IMPACC — CONNECTIVITY

Table of Contents

For further information contact the Advanced Product Support Center (APSC) at 1-800-809-2772. For referenced documents (IL's, Application Notes) contact APSC or dial FRED (Fax Retrieval of Engineering Documents) at 412-494-3745.

Communications Overview

Introduction

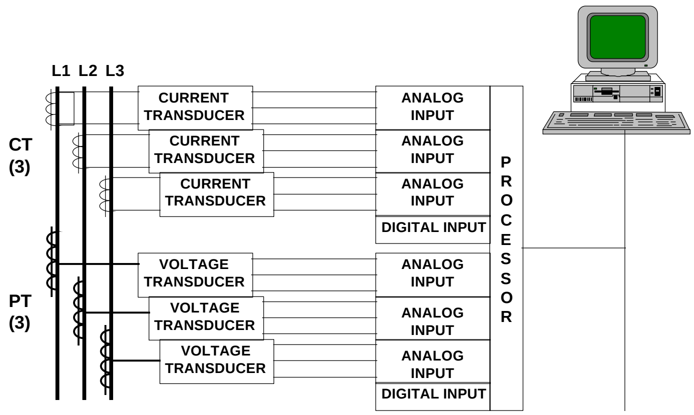
The purpose of a communication network is to get data from one place to another. Our customers are using communication networks for literally thousands of reasons including providing information to decide how to allocate energy costs, determining the efficiency of a given process, alerting them of problems with their distribution system, and helping troubleshoot systems when an interruption occurs. They are also using communications to remotely control processes. The advent of communications has dramatically improved the productivity and efficiency of all market segments. As with all of our products, different customers have different requirements that a communication system needs to fill. A commercial office building looking to bill once a month has a much different spec for communication than a transfer line in an automotive plant. As a result, there are several different types of communications devices and systems. Our customers will evaluate several things when determining which communication system is right for them. These include:

- Installed cost - sensor, communication device, network wire, display hardware & software
- # of sensors supported on a network
- Distance - How spread out the devices are & how much wire is required to connect them
- Throughput - Amount of data that is needed to be transmitted per unit time
- Reliability of data - Certainty that the data sent is data received
- Availability of network - What is the uptime of the network under various conditions
- Connectivity - How easily is data transferred between different networks

A communication system has “ratings and features”, much like the other C-H products we sell. This discussion will attempt to define the characteristics and terminology of communication networks and give a feel for what a customer is looking for in a network.

Sensors

There are several individual parts required for a communication network. The first part is taking the data from a **sensor** (i.e. a current transformer) and converting that data (0-5 amps) to an **analog** or **digital** signal. The product that originally performed this function was a **transducer** (i.e. a current transducer). It took the 0-5 amps and converted it to a proportional analog signal (i.e. 4-20 mA, 0-10V, etc.). That method proved to be fast, but expensive. In addition to the sensor and transducer, a shielded 3 conductor cable and a translator (i.e. an analog input module in a PLC) for each piece of information was required. That meant 3 transducers, 9 wires, 18 terminations, 3 analog inputs for 3 phase currents alone. The information could also only be sent relatively short distances.



Analog network - 1 circuit

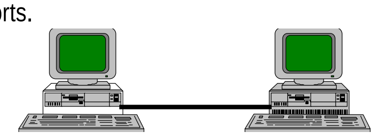
With the introduction of the **microprocessor** came **digital** devices & networks - the ability to take the current (0-5 amps), convert the raw number to **1**'s and **0**'s (i.e. an IQ Energy Sentinel) and send it to another place. There was no advantage if you sent a single phase current, but if you sent all 3 phases, all 3 voltages, energy, power, status and control, the reduction in cost was substantial (up to a 4 fold reduction). The data messages in a digital network are typically sent **serially** - one data message after another. A key component of the success of digital communications is getting the data where it needs to be when it needs to be there. That time includes sensing the data, sending it over the network, and translating the data into a usable format (i.e. present it on a computer screen or present it to another device so that it can interpret it and act on it). In an analog network, the time includes the translation in the analog module, the scan time in the PLC plus the time it takes to display it. The time it takes for a specific amount of data to complete that cycle is **throughput** of a network.

The Physical Layer

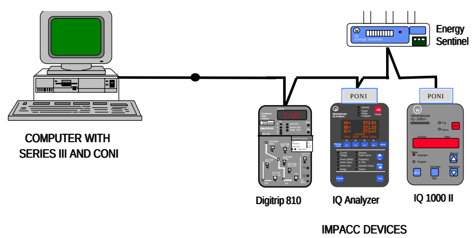
The next step is to get that data (1's & 0's) from one point to another - that is called the **physical characteristic** or **physical layer** of a network. The physical layer consists of several components.

