WWW.CHEMICALPROCESSING.COM

CHEMICAL PROCESSING

LEADERSHIP | EXPERTISE | INNOVATION

Special Report

CONSIDER THESE SAFETY-INSTRUMENTED SYSTEM BEST PRACTICES

Start ▶

SPONSORED BY

EMERSON™
Process Management

PutmanMedia®

TABLE OF CONTENTS

AD INDEX

Consider HIPS for Reactive Processes

Such safety-instrumented systems offer advantages over pressure relief valves

By Angela E. Summers, Ph.D., P.E., president of SIS-TECH Solutions

AN UNCONTROLLED reaction can cause overpressure in a vessel and thus lead to significant safety hazards. Industry standards from the American Petroleum Institute and the American Society of Mechanical Engineers provide criteria for the design and protection of vessels from rupture and damage caused by excess pressure.

Pressure relief valves (PRVs) generally are used to meet API Recommended Practice 521 [1] and ASME Boiler and Pressure Vessel Code, Section VIII [2]. However, safety instrumented systems (SIS) called high integrity protection systems (HIPS) provide an attractive alternative in many cases. This article discusses how to assess, design and implement an HIPS.

USUAL PRACTICE

In conventional design, the primary means of protection against vessel overpressure is a PRV. It is a simple mechanical device that opens when pressure exceeds a set level. The pressure is relieved through the PRV to the atmosphere or to a contained collection system such as a flare, scrubber or thermal oxidizer.

PRVs boast relatively high integrity, as long as they are properly sized, located, inspected and maintained. Table 1 summarizes reliability data for a single-valve relief system, as published in "Guidelines for Process Equipment Reliability Data" [3]. It shows substantial uncertainty in the failure to open on demand.

Reactive chemicals and their associated processes present complex scenarios for PRV design. Small deviations in reactant concentration or reaction conditions can put the reaction on a path that the process design, control system and operator procedures cannot adequately manage. Unfortunately, many PRVs are improperly sized for reactive processes, because relief rate calculations often are based on a design and operational envelope that ignores potential reaction paths that are not well understood.

Numerous incidents, including those at Georgia Pacific (Columbus, Ohio, 1997), Morton International (Paterson, N.J., 1998), Concept Sciences (Hanover Township, Pa., 1999), Chevron Phillips Chemical Co. (Pasadena, Texas, 1999) and BP Amoco (Augusta, Ga., 2001), have proved that there are reactive scenarios under which a PRV is ineffective. They point to a number of general scenarios in which PRVs should not be considered:

- Reaction generates pressure at an uncontrollable rate (e.g., runaway reaction or decomposition) such that an impractically large vent area is required or, in the worse case, an adequately sized PRV is not possible;
- Reaction takes place in a localized area (e.g., hot spots), propagating pressure at a rate so fast that containment is lost before PRV is able to act;
- Reaction occurs in a localized area, raising

temperature above thermal decomposition point and causing an internal detonation or fire;
- Reaction produces, during normal operation, materials that partially or completely block PRVs; and
- Polymerization reaction continues as material is being relieved through PRV into lateral headers, plugging the relief device or lateral header.

Thus, the very nature of the reactive process often makes a PRV impractical. For such cases, HIPS should be investigated as a means to supplement the PRV for overpressure protection.

HAZARD ANALYSIS

Successful implementation must be based on a hazard analysis of each potential overpressure scenario. The analysis should follow a structured systematic approach, using a multidisciplinary team. It should document the event propagation from the initiating cause to the final consequence (also referred to as the "overpressure scenario"). The analysis must examine operating and upset conditions that result in overpressure. It must include a thorough review of each step involved in startup and shutdown, in addition to normal operation. For batch and semi-batch processes, scrutinize each step of the operation using typical deviations and batch-oriented deviations, such as skipped steps, steps out of sequence, steps incomplete, steps at wrong time, recipe incorrect, etc.

The analysis should include a detailed examination of reactive scenarios and brainstorming on potential reaction paths that could lead to high pressure. Examine all reaction paths, including those that may require multiple errors or failures to begin propagating. Once the reaction paths are understood, HIPS can be designed to address each reaction scenario. In many cases, only one or two HIPS are required for mitigation of all potential reaction scenarios.

PRV FAILURE TO OPEN ON DEMAND

PRV TYPE	FAILURE TO OPEN ON DEMAND		
	Lower	Mean	Upper
Spring Operated	7.90E-06	2.12E-04	7.98E-04
Pilot Operated	9.32E-06	4.15E-03	1.82E-02

DETAILING CRITICAL CONDITIONS

A safety requirement specification (SRS) describes how and under what conditions the HIPS will mitigate each overpressure scenario; it includes a functional logic description with trip set points and device fail-safe state. Choosing when and under what conditions to trip the unit is probably the most difficult decision to make in the design of the HIPS. For reactive processes, the design is often complicated by the process dynamics and by intricate process variable interactions.

HIPS design may use single process variables when the reaction path is relatively easy to detect. For example, on high temperature the HIPS will stop the catalyst feed or, on high pressure it will inject reaction kill solution. Single process variables also can prevent the start-up of the reactor under unsafe operational

conditions. For example, the catalyst cannot be added until a fixed volume of solvent, which serves as a heat sink, is in the reactor.

Multiple process variables are used when the reaction path is more complex. These HIPS often use flow/mass ratios, temperature/pressure relationships and kinetic calculations. While it is best to try to keep the HIPS as simple as possible, if the reaction paths are intricate, the HIPS complexity will escalate.

When using reactor kill systems, it may be possible to use preemptive interlocks to prevent the reaction from progressing to the point where it must be killed. These interlocks may close reactor feeds, open a pressure control vent or close catalyst valves. If the temperature or pressure continues to increase after the preemptive interlock, a reactor kill is initiated. By using a preemptive interlock, the plant is able to recover more quickly from the process upset and suffer less production loss and downtime.

