Valve system controls for safety

By G. Paul Baker

Reactive chemical processes have inherent hazards.

These range from violent releases of energy to exposure of personnel to toxic substances.

Safety Instrumented Systems (SIS) are used to reduce the risk of these potentials by monitoring process parameters, determining when one has exceeded its safe limit, and typically, stopping the reaction by blocking the reactant flows.

Failures of the SIS fall into two categories. Obvious failures are the source of nuisance shutdowns, which cost the end user in time, resources, and most importantly, production.

Hidden failures are dangerous in that they will allow the process to proceed until a hazardous event occurs, injuring workers by ruptures, explosions, or exposure.

As industry standards and regulatory requirements have tightened, SISs have improved, and they minimize the hidden failures, essentially by using diagnostics to convert hidden failures into obvious failures.

This approach results in an increase in safety, but also in an increase in nuisance trips. The improved safety costs the end user more money in lost production.

In the 1990s, the two-out-of-two-diagnostic architecture (2oo2D) came out. This structure provided two diagnosed parallel channels through the logic solver, with both channels being capable of holding the block valve in its normal operational state.

This approach requires a high level of diagnostics because a dangerous failure in either channel will allow a hazardous event to occur. The benefit, then, for this architecture is that for those obvious failures in either system, a nuisance trip will not occur.

The 2oo2D architecture would not extend through the final control element since currently available block valves do not have sufficient diagnostic coverage.

In addition, adding a second valve in parallel with using the currently available technologies will significantly increase the hidden failures and their resulting hazardous events.

FAST FORWARD

- Improved safety brings more nuisance trips, which means lost production.
- The single block valve is the weak point of the 2oo2D architecture.
- Parallel valve technology can provide 95% diagnostic coverage.

A matrix that substantially increases the level of safety in the process industries while significantly reducing the number of nuisance trips

The single block valve, then, is the weak point of the 2oo2D architecture.

The available valves with integral diagnostics will partially close the valve by an amount of 15% to 25%. Through various means, these systems try to predict the potential the valve will close completely when asked.

While stem force or torque will reveal some characteristics of the actuator/stem assembly, it cannot decipher what is actually happening at the level of the process. A foreign object, such as a crescent wrench, could be within the plug, allowing movement of 15% to 25% while preventing any significant closure.

What we need is a valve technology with sufficient diagnostic capability to allow two valves to operate via parallel installation.

There is an emergent parallel valve technology that has the capability of providing 90% to 95% diagnostic coverage. It consists of two block valves mounted into a parallel pipe manifold.

The manifold works in such a way that when one valve is closed and the other opened, the fluid flow through the opened valve will pull down the pressure in that portion of the manifold connected to the closed valve. The pipe system is symmetrical, so the “pull down” effect will exist when either valve is closed.

A compound range, differential pressure transmitter is part of this system. It measures the differential pressure between the outlets of the valves. While both valves are open, the transmitter’s signal will be at the midpoint, i.e. 12 mA on a 4-20 mA range. When one valve is closed, the signal will move in one direction from the midpoint. When the other valve is closed, the signal will move in the opposite direction from the midpoint.

The signal feeds into a specially designed electronic controller, or into a specially configured PLC. When there is a need to test the valve system, the controller or PLC will alternately close one valve and then the other, checking at each ½ cycle for the proper amount and polarity of differential pressure between the valve outlets. (The second valve cannot close until the first valve is verifiably full open).

If the closed valve’s plug does not sufficiently block off the fluid flow, the required amount of differential pressure will not emanate, and the system senses the failure. Additionally, fully opened and fully closed limit switches from each valve transmit to the controller or PLC. If the system does not detect proper valve stem status at each phase of the test cycle, it assumes a failure, and the proper failure-mode procedures are taken.