1) **Topology**: How the two points will be connected together. Networks are typically connected in 3 modes.

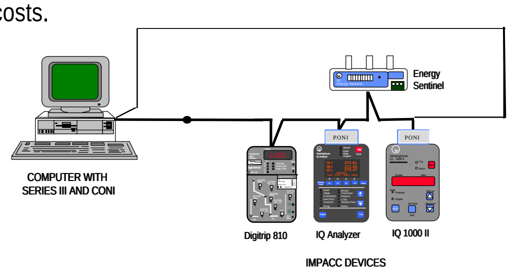
- **Point to Point**
  One device connected to another device. Advantages: simple, inexpensive for one device communicating to another. Disadvantage: Very expensive for more than 2 devices - requires additional repeaters or communication ports.



- **Bus**
  Multiple devices connected together on a single wire. Advantages: simple, inexpensive, for multiple devices. Disadvantage: If line is broken, lose communication to devices beyond break.



- **Ring**
  Multiple devices connected together on a single wire forming a loop. Advantages: If data line breaks, messages still can be heard by all devices. Disadvantage: More expensive, doubles wiring and communication costs.



Each of the above may be **redundant** - two wires running in parallel such that if one wire breaks, the network is still intact.

2) **Media**: How the network is physically connected together. Data is typically transmitted over (in increasing cost):

- **Straight wires** - An example is telephone cable (26 gauge, 4 conductor)
- **Twisted Shielded Pair (TSP)** - 2 conductor, twisted wire with a metal shield around it. The wire is twisted and shielded to help prevent electrical **noise** from getting onto the wire or from the communication wire into other circuits. (Noise is not good because it can change the 1's to 0's, changing the value of the data.)
- **2 TSP** - Two twisted shield pair of wires in a single cable used for networks that have separate transmit receive requirements or that send duplicate signals down 2 cables to check for data corruption.

- **Coax cable -** A single conductor surrounded by a plastic material, a shield, and an outside coating.
- **Fiber Optic Cable -** A thin glass or plastic tube used to conduct light signals.
- **Air -** No physical wires.

3) **Physical Signaling -** The signal level and type used to get the 1's and 0's down the network. Examples include:
- **Voltage level -** Different voltage levels mean a 1 or a 0 (i.e. +12V=1, -12V=0)
- **Impedance -** Different impedance's signify 1 or 0.
- **Frequency -** Different frequency levels (FSK- FM radio is an example) or amplitudes of the frequency(ASK- AM radio…) mean 1 or 0.
- **Light -** Presence or absence of light mean a 1 or 0.

The physical spec contributes to cost, how many devices are supported on the network, the distance the network will cover, the reliability of the data, and the availability of the data. A point to point network, over existing spare telephone lines, using voltage signals may be inexpensive for data from one device, but is expensive if you communicate to more than one device(one wire to each device) and the data is not very reliable as electrical noise can corrupt the data easily. A bus network, using twisted shielded pair with FSK signaling is slightly more expensive than existing cables, but it can support lots of devices and data reliability is very good (electrical noise does not affect FSK signals).

Protocol

Now that the data can get from one place to another, we have to define a format such that the both ends of the network understand what the various combinations of 1's and 0's mean - that is the network's **protocol**. The protocol consists of:

1) **Access method or bus arbitration -** who decides when a device sends data. There are several types of networks:

- **Master - slave**
  A single device (i.e. a personal computer) controls and manages the communications on the network. It asks for information from devices (slaves) on its network and gives information to the slaves.
- **Peer to peer**
  Each of the devices on a network can talk on the network, unsolicited, directly to any other device on the network. The communication is managed in a couple of ways. One method is a **token**, or permission to speak, is passed around the network to each device in turn. It tells what it has to say and asks what it needs to know, then passes the token to the next device. Another method is **multiple access, collision detection**. In that method, a given device checks for network activity if it needs information or needs to send information. If no one else is talking, it starts. If another device is talking, it waits until the first device is done. If two devices talk at once, both devices realize it, stop talking, each wait a predetermined amount of time before starting again. Each device on the network has a different amount of wait time, depending on its priority and the amount of time since it last spoke.

2) **Message Structure -** What size, how messages are organized, and what messages mean. Each 1 or a 0 is a single **bit.** A message can consist of any number of bits. The position of the bit as well as its value (0,1) is important and defined by the protocol. Messages contain **overhead**, information necessary to determine where the message came from, the type of message it is, the device address, error detection, and start/stop designation, in addition to the data that is being transferred. The amount of overhead varies by protocol and has a significant impact on the thruput of a network (i.e. a protocol that defines a 25 bit message that requires 1 start, 1 stop bit, a 5 bit address, 5 bits error detection, 1 bit for data message indication, leaves only 12 bits for data. To transfer 96 bits of data, requires 200 bits to be transmitted.).

