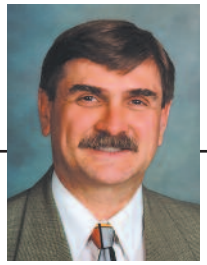
Originally appeared in:
HYDROCARBON PROCESSING®
October 2003 issue, pg 116
Used with permission.
www.HydrocarbonProcessing.com



HPI IN AUTOMATION SAFETY

WILLIAM GOBLE, CONTRIBUTING EDITOR

wgoble@exida.com

Periodic functional testing—Is there a better way?

Process design engineers work hard to create inherently safe processes. To a great extent, this effort is successful and the general industry safety record continues to get better. Consequently, potentially dangerous conditions (hazards) are infrequent. This situation makes safety instrumented system (SIS) design and maintenance the hard job that it is. An SIS may sit without a hazardous demand for years. If the SIS never takes action, how do we know it works?

The answer of course is that we must test the SIS. This testing has been the topic of some interesting discussion recently. Two issues have surfaced to challenge the conventional testing methods where each safety instrumented function (SIF) is functionally exercised. One online test method involves opening a bypass valve then stimulating the process sensor to trip the SIF. This test exercises "the entire loop" and all components in the loop. One can watch the shutdown close (or open). Obviously the sensor and the logic solver are working properly or else the loop would not trip. Alternatives involve blocking the shutdown valve and testing to show that the SIF attempts to close the shutdown valve. If the process is offline, the test can be done in a similar way but without the need to use a bypass valve or a valve blocking device.

How good is this testing? Many variations exist in the test procedures that have been written but the fundamental concepts always involve stimulation of each SIF with verification that the expected action does indeed occur. The first challenge to this proven technique comes from the question "How good is this testing?" There have been examples of marginal, intermittent failures not detected during a functional test. Some of these examples include components that work only a portion of the time. This can happen due to impending wearout, corrosion, dirt or other things. A margin intermittent component that functions 50% of the time has a 50% chance of being detected during a functional test. Fifty percent is not very good.

The second challenge comes from diagnostic components. Many automatic diagnostics are now present in the equipment used for SIS design. We depend on these diagnostics to detect dangerous component failures. We take credit for these diagnostics during SIL verification calculations. *But rarely do these diagnostics get included in a periodic functional test.* For the most part, these diagnostics may or may not be working due to internal equipment failures. A functional test that merely causes a trip will not test a diagnostic function. If the SIL verification calculations were done without taking credit for the diagnostics, the resulting SIL levels would drop considerably!

Some have considered what additional testing must be done to verify that the diagnostics still function. Think about that problem for a moment. A functional test would involve simulating an interval failure of the equipment. Are we suggesting that one jam a screwdriver into the safety PLC to see if the diagnostics detect a failure? No, definitely not.

■ If the SIL verification calculations were done without taking credit for the diagnostics, the resulting SIL levels would drop considerably!

Periodic test and inspection procedures. IEC 61508 requires that instrumentation manufacturers write periodic inspection and test procedures for their equipment. Those procedures are supposed to be part of the user documentation, usually found in a document called the "Safety Manual." To date, many certification agencies judging IEC 61508 compliance seemed to have missed that requirement since these procedures are quite hard to find. One safety PLC vendor has analyzed the problem and published a recommendation. They have accounted for all potential dangerous failures and the automatic diagnostics failures and concluded that nothing can practically be done by the user. Their procedure is to simply replace the PLC every 10 years.

Effectively they are saying that no user functional test will ever detect a failure not already detected by the automatic diagnostics, even accounting for the fact that the diagnostics may fail. Functional testing for their equipment is worthless.

Many manufacturers are now working on advanced test procedures that will detect both residual dangerous failures and diagnostics failures. Detailed component-level FMEDA analysis is

showing what needs to be done. I have seen some of these proposed methods and they have nothing to do with "functional testing." The nice thing is that these new techniques appear to be easier and faster than our traditional methods. It looks as if we can do a better job for less cost. Stay tuned, you will see some nice things in the near future. And ask yourself, can you give up your functional test procedures? HP

The author is principal partner, exida.com, a company that does consulting, training and support for safety-critical and high-availability process automation. He has over 25 years of experience in automation systems doing analog and digital circuit design, software development, engineering management and marketing. Dr. Goble is author of the ISA book *Control Systems Safety Evaluation and Reliability.* He is a fellow member of ISA and a member of ISA's SP84 committee on safety systems, and can be reached by e-mail at: wgoble@exida.com.