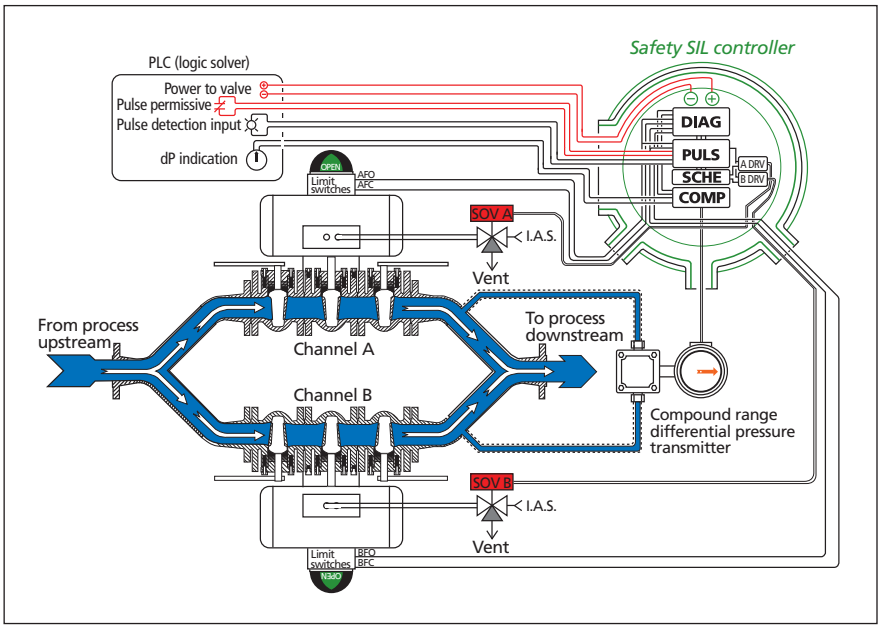
Lastly, the controller or PLC will check for null (zero) differential pressure before a cycle can start. If a differential is present, the system will

not cycle, and the presumption is there is a failure. The concept is the cycling (pulsing) is the signal. If there is a failure in any part of the valve system, cycling cannot occur. Conversely, if the entire system can cycle with the logic solver sensing the pulse, it will be capable of blocking in the fluid flow when there is a demand. In a phrase, as long as you are cycling, you are safe.

The list of failures, which will prevent cycling, is comprehensive and includes failure of the power supply or I/O module of the driving PLC, any broken wire between the PLC and the system, including any wiring to any limit switch or to either solenoid valve. Other failures that will interrupt cycling are a failed IC or component on the electronic controller (if the independent controller is used), a defective coil on either solenoid valve, a plugged exhaust port on either solenoid valve, a plugged sensing port on either or both sides of the differential pressure transmitter, etc. All of these latter failure conditions are discrete. That is to say, each component would either allow the system to cycle or it would not. The diagnostic coverage for these components would therefore be very close to 100%.

For this technology, the differential pressure measurement will be the limiting factor for the overall diagnostic coverage. The accuracy of this transmitter, in conjunction with its range, will limit the minimum amount of leakage through the closed valve it can sense. The differential between the valve outlets is a function of the square of the flow through the opened valve. Differential pressure transmitters are presently available with accuracies of 0.05% of span or better. These high accuracy transmitters will allow for the detection of leakage under 2.25% (the square root of 0.05%), which translates to an effective diagnostic coverage of 97%. This is sufficient coverage to allow this 2oo2D system to provide increased protection against dangerous, hidden failures. The parallel, fault-tolerant structure allows for one of the valves to fail while preventing a nuisance trip. There will always be at least one valve opened, so there will be no interruption of the process. In the case where one valve has failed, the remaining operational valve will preclude a nuisance shutdown.

Parallel valve technology



Source: Safety Cycling Systems

Justify installation

The cycling of the valves to test for a failure will obviously increase valve wear and promote premature failure. If a PLC is to directly drive the valve system, the configuration should only test (cycle) the system at the period required to maintain the Safety Integrity Level (SIL). Since stroking the valves only happens while the plant is on-line, the testing can be as frequent as required to accommodate high SILs. The design of the independent electronic controller includes a dry contact input that, when closed, will permit the cycle testing to proceed. When and if the independent controller is in use, the programming of the shutdown PLC would request testing at the prescribed intervals. In both of the above instances, valve stroking is limited to that frequency required to maintain a desired safety level, thus minimizing wear and tear on the valve system.

