Digital communications guarantee valid safety shutdowns

By Steven M. Oxenberg

Integrated digital-analog systems increase safety, provide real-time data.

For years, the inability of 4–20 mA analog-output field instruments to communicate to safety interlock devices hindered improvements in safety system performance.

But a simple solution that has been available for more than a decade—digital communications between the field instrument and the safety system—overcomes analog-input systems' limitations and maximizes transfer of information from instruments to control rooms through stand-alone use or integration with those systems.

Engineers at plants with superior safety records knew the benefits of digital communications years ago, but they couldn't use the technology because safety committees did not understand the advantages. So standards prohibited those systems until the committees finally accepted microprocessor-based smart transmitters in safety systems.

Now, global corporations whose safety records significantly exceed the industry's average have adopted digital communications in safety systems. With these new systems, which are rapidly becoming the significant mechanism for increased plant safety, engineers obtain the most economical way to provide the highest degree of safety for employees and the towns in which plants reside.

What is the 4–20 mA signal?

In analog automated process communications, the milliamp (mA) current signal varies proportionally to the process variable. The lower and upper limits of the 4–20 mA range correspond to the calibration range's lower and upper limits (0% to 100%). (See September 1999 *InTech*, pages 174–175.)

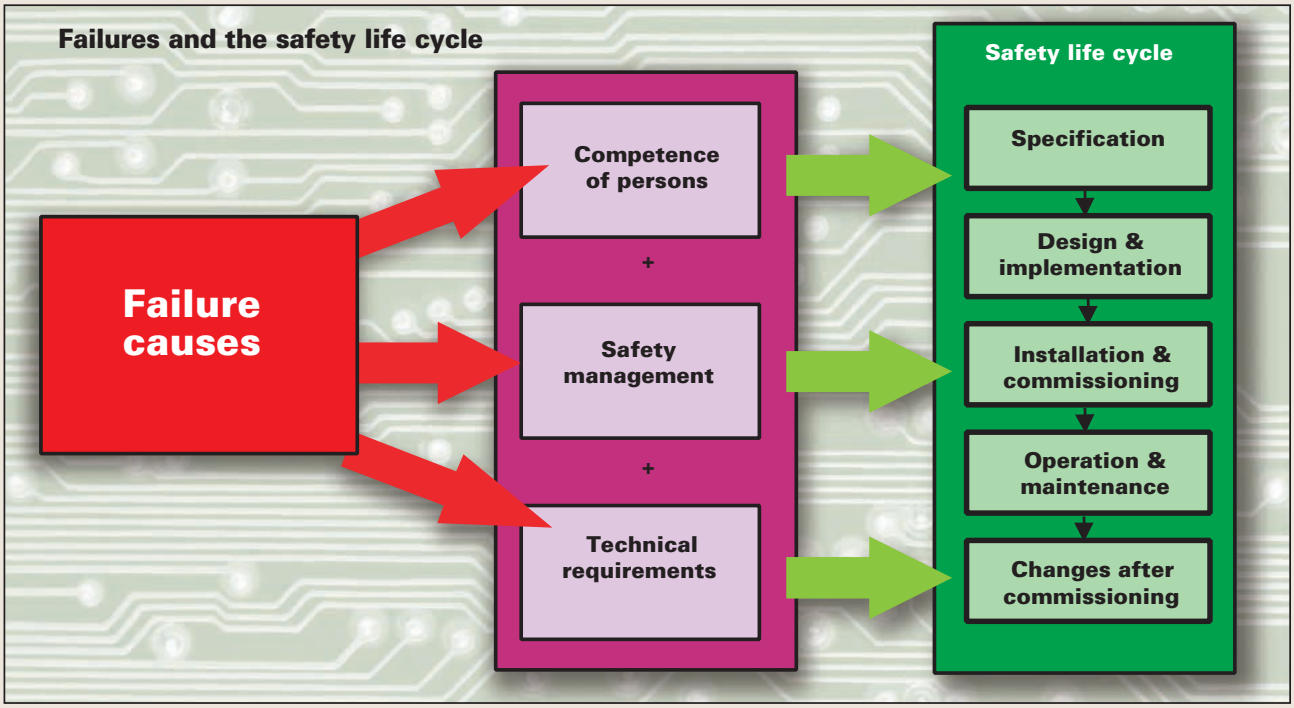
Limitations of analog signaling include limited signal range, limited transfer of information, inability to validate measurement values, required transmitter reranging, and unequal fail-safe direction probability.