The potential rate of pressure escalation must be compared to the HIPS response time to ensure that it is fast enough to prevent vessel overpressure. The HIPS response time must be evaluated by considering the time it takes to sense that there is an unacceptable process condition; the scan rate and data processing time of the logic solver; and closure speed of the final element. The valve specification must include the acceptable leakage rate, because this affects potential downstream pressure and relief loading. The valve actuator must provide sufficient driving force to close the final element under the worst-case upset pressure condition.

The SRS also includes documentation of the safety integrity requirements, including the Safety Integrity Level (SIL) and anticipated testing interval. At a minimum, the integrity of the HIPS should equal that of a PRV. The data in Table 1 implies that the HIPS should be designed to meet either SIL-2 or SIL-3, depending upon the type of PRV. However, bear in mind that the failure modes of a PRV and the HIPS differ. A PRV that fails to operate at the set pressure nevertheless may operate at a higher pressure, whereas HIPS is more likely to fail completely. The failure-to-open-on-demand uncertainty, coupled with the difference in the failure modes, results in the majority of users setting an SIL-3 target for the HIPS.

REFERENCES:

1. "Guide for Pressure Relievin and Depressuring Systems," Recommended Practice 521, American Petroleum Institute, Washington, D.C. (1997).
2. "Boiler and Pressure Vessel Code, section VIII–Pressure Vessels," American Society of Mechanical Engineers, New York, N.Y. (1999).
3. "Guidelines for Process Equipment Reliability Data," Center for Chemical Process Safety, American Institute of Chemical Engineers, New Yor, N.Y. (1989).
4. "Functional Safety Electrical/Electronic/Programmable Electronic Safety Related Systems," Document IEC 61508, International Elecrotechnical Commission, Geneva, Switzerland(1998).
5. Summers, A.E., "High Integrity Pressure Protective Systems" in "Instrument Engineers' Handbook", 3rd ed., CRC Press, Boca Raton, Fla. (2002).
6. Summers, A.E., "Using Instrumented Systems For Overpressure Protection," Chem. Eng. Prog., 95, p. 85 (Nov. 1999).

INTEGRITY AND ARCHITECTURE

It is important to recognize that the HIPS consists of the entire instrument loop from the field sensor through the logic solver to the final elements, along with support systems required for successful HIPS functioning, such as power, air or gas supplies.

Process sensors. The process variables commonly measured in HIPS are pressure, temperature and flow. Most HIPS applications require one-out-of-two (1oo2) or 2oo3 voting transmitters for all field inputs. Redundant inputs enable the incorporation of input diagnostics, significantly increasing the integrity of the field inputs. Separate process connections also are required to decrease common cause faults such as plugged process taps.

Logic solver. This hardware must meet the required SIL, which often means that it must comply with SIL-3 performance requirements, as provided in IEC 61508 [4]. The logic solver can be relays, solid state or programmable electronic systems (PES). If a PES is used, it must provide a high level of self-diagnostics and fault tolerance. Redundancy of signal paths and logic processing is necessary, and the trip output function must be configured as de-energize to trip.

Final elements. HIPS must use a minimum of dual final elements in a 1oo2 configuration. The final elements typically are either: relays in the motor control circuit for shutdown of motor-operated valves, compressors or pumps; or fail-safe valves opened or closed using solenoids in the instrument air supply. When valves are used, both valves must be dedicated block valves.

Solenoid operated valves (solenoids), configured as de-energize to trip, are used to actuate the block valves. The solenoid(s) should be mounted as close to the valve actuator as possible, to decrease the required transfer volume for valve actuation. Finally, the exhaust ports should be as large as possible to increase the speed of the valve response.

The HIPS must provide an installation that is as safe or safer than the PRV it replaces. To document that this has been achieved, the complete design and operation of the HIPS should be quantitatively verified to ensure it meets the required integrity. HIPS typically are SIL-3 SIS and are often the only layer of protection against the overpressure event. Consequently, many users require an independent third-party evaluation of the appropriateness of the design and the determination of the SIL.

AN ATTRACTIVE ALTERNATIVE

HIPS can be used to safely mitigate potential reactive overpressure scenarios. As with any instrumented system, good design depends upon good specification. For HIPS, the origin of the design is the process hazard analysis, which must identify all overpressure scenarios. Then, the HIPS is designed to handle these scenarios. HIPS is often the "last line of defense;" so, its failure during a reactive scenario will result in loss of containment. Consequently, ensuring the integrity of the HIPS through proper field design, device testing and maintenance is mandatory for safe operation.

ANGELA E. SUMMERS, Ph.D., P.E., is president of SIS-TECH Solutions, Houston, Texas, a consulting and engineering firm specializing in safety instrumented systems.

Acknowledgment: This paper is based on a presentation made at the 6th Annual Symposium of the Mary Kay O'Connor Process Safety Center, College Station, Texas, Oct. 28-29, 2003.

Get the Most Out of Your HART SIS

Several HART parameters and best practices ensure its capabilities are fully realized

By Alan Harris, Emerson Process Management

HART DIAGNOSTICS in safety instrumented system (SIS) field devices have been used for many years by several different SIS vendors. HART diagnostics provide much more information on the health of a field device than can be determined from a standard 4–20 mA signal. For this reason, greater safety integrated level (SIL) (by turning Dangerous Undetected failures into Dangerous Detected failures) and longer proof testing intervals can be achieved by integrating HART diagnostics from intelligent field devices into the SIS.

Most SIS vendors don't have the capability to use the HART diagnostics in the SIS logic. Instead, their systems simply use HART multiplexers to strip off the HART signal, usually on a field termination assembly (FTA), and then send the HART signal to a separate asset management system (AMS) platform to alert the maintenance group of unhealthy devices. These systems don't have the capability of using the HART diagnostics directly in the SIS logic. Nor do these systems have the capability of efficiently generating operator graphics, alarms, or historization of the device diagnostics.

