Integrated safety

Integrated safety systems: keeping it safe

Kristian Olsson

Safety is paramount in the operation of any plant. It goes without saying that any threat to humans is unacceptable. The implications of safety can, however, reach beyond the basic protection of people and equipment. For example the negative publicity over a safety-related incident can have far-reaching repercussions for the company involved and in some cases even for the entire industry.

With the increasing complexity of processes, and different manufacturers supplying different systems within the plant, ensuring an overall high level of safety can be challenging. ABB believes that the safety system of the future is no longer an “add-on”, that is designed and supplied separately from the rest of the plant or process, but an integral part of it.

ABB’s Industrial IT System 800xA High Integrity safety system is an integral part of the company’s System 800xA offering of control systems.

Growth projections by the ARC advisory group indicate that the global safety systems market will continue to grow by approximately 12.5 percent annually until 2012 [1]. The booming demand comes primarily from the oil & gas and petrochemical segments, and is further augmented by the tightening of safety regulations and the worldwide adoption of IEC 61508 and IEC 61511 as "best practices" in non-traditional safety industry segments.

Safety systems are no longer exclusively deployed in traditional markets and applications such as fire and gas applications or in emergency shutdown systems in the oil & gas and the chemical industry. Demand is increasing in other sectors such as the power generation, pulp & paper, mining and even semiconductor industries, with applications ranging from traditional boiler/burner management systems to hazardous-materials handling and asset-protection applications.

By nature, a safety system constitutes a critical part of any plant-automation system.

Besides the overall drive towards more stringent regulations and the growing acceptance of the IEC 61508 / IEC 61511 standards, broader deployment of safety systems is primarily motivated by increasing concern in the public domain for safety and environmental aspects (resulting in reputational risk for the operator) and as a means to reduce premiums (when insurance companies use such standards to evaluate and benchmark a plant's risk-reduction measures).

ABB in safety systems

Having begun development of its first safety system in 1978 (which went online at the Statfjord B platform in the North Sea in 1979), ABB has gained almost 30 years of experience with safety systems. ABB enjoys a unique position among safety suppliers due to an early strong presence on the Norwegian continental shelf, where national safety standards were developed and implemented long before more recent international standards were formulated and accepted.

During its long presence in the market, ABB has produced several generations of safety systems characterized by varying technical solutions. These range from the Safeguard family of systems developed in Norway, through the triple modular redundancy (TMR) type Plantguard system to the most recent addition: the modular and scalable 800xA High Integrity system, which is part of the System 800xA portfolio.

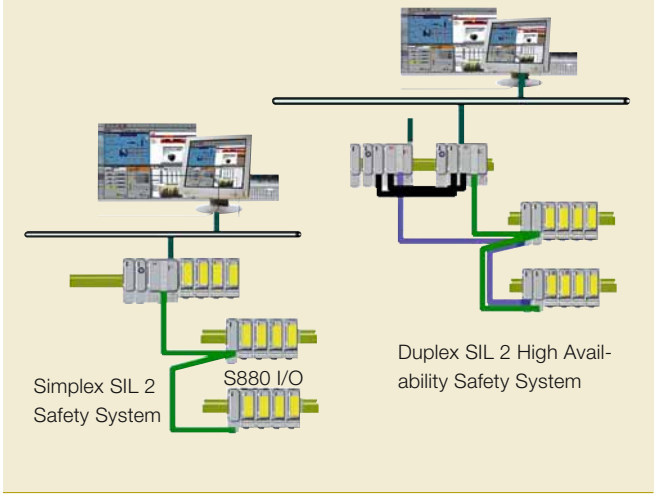
The 800xA High Integrity system belongs to the latest generation of integrated safety systems, ie, a safety system capable of being tightly integrated to a regular process-control system. ABB is proud to have been delivering integrated safety systems for close to 25 years, with experience dating back to the implementation of an integrated safety system on the Gullfaks A platform which went online in 1984.

By nature, a safety system constitutes a critical part of any plant-automation system and as such can require access to qualified support at any time – regardless of its location in the world. ABB's highly developed local presence on all continents with skilled safety engineers offers end users critical around-the-clock support that helps maximize plant uptime. Additional customer confidence is gained through a global process to achieve third-party accredited certification by TÜV Rheinland, for compliance to IEC 61508 and IEC 61511, currently underway at 16 local ABB system delivery and support organizations worldwide [3]. ABB safety system installations in well over 45 countries around the world are a further testimony to a strong local presence and

well-distributed competence throughout the organization.

As a supplier of safety products, ABB is facing a challenging balancing act in striving to further develop its safety-systems offering to better meet customer demand and enhance customer value while at the same time maintaining a stern view on compliance issues. For ABB, safety remains paramount. Development techniques utilizing the V-model[1] , strict coding guidelines, separate development teams (ie, diverse implementation) and a strategy of diverse technologies ensure a structured approach throughout the entire development process.

1 Simplex and duplex safety systems



Safety products can today be designed to achieve reliability levels meeting specifications set by international standards without resorting to complex hardware-redundancy schemes.

Continuous supervision by the third-party independent certification organization TÜV provides additional end-user confidence.

Converging market requirements

Over recent years, as the implementation of safety systems has become increasingly frequent – or mainstream – and end users have begun to fully appreciate the possibilities and limitations of such systems, the pressure for their further enhancement has risen. End users in pursuit of such goals as reduced cost of ownership, improved operational excellence and increased engineering efficiencies are driving a transition from traditional stand-alone safety system practices towards an integrated approach, seemingly in agreement with independent research bureaus such as ARC [4]. Simultaneously, a strong influence from international standards and a growing safety concern among various third-party interest groups is driving safety-product and system suppliers to incorporate new ideas and requirements, while maintaining a vigilant approach to compliance issues.

The framework of IEC 61508 and IEC61511 provide suppliers with clear guidelines and best practices on developing and optimizing their safety offering. It also offers end-users the means to efficiently benchmark system risk reduction capabilities, albeit without absolving them from their final responsibility for the safe operation of the plant. By requesting an SIL2- or SIL3-rated safety system, an end-user is getting a clearly defined level of risk reduction.[2]