Analog equals false alarms

Because of analog-input systems' inability to differentiate between process and maintenance problems, plants' false-alarm rates may be as high as 66%.

This creates problems because with no way to positively validate the analog 4–20 mA signal,

Digital solves safety life-cycle concerns



Safety concerns mentioned in ANSI/ISA-S84.01-1996 and IEC 61508 safety standards, and typically referenced in the safety life cycle, find solutions through digital communications. The life-cycle model takes a whole view of plant safety and allows a broader appreciation of how to improve the safety of the entire plant.

most safety interlocks connected to analog-output field devices activate every time the signal exceeds a preset safety threshold. Exceedances come from the process moving to an unsafe level or a field device's diagnostic indicating a maintenance problem. Sometimes the signal gathers stray noise or suffers from loose or corroded connections.

The field device trying to indicate a maintenance problem initiates the shutdown. If operators catch the situation, they can stop it. Even so, resulting side effects hamper safe and profitable plant operations. At best, false or nuisance alarms sound; at worst, the plant shuts down. Between these extremes are minor process upsets that reduce product quality and value.

Digital sounds no Klaxons

Since false alarms reduce plant safety by potentially creating situations in which personnel must enter a hazardous area to diagnose possible dangerous conditions, digital process alarm trips fast become the logical and safer choice.

Information transfer involves more than just process measurements: You must validate the transferred information. Digital communications allow an independent diagnostic status to validate those values. This ability positively differentiates process problems requiring safety action from maintenance problems requiring no safety intervention.

PV value	PV status	Action
OK	Good	Safe
	Bad	Maintenance required
Trip	Good	Process alarm trip
	Bad	Maintenance required

Source: Honeywell, Inc.

Process measurement validation differentiates problems. (Note: Analog-output transmitters would cause a trip under conditions in shaded area. PV equals process variable.)

Digital communications also provide specific, detailed, diagnostic information about the field instrument. Having this information available in the control room reduces repair time and personnel exposure to accidents. For example, "bad status" indicates repair is required. "Good status," which happens when the process measurement value exceeds a safety threshold, is positive validation that the safety interlock system needs to respond immediately. This immediate response is possible with digital signals.

Terminology

ANSI	**American National Standards Institute**
IEC	**International Electrotechnical Commission**
mA	**milliamp**
MTTF	**mean time to failure**
NAMUR	**Normen Arbeitsgemeinschaft Meb und Regeltechnik**

Typical analog vs. digital safety-shutdown response times

Transmitter output	Transmitter response time	Communication transport time	Interface module response time	Safety system delay time	Total delay time
Analog	100 ms	0	0	1 s	1.1 s
Digital	250 ms	275 ms	50 ms	0	0.575 s

Source: Honeywell, Inc.

Users can now configure safety shutdown systems to respond faster and avoid process upsets or false shutdowns. Removed are analog systems' typical damping and time delays of 1 or more seconds, used to compensate for process variable uncertainty.

Safety standards recognize frequent reranging as a leading cause of safety systems' failure to respond.

Digital requires no reranging

The limited resolution forces reranging of analog-output transmitters often for process changes, increasing the probability that errors will occur in the transmitter configuration database and setting up undetected hazardous situations.

