PLC COMMUNICATIONS IN A PROCESS CONTROL SYSTEM

by GR MacKenzie, AEG

COMMUNICATION

Communication has become a major part of any process control automation system. Today PLC communication is as much for data acquisition as plant control. The first thing the designer often asks is 'how'? But shouldn't he first be asking 'why'?

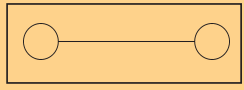
Before one can consider how to implement a communication system, one has to consider what the final objective is. What is the importance of the data, what is the amount or volume of data to be transferred and when or how often is the data required. All of these are factors of why the communication is needed. Once all this information is known, one is much better placed to decide how this is to be done.

In order to make this final decision however, we first need to look at the options.

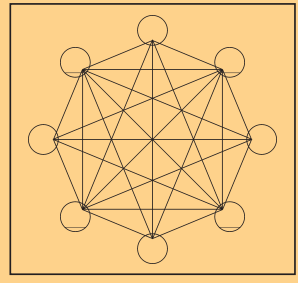
Topologies

The topology of a network refers to the 'structure' of the network, ie how all the machines, termed participants or users, are connected.

The most simple topology is point to point - a single link between two machines (Figure 1a). This generally works well in very small installations. When the installation grows and communication is required between all the 'participants' in the system, the configuration becomes very messy, see Figure 1b. This is commonly known as a mesh topology. As seen here, to connect eight users will require 28 lines therefore 56 interfaces. A ninth user is an additional 8 lines and 16 interfaces. This is clearly very expensive in hardware and installation.



1(a) Point-to-point topology



1(b) mesh topology.

Figure 1(a) Point-to-point topology and (b) mesh topology.

As sites got bigger, so the bus or local area network (LAN) was developed. The concept here is to have one communication interface per user, and a single cable (or medium) connecting all users. Physically this is normally achieved in a tree (Figure 2a) or daisy chain (Figure 2b) structure. The tree topology uses taps or splitters to separate information from the main bus (trunk) and transmit it down the branches to the users. The daisy chain topology is very similar but has the main bus cable running into and out of the communication interfaces of the users. This method requires isolation between the electronics of the interface and the bus itself to prevent a failure of the interface from affecting the bus.

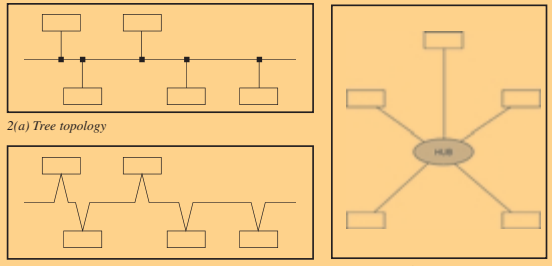


Figure 2(a) Tree Topology, (b) Daisy Chain Topology and (c) Star Topology.

It is also necessary in some applications usually restricted by geographical layout to configure a network in a star topology (Figure 2c). This works a little like a tree network with a very short trunk and long branches.

After the development of bus type communication there immediately arose the problem of control of the bus. In point to point communication the control is a master-slave type control. This works well, as if either user fails, no communication can take place anyway. In a bus configuration, however, this is not always the case. For installations where the 'master' device is always in control and the slaves are 'dumb' devices which need only to communicate with the master, this topology is sufficient. In a distributed control environment however, where all users need access to the bus, the failure of a master station and subsequent loss of the communications network is not acceptable.

This leads to the concept of 'peer to peer' communication. In this format, no single user has control, but a protocol is developed to allow control of the bus to be shared between all participants. In PLC communications this normally takes the form of a 'token passing' network or 'carrier sense multiple access/collision detect' (CSMA/CD) network.

Token passing means that all participants on the network have a list of all the participants on the network including itself, usually in the form of an address or node number in ascending order. At any time, one of the participants has the token for an amount of time equal to or less than a pre-defined maximum time. During this time it may send data to or request data from any other node. When it is finished, or its maximum time has elapsed, it will 'pass-on' the token to the next node in the list of participants and listen, as though it were a slave until it receives the token again.

CSMA/CD networks, or what is more commonly known as Ethernet, work on the principal of there being no absolute control of the network. Each user on the network detects for itself whether it is connected to the network. This is known as carrier sense. Once it detects a carrier on the network it sees the network as alive and accesses the network, sending to or requesting data from another user. Clearly as there is more than one user on the network, more than one user may try to access the network at the same time, multiple access. Electrically these two messages will corrupt each other, so when this occurs, both users which have transmitted data will detect data on the network other than what it sent, collision detect. Both users then stop communicating for a random amount of time and then try again.