The DeltaV SIS, however, has the capability to either pass on the diagnostics to an AMS or the basic process control system (BPCS) or to use the diagnostics in the SIS logic. This capability has many added benefits over traditional SIS:

- The SIS can use the HART diagnostics to determine if a field device is unhealthy. If the device is unhealthy, the SIS can take action to remove the device from voting or trip the system if required.
- The HART diagnostics can be displayed on detailed operator faceplates or displays to efficiently alert the operator and the maintenance group of unhealthy devices.
- Historization of HART alarms can be recorded with the same tool as the BPCS and SIS alarms.
- The alarm banner on the operator graphics can show HART alarms, which will quickly alert the operator of critical devices that are unhealthy and require greater monitoring from the operator.
- Different HART signals can be used to monitor and alarm various conditions in the field without the requirement to run separate wiring for these signals — resulting in significant cost savings.

Several HART parameters and best practices used in the application of HART in the DeltaV SIS ensure its capabilities are fully realized. In this article, Rosemount and Fisher device capabilities are used to describe the HART protocols. Other vendors may use slightly different configuration/functionality for their HART devices.

BUILT-IN HART DEVICE STATUS SIGNALS

The DeltaV SIS automatically reads various HART status signals from transmitters and the DVC6000 series positioner. The system also can determine device health based on these parameters. These parameters can be configured to assign a faulty status to the device and perform the following:

Degrade transmitter voting. If a transmitter is determined to be bad via these built-in HART status signals, the SIS can either remove the transmitter from the voting logic (i.e. a 2oo3 voted group of transmitters degrades to 1oo2 or 2oo2 with the bad transmitter viewed as faulty) or the transmitter can be alarmed simply via operator graphics.

Trip a valve. While unlikely to be used due to availability concerns, the built-in HART device status signals can be used to trip valves that use a HART-enabled positioner or alarm the valve via operator graphics.

The following built-in HART device status signals (shown below) are used:

- PV out of limits
- Analog-digital mismatch
- PV output saturated
- PV output fixed
- Loss of digital communications
- Field device malfunction.

It is up to the end user to determine if these status signals should be used for transmitter voting degradation or tripping of valves.

Configuration of these built-in HART status signals that affect transmitter or valve status within the DeltaV SIS logic can be performed via the DeltaV Explorer. After creating a HART-enabled channel in a CSLS (CHARM Smart Logic Solver) HART-enabled analog input or DVC output CHARM, drill down into the channel and double click on the HART_ERRORS parameter. By default, the CSLS will ignore all of the built-in status signals (Figure 1).

PV out of limits. The HART instrument is reporting that the primary variable read by the transmitter is outside of the 4–20 mA range. This signal can be used to detect open/short circuits in the transmitter wiring.

Analog-digital mismatch. The HART instrument is reporting a difference between the analog 4–20 mA signal and the digital process variable (PV) signal. This functionality can be used to determine a small ground in the home run cable to the instrument or an intermittent device. If a ground loop exists in the loop, the trip limit of the device may never be reached even under trip conditions due to earth leakage. This diagnostic should detect the difference and the SIS can perform the required action (trip or alarm), as shown in Figure 2.

PV output saturated. The analog and digital signals for the PV are beyond their limits and no longer represent the true applied process. If the process variable goes outside of the 4–20 mA range, the HART transmitter will drive the mA output and the PV to the saturation values, but no further. The transmitter will clamp the analog output and PV to the saturation values (not the 4 and 20 mA values). PV's between the 4–20 mA limits

CONFIGURATION

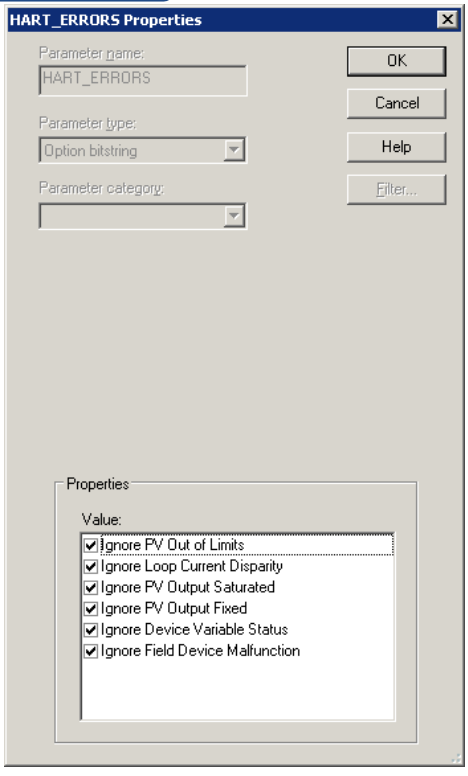

Figure 1. Users can configure what specific device condition affect transmitter or valve status within the DeltaV SIS logic.

GROUND LOOP

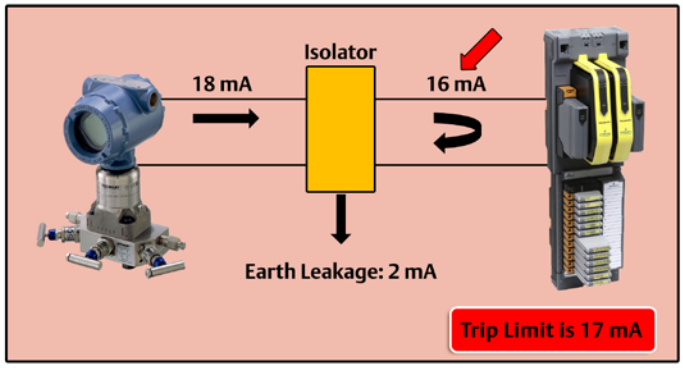

Figure 2. If a ground loop exists in the loop, the trip limit may never be reached.

and the saturation limits may still be valid signals.

Figure 3 shows a Rosemount 3051S pressure transmitter user manual. The low and high saturation (3.9 mA and 20.8 mA respectively in the Alarm Level) are the saturation setpoints. The 3.75 mA and 21.75 mA values are the transmitter failure setpoints.

