

Industrial Safety Systems

With Redundant Communications Networks

By Tony Pipitone
Manager of New Product Development
General Monitors, Inc.

Introduction

Dramatic shifts in electronics technology over the past five years have affected the design of industrial safety systems for oil/gas applications, as well as applications in other process industries. Multi-drop serial communications networks are slowly replacing the long standard 4-20mA current loop for measuring process variables.

Two purposes are served by this change: it provides more information about the process to the process control computer, and it significantly reduces installation-wiring costs. Instead of each instrument being wired directly to the control room in a plant, a multi-drop network is implemented using one network cable. While such networks may be based on different protocols and hardware specifications, they all provide the same benefits: reduced costs and better control of plant operations.

Employing serial communications for safety instruments has been slower to find acceptance. Safety instruments are installed for the protection of personnel and property, usually under state or federal regulations. It has been difficult to convince plant safety engineers to give up their hard-wired solution for so-called “unreliable” communications networks.

To allay these concerns, one method developed is to provide a dual-redundant serial communications network. A separate communications card in the DCS system is connected to each network. Another alternative is separate distributed control systems (DCS's), one connected to each network that results in complete system redundancy.

There are a number of inherent advantages to designing a dual-redundant serial communications network for industrial safety instruments. This type of network results in the ability to communicate on either communication channel separately, or with both channels simultaneously. Such versatility provides the ability to work with many different plant control system configurations.

Advances In Networking Technology

The focus of the instrumentation industry, of late, has been on the technology of networking. You cannot visit an industry related web site without seeing the word “fieldbus” displayed prominently. We use the term ‘fieldbus’ loosely to describe the many varieties of instrumentation networks that have had an enormous impact on the way plants operate. In the past, control rooms were large, crowded rooms filled with dozens of 19-inch racks and cabinets containing hundreds of input cards for each field instrument, along with massive amounts of wiring. Over the past few years such rooms have become much smaller, containing just a few cabinets of interface equipment and several personal computers.

Reducing control room complexity is not the only advantage of networked instrumentation. Employing a network now facilitates the communication of many process variables to the control room rather than the one 4-20mA process variable available in traditional systems. Such a capability allows the communication of specific fault conditions to reduce down-time, instrument calibration data for preventive maintenance, the ability to re-configure the instrument from the control room, and many more.

A key advantage resulting from networked instrumentation is the reduction of installation and maintenance costs. For example, a U.S. based oil company in Alaska commissioned a new installation in 1997. This was one of the first large-scale fieldbus installations in Alaska’s North Slope oil fields, which became a virtually unmanned facility. A small team spends one day per week at the facility performing maintenance. Some of the fieldbus-related savings were as follows:

<i>Installation Savings (Typical)</i>	
Home Run Wiring Reduction	98%
Wiring Cost Reduction	69%
Instrument and Control Room Wiring Reduction	88%
Instrumentation QA/QC Reduction	83%
Savings on Wire Tags and Terminations (Reduction from 1150 to < 200)	\$500,000
Savings on I/O Hardware	\$90,000

Now that this pilot plant has proven itself, the process will be repeated for upwards of 550 identical installations. The potential savings are enormous.

Despite all of the advantages listed here, deploying this technology continues to be a challenge. In many process control systems a failure may result in lost revenue, but the failure of a safety system to detect unsafe conditions could result in loss of life or complete loss of the plant. Neither of these is acceptable to plant safety engineers or plant operators. Of course, the solution is to make the networked safety system as reliable as the hard-wired, traditional safety system. The answer is redundancy.

Traditional Safety Systems—An Overview

The standard traditional safety system includes a field instrument, such as a combustible or toxic gas detector, mounted in an area where a gas leak or fire is likely to occur (*Figure 1*). The detectors are typically located around valves, pumps, or compressors. Each instrument is wired to a dedicated control card or a 4-20mA input in the control room (*Figure 2*) via a 3-wire shielded cable which provide power, common and 4-20mA. A 4-20mA output from the instrument provides gas concentration information (4-20mA proportional to 100% of detected gas range), and fault information ($< 4\text{mA}$). Safety engineers consider the 4-20mA wiring to be *fail-to-safe* since a broken or shorted power or 4-20mA wire will be detected as a fault in the control room.