Transmission media

The transmission medium is the physical path between transmitter and receiver in a communications network. The media that have been used in local networks include twisted-pair wire, coaxial cable and optical fibre. In addition, forms of electromagnetic propagation, through the atmosphere, can be employed for building-to-building connections or over large geographical areas.

The various media can be described using the set of characteristics described below.

- physical description: the nature of the transmission medium
- transmission characteristics: include whether analogue or digital switching is used, modulation technique, capacity, and frequency range over which transmission occurs
- connectivity: point-to-point or multipoint
- geographic scope: the maximum distance between points on the network
- noise immunity: resistance of the medium to contamination of the transmitted data
- relative cost: based on costs of computers, installation, and maintenance.

Transmission media or channels have the following transmission characteristics:

- bandwidth: this is an electrical characteristic of the transmission line or circuit. It indicates the range of frequencies (measured in Hertz) which can be successfully trans-miffed over the line
- baud rate: the number of single elements or condition changes per second. This defines the signalling rate on the transmission line. A signal element is a discrete voltage, phase or frequency value
- channel capacity: this is the maximum rate at which it can carry information without error. For digital information, this is measured in bits per second and: capacity = baud rate x number of bits per signal element

Signalling modes

Transfer of data over a transmission medium occurs in one of two modes:

Baseband signalling is the transmission of the digital signal at its original frequency, without modulation (see Figure 3a). A string of 1s and 0s will result in a DC signal so this is also known as DC signalling. This is commonly used in local area networks.

The capacity and the inductive effect of the wire or cable, result in distortion of the signal as shown in Figure3b. This distortion depends on the length of the transmission medium and the frequency. Baseband signalling is suitable only for local transmission over distances typically less than one kilometre. The actual maximum distance depends on the transmission rate for a given transmission line at given power of a transmitter. This is the most common method of signalling in PLC systems as distances seldom exceed these values.

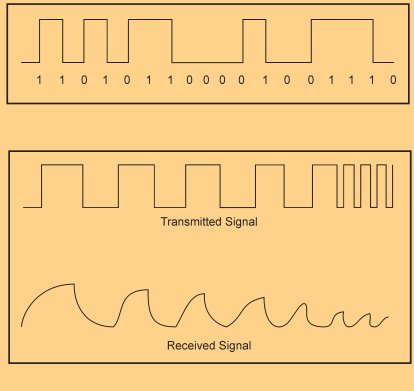


Figure 3(a) and (b). Baseband transmission

Switched or leased lines from public carriers, telephone network, are generally not suitable for baseband transmission. The signals on these lines are amplified by regenerators which do not pass DC signals. In addition, these carrier lines are often loaded with an inductance to reduce the distortion of analogue signals. It is possible to lease an unloaded local line, which does not have any regenerators.

Broadband transmission uses the digital signals to modulate a carrier signal using one of the modulation methods discussed below. The carrier frequency must be within the bandwidth of the channel. This technique must be used for networks that use voice-grade lines which generally have a bandwidth of 300 - 3000 Herz. It is becoming quite common to use

the public telephone network for PLC diagnostics and programming remotely, but seldom for data acquisition because of the slow speed, maximum generally of 2400 baud. Broadband signalling is nearly always used in wide area networks,(WANs), but also for some LANs based on cable television technology.

Modulation methods

- amplitude modulation: two different amplitudes of a carrier, for example 1500 Hz are used to represent a 1 and a 0.
- frequency modulation: this is also call frequency shift keying (FSK). A 0 and a 1 are presented by two different carrier frequencies. This is the most common method of modulation for telephone line modems.
- phase modulation: there are two different types of phase modulation:
  - a) a phase shift of 180(in the carrier occurs each time a binary zero is transmitted. No phase change takes place for a binary 1.
  - b) phase shift keying (PSK) in which a zero and a 1 are represented by two carrier signals 180° out of phase

The above methods all have two signal levels so each signal element represents one bit of information. It is possible to have variations and combinations of these techniques which result in more than one bit per baud.

Baseband and broadband

The principle characteristics of base-band and broadband systems are listed in Table 1.