Safety standards recognize frequent reranging as a leading cause of safety systems' failure to respond and, therefore, require well-disciplined "management of change," such as defined in the U.S. Occupational Health and Safety Administration's Rule 29, Code of Federal Regulations 1910.119.

Because analog-output transmitters require more frequent configuration changes, it becomes more important to track and document changes. Used most often are manually written or off-line communication schemes such as HART. However, neither scheme fits safety well: The manual-entry method is mistake prone, and off-line communication schemes do not guarantee that the system configuration matches that of the transmitter.

Digital devices, however, require no reranging. Unlike the fixed resolution of analog-output transmitters, digital transmitters use floating-point numbers and communicate virtually any measurement with the same resolution. Also, for an exact data match, systems automatically match digitally communicated transmitter-range information with that of the safety system.

Operators typically monitor digital communications in real time for changes by the control and/or safety system, automatically logging any activity. This tight level of data integration ensures configuration databases always match.

Status monitors' failings cause time delays

Users try status and configuration monitors to solve the limitations of analog output. Some monitors communicate using hybrid protocols, such as HART field communications, to extract information from the signal.

The status monitor validates a field instrument's 4–20 mA output signal by monitoring only transmitter diagnostic status. HART status monitors typically communicate with the field

IEC 61508 blurs real problems of poor change management and human error

The existing ANSI/ISA-S84.01-1996 safety standard is quite broad and covers many industries.

The IEC's draft standard 61508—*Functional safety of electrical/electronic/programmable electronic safety-related systems* is a work in progress and will not likely become a full standard until the year 2001. While very detailed, it does not document all available technologies. It covers overall plant safety and deals primarily with implementing devices using traditional 4–20 mA analog signaling.

IEC 61508 focuses on quantitative ways to improve field instruments by increasing the diagnostic coverage of electronic circuitry. As that can happen only by adding more electronics and software, the field device's overall mean time to failure (MTTF) actually decreases. For example, a typical smart pressure transmitter may have a 90-year MTTF. But one with added diagnostic coverage may have only an 80-year MTTF.

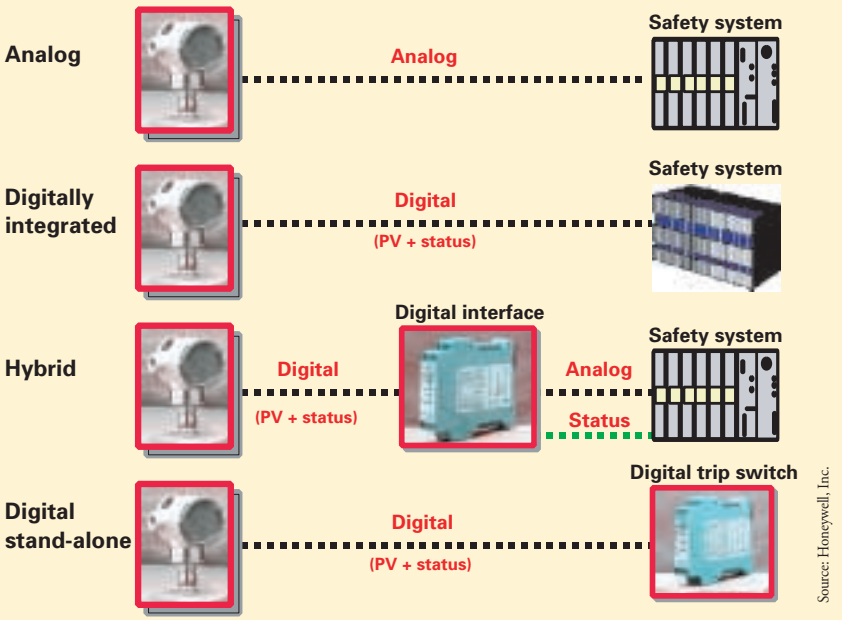
IEC 61508 reveals that a field instrument with worse reliability but better diagnostics provides a safer solution. This conclusion is regrettable because a transmitter with improved diagnostics has no improved means of communicating information to the safety interlock. The result of implementing this standard is the loss of most benefits gained through improved diagnostic coverage.