It should be noted that this is a digital HART alarm that is separate from the open/short circuit detection performed by monitoring the 4–20 mA analog signal in the CSLS. Usually, SIS transmitters are configured in the CSLS to detect faulty transmitters (open/short circuit) by monitoring the 4–20 mA analog signal and removing a transmitter from a voting configuration when that analog signal is outside of a specified range. It is good engineering practice to set the faulty transmitter ranges for the 4–20 mA analog value in the CSLS equal to the failure alarm setpoints from the HART device. If the transmitter detects an error, it will send the PV to the failure alarm setpoint. Values within the low/high saturation areas are still valid values according to the transmitter. If faulty transmitter setpoints using the 4–20 mA signal in the CSLS are set within the saturation range, spurious trips of the process may occur even though the transmitter may not be faulty.

PV output fixed. The analog and digital signals for the PV are held at the requested value. They will not respond to the applied process. The output is fixed when a transmitter has been taken out of service during calibration or maintenance (changing a range, for example). Unless the transmitter has been put back in service, the outputs will continue to be fixed indefinitely.

Loss of digital communications. This status bit is set when the HART digital communications with the device is lost. The 4–20 mA analog signal may still be valid, but the digital HART signal is not available.

Field device malfunction. The device has detected a hardware error or failure on the device. This pertains to a variety of errors that can occur. Malfunctions in the memory, A/D converters, CPU, etc. are covered under this status bit.

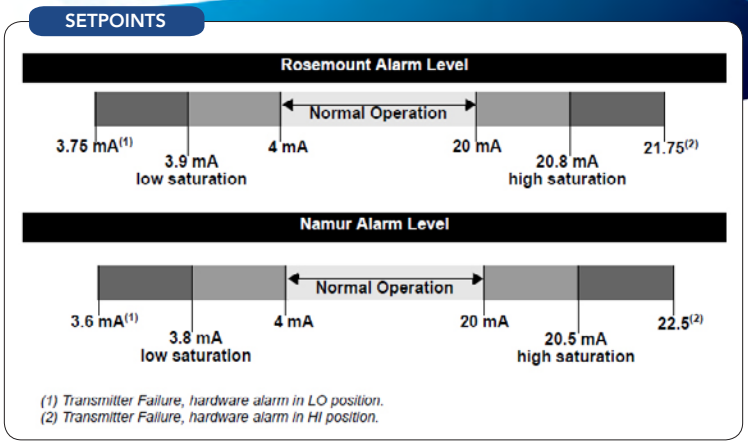

Figure 3. A Rosemount 3051S pressure transmitter user manual shows the low and high saturation are the saturation setpoints.

ADDITIONAL HART PARAMETERS

In addition to the built-in HART status bits, several other HART variables can be used. These HART variables are dependent on the type of device. While the status signals can be used directly in the SIS logic, these additional HART parameters pass through the SIS to the BPCS and AMS. If these parameters are to be used in SIS logic, they must first be programmed in the BPCS as a parameter reference and then sent down to the SIS logic.

It should be noted that HART is not a safety-rated platform. You should never substitute HART signals for hardwired signals when the hardwired signal is being used to detect a hazardous condition with a SIL rating. For example, valve position is a HART parameter in the DVC6000 series positioner. If valve position is being used to detect a hazardous condition with a SIL rating, the valve position must be read using limit switches or position transmitters. However, if valve position is a diagnostic used to determine the status and health of the valve, then the HART parameter can be used. HART should only be used for diagnostic purposes.

FIELD DEVICES

Most Rosemount devices use the HART_PV, HART_SV, HART_TV, and HART_FV variables to send configurable device information to the DeltaV and DeltaV SIS.

WATCH THE VIDEO

Check out this overview of the modern DeltaV SIS that continually monitors the entire safety loop, providing information on device health to prevent spurious trips along with alerts for preventive maintenance.
www.youtube.com/watch?v=Y97M2ZoVNGI

FISHER DVC6000 SERIES POSITIONER

This device sends four configurable slot variables in addition to the HART variables (which are not configurable in the DVC6000 series positioner). The available HART variables are:

- HART_PV – Loop Current, mA or %
- HART_SV - Auxiliary Contact Status, 0 or 100%
- HART_TV - Output Pressure, psi, bar, or kPa
- HART_FV - Travel, %.

Initiating a **partial stroke test** (PST) and the success of the PST are HART parameters used in the DVC6000 series positioner. The PST can be initiated in the DeltaV SIS, AMS, an operator graphic, or via a HART handheld device. The test is run in the DVC6000 series positioner and the success/failure of the test is sent back to the SIS or AMS to be shown on operator graphics or for historization. It is good engineering practice to include the requirement for a successful PST during any commissioning process for a valve with a DVC6000 series positioner. Both the max travel movement and the travel speed of the PST are configurable.

Automatic test interval. The DeltaV SIS and the DVC6000 series positioner can be used to automatically start PSTs at required intervals. An alarm can be created to alert the operator that a PST is about to occur. In addition, the last successful PST time can be displayed on operator graphics, as well as the time until the next PST is due.

Valve position is a HART signal present in the DVC6000 series positioner. Valve position can be read in the BPCS and SIS via the HART_FV parameter from the device. Valve command disagree alarming can then be performed in the BPCS or SIS based on the HART command, rather than having the requirement of using hardwired methods to perform this alarming via limit switches or position transmitters.

Air supply pressure can be configured in the DeltaV SIS as a slot code variable (code # 8) that can be read in the DeltaV. The pressure value can be used to detect low and high air supply pressure and possible plugging of the air supply line via water, oil, or particulate matter.

Valve friction and subsequent wear on the valve can be detected by monitoring the valve signature when a PST has occurred. A valve signature can be taken when a valve is put into service. When a PST is performed at a later time, the valve signature can again be taken and compared with the initial PST valve signature. Valve friction can be detected by looking for erratic movements of the valve on the valve signature compared with the initial signature.