Figure 1: Toxic Gas Detector



Figure 2: Control Room Cabinets

The detector often must be located many thousands of feet from the control room. In a large installation, such as an oil refinery, there is generally a need for several hundred thousand feet of instrument wiring in the form of *home-run wiring* (direct wiring from detector to control room). It is a costly solution in terms of the purchase cost of the wire, the installation cost, and the cost of the installed conduit or cable trays to handle the wiring. In designing such a system, the cost of control room space must also be considered. Each of the detectors must be configured manually at the detector by way of dip-switch

settings or software selectable settings. These settings include alarm trip levels, relay settings, and fault current levels.

Safety Instrument Requirements

Safety instruments requirements vary depending on the type of instrument being used. They are based on internationally recognized standards developed by organizations such as ISA, IEC, CSA, UL, FM, and others. Requirements for combustible gas detectors, as an example, can be found in standards by ISA (ISA SP12.13), CSA (C22.2 N0. 152M-1984), FM (6310, 6320) and EU (EN50054 and EN50057). Such safety standards are generally consistent from organization to organization, with a few minor exceptions. They include requirements for accuracy, repeatability, temperature variations, response time, and shock and vibration, along with many others.

One of the key safety requirements for any hazardous gas detector is response time. Aggressively responding to the release of a toxic or flammable gas quickly can mean the difference between life and death. Combustible gas detectors, for example must upon the application of a combustible concentration of gas read 50% of the applied gas concentration within 10 seconds. These types of requirements have implications for networked safety instruments that will be explained here.

While not completely defined in these standards, the basic, and most important, requirement for safety instruments is *fail-to-safe*. Operation as a fail-to-safe device implies that all failures of the instrument are detectable and occur in a manner, which: does not cause false alarm conditions and is apparent to the safety system by annunciation of a fault signal. A partial list of failures that must be detected is given here:

- Open or Short failures in the gas or flame sensing element
- Loss of Power
- Open or Shorted 4-20mA line
- Microprocessor failure / runaway
- Sensor drift outside of acceptable limits

When evaluating communication networks for safety instruments, the *fail-to-safe* requirement has different implications. *Fail-to-safe* operation must be applied to the communications network *as well as* the instrument. Detected failures must include:

- Short or open of network cable
- Transmission Data Errors
- Instrument communication failure
- Instrument failure

Moreover, a failure of the instrument should not have an adverse effect on the rest of the network. Meeting these requirements is generally achieved by isolating the instrument's communication circuitry, error-detection and correction algorithms, and the detection of time-outs by the network controller.

Redundant Communications Solution

To achieve the requirements for reliability and *fail-to-safe* as demonstrated in traditional safety systems, while adding the advantages of reduced cost and improved data availability for the plant control system, the answer is to provide redundant communications capabilities for each safety instrument.

Redundant communications capabilities are implemented by designing two independent, low-cost, multi-drop, isolated communications circuits into the instrument. Another critical consideration in the solution is the real-time interrupt-driven communications software to meet the response time requirements discussed earlier. Complete flexibility of node address for each of the communications channels allows implementation of the redundant network in two ways:

Minimally Redundant Network

With this type of system, two communication channels are given different node addresses and connected to the same network and controller (See Figure 3). Redundancy guards against failures of the communications circuitry in the instrument, but not against failures of the network cable or controller.

