Originally appeared in:
HYDROCARBON PROCESSING®
January 2005 issue, pg 94
Used with permission.
www.HydrocarbonProcessing.com

Article copyright © 2005 by Gulf Publishing Company. All rights reserved. Not to be distributed in electronic or printed form, or posted on a Website, without express written permission of copyright holder.

HPIN AUTOMATION SAFETY

WILLIAM GOBLE, CONTRIBUTING EDITOR

wgoble@exida.com

Separation between control and safety

It is pleasure to see that the new *ANSI/ISA 84.00.01-2004 (IEC 61511+)* standard has been issued. It replaces the now obsolete *ISA 84.01-1996.* This standard is word-for-word identical to *IEC 61511* except that a "grandfather" clause has been added for the US. This effort took time and much of the effort was devoted to a discussion about the language regarding the separation of control and safety.

The issue involves proposed designs where control functions and safety functions use common equipment, especially the logic solver. There is no absolute prohibition against this practice in the standard. However, current requirements do effectively force any engineer who attempts combining control and safety to follow a gauntlet of tasks designed to spell out issues and identify design flaws.

Conditions of concern. The first variation of this situation exists when the equipment is not classified as a safety instrumented system. In that case, the design does not follow all of the rules of *ISA 84.00.01-2004 (IEC 61511+)* to prevent design mistakes. In that case, the standard clearly states that any safety instrumented function cannot have a risk reduction greater than 10. This is the bottom of SIL1 range, so this design cannot meet SIL 1 requirements. The practical effect of this requirement is that a designer cannot combine control and safety functions in the same equipment unless the equipment is classified as a safety instrumented system and follows all of the design rules of the standard.

If the equipment is classified as an SIS, then the task is equipment justification. This must be done by either a "prior use" justification or equipment must be assessed per *IEC 61508.* Most choose the *IEC 61508* certification route, especially for the logic solver.

Hurdle 1. Assume the designer has chosen an SIL 3 capable certified logic solver for control and safety. The next task is an analysis showing that no control system failure can cause a hazard. If control system failure can initiate a hazardous sequence, then safety instrumented functions MUST NOT be designed into common equipment without detailed quantitative risk analysis. The language in the standard is strong and clear. Often, the initiating event analysis identifies a problem with combined control and safety.

Hurdle 2. Assume the designer is still determined to proceed with combined control and safety even with the possibility of hazards initiated by a system failure. Another task that must be done is a quantitative analysis that must be conducted for all components where failure may initiate a hazard. For those failures with no other protection layer, the frequency of failure will result directly in an incident. The detailed quantitative analysis must show that these failures will not increase risk beyond tolerable levels.

Hurdle 3. Assume all analysis work is complete, and the designer still meets tolerable risk requirements. Now, the designer should consider maintenance and operational procedures required for the SIS. The standard has many requirements for management of change, proof testing and security. A designer should evaluate the effects of having all of these procedures in effect for the control system. Will the owner really follow all of these procedures? If the procedures are followed, will the lifecycle cost increase significantly? Typically, this step halts any designs that make it through the early tasks.

■ Designers can combine control and safety functions with common equipment. However, the complexity and costs for such systems can also be burdensome.

Observation. I realize that some design situations might be solved by using a combined control and safety system. But these situations are truly rare, especially within the process industries. When I think about all the analysis that must be done and the chance for mistakes, I worry. When I think about the potential operations and maintenance complexity and the chance for a mistake, I worry. Still, I really like the standard as written. It strongly suggests separation and forces careful analysis when this path is not chosen.

If you are the designer attempting to save a dollar by combining control and safety into one set of equipment, stop and think about lifecycle costs. Are you sure the design meets needed risk reduction? If you are a designer trying to combine control and safety into one box for a good technical reason, then double check that your analysis is accurate and conservative. Confirm that your operational and maintenance procedures are realistic, complete and accurate. If anything does go wrong, then your design will be scrutinized very closely. **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.

Article copyright © 2005 by Gulf Publishing Company. All rights reserved. Printed in U.S.A.