BASEBAND	BROADBAND
Digital signalling	Analog signalling (requires RF modem)
Entire bandwidth consumed	FDM possible- multiple data
By signal	Channels, video, audio
Bi-directional	Uni-directional
Bus topology	Bus or tree topology
Distance up to a few kilometres	Distance up to 10s of kilometres

Table 1. Bus/tree transmission techniques

Protocols

The protocol of a communication system is defined as 'the specification for coding messages exchanged between two communication processes'.

A data communication protocol will typically have three phases: establishment, message transfer and termination, see Figure 4. The message transfer will normally contain the length of data being transferred, the data itself and certain error checking information. In a network system, the address of the node to which the data is being sent is also needed.

The PLC industry, even to this day, is notorious for its development of protocols. Each PLC on the market has its protocols for data transfer between two similar machines, but no two PLCs supplied by different manufacturers can communicate with each other on their proprietary communication protocols.

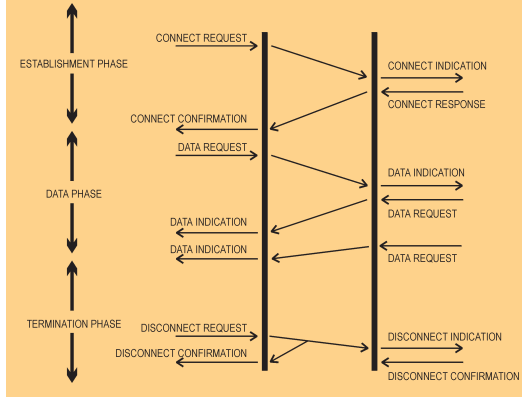


Figure 4. Connection Protocol

This has been overcome by some of the European manufacturers who have developed non-standard interface cards using the transmission protocols of other PLC manufacturers.

Interface standards

Over the course of time certain interfacing standards have been generated by industry in order to make communication between systems from two different manufacturers more simple. These standards typically defined the communications medium, transmission voltages, speed of communication, (baud rate), and maximum distance sometimes related to speed.

The first such real standard was RS232. This was written by the Electronic Industries Association (EIA) in the USA and was fairly complex, including the definition of 22 terminations between the two interfaces. Today of course, few people use more than four wires and a screen for RS232 communication, using a subset of the original, RS232C. Most, if not all, PLCs today have an RS232 interface, for instance:

AEG Modicon - Modbus
Allen Bradley - Data Highway
Siemens - 3964R (CP525)

Some RS232 protocols today also allow for the addressing of nodes, thus providing for network communication from a standard R5232 interface. The main advantage of this being cost as RS232 interfaces are very simple and thus cheap, plus of course the fact that most PCs, which are used more and more in automation systems today, have at least one PS232 (serial) interface as a standard.

RS232, however, has some limitations. Distance, a maximum of 50 ft by definition (without modems) is a major problem, and a maximum transmission speed of 19200 bits per second (baud). This led to the development of several other interface standards, the most common in the PLC industry being RS485, IEEE 802.3 (CSMA/CD) and IEEE 802.4 (token bus).

OSI standardisation

The open system interconnection, OSI or seven layer model, is undoubtedly becoming the standard model for communications definition. Whereas RS232 and IEEE 802.3 for instance are interface standards, the OSI model is an attempt to set up standards for the whole communications structure. In this model, the interface standards become part of Layer 1, the physical layer. If one looks at the 'OSI wineglass' of protocols, Figure 5, one gets an idea of the complexity of the communications problems. It shows the many functions covered by upper layers and multiple options for physical media at the lower layers. The session and transport layers, however, have fewer layers and are now international standards.

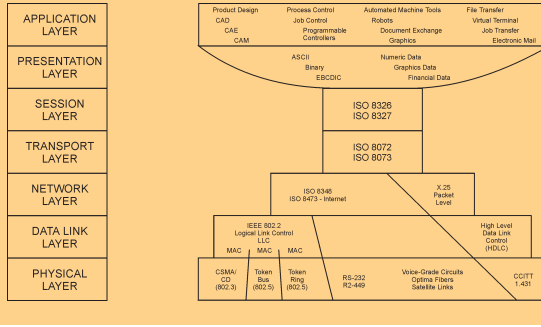


Figure 5. OSI (7 layer) Model - 'Wineglass'

An introduction to MAP

As early as the late 1970s, General Motors in the USA were estimating that over 50% of automation costs within GM were going into communications functions, and the continual lack of well-defined standards was seen simply as adding to this cost. This led in November 1980 to the establishment of the MAP (manufacturing automation protocol) task force. 1988 saw the publication of the MAP 3.0 specification and to this date several PLC manufacturers have released MAP 3.0 compatible interfaces.