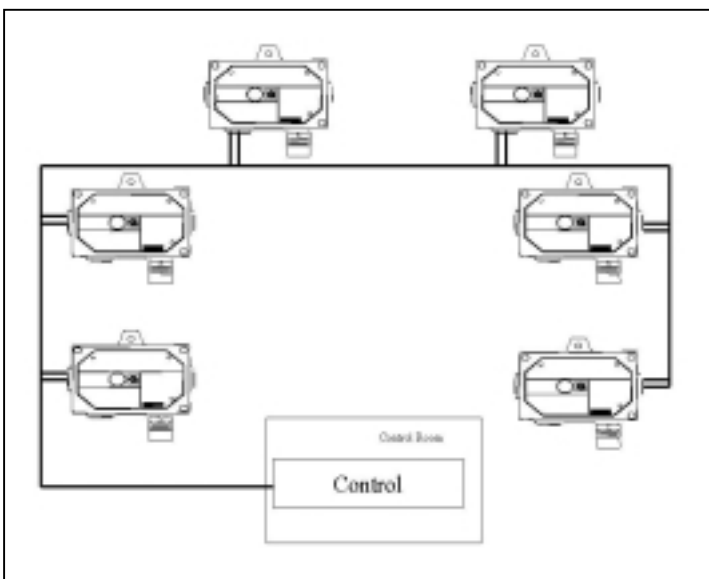


Figure 3 Minimally Redundant Network

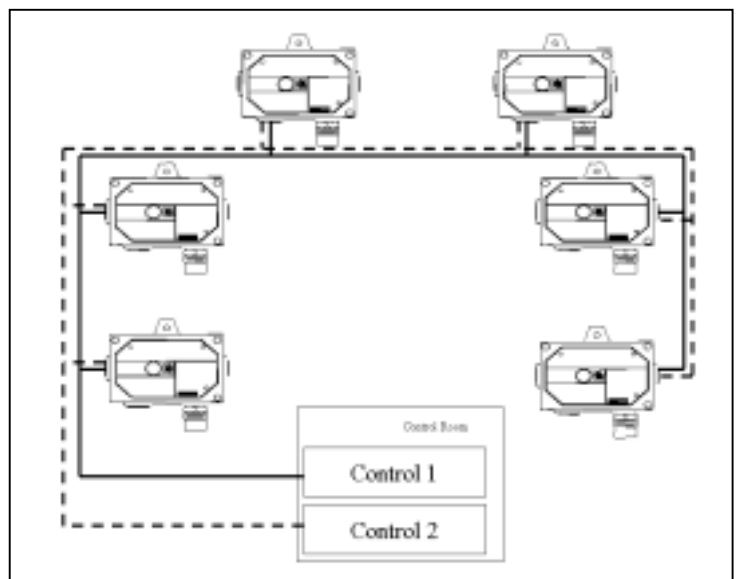


Figure 4 Fully Redundant Network

Fully Redundant Network

To design a fully redundant network, the two communications channels are given the same (or different) node address and are connected to two independent controllers in the control room (See Figure 4). The system with type of configuration is protected against a failure of the communication circuit in the instrument, a failure of the network cable, and a failure of the controller itself. Each controller will have the ability to take action to protect the plant in the case of a gas leak. A redundant communications channel can be run simultaneously with the primary channel, or can be implemented as a “hot backup”.

Choosing The Physical Layer / Protocol

Several factors were reviewed when deciding upon the physical layer hardware:

- **Isolation** – a failure of the circuitry must not bring down the network. This issue is key to meeting the *fail-to-safe* requirement
- **Industry Standard** – A physical layer accepted in the industry is required to interface to existing standard control systems
- **Noise Immunity** – The selected physical layer must be able to withstand the heavy industrial environment, including the stringent European CE Marking requirements
- **Multi-Drop Capability** – Multi-drop network configuration required for reduced wiring costs
- **Nodes per Network** – Capability to handle many nodes per network reduces the cost of control room hardware and/or repeaters
- **Cost** – the selected circuitry must be low cost, since two circuits are required per unit

Physical layer hardware chosen for this system is based on the EIA-485 (also known as RS-485) standard. Many vendors offer readily available inexpensive drivers. It is simple to isolate the circuitry using optocouplers. Most programmable logic controllers (PLC's) and DCS systems have EIA-485 driver cards available. EIA-485 drivers operate differentially and have high common-mode rejection capability. EIA-485 is designed for multi-drop capability and is able to have as many as 128 nodes on a network without repeaters.