Component failures will typically describe a "bathtub curve," where the high initial failures are from manufacturing variation. The late increase in failures is from decreasing component strength as the part wears out due to stresses over time. At the current time, most industrial devices undergo initial stress testing to expose those manufacturing variations that would result in initially high failure rates on the front end of the bathtub curve. These devices are usually in reparable systems, so new, tested components can accommodate the ensuing rise in failures. This produces a memory-less system that should remain at the low failure rates of the middle of the bathtub curve, so long as one repairs the failure within a short period of time. This approach allows industry to utilize fault-tolerant systems, allowing the system to remain in service while the repair of the detected failure happens. The Markov Model is the best method of determining the behavior of a fault-tolerant, repairable system. When using a Markov Model to calculate the Probability to Fail on Demand of such a system, the Mean-Time-To-Repair becomes an important consideration. This is because the longer the system remains in service with a single fault, the greater probability there will be for a second, with potentially disastrous consequences. If on-line repair time could be limited (to 24 hours for instance), the SIL of this type of safety system could be maintained. There are manual block valves installed on either side of both automated valves. Should there be a failure

in one of the valves, the manual valves would allow the failed valve to be repaired or replaced on-line, thus allowing the system to return to its fully operational state without interrupting production.

With a specialty chemical production unit generating over $30,000 worth of product per hour, nuisance trips have a significant impact on the company's bottom line.

In addition to the lost production, staff will have to analyze a shutdown to verify it actually was a nuisance trip, consuming additional resources in time and personnel. Furthermore, the plant would have to go through the start-up process again, costing even more in resources, all the while losing production.

A typical nuisance trip can easily cost the end-user three to four hours in lost production and services from multiple instrument technicians and other personnel. The elimination of just one nuisance trip during the operational lifetime of this cycling technology can easily justify the cost of installation.

Mean time between trips

William M. Goble, Ph.D. of Exida produced a 2007 study comparing this new cycling technology with other safety architectures currently in use.

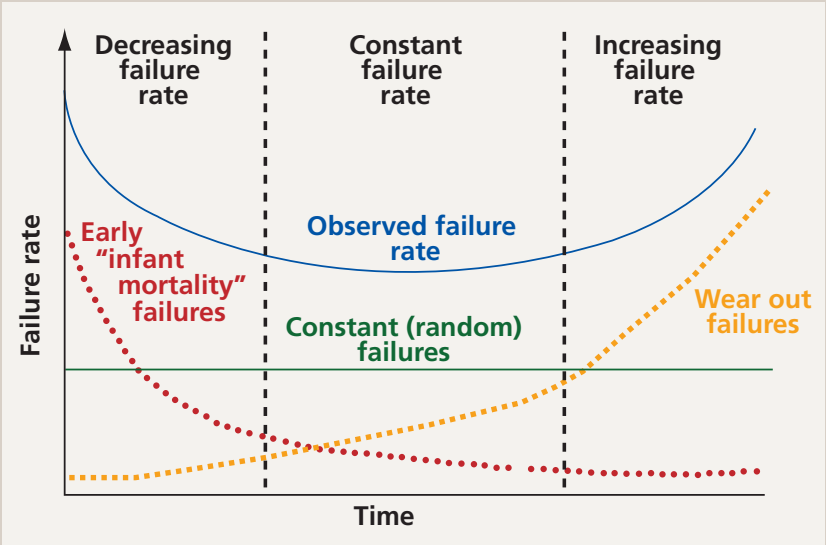
The study set up a typical safety function in a SIS with the failure characteristics of the sensors and the logic solvers remaining the same through the various architectures. The one-out-of-one (1oo1) architecture consisted of a single sensor fed through a single channel logic solver operating a single block valve. The one-out-of-two architecture (1oo2) had dual diagnosed channels in the logic solver, with two block valves in series, each being controlled by one of the separate channels. We studied these two forms and compared them with a 2oo2D system using the new technology at two levels of diagnostics, 90% and 95%.

The 1oo1 system provided a Risk Reduction Factor (RRF) of 50 in terms of dangerous failures, with the block valve contributing a mean time between nuisance trips of 199 years.