Where does MAP however fit into the scheme of things as a PLC user? The concept of MAP was really designed for inter-computer communication, ie large volume data and file transfer. At the PLC, cell control level, control and data transfer is required to be 'realtime'. This led initially to the concept of Mini MAP. Mini MAP is completely non-MAP compatible and is designed to inter-connect low-cost devices via a time-critical network which could ultimately be linked to a carrier-band MAP backbone.

Field bus

This Mini-MAP concept led to the drive to specify a non-MAP compatible, low cost, real-time bus which would inter-connect devices at the lowest level. Such buses were termed 'field buses', but even here standardisation seems far off.

Intel already had in existence its Intel Bit Bus which had many of the characteristics required. Based on RS485 at the physical layer, it could communicate with both field devices and PLCs at up to 1200 m using twisted pair cable and standard connectors. A few European PLC manufacturers immediately adopted this standard.

This Bit Bus, however, was also seen to have a major shortfall, in that it was based on a master-slave topology. At this time, the major field-bus standard contenders are Profibus, Modbus Plus and FIP Bus. We look at the first of these:

Profibus

Most of the PLC and field device manufacturers in Europe got together in the late 1980s to set up the Profibus (process field bus) working group. The specifications generated out of this group for a standard field bus communication were:

Characteristic features

The various application fields, for example control, factory automation, power distribution, building automation, primary process industry, etc, have the following characteristic bus requirements:

- network topology: linear bus with or without terminator, including drop cables and branches (tree)
- medium, distances, number of stations: depending on the signal characteristics, for example, for shielded twisted pair, (1.2 km without repeaters, 32 stations)
- Transmission speed: depending on network topology and line lengths, for example, step-wise from 9.6 to 500 kbits/s
- redundancy: second medium is optional
- addressing: 0 to 127 (127 = global addresses for broadcast and multi-cast messages), address extension for regional address, segment address and service access point, (LSAP), 6 bit each
- station types: masters (active stations, with bus access control); slaves (passive stations, without bus access control); preferably at most 32 masters, optionally up to 127, if the applications are not time critical
- bus access: hybrid, decentral/ central: token passing between master stations, and master-slave between master and slave stations

The Profibus user organisation includes the following members: AEG AG; Robert Bosch GmbH; Endress + Hauser GmbH + Co; Khockner-Moeller GmbH; OMRON Electronics GmbH; Siemens AG; Weidmuller GmbH.

Set up in December 1989, the intention of the organisation is that:

- the exchange of information of all parties interested in the Profibus is to be supported
- the work on draft standards for further development of the Profibus concept will continue
- projects concerning the extension of functions will be supported
- the right of qualified and tested products to carry the name Profibus will be introduced and supervised
- public relations to inform all parties interested in Profibus standards

Modbus Plus

Developed by AEG Modicon in the USA, this is becoming possibly the most widely used network in new installations in that country. The approach to developing this network, however, has been very different to that of Profibus. After releasing the bus in 1989, Modicon formed a program known as the 'Modconnect Partners' program with several leading suppliers of computer and automation products in the USA. As of January1992, this included IBM, Uticor, US Data, Datalogic, Xycom, Hilco Technologies and Digital Equipment Corporation (DEC). These manufacturers have all developed products or applications for direct integration onto Modbus Plus networks.

Although not associated with the Profibus group, the characteristics of the two networks are very similar.

- network topology: linear bus with terminator, daisy chain
- medium, distances, number of stations: shielded twisted pair, (450 m without repeaters, 32 stations, (1800 m with repeaters, 64 stations. (Longer distances with optical fibre)
- transmission speed. 1 Mbits/s
- redundancy: second medium is optional
- addressing: 0 to 64
- station types: masters (active stations, with bus access control); (Slaves (passive stations, without bus access control) still under development)
- bus access: hybrid, decentral/central: token passing between master stations and master-slave between master and slave stations

The overall concept

Figure 6 shows the overall concept driven by the MAP/fieldbus concept. What is seen here is a clear indication that the right network must be chosen for the right application.

At the plant/cell control level where 'real-time', fast response communication is required, fieldbus is used. At the higher management level, where large file transfer occurs, a MAP backbone between all computers is a reality.