SAFETY CERTIFIED ROSEMOUNT 3051S PRESSURE TRANSMITTER

One of the HART diagnostics for the Safety Certified Rosemount 3051S Pressure Transmitter is **impulse line plugging**. The 3051S determines a plugged impulse line by monitoring the normal deviations in pressure. Under normal conditions, slight deviations or noise in the pressure will be present on a millisecond scale. As flow decreases or plugging occurs in the impulse line, these deviations will decrease to a minimum value. Care should be taken when using this diagnostic to ensure that that plugged impulse line alarms are masked or transmitter failure actions are cancelled when there is no flow in the process (such as when the unit is shutdown or when minimum flow conditions exist). Additional logic in the SIS may be required to mask this alarm during no or low flow conditions.

Damping is a configurable value in HART transmitters that introduces a delay in the output of a transmitter. This parameter is used to smooth variations in output readings when sharp, rapid changes to the process input occurs. The factory default value is 3.2 seconds. Care should be taken when using this variable in SIS loops. SIS applications sometimes have a delay timer in logic (usually around 500 msec to 1 sec) to avoid spurious trips when short spikes occur with the process variable. The SIS should be engineered to ensure that the damping in the transmitter coupled with the delay timer in the SIS logic does not exceed Process Safety Time requirements for the Safety Instrumented Function (SIF).

Terminal Temperature is a measure of the temperature on the transmitter. It is not a measure of the process temperature. The sensor temperature can be read in the system via a HART parameter (default is the HART_SV parameter) and can be used as a check to determine that heat tracing is functioning properly. This parameter could also be used as an aid to determine if impulse lines have plugged in processes where plugging occurs when heat tracing has failed.

SAFETY CERTIFIED ROSEMOUNT 3144P TEMPERATURE TRANSMITTER

This temperature transmitter has **thermocouple redundant** sensors that can reduce the number of spurious trips that occur due to the fact that the secondary sensor can supply the temperature measurement if the primary fails. There are several different variations of the 3144P that can be ordered. SIS applications will generally use the U2 (Average Temperature with Hot Backup and Sensor Drift Alert — Warning Mode) or U3 (Average Temperature with Hot Backup and Sensor Drift Alert — Alert Mode).

A **sensor drift alert** provides one of the best methods of detecting sensor drift and subsequent failure via deviation alarming. This capability is a built-in, configurable feature in the 3144P. If deviation alarming is used in the transmitter as a HART alarm or in the SIS as a programmed alarm in logic, this credit should be used in the SIL calculations.

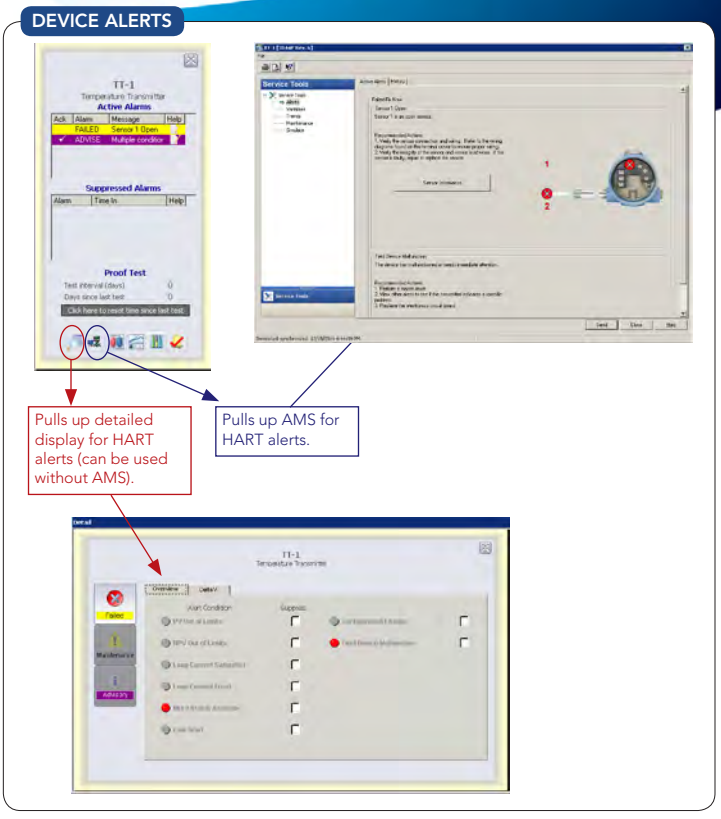

Figure 4. Alerts can be monitored either from an AMS or in operator graphics.

See the **damping** description for the 3051S. The default damping in the 3144P is 5 seconds.

See **terminal temperature** description for the 3051S.

Different **sensor types**, such as a RTD and a thermocouple, can be used when the dual sensor configuration is chosen.

This can reduce the amount of common cause in the sensor and should be reflected in the SIL calculations.

MICRO MOTION CORIOLIS MVD TRANSMITTERS

The **Micro Motion Coriolis MVD Single Variable Flow Transmitter Model 1700** features a **Mass or volume total** that can be used, particularly in tank farms, pipelines, and terminal management applications, when the total amount of material that has passed through the transmitter in a period of time is requested.

The **Micro Motion Coriolis MVD Multivariable Flow and Density Transmitter Model 2700**

includes a **Temperature** setting that can be used for deviation alarming with other temperature transmitters nearby in the process to detect faulty temperature transmitters if the deviation becomes too large.

Density can be used for detection of dual phase liquids or for the detection of foreign material that may not be desired in the process flow. Density can be used to check the quality of the process material or to detect plugging in the flow tube.

Coriolis meters detect flow by measuring the vibration frequency of the piping in which the process flows. By monitoring for low **tube frequency** a plugged flow line can possibly be detected. In addition, an unusually high tube frequency can indicate sensor erosion.

Excessive **drive gain** can be the result of excessive slug flow (liquid in a gas flow or gas in a liquid flow). Slug flow can be caused by cavitation or flashing of liquids. By monitoring the drive gain, slug flow can be detected. In addition, erratic drive gain can be the result of foreign material caught in the flow tubes.