3) **Baud Rate -** How fast data is transmitted, usually designated in bits per second (i.e. 9600 baud = 9600 bits per second or approx. 0.02 seconds to transmit 200 bits).

To make communications work for you, you have to define the sensor, the physical characteristics of the communication network, the protocol that the network will use, and write software to interpret the data once it gets where it is going. Even though the physical specification is identical, two devices may not talk because of different protocols. An analogy is a boss describing how he would like something accomplished to a group of employees ("bus" communication (topology), over air (media), using sound (signal characteristics)). If the boss speaks a different language (message structure) than the workers understand (German vs. English), no communication will take place.

Protocol typically affects throughput of a network and its connectivity.

Answers to Some Commonly Asked Questions

Why not develop one physical layer and protocol that all companies will use for communications?

Efforts have been made to standardize communications since the early 1970's. Most end user customers want that and C-H as a company supports that philosophy. The issue is however that no communication specification meets all application needs and as a result, agreement on that one protocol/physical characteristic has been illusive. Some of the selection characteristics for a network are as follows:

- # of devices supported
- Length and flexibility of data line routing
- Noise immunity
- Throughput of data vs. data requirements
- Data structure (small, medium, or large data messages)
- Electrical isolation/withstand
- Connectivity (the ability for one system or network to talk to another)
- Installed cost

Eventually, there will probably be multiple lower level networks in a plant, all doing what they do best for their application, with a gateway (a method of connecting different networks together) to other networks that need to access its information (i.e. the Modbus gateway for IMPACC).

What is an open protocol vs. a proprietary protocol?

A proprietary protocol is one in which a company elects to keep its protocol and physical characteristics secret and to maintain control of all interfaces. Open systems are a matter of degrees. On one end of the spectrum, a company may develop gateways to its system. On the other end, a protocol/physical layer is made available to everyone, hardware can be manufactured by anyone, and the protocol characteristics are such that each companies products will communicate exactly like any others. IMPACC is an open protocol in that the protocol is published, support software is given to third party companies to develop both hardware and software interfaces. The physical layer is less open, in that communication chip availability is controlled by C-H. That chip is sold to third parties, and communication card interfaces are sold, but not freely available. Device Net is open from a protocol standpoint and more open from a physical layer, in that the "chip" is sold by multiple vendors.

What are some communication standards sanctioned by independent governing bodies?

Currently, there are no standards groups that "sanction" both the physical and protocol specifications. IEEE has developed several physical layer standards - RS 232, RS 422, RS 485. Note that since the protocol has not been standardized, almost all manufacturers that have implemented one of those standards, have developed their own protocol - therefore none truly "communicate" with each other. IEC, NEMA, IEEE, ISA, etc. are all investigating standards for both physical & protocols, but are far away from sanctioning any one protocol and physical standard.

What affects throughput?

Throughput is affected by both physical and protocol characteristics. The number of devices talked to, the media/physical signal used (light travels faster than electrical impulses), the bus arbitration method (master slave/peer to peer), the amount of data each device sends back, the amount of useful data sent back (i.e. if all you want is energy, but you have to get all information, a lot more bits will be sent), and the baud rate all determine throughput. In addition, noise immunity is affected. Typically, the higher the baud rate, the lower the noise immunity for a give number of devices and distance.

What affects noise immunity?

Typically the selection of physical signaling, type of wire, and baud rate, affects noise withstand in that order. Light over fiber cable or frequency over twisted pair (FSK) are the most noise immune. Typically, the lower the baud rate, the better the noise rejection. Error detection just allows you to live with a noisy communication by rejecting the message, and asking for a new transmission (slowing down throughput).

What is the physical & protocol layers of IMPACC?

IMPACC was developed for communications in an electrical distribution system. The application is primarily monitoring, with some low to moderate speed control (shedding breakers in demand applications, etc.) The application typically is somewhat price sensitive, requires large numbers of devices to be monitored (average 300 devices), is very distributed, and is subject to extreme electromagnetic interference. IMPACC uses the INCOM physical & protocol layers (a development of the old Westinghouse R&D group). It uses a bus topology over a twisted shielded pair of wires using frequency (FSK)signaling method. This physical layer was chosen to keep installed cost low by connecting up to 1000 devices on a “bus”, allowing that cable to be run in conduit with or next to power cables with complete noise immunity, and allowing up to 10,000 feet of cable. The message structure is also extremely efficient in an effort to keep throughput high at 9600 Baud. Each data message consists only of data asked for, minimizing the number of bits required to be transmitted and maximizing throughput.