Selection of the protocol was also based on several factors:

- **Availability of Software drivers for standard control systems**
- **No Physical Layer Restrictions**
- **Industry Acceptance**
- **Low Software Overhead**

For this system, the Modbus© protocol was selected because it met all of these requirements. Even though it is not generally regarded as one of the premier “Fieldbuses”, Modbus has a wide industry acceptance. It is a simple master/slave protocol that is well suited for small to medium complexity instruments that do not need to pass large amounts of data. A number of companies offer software drivers, such as Intellution, Wonderware, Allen Bradley, and GE Fanuc. Modicon, the developer of Modbus, does not specify the physical layer, although the two variants, Modbus-RTU and Modbus-ASCII typically use EIA-485 and EIA-232 respectively.

Shown here is an example of a Modbus register read query:

Address	Function Code	Start Address Hi	Start Address Low	#Registers Hi	#Registers Low	16-bit CRC
---------	---------------	------------------	-------------------	---------------	----------------	------------

The master sends a query, specifying the node address and function code (read registers), the starting register address, the number of registers to be read, and a 16-bit CRC of the message.

Response from the slave device is provided in the following format:

Address	Function Code	Byte Count	Data Hi	Data Low	16-bit CRC
---------	---------------	------------	---------	----------	------------

The slave repeats the address and function code, sends a count of the data bytes to be returned, the data, and a 16-bit CRC of the reply.

Using a simple protocol, such as this one, allows a fast response time due to the low software overhead in the slave device, which allows for redundant communications in even the simplest microcontroller-based systems.

Hardware

Figure 5 shows a block diagram for the complete instrument. A high performance 8-bit microcontroller is utilized to minimize communications latency. Each channel communicates with the microcontroller through a three wire serial interface operating at 1.2 Mbits/sec. A separate hardware interrupt is provided for each channel to alert the microcontroller of newly arrived messages from the Modbus Master.

