Integrated safety
How a simpler system can increase effectiveness

Throughout oil and gas operations in the Gulf of Mexico and the U.S. Southwest, safety systems that have been working since the 1970s and '80s are reaching the end of their already extended life cycles.

Spare parts are becoming harder to find and stock, and original equipment manufacturers (OEMs) are easing away from supporting systems that are two and three generations old.

Safety systems are often perceived as costly technology that requires complex engineering. Because existing systems have been in place for so many years, it's often difficult for some companies to justify budgets for new systems, sometimes ignoring or minimizing their value to the plant operations.

But safety standards and certification requirements have changed over the years. So have approaches to the design and implementation of safety systems – a fact that affects not only the replacement of aging systems, but also the selection of safety and control systems in new facilities.

Traditionally, for example, the required Safety Integrity Level (SIL) has often been achieved through complex system architectures that emphasize redundancy and isolation from process control systems.

But that approach creates a different set of issues that affect not only safety but also operating costs. First, it results in complex systems that can be more difficult to operate and more expensive to maintain, says Luis Duran, Product Marketing Manager for Safety Systems at ABB.

It's harder for operators to do their job when they must be trained on multiple interfaces. In addition, when process states are changing quickly and operators most need instant access to information, it may be difficult to identify the relevant data in a timely manner, much less respond to it effectively.

"I believe in technology, but I also believe in the function of people," Duran says. "It's important to consider the human

element in the design of safety systems. You can have an instance of operators working to reduce pressure in a vessel when the safety system kicks in. So the pressure may drop, but the operators may not have any idea if it's a result of their actions or something the safety system did."

A common approach to resolve such circumstances is the development of a custom interface that combines information from the safety and process operating systems. It seems simple enough, but it's not "plug and play" technology. While trying to address one set of issues, this solution can create new ones. Such interfaces are notoriously expensive in both initial and life cycle cost; and each is a custom development, so there is no assurance the interface will ever work as well as intended. They also can create gaps in accountability that are difficult to identify and resolve.

As an example, Duran points to the need to follow a Functional Safety Management System – both in the development of the interface (including design documents, validation and verification testing, etc.) and later while it's in operation, when there is a need to synchronize a safety system database with that of the process control system. "If there's a change to the data map on one side, who maintains it on the other side to assure the process control system is showing what's actually happening?" Duran asks. "With a custom interface, you gain visibility so the decision-making should be better. But then you also introduce entirely new issues, things like management of changes, version control, maintenance, access control and security. You create a lot of gray areas, and in safety systems there just isn't room for ambiguity."

There is another approach to managing these issues: Integrated safety and process control. In such a design, the safety system works independently of the process control system, but has been designed specifically to allow high levels of visibility and understanding to be delivered to operators through the control-system interface.

The concept isn't new; ABB installed the first such large-scale system in 1984 on a North Sea oil platform, and has introduced four subsequent generations of technology – the latest being its 800xA High Integrity system in 2005. But the concept of integrated safety is still often misunderstood.

"There can be confusion about what this really means," Duran cautions. "It doesn't necessarily mean you're mixing process control and safety. You're maintaining the independence of each system. There are still two independent layers of protection. But it's a functional independence."

Hallmarks of an integrated safety system include:

- A process control system designed to enable integration through such fundamental features as open standards and Aspect Object technology – which allows system components to be easily recognized for fast installation and smooth data transfer
- A safety system – designed and certified according to the functional safety standards and best practices – that feeds data seamlessly to the process control system
- Field devices and instrumentation built around open standards for improved flexibility, effective bidirectional movement of data and reduced system life cycle costs
- Built-in intelligence to present all data to operators through a single interface in a way that increases their visibility, knowledge and control
- Testing, validation and finally certification to all necessary standards

Functionally, the advantage of such a system becomes clear, Duran says. “From the operations standpoint, the operator can monitor what’s happening in the regular process control and, when a situation arises that calls for some kind of action, he can look for a holistic solution. You can take action before it becomes a safety issue. And if it does become a safety issue, you have more ability to keep track of safety mitigation as it is happening.”

There are other advantages as well.

Cost: An integrated safety system can be less expensive to own and operate. By reducing duplication of some aspects of the independent networks – to whatever degree is desired by the user – equipment, training and development time are all trimmed. Other cost savings include elimination of the safety-system interface and ongoing maintenance of separate systems.

Security: In the case of ABB’s System 800xA, access control and security are built into the system as an off-the-shelf set of features, including user privileges, user action validation and a common audit trail. It also includes such extended capabilities as write protection, SIL access control and authorization, bypass management, and override mechanisms. The result is a robust set of security controls that apply uniformly across all systems.

Engineering: A common engineering environment for both the process and safety systems simplifies the work that engineers do. It reduces training costs and expenses related to problem-solving between disparate systems, and may improve response time when troubleshooting. Of course the safety components of such an engineering environment must also follow the standards and adhere to the design, testing, validation and certification of the safety system.

Duran emphasizes that the degree of integration is flexible. The end-user can decide how much separation to maintain between safety and process control; even if fully segregated systems are utilized, many of the functional benefits above can still be achieved by using an integrated technology platform such as System 800xA. As an example, he points out that potential common causes are analyzed and minimized during the design phase by the development team, and independently reviewed by the assessor (such as TÜV) during the certification of the product – effectively making the system smarter and safer from the day it's turned on.

Further, integrated testing is performed during the design validation and verification test, which includes network security as part of the test protocol. Duran points out that version control, compatibility and interoperability testing are included in the release procedure.

The result is a set of common best practices can result in implementation of an integrated safety system that costs less, works better and even extends the capabilities of the process control system.

"As safety systems get replaced, or as new projects are developed, there is an opportunity to decide how you want to address safety in your operation – not just today but for the next 20 years," Duran says. "With an integrated safety system, the strategy is very simply to provide an operating environment that runs better at less expense for a longer period of time."

For more information please contact:

Stephanie Jones
Oil, Gas and Petrochemical
ABB Inc.
3700 W Sam Houston Pkwy South Ste 600
Houston, TX 77042 USA
Phone: +1 713 587 8404
E-Mail: stephanie.m.jones@us.abb.com

www.abb.com