0 Reason of using embedded system

We can see using of PLCs from Allen-Bradley, Siemens, Wago in the control of industrial technology process. Almost all PLCs is not convenient to control of a real-time application because one scan cycle of the PLC is longer then time to regulation action. Forasmuch as a solution of control of technology process must contain control real-time application sometime, it is necessary find technical solution which is compromise between price and quality of control. Embedded systems is possible solution of the situation.

3.0 PLC and embedded systems

3.1 Network between PLC and embedded systems

Network can be centralized or decentralized between embedded systems and PLC. Life cycle of communication is same for both type, but is different in the detail which arise from configuration network.

In case, that configuaration of the PLC or program into the PLC doesn't able to communication with more embedded systems, the central configuration network is used. Interface between PLC and embedded systems is special embedded system which is master for other embedded systems. The centralized network contains network with one embedded system.

In the configuration network, the PLC is master which communicates only special embedded system and which is connected to same network as PLC or is connected with serial channel RS485/RS422. The master embedded system (MES) receives commands from PLC. The MES decodes commands and sends other commands to slave embedded systems (SESs). SESs receive these commands, execute it and send acknowledge of receiving command or data with new information about their periphery. The MES receives data and saves it in the memory. When the PLC asks about data, the MES sends it him. Refresh information of periphery is indepen-dent on frequency of communication between PLC and MES, but is not longer then one scan cycle of the PLC. It is necessary to refresh all data must be in one virtual scan cycle of PLC to consistent information.

The MES detects states of connection with the PLC and slave embedded systems. If connection is lost, the MES gives notice to SESs about losing connecting with PLC. SES make several reaction to the state. Some SES doesn't need make reaction and some SES must make reaction and shut-down all his

periphery. After reconnection between PLC and MES, the MES sends information about reconnection and new data to SESs. If the MES lost connection with some SES, the MES gives notice to other SES and the PLC. When the PLC receives notice, decises of resolution about reaction to fault connection. If the MES reconnects to the SES, the MES sends new data to SES.

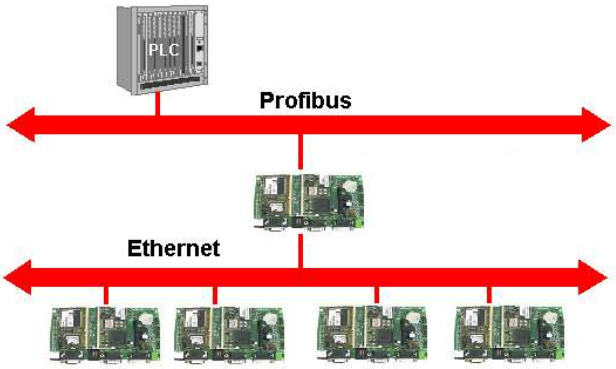

Fig. 1: Centralized network

The MES detects states of connection with the PLC and slave embedded systems. If connection is lost, the MES gives notice to SESs about losing connecting with PLC. SES make several reaction to the state. Some SES doesn't need make reaction and some SES must make reaction and shut-down all his periphery. After reconnection between PLC and MES, the MES sends information about reconnection and new data to SESs. If the MES lost connection with some SES, the MES gives notice to other SES and the PLC. When the PLC receives notice, decises of resolution about reaction to fault connection. If the MES reconnects to the SES, the MES sends new data to SES.

If the PLC detects fault connection with the MES, the PLC decises about reaction and gives notice about lost connection to supervisor control system. Communication between MES and SES is detected by SES. If the SES detects fault connetion, SES shut-down his periphery or makes other action.

The second way is decentralized network. No master embedded system in the network and a PLC direct communicates with all embedded systems. The PLC has seperated memory for communication with each embedded system. All information about states and history of communication is saved in the seperated memory. Number of packet, data which was received from embedded system, data which was sent and will be sent are saved in the seperated memory too.

If embedded systems not communicate theirself, the PLC have to control communication on the bus, otherside it is necessary use profibus, ethernet or control unit of bus to communication.