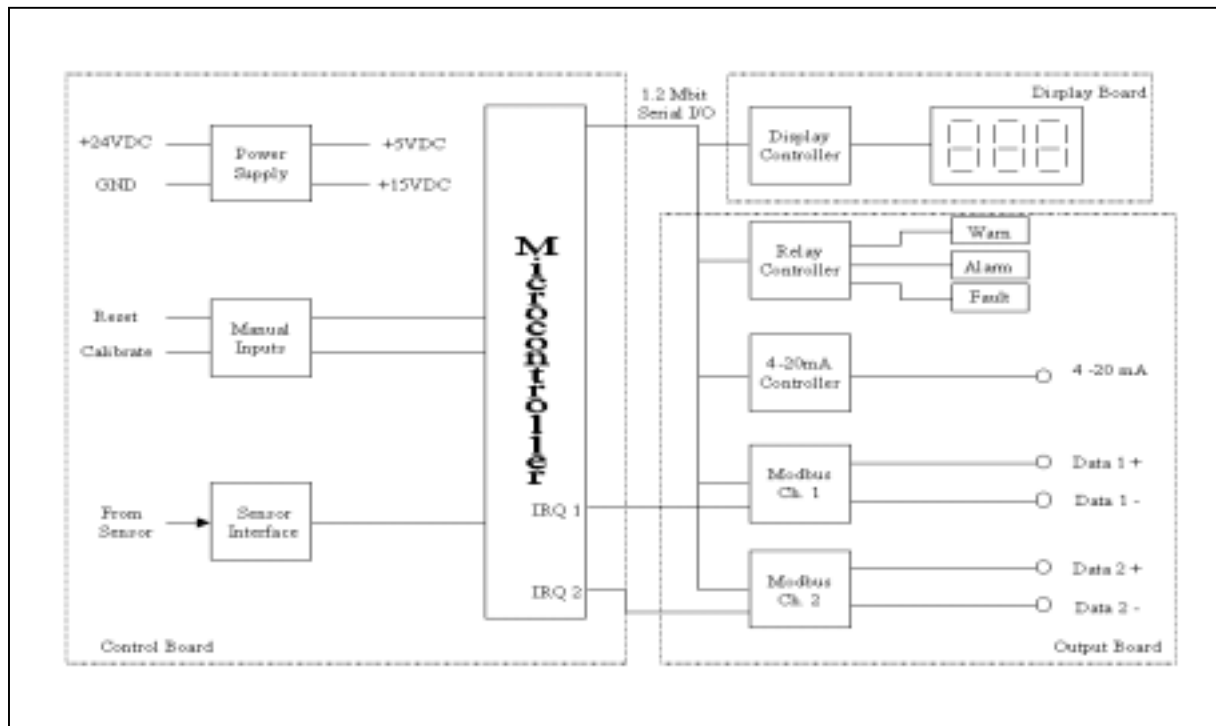


Figure 5 Instrument Block Diagram

Communications circuitry consists of a Universal Asynchronous Receiver Transmitter (UART) which has the capability of buffering a complete Modbus message in a receive FIFO. Once a complete message has been received, it alerts the microcontroller by asserting the interrupt line. The EIA-485 driver connects directly to the UART via the Tx, Rx, and RTS lines. The RTS line is used to control the direction of data flow. Capacitors and ferrite beads provide noise filtering for the communications lines. The circuitry and software will support 8-N-1, 8-N-2, 8-E-1, 8-O-1 data formats, and baud rates of 2400, 4800, 9600, 19200.