Unfortunately, the standard contains too much detail on how to quantify and measure safety of device electronics. This microscopic focus on device electronics gives readers a tunneled, misleading vision of safety because reliability analyses show electronics are the most reliable, while mechanical components are the least reliable. Also, safety studies by groups such as the U.K. Health & Safety Executive point to poor change management and human error as the leading causes of failures.

Hybrid synchronized status improves

In a one-out-of-one safety architecture, in which all systems must operate for the process to function safely, four ways exist to connect smart transmitters to safety interlocks: traditional analog, digital integration with analog, a hybrid synchronized-status solution, and digital stand-alone. Note that no HART solution is possible in safety-critical applications because there is no guarantee the diagnostic synchronizes with the analog signal.

A hybrid solution requires a digital interface module. It accepts a transmitter's digital-output signal and splits out process measurements as analog-signal components, along with the transmitter diagnostic status. In effect, the interface module extends the safety system and usually contains comprehensive internal diagnostics based on the IEC's draft standard 61508.



Note: PV = process variable

instrument at a 500-millisecond to 2-second rate. Because diagnostic status does not synchronize to the process measurement's output signal, safety interlocks must act on the analog 4–20 mA signal.

Slower to respond than the status monitor, the configuration monitor detects field-instrument configuration changes. In a multiplexed system, 1-minute to 1-hour delays are typical. But even though the configuration monitor detects changes, it does not guarantee correct initial field-instrument configuration or a match to the safety system.

Both categories respond slowly, so operators rarely connect them to safety interlocks. As a result, safety engineers often add small amounts of damping and/or time delays—often 1 second or less—to reduce the false-alarm rate. However, this technique decreases safety by delaying shutdown action if the situation is hazardous and requires a shutdown.

Digital is fail-safe

Analog-output transmitters rely on driving the 4–20 mA signal to the proper fail-safe direction to indicate diagnostic faults. But driving the analog-output within the narrow levels specified in Normen Arbeitsgemeinschaft Meb und Regeltechnik standard NE-43 may be more than a faulty transmitter can do. Additionally, sometimes the transmitter's output circuit fails and goes in the opposite direction of the fail-safe configuration.

Digitally communicating transmitters overcome these limitations and provide higher system availability. These transmitters have no directional bias, and any failure-to-communicate status allows repeatable system operation. By not requiring special safety transmitters, digital systems also keep stocking costs low and keep the full range of device options available.

Digital systems also increase plant safety and provide safer overall solutions by addressing a greater portion of the safety life cycle described in the International Electrotechnical Commission's draft standard 61508.

With digitally communicating systems, users see lower costs—if fewer digital devices are needed to meet safety levels—as well as faster shutdown speed, reduced false alarms, and the ability to use multivariable transmitters. The real value of digital systems surfaces when overall plant safety life-cycle costs drop and new safety records appear. IT

NAMUR augments ISA's analog standard

The 4–20 mA standard, ANSI/ISA-S50.1-1982 (Reaffirmed 1992)—*Compatibility of analog signals for electronic industrial process instruments*, does not address safety.

As a result, the German standards group Normen Arbeitsgemeinschaft Meb und Regeltechnik (NAMUR) issued NE-43, which addresses implementation of diagnostic safety bands into the 4–20 mA signal range.

NE-43 designates a 0.2 mA band at each end of the range to signal diagnostic problems. In practice, though, given drift and calibration errors, users often consider the NAMUR range too narrow to be useful. Thus, NE-43 is not well known and, therefore, seldom used to annunciate diagnostic information.

Behind the byline

Steven M. Oxenberg is an application consultant for Honeywell, Inc., Fort Washington, Pa. His address is steven.oxenberg@iac.honeywell.com.