External pressure and temperature may indicate the need for pressure/temperature compensation that should be performed.

See the **damping** description for the 3051S.

DEVICE ALERTS

Device alerts can be applied to all HART devices in the DeltaV SIS. These alerts can be monitored either from an AMS or in operator graphics (Figure 4). User manuals and other white papers exist that describe these alerts in detail. Therefore, only a brief description of these alerts will be given here.

These alerts can be pulled up by an operator or a maintenance group from the operator graphics. Access to these alerts is from the faceplate for an instrument on an operator graphic. The DeltaV SIS is the only SIS on the market that allows these device alerts to be seamlessly and efficiently displayed to operators and maintenance technicians. Other vendors either require the use of HART multiplexers, an AMS, and a connection between the AMS and the BPCS in order to see the HART alerts on an operator graphic. The system also can historize these alarms in the same SOE recorder or historian as other SIS alarms. This creates one repository for SIS alarms, rather than several different databases between the AMS and the BPCS.

In addition, device alerts are configurable to allow different alarm priorities to exist for different alerts. Configuration is performed by selecting the properties for a HART device from Explorer. From there, the alarms can be enabled and the priorities configured (Figure 5).

OTHER BEST PRACTICES

In addition to the best practices outlined, the following items should be addressed when using HART devices.

- Currently, HART 5 can only use eight characters in the tag name for the device. The DeltaV/DeltaV SIS can read HART 5 or 7 devices, and currently Rosemount transmitters are generally HART 5 or 7 devices. This

SIS INTEGRATION

Learn how DeltaV SIS with Electronic Marshalling addresses common challenges associated with third-party DCS or PLC integration when offered as a standalone SIS solution. In addition, Jimmy Miller, DeltaV SIS business development manager, discusses the value of having a highly integrated Control and Safety System (ICSS).
www.youtube.com/watch?v=zHEwhh2NQgQ

requirement should be taken into account when assigning tag name standards in the SIS and the BPCS.

- Many Rosemount and Fisher user manuals supply diagnostic tests to be used during proof test intervals, including the diagnostic coverage factor. The diagnostic coverage factor should be used in SIL calculations to provide an accurate representation of the percentage of dangerous undetected faults discovered from the diagnostic routine.
- Loss of HART communications will not trip a DVC6000 series positioner. If HART communications to the DVC6000 series positioner is lost but the 4-20 mA signal is still active, the DVC6000 series positioner will still continue to operate the valve. In addition, if HART errors are not ignored (for example, you have chosen to trip the valve if PV output is fixed) the valve will continue to operate if HART communications are lost. This function can be tested by connecting a DVC6000 series positioner to the SIS logic solver and placing a 10 µF capacitor across the + and – terminals. The capacitor will cause HART communications to be lost but will allow the 4–20 mA signal to reach the DVC6000 series positioner. The DVC will still continue to operate and keep the valve in the operating position even though HART communications are lost.
- Device alerts for HART devices are only activated when they are enabled via the checkbox in the channel properties dialog box.

During FAT, it may be beneficial to disable the device alerts so that fewer alarms will be shown during testing when the actual device is not connected to the DeltaV SIS. Device alerts for HART devices do not require the physical presence of the device in order to be programmed.

ALAN HARRIS is Solutions Consultant for Emerson Process Management. He can be reached at Alan.Harris@Emerson.com.

ADDITIONAL WHITE PAPERS

These white papers also discuss the use of HART in Emerson systems and may be of value:

1. "Using HART to Increase Field Device Reliability". Adler, Bud. ISA. 2001.
2. "Configuring PlantWeb Alerts in a DeltaV System". Emerson White Paper. March 2009.
3. "DeltaV HART Capabilities". Emerson White Paper. March 2009

ALARM CONFIGURATIONS

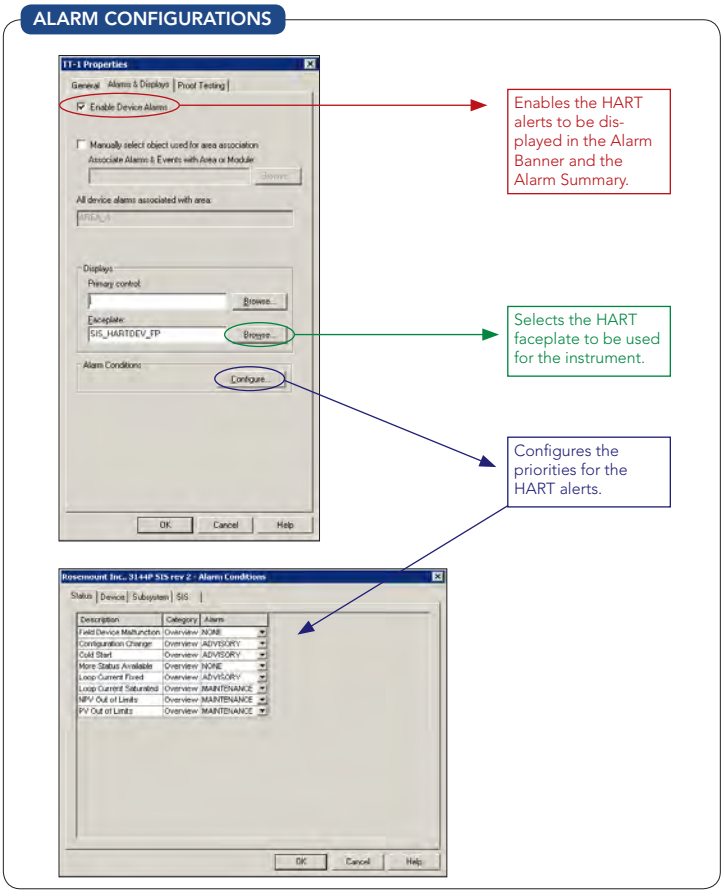

Figure 5. Various alarm priorities can be set for different alerts.