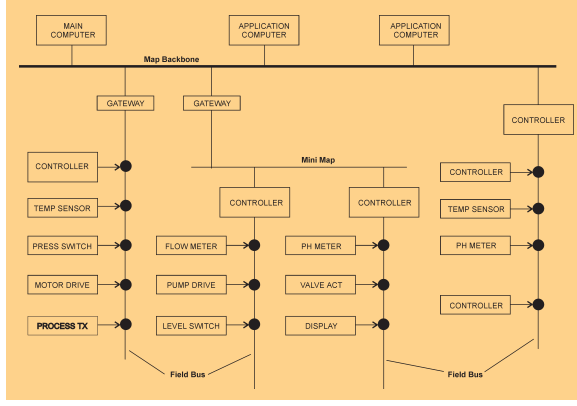


Figure 6. Possible MAP interconnections

The $6 million question

Finally we come to the six million dollar question 'How do I decide on the communication for my plant'? Some of the points mentioned before are pretty clear.

Cost is a very big factor, both the cable and the installation. It is not always wise to skimp; however, engineering is becoming by far the most expensive part of any automation system and an undersized communication network will eventually cost much more in engineering to achieve the required performance. On the other hand, a lot of money can be wasted on an expensive network which is badly engineered. The solution is to get some advice, but know enough to make sure you are given what you want.

Redundancy of networks is becoming very popular. This is not a standard product, and if it is, should it be?

Each customer has his own requirements from a redundant network. Should all data be sent on a master network and the second a stand-by; should data be shared on both networks if they are healthy; should a complete network be failed because of one fault; or should only that data be re-routed, the options are endless. Remember though the cost of engineering these solutions. Add this to the cost of the extra interfaces required and it gets expensive. Most people at the end of the day are worried about cable break, a better (and cheaper) solution then is dual cable not dual networks.

Speed can be misleading. A baud rate of 9600 bits/second is exactly that. This is a bit rate of the interface protocol. It does not reflect the amount of data which can be transmitted on the network in one second. Remember that data transfer is only one of the sections of a transmission protocol. Tests by Modicon for instance show that the Modbus Plus communication network, operating at 1 Mbaud, has a guaranteed minimum throughput of 20,000 registers (16 bit) per second, per network.

The most expensive is not always the best. The use of ethernet for inter-PLC/PC communications has long been debated. At 10 Mbaud it is surely the 'fastest' PLC network available, but is it always? A critical feature of any control network is determinism. Simply - can you the user guarantee that data in one PLC when sent will reach its destination within a specified time?

The answer is no. By the very nature of ethernet, CSMA/CD, as more data is put onto the network, so more collisions occur, more random 'back-off' times and no guarantee of performance. Token passing, although slower, generally 1 to 2 Mbaud has guaranteed performance, and is generally cheaper. The maximum transmission time for any network configuration can be calculated.

A classic rule for any PLC application is that repeatability is more important than speed. It is better that data is received within 1 second all the time than within 100 ms most of the time. Don't write off ethernet though. It definitely has a role at a higher level (Figure 6) where file transfer is occurring between computers.

Bridges are very useful for isolating similar networks. Separate areas of plant can run on dedicated networks providing very high speed data transfer between users. The bridges then provide a link between the networks for the occasional data transfer required between plant areas.

Fibre-optics is coming more and more into its own. The cost of cable is dropping and will eventually rival that of twisted pair, certainly cheaper than co-ax. 3M has now released hand installation kits with relatively low dB losses, doing away with the need for expensive installation equipment. The immunity to lightning (very useful in SA) and HV interference is a big plus point. The cost of the fibre-optic modems, however, is still relatively expensive.

Also consider maintainability. Who is going to do it? Do you want, as the end client, to have to call out the network supplier each time a node fails or you want to add another PLC/node to the network? Ask for a demonstration of the communications system including setting up and programming of the data messages.

Communications is a practical problem to which there is generally a practical solution. Do not be fooled by 'buzzwords'.

Understand your requirements and your application, then find the correct network for your system.

Bibliography

[1] Kennedy 'Electronic Communication Systems', Third Edition, McGraw-Hill, 1984

[2] Voelcker J. Helping Computers Communicate', IEEE Spectrum. 1986

[3] Rodd MG and Deravi F- 'Communication Systems or Factory Automation', University of Wales, Swansea, 1987

[4] Stallings W. 'Local Networks', Macmillan, 1984

[5 Information on Profibus from DIN 19245 Part 1