The 1oo2 system substantially increased the RRF of the dangerous failures (359), but at the same time, the block valves' mean time between nuisance trips went down to 105 years. This system would be over seven times safer than the 1oo1 approach, but at a cost of almost twice as many nuisance shutdowns. Production personnel would find this especially annoying.

The cycling, parallel two-valve system with 90% diagnostic coverage would be able to detect a minimum of 10% leakage through a valve when it cycled closed. When used as part of a 2oo2D SIS, this would generate a Risk Reduction Factor of 240, almost five times better than the

Splish, splash, I was taking a bath



Source: U.S. Army, Wikipedia

The bathtub curve is widely used in reliability engineering.

It describes a particular form of the hazard function, which comprises three parts:

- The first part is a decreasing failure rate, known as early failures or infant mortality.
- The second part is a constant failure rate, known as random failures.
- The third part is an increasing failure rate, known as wear-out failures.

TERMS AND CONCEPTS

SIS: A Safety Instrumented System (SIS) is an independent system composed of sensors, logic solvers, final elements, and support systems. Upon detection of unacceptable process conditions, the SIS performs specified functions to achieve or maintain a safe state of the process.

2oo2 is a two-out-of-two voting arrangement and means there are two criterions (requirements, tasks, operations) for something to occur, say closing a valve where one might configure a second solenoid such that one would have de-energize both (two) solenoids for the valve to close.

Block valve is a quarter-turn (90°) valve that blocks the flow of fluid through pipe, as opposed to a modulating valve used to proportionally regulate the flow. Block valves are typically either fully open or fully closed and are the normal final control element used in a shutdown system.

Nuisance trip is a situation in which a safety device activates but there is no real danger. Circuit breakers tripping, fuses blowing, GFCIs opening, and motor overload contacts shutting off are the type of safety device that produce nuisance trips.

SIL: The Safety Integrity Level is the relative level of risk-reduction provided by a safety function or it specifies a target level of risk reduction

1oo1 system, but not quite as good as the 1oo2 architecture. However, the block valve systems mean time between nuisance trips has risen to 1958 years—almost a factor of 10 better than the 1oo1, and 18 times better than the 1oo2. This is a significant reduction in nuisance trips and would result in substantial savings to the end user.

Ninety-five percent diagnostic coverage on the cycling block valve system means a 5% leakage is detectable in a closed valve while in service. Such coverage will essentially maintain the block valves mean time between nuisance trips (1955 years) but provides a better RRF than either the 1oo1 or the 1oo2 architectures, (RRF = 442).

"The 2oo2 architecture using the Safety Cycling Systems approach provides improved safety and significantly improved MTTFS (Mean-Time-To-Fail-Safe, low false trip rate). If the diagnostic coverage factor could reach 95%, superior safety and a significantly improved MTTFS would both be achieved," said Goble.

The MTTFS represents the average time between nuisance trips and produces an interesting relationship embedded in the Goble Study.

The report shows a substantial improvement in the overall system MTTFS over available types when using the 2oo2D valve system. The enhancement varies from 3.7 times longer than the 1oo1 architecture, to 6.4 times better than the 1oo2 type.

This improvement derives mainly from the enhanced MTTFS of the 2oo2D valves. The valve contribution for the overall system MTTFS of the 1oo1 and 1oo2 structures is 81.55% and 89.10% respectively.

However, for the 2oo2D, both at 90% and at 95% diagnostic coverage, the valve contribution to the overall system MTTFS is only 30%.

In conclusion, the cycling, parallel, 2oo2D block valve system, should substantially increase the level of safety in the process industries, while significantly reducing the number of nuisance trips, thereby justifying the cost of installation in terms of both safety and production.

ABOUT THE AUTHOR

G. Paul Baker (gpaulbakerjr@cox.net) is an ISA senior member. He holds the patents on the SafetySIL technology, and he has been active in industrial instrumentation, control, and safety systems in the petrochemical industries for over 35 years.

View the online version at www.isa.org/intech/20071202.

RESOURCES

Selecting hydrocracker safety integrity levels
www.isa.org/link/Hydrocracker

Simplified equations verify SIS
www.isa.org/link/SimpleSIS

Determining the required safety integrity level for your process
www.isa.org/link/SILprocess