Perform Proof Tests with Confidence

Modern method improves efficiency, reduces errors, and meets compliance requirements

By Sergio Diaz, Emerson Process Management

PROOF TESTS assure the effective operation of safety instrumented systems at the designed safety integrity level. Proof tests on traditional safety systems require a considerable amount of effort, can add risks, and can be prone to errors. Often, proof tests are done with multiple technicians in the field and one technician in the control room verifying safety system reaction. However, when a team uses a modern safety system with smart devices, the proof testing process is much safer and more efficient.

This white paper shows a proof testing approach that minimizes the field runaround as well as the potential for inadvertent alteration of safety system operation.

PROOF TEST DEFINITION AND REQUIREMENTS

As defined by IEC61508 standard (part 4 – Definitions and Abbreviations), a proof test is a periodic test performed to detect dangerous hidden failures in a safety-related system.

For example if a valve in the field is stuck open, the proof test must reveal that condition so the valve can be corrected before it is demanded to act in the safety system process. If that valve were to fail when demanded, the safety system would not protect lives and property.

The effectiveness of the proof test depends on failure coverage and repair effectiveness. If a repair is required, it should restore the safety system to an "as new" condition or as close as practical to this condition. When a repair is made, proof testing should prove the integrity and safe operation of an SIS (safety instrumented system) so that the safety system will operate as required when demanded.

Frequency of testing varies across industries and facilities, based on the required safety integrity level and the safety system's undetected dangerous fail rate. Sometimes testing is performed annually, but in some cases testing intervals are longer.

Testing frequency directly impacts regulatory compliance and safety calculations, such as Safety Integrity Level (SIL).

SIL RELATED TO PROOF TESTING

SIL is an indication of the risk reduction provided by the safety system and is calculated based on the failure rates of various safety system components and other information, such as repair rates. SIL can be calculated according to an equation, a fault tree, or Markov model.

One of the variables involved in SIL calculations is the testing interval (TI) or proof testing interval — the interval between manual functional tests of components.

If a Safety Instrumented Function (SIF) does not meet its SIL-designed requirements, test intervals can be modified to a reasonable interval, and then the Safety Integrity Level of the SIF recalculated.

Obtaining a high-quality proof test performed at regular intervals is critical in meeting SIL and regulatory requirements.

BEST PRACTICES IN THE PROOF TESTING PROCESS

A proof test should assess the complete safety loops within the safety system — including the logic solver, and the process measurement and the actuating devices. The ideal proof test involves executing "end-to-end" testing.

As indicated in "Proof Testing of Process Plant Safety Instrument Systems" white paper, (see reference) it might not be necessary to prove the operation of a final element for each independent initiator. Once the

final element has been proven in the required proof test interval, all that is required is to prove each initiator.

If "end-to-end" testing is not possible, then each individual component could be tested at different times. These important items must be considered:

- An SIS proof test must reflect actual operating conditions as closely as possible.
- Any SIS overrides must be subject to strict controls to ensure their safe application and timely removal.

Records remain key in the testing process. All proof tests should indicate who performed the test and the results of the tests.

As needed, proof test procedures should include a record of physical inspection to identify any significant degradation of the installation.

STREAMLINED PROOF TESTING TOOLS

Proof testing must be extensive and comprehensive. It also must be done at the specified intervals stated during SIL determination.

Devices and systems across the process are involved. Emerson safety system components, devices, and applications strive to make the task efficient, while never moving the focus away from safety.

INHERENTLY EFFICIENT PROOF TESTING

Following are some of the embedded tools in DeltaV SIS that reduce the time and effort required for testing different components.

Logic Solvers. DeltaV SIS Logic Solvers (LS) should be proof tested according to the specified proof test interval to ensure there are no dangerous faults present that are not being detected by continuous runtime diagnostics.

- A proof test causes an LS card to run its power-up test while the partner card is active. DeltaV SIS offers two types of proof tests:

  Manual: The user initiates a manual proof test of the logic solver from the DeltaV SIS Diagnostics application.

  Automatic: Automatic proof tests can be set to occur automatically at user-specified intervals, with a warning provided to the operator. The interval is set using the Logic Solver properties in DeltaV SIS Explorer.

DeltaV SIS provides alerts to remind users about proof tests and to warn the user if the proof test is overdue.

Characterization Modules. DeltaV SIS LS Characterization Modules (CHARMs) should be proof tested according to the specified proof test interval to ensure there are no dangerous faults present that are not being detected by continuous runtime diagnostics.

A manual proof test for a CHARM is initiated from a diagnostic application and from a DeltaV workstation and causes the LS CHARM to go through reset and perform power-up testing. You can choose the proof test interval for an LS CHARM based on the associated SIF.

HART Devices. Proof testing of HART devices in a safety system is an important function to keep the safety system operating correctly.

When partnered with AMS Device Manager, DeltaV SIS streamlines HART device proof testing.

TOOLS TO ASSIST IN TESTING

These Emerson tools assist in streamlining proof tests and extending the time between testing:

- Bypass Management
- Partial stroke testing (PST) capabilities
- AMS Device Manager
- Syncade Workflow

Bypass Management. During the proof test of individual components, it is necessary to implement some bypasses to prevent a spurious trip. It is critical for the safety of the plant, to carefully manage those bypasses and make sure any bypass is removed once the tests are completed.

DeltaV SIS includes functionality to implement

REFERENCE

H.T.Dearden CEng FInstMC, Proof Testing of Process Plant Safety Instrumented Systems, Version 1, November 2011

and manage maintenance bypasses.

- User privileges can be assigned to bypass user actions. In this way, only authorized personnel can perform bypasses.
- Users can specify whether a maintenance bypass reduces the number of votes to trip within a voting scheme.
- Bypass timeouts and reminders can be set to alert users when a bypass timeout is imminent.
- Faceplates allow operators who have sufficient privilege to bypass a sensor during proof testing directly from the operator interface without using another engineering tool.

Partial stroke testing tools. In certain applications, users may use a PST to extend the time between full proof tests of valves. DeltaV SIS allows users to easily manage those PSTs.