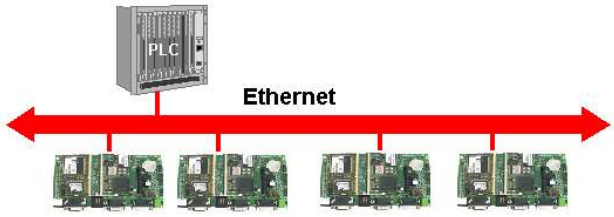

Fig. 2: Decentralized network

How it was said, if embedded systems not communicate theirself, the PLC must communicates with embedded system by embedded system to receives and sends data. Question of this communication is monitoring of state bus. This question have two main answer. First resolution, embedded system listen bus and state „Communication is OK“ is state, when the embedded system listens some communication. Second resolution, each embedded system must communicates with the PLC to time-out. If the PLC not communicates with the embedded system on time, the embedded system sets information fault and makes reaction to losing communication. The PLC makes similarly things. If embedded systems communicate theirself, control of bus is more difficulty because each device needs connect to the bus. If profibus, ethernet are used, problem is solved, because these busses have standart protocol. If RS485 is used, it must be used Central Control Bus, which gives authentication to communication. Algorithm of giving authentication will be dependent on device's requirements of using bus. Example the PLC has authentication two-time often than other devices. Cycle of giving authentication must contains time for refresh information about devices which are connected to the bus. Disadvantage is losing of communication when some device get into deadlock after getting authentication and device doesn't return control bus to central control bus . One of ways, it can be using time-out. It means using limited time, when a device must return control of bus to Central Control Bus (CCB). If the device does not return control of bus, CCB sends to all devices cancel-packet and than CCB refreshs information about devices. In case CCB find wrong device, CCB sends information to the PLC and other embedded systems. After refreshing of information CCB gives authentication some device. The PLC and embedded systems must detect state of bus theirself too.

Special way of communication is way, when the PLC communicates with master embedded system which is master for other embedded systems in the decentralize network. Communication PLC with embedded systems is same as in the centralize network. This model has a adventure, if master embedded system is wrong or is disconneted, master

embeded system may replace by other embedded system. Signal to change is given by the PLC or supervizor of embedded system.

3.2Communication PLC and Embedded system

Communication PLC and embedded system is type master – slave. Master is PLC and Slave is embedded system. The PLC starts communication with sending data to embedded system. Sended data must contains head of packet, data and CRC. Content of packet head is dependent on configuaration network between PLC and embedded system.

Fig. 3: Structure of packet

If the PLC communicates with one embedded system, head of packet contains only code of message and number packet. If the PLC communicates with more embedded systems, the head of packet contains address of device, code of message and number packet. Code of message is used to decision of data processing in the embedded system. Number packet is inique number by defined time.

Second part of packet is data for embedded system, which has variable number of data. If traffic is not too high on the bus, it may use definite number of data which is writen in the head od packet.

The third part of packet is CRC of previous data. Function XOR of previous data is simple function of CRC. Other fuction CRC may be cyclic code too. If length of packet is not too long, CRC is possible insert into data. i.e. make function CRC two previous byte and write to third byte.

Generally, method of CRC of packet is compromise between data protection and computing time for creating CRC of packet.

The PLC starts communication with embedded system because the PLC is master for embedded systems. Unique number is written in the head of each packet which is sent to the embedded system. The embedded system receives packet and packet processing. If the PLC wants data from embedded system, the embedded system creates packet, copys number PLC's packet into packet and sends it. The PLC waits for data from embedded system and if data doesn't come to the PLC on time, the PLC makes reaction to losing connecting with the embedded system. If the embedded system is important for all system, the PLC controls shutdown system or make signal to replace wrong device. If the PLC receivea data on time and wants next data, increments number packet and sends requierement to the embedded system. Number packet must be unique by defined time. If we know, that number of packet is less 65000 by day, we use two byte for number packet and increment number with number of packet. And after 24 hour, we reset number packet. If number packet is used, it is easy detected losing communication. If the PLC detects losing of communication, the PLC sends reset packet and wait to acknowledge of reset packet from embedded system. If the PLC finishs communication with embedded system, sends finish packet and wait for acknowledge of finish communication.

Very important thing is testing of communication when PLC mustn't data from embedded system, because embedded system must know that connection is correct.

3.3 Connection PLC and embedded system

The embedded system can be connect to PLC with several way, but basic ways are Profibus, ethernet, wireless and serial channel RS485/RS422.

Profibus is used when embedded system has profibus interface. If the embedded system has not this interface, it is possible embedded system connect to the bus over transfomer profibus – RS485. Disadvantage of this connection is limited rate of serial channel between transfomer and embedded system.