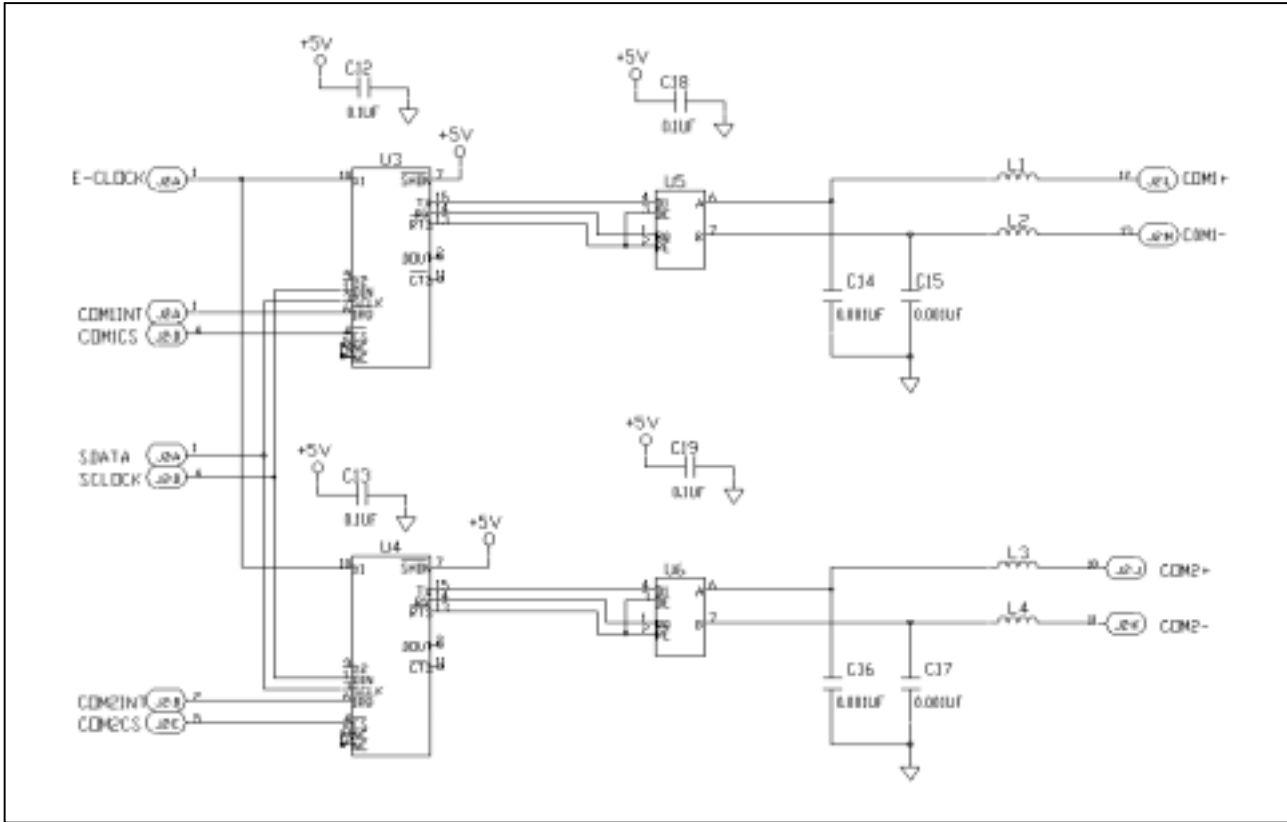


Figure 6 Communications Circuitry

Software

For ease of development, maintenance and portability, the real-time software for the instrument is written in ANSI C. Non time-critical software runs under the control of a 28mS frame timer in an infinite loop. Time critical software such as timer routines and the communications processing routines are interrupt driven. The interrupts are prioritized to provide minimum communications latency, while still allowing the timer routines to maintain their accuracy.

A Modbus communications event starts with a message placed on the bus by the Modbus master. All slave devices receive the message into their receive FIFO's. Once a complete message has been received, the UART asserts the interrupt line to the processor, signifying reception of the message. The communications routine first checks to see whether the message address matches its programmed node address. If the address does not match, the message is flushed from the FIFO. If it does match, the function code is checked to make sure it is also valid.

When the function code for a read data (Modbus Function Code 3) is detected, the starting address and number of registers is decoded. The CRC of the message is then calculated and compared against the transmitted CRC. Should they not match, an exception message is returned to the master. If the CRC is correct, the read reply message is assembled and transmitted.

If the function code is for a write command to the slave (Modbus Function Code 6), the register address and command data are decoded. The CRC is verified, and if valid, the command action is taken by the instrument. The command is then echoed back to the Modbus Master.

Modbus provides the capability to deal with illegal operations in the form of exception codes. Invalid, illegal, or unsupported requests by the Modbus master receive an exception code in the response message. Exception codes supported include illegal function code, illegal register address, illegal data value, and slave device busy. Exception code reply messages include the slave address, function code with the MSB set, the exception code, and the CRC.

Some of the Modbus commands for the instrument are provided here:

<u>Parameter</u>	<u>Function</u>	<u>Type</u>	<u>Scale</u>	<u>Access</u>	<u>Register Address</u>	<u>Master I/O Address</u>
Analog	0-20mA Current Output	Value	16-Bit	R	0000	40001
Mode	Indicates and Controls Mode	Bit		R/W	0001	40002
Status/Error	Indicates Errors	Bit		R	0002	40003
Not Used	N/A	N/A		N/A	0003	40004
Unit Type	Identifies the Unit in Decimal	Value	16-Bit	R	0004	40005
Software Rev	Indicates the Software Revision	ASCII	2-Char	R	0005	40006
Not Used						40007 - 40013
Alarm Settings	Read or change settings for the high alarm	Bit	(0-15)	R/W	000D	40014
Warn Settings	Read or change settings for the low alarm	Bit	(0-15)	R/W	000E	40015
Com1 Address	Read or change settings for the Com1 Address	Value	8-Bit	R/W	000F	40016
Com1 Baud	Read or change settings for the Com1 Baud Rate	Bit	(0-7)	R/W	0010	40017
Com1 Data Format	Read or change settings for the Com2 Data Format	Bit	(0-7)	R/W	0011	40018
Com2 Address	Read or change settings for the Com2 Address	Value	8-Bit	R/W	0012	40019
Com2 Baud	Read or change settings for the Com2 Baud Rate	Bit	(0-7)	R/W	0013	40020
Com2 Data Format	Read or change settings for the Com1 Data Format	Bit	(0-7)	R/W	0014	40021

Conclusion

A solution has been proposed, tested and is now in successful operation for providing redundant communications capabilities for safety instrumentation. The solution provides a low-cost, medium performance communications network based upon industry standard hardware and software. Integration of safety instruments into plant-wide control and information networks, along with their process control counterparts, is essential. The advantages of reduced plant wiring costs, improved instrument data to the control room, and improved maintainability cannot be ignored. Above all, plant safety cannot be compromised for any technology. The fail-to-safe nature, fast response time, and fully redundant capabilities of this proposed solution provide the safety assurances needed for installations worldwide.