- An alarm is generated on partial stroke failure.
- The valve is available on demand even while the partial stroke test is in progress.
- PSTs can be automatically initiated by the DeltaV SIS logic solver or manually initiated from standard operator faceplates.
- The DeltaV SIS system communicates with the DVC6000 series SIS via the HART protocol so no additional wiring or components are required to automate PSTs.
- PST results are automatically recorded in the DeltaV Event Chronicle for easy documentation.

AMS Device Manager. Use AMS Device Manager in concert with the DeltaV SIS to diagnose and troubleshoot safety instruments — ensuring they will perform effectively upon demand.

- Time interval: Proof test capabilities in SIS devices can be activated by AMS Device Manager, enabling partial online testing of a safety instrumented function. This online testing allows you to extend the interval between offline proof tests.
- Interlock checkout: The QuickCheck SNAP-ON™ application facilitates and accelerates interlock checkout — saving time and improving safety.
- Installation and operations: AMS Device Manager can be effective in SIS installation and commissioning, SIS maintenance, SIS modifications, and the design requirements associated with those phases.
- Field trips: Sending technicians into the field to manually place devices in loop test mode is time intensive and exposes technicians to a variety of safety hazards: heights, extreme temperatures, and chemicals. By using the QuickCheck application, you can group, monitor, and fix the output of HART transmitters from the safety of AMS Device Manager workstations.
- Records: AMS Device Manager automatically creates a record of all online tests and allows personnel to enter additional comments if desired. Results of tests and inspections are also automatically recorded.
- Errors: Compared with current practices, using AMS Device Manager auto-features reduces errors and improves traceability.
- Meeting IEC 61511: AMS can be used effectively to meet many of the requirements of IEC 61511 in safety instrumented systems. Section 16.2.2 states that: "The user shall maintain records that certify that proof test and inspections were completed as required." The AMS Audit trail feature can be used to provide records that proof test and inspections were completed as required.

REDUCE PROOF TESTING RISKS

DeltaV SIS with Electronic Marshalling and partial stroke tests can deliver safer, more efficient proof testing and help meet compliance requirements. Watch the video to learn more.
www.youtube.com/watch?v=95Aj7QqEm_c

Syncade Workflow. Operating in tandem with DeltaV, the Syncade Workflow application can be configured to guide the tester through the manual steps as well as executing the automated steps eliminating errors due to misinterpretation of paper work flow.

- The Syncade Document Control and Archiving (DCA) system records manual interactions and results from automated steps.
- The Syncade Training module maintains personnel training records. Only a person trained for a task can execute it.
- The Syncade Equipment Tracking (ET) module can handle all proof test scheduling.

PROOF TESTING EXAMPLES

Proof tests are conducted according to well-defined procedures. Full proof testing and partial proof testing explained here are for the test of single devices.

Full proof test: The goal is to return the PFDavg (Probability of Failure on Demand) back or close to the instrument original targeted PFDavg.

Note that the following modern full proof test does not require personnel to be sent into the field to verify that the test was completed, to reset the valve, or to document the test. All of the actions are completed online via HART communications.

Following are ways that the DeltaV system assists in comprehensive (or full) proof testing of a transmitter.

- In the event that you choose to put a bypass in your system during the test, the DeltaV SIS system assists in management and restoration to normal operation once the test is complete. DeltaV SIS has provisions for alarming the user and for automatically removing the bypass after a specific period of time.
- The DeltaV SIS interface enables the operator at the workstation to retrieve diagnostics during and after testing and to take appropriate action.
- From the operator workstation, the operator can send a HART command to the transmitter to go to the high alarm current output. The system verifies that the analog current reaches that value.
- Similarly, the operator can send a HART command to the transmitter to go to the low alarm current output. And again the system verifies the analog current reaches that value.
- A two-point calibration of the transmitter over the full working range is accomplished from the workstation rather than travelling to the field.

Partial proof test: Partial testing evaluates different components at different times and frequencies if a facility is unable to perform an "end-to-end" test. A partial proof test can also be done to test a subset of function of single components (i.e. partial stroke test on a valve). The goal is to bring the instrument's PFDavg back to a percentage of the original PFDavg. This does not replace the full test of a component but might extend the period between full tests.

SAFETY FOR PERSONNEL AND ASSURANCE IN THE PROCESS

Critical to assuring safe operation of safety instrumented systems, proof testing also is required to meet designed safety system SIL levels.

Because proof tests on traditional safety systems can involve inefficient processes and can add risks, Emerson has designed DeltaV SIS tools to assist users in completing end-to-end and individual component proof tests.

Whether full proof testing or partial proof testing is required, the goals of the Emerson tools include:

- Assist in streamlining proof tests
- Create a safer and more efficient process
- Avoid potential for inadvertent alteration of safety system operation
- Potentially extend the time between testing.

Please contact your local Emerson representative to discover additional benefits in confidently performing efficient and safe proof testing.

SERGIO DIAZ is Product Manager — DeltaV SIS for Emerson Process Management. He can be reached at Sergio.Diaz@Emerson.com.

My system architecture shouldn't stop me from having a modern safety system. I need the best technology available today.

YOU CAN DO THAT

DeltaV SIS. Whether your choice is standalone, interfaced or integrated— DeltaV SIS. That's modern. You shouldn't be limited by your existing control environment to employ today's state-of-the-art technologies. DeltaV SIS with Electronic Marshalling and CHARMs technology simplifies design, installation, wiring and commissioning of SIS projects. Modern technology increases capacity and reduces the footprint of your SIS system by eliminating traditional marshalling cabinets. Now you can implement a standalone safety system or integrate with your current control system for even more benefits—either way, the choice is yours. Scan the code below or visit: **ModernSafetySystem.com** to learn more.

EMERSON™
Process Management

The Emerson logo is a trademark and a service mark of Emerson Electric Co. © 2014 Emerson Electric Co.

EMERSON. CONSIDER IT SOLVED.™