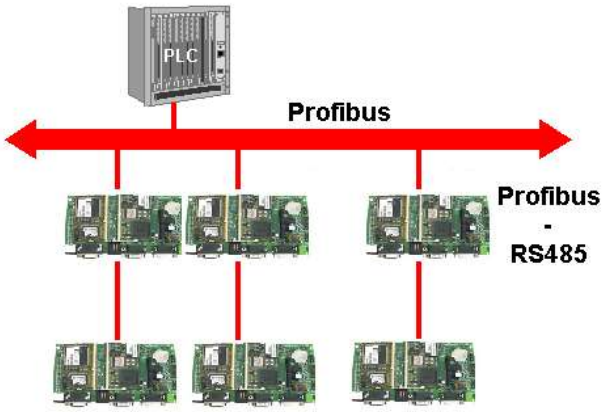

Fig. 4: Profibus with RS485

Other way is connection embedded system and PLC with ethernet. This communication is faster and it is possible fast transfer large data. Speed of communication is limited by data processing in the program. If embedded system has not this interface, it is possible embedded system connect to the bus over transfomer ethernet – RS485. Disadvantage of this connection is limited rate of serial channel between transfomer and

embedded system.

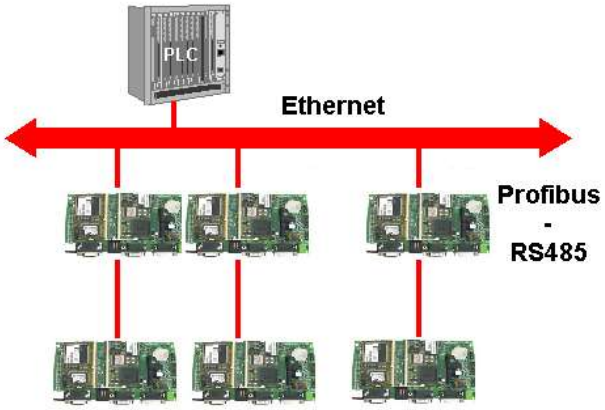

Fig. 5: Ethernet with RS485

Wireless connection is necessary used when the PLC and embedded system is not possible connect together with wires. If the embedded system is far from PLC, it is possible used GSM module and using public GSM network. If distance is less 50 meters, it is possible used Bluetooth. If it is used wireless connection, it is necessary regard data protection of communication.

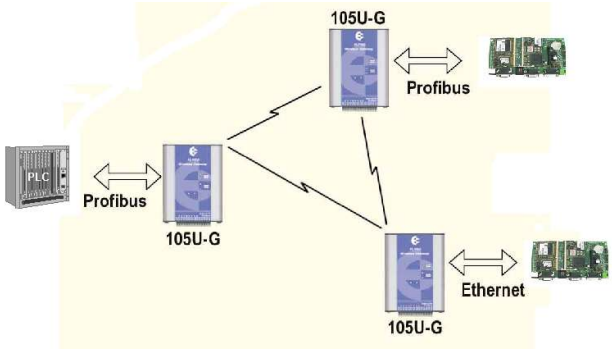

Fig. 6: Wireless

4.0 Conclusion

The communication PLC with embedded system is dependent on the structure of network. In the centralized network, the PLC communicates with one embedded system which is master for other embedded system. In the decentralized network, the PLC communicates with all embedded systems. Control of communication on the decentralized network is more difficulty then on the centralized network. History of the communication is same as in the centralized network as in the decentralized network, because communication is type master - slave, master is PLC and slave is embedded system. The communication must be protect data from transfer error. Every packet must contains head of packet, data and check-sum. Address of device, packet number and code of message are in the head of packet. Connection may be with several busses include wireless.

5.0 ACKNOWLEDGEMENTS

This paper has been supported by Grant Agency of the Czech Republic, project number 102/05/0467 "Architectures of Embedded Systems Networks"

References:

[1] Elprotech Technologies ,105U-G Wireless gateway ,*Datasheet*, URL:<http://www.elprotech.com>
[2] Janeček, Jan: *Distributed system*, CTU FEE, Prague November 2000
[3] Havlik, Dusan: Railway model,*Master's thesis*, CTU FEE, Prague 2004
[4] Electronic catalog Siemens, URL: <http://www.siemens.com>