Flow Control Network.com

November 2006

SIS Expert Answers 5 Key User Questions

Dr. A. Speaks Out on Safety Systems Design

Angela Summers, Ph.D.

***Angela Summers, Ph.D.**, a.k.a. "Dr. A," is the CEO and founder of SIS-TECH Solutions and SIS-TECH Applications of Houston, Texas. Dr. A earned her Ph.D. in Chemical Engineering at The University of Alabama and is a Licensed Professional Engineer in the State of Texas. She is the U.S. representative to IEC 61508/61511 committees, and she chairs the ISA SP84 committee responsible for developing the guidance documents on safety integrity level verification calculations (TR84.02) and on the implementation of the ISA 84.01/IEC 61511 (TR84.04). In 2005, Dr. A was awarded ISA's Albert F. Sperry Award "For outstanding contributions and leadership in the specification, development, and implementation of safety instrumented systems for the process automation industry." She has published more than 40 papers and contributed chapters for the* Instrument Engineers' Handbook*,* Lees' Loss Prevention in the Process Industry*, and* Perry's Handbook of Chemical Engineering*. She is currently completing a new book for the Center for Chemical Process Safety on safe and reliable instrumented protective systems. Dr. Summers can be reached at* ASummers@SIS-TECH.com *or 281 922-8324.*

***Dear Dr. A:** Please help us settle a friendly argument. One group claims we need third-party certification for our field devices. My group, a much smaller group by the way, claims that ISA 84.01/IEC 61511 allows us to choose our devices based on "prior use" and thus "self-certify" our SIS devices. Who's correct — a humiliating assignment goes to the loser?*

Dr. A: There is simply no requirement for certification anywhere in ISA 84.01/IEC 61511. In fact, the standard does not contain the word "certify" or its derivatives. Field devices should be selected based on proven performance in the operating environment. A device that works perfectly in one service may fail miserably in another. All equipment must be in essence "self-certified." For the process industry, ISA TR84.00.04 and the soon-to-be published CCPS book, Guidelines for Safe and Reliable Instrumented Protective Systems, refer to this process as "User Approval."

All safety system devices should be subjected to a user-approval process, which determines and documents that the device is suitable for the intended purpose, classification, operating environment, and function complexity. The process should consider available analysis, testing, and in-service performance information to determine the device's fitness for the application. A device should not be user-approved until sufficient experience has been gained in a similar operating environment that you know how it works, how it fails, how frequently it fails, how to detect its failure, and how to correct the failure. For SIS devices, the user of a product must feel confident that they understand the required frequency of inspection, maintenance, and proof testing to maintain its mechanical integrity in an "as good as new" condition.

New technologies should be implemented in control system or other nonsafety applications prior to using it in an SIS. The standard calls this "prior-use" information. If you purchase an unproven new product, installing it in a control system application could cause you problems in controlling the process, maintaining production, or achieving product quality. The SIS operates very differently. It is a dormant system, waiting in a standby mode for an unacceptable process condition to occur. You want only proven devices in SIS applications. That way when the new device you purchased fails, the SIS is waiting there and fully capable of taking the proper action to prevent a process safety incident.

***Dear Dr. A:** Can you explain, in simple terms, the meaning of "safe failure fraction" (SFF); and is it really possible to achieve nearly 100 percent SFF, as some manufacturers are claiming?*

Dr. A: A 100 percent SFF is achieved when you assume perfection — perfect design, diagnostics, manufacturing, installation, commissioning, validation, inspection, maintenance, and proof testing. Frankly, I think the claim is ridiculous and is incongruent with a safety culture that would demand conservative estimates based on what can reasonably be achieved in the real world.

The safe failure fraction is the ratio of the safe and detected dangerous failures to the total failures (safe and dangerous). The safe failure fraction can be made higher by detecting more dangerous failures and classifying them as detected dangerous. IEC 61508 considers this classification as acceptable as long as the operator of the equipment recognizes that the failure has occurred. It is then the responsibility of the operator to maintain process safety.

The IEC 61508 scope is restricted to the Electrical/Electronic/Programmable Electronic System (E/E/PES). Many argue that IEC 61508 covers the wetted parts of field devices. Many certification reports even list the mechanical components in the product description. However, when you look at the analysis assumptions, you find the mechanical parts are assumed to work perfectly or near perfectly in a perfect operating environment. Conversely, owner/operators see more frequent mechanical failure than E/E/PE failure.

For example, I have a third-party assessment report where a digital valve positioner (DVP) is assumed to vent perfectly. This is not achievable in the real world where moisture, rust, and particulates in instrument air systems cause everything but perfect venting. Yet, the product claims a 100 percent SFF. This is the problem with using predicted %SFF versus observed %SFF. Process industry experience has not yet demonstrated what a DVP can achieve, but owner/operator experience for a standard positioner is an observed SFF between 65 percent and 80 percent.

Dear Dr A: *We have read about and attended demonstrations of using digital valve positioners (DVP) to perform partial-stroke valve testing of automated block valves. Are we correct in assuming that by deploying DVP technology we will achieve all the requirements of a "proof test" as defined in IEC 61511-1?*

Dr. A: No. A proof test of an automated block valve is far more than a partial-stroke test. It is also more than a simple function test. A manufacturer performs a function test. An owner/operator must perform a documented and witnessed proof test. A proof test is a documented test, or series of tests, performed to detect failures in a protective system and includes inspection and preventive maintenance activities necessary to maintain the equipment in its "as good as new" condition.

A proof test will generate documentation that provides an audit trail to the date, person, permit approval, test equipment, and test procedure. If you have an incident, I should be able to interview the individual who did the test, review any permit approval documents, review the calibration reports for any test equipment, review the proof test procedure, and the resulting documentation. This is necessary for any investigation team, lawyer, or regulator.

Dear Dr. A: *For throttling control valves serving as emergency shutdown valves, some of our clients declare that the partial-stroke testing coverage can always be claimed for these valves without additional analog outputs in the SIS. They think the DCS essentially conducts the partial-stroke testing every day for these throttling control valves. What's your opinion?*

Dr. A: The throttling of a control valve is not a partial-stroke test; it is an inherent part of its specification. The control valve failure rate is related to how the process impacts it in the control application. The ability to fully open or fully close the valve in response to a process demand is not demonstrated by modulation. The positioner is an essential component of the control loop, modulating the control valve in response to an analog output from the DCS.

Positioner failures are the leading cause of control failure, so the positioner should not be used to actuate the valve in an SIS application when preventing events associated with a loss of control. Instead, a solenoid-operated valve should be used to independently close the control valve.

Dear Dr. A: *Is there a practical alternative to installing "smart" positioners that provides similar diagnostic data and that supports automated partial-stroke testing of block valves?*

Dr. A: It comes down to business value and potential impact of nonperformance. Positioners are required for control system applications. They are not required for SIS block valve applications. As discussed previously, you do not partial-stroke test a control valve using a positioner. Positioners have small Cv vent ports and mechanical components, which are known to experience significant degradation in performance when the instrument air supply contains moisture and/or particulates.

The small vent port allows tighter and smoother process control but rust and particulates build up in it, while the mechanical parts tend to stick and hang up. Over time, higher air pressure must be applied to the valve actuator to achieve the same valve movement. Positioner problems are so well known that any process with reliability concerns has a full flow bypass around the control valve to facilitate online positioner repair. Perhaps with time, the DVP technology will allow us to detect positioner problems earlier so that maintenance can be planned rather than being executed on an emergency basis.

In contrast, for SIS applications, we need to actuate the valve with something that is reliable and proven to work in an environment where it is rarely expected to move. We want to use a large Cv device to move the valve quickly to the safe state, allowing the process to achieve safe operating conditions within the process safety time. A better option is the proven-in-use one. Solenoid-operated valves have significantly larger Cv vent ports than positioners, which need small orifices to tightly control valve position. Solenoids have been used for this purpose since the beginning of automation to actuate both control and block valves used in SIS applications. They can be installed to allow online repair without a physical bypass around the valve.

www.sis-tech.com