Reprinted from:
HYDROCARBON PROCESSING®
June 2004 issue, pg17
Used with permission.
www.HydrocarbonProcessing.com

HPI INTEGRATION STRATEGIES

ASISH GHOSH, CONTRIBUTING EDITOR
aghosh@arcweb.com

Look for enhanced process safety functions

Since the publication of the IEC 61508 safety standard and, more recently, the IEC 61511 standard for process safety, interest in rigorous safety analysis and applying certified safety instrumented systems (SISs) has increased considerably among the user community. As users are becoming more knowledgeable about safety issues, they are increasingly focusing on overall safety.

Users want their safety systems to satisfy their needs more cost-effectively through closer integration of safety with control systems. They are looking for a flexible architecture with more scalability. Users are also looking for increased functionality for modifying alarm limits based on process conditions and orderly shutdown procedures in case of an emergency.

Increased focus on overall safety. The main cause of a safety system failure is not due to logic solvers, but the failure of field devices. In recent years, there have been significant advances in the development of the architecture of logic solvers with voting circuits and advanced diagnostics. However, they do not address over 90% of the causes for failure, which are due to malfunctioning field devices. An integrated safety approach is needed, where field devices are incorporated in the overall design. The protective system should provide:

- Automated sensor calibration and validation
- Environment condition monitoring of the sensors
- Valve movement testing at regular intervals.

Sensor calibration should be an integral part of a safety system. Use of protocols, such as HART and FOUNDATION Fieldbus, with intelligent transmitters allows for remote monitoring and diagnostics. Common-cause failures of electronic components are frequently due to environmental conditions, such as elevated humidity and temperature, which need to be monitored closely.

Standard valves in safety applications have the continual concern relating to the ability to trip on demand. Control valves are being designed to have very low probability of stem seizure and packing failure. Limited valve movement testing should be an integral feature of a safety system.

TÜV-certified control valves are now available in the marketplace. Using field instruments certified for safety applications will reduce the burden of choosing the right instruments for safety applications. Certified instruments are expected to be more widely used when their price is no longer significantly higher than common instruments.

Closer integration with control systems. Keeping control and safety systems completely independent used to be a common practice. Control and safety systems provide different layers of protection, which is one of the core issues regarding their separation. Users want certain levels of separation because they do not want common-cause failures.

There are, however, logical reasons for using common or similar systems for control and safety functions that allow common data mapping and similar engineering tools, which lead to lower engineering and training costs. The safety standards are ambiguous on the issue of separation—except for the nuclear industries, where it is mandated.

Closer integration of control and safety systems also allows statistical correlation of input values to control and safety systems. However, appropriate barriers, such as firewalls, must be maintained between the two domains to maintain the integrity of both the systems. Proper access protection and visual differentiation between them should be provided to ensure against willful or inadvertent corruption by engineering or operation staff.

Flexibility and scalability. TMR (2003) and Duplex (1002D) systems are the most commonly used safety systems. However, other architectures, such as Quad (2004D) are now offered by safety system suppliers. Users are now looking for systems that offer configuration flexibility, where they can put together two or more safety controllers to get the required SIL level protection and availability, ideally on a loop-by-loop basis.

Safety systems should be more scalable, where one controller will handle a limited number of I/O, but will work together with other controllers to handle much larger applications.

Enhanced function blocks. Safety systems usually provide facilities for simple sequencing (usually without looping), allowing orderly shutdown of a process on detection of a failure condition. Normal startup and shutdown procedures are usually carried out manually or by the control system, with little role for safety systems.

Incorporating these functions in a safety system with enhanced function blocks can significantly reduce risks. Enhanced function blocks will also make it easier to configure tasks for monitoring trip levels, deviation percentage, pretrip alarm and degradation behavior. They will make it easier to bypass specified alarms during startup.

Recommendations. Look for a safety system that incorporates I/O components in its overall design and offers close integration with control systems, with effective barriers that ensure their integrity. Use certified field instruments wherever possible, which will reduce your burden on checking their suitability for safety applications. Check for features, such as scalability, flexibility and function block capabilities. **HP**

The author is a vice president of ARC Advisory Group. His areas of focus include batch control, safety and security on process industries. Mr. Ghosh has presented and published numerous papers in these subjects including a recent study entitled "Safety and Critical Control System Worldwide Outlook." He has over 30 years of experience in process control in the chemical, petrochemical, aerospace and mining industries. He is a member of the ISA/SP88 and IEC WG11 committees. Mr. Ghosh is a graduate of Delhi University, India, and has a diploma in advanced studies in control engineering from Cambridge University, UK. He can be reached by phone at (781) 471-1121 or by e-mail at aghosh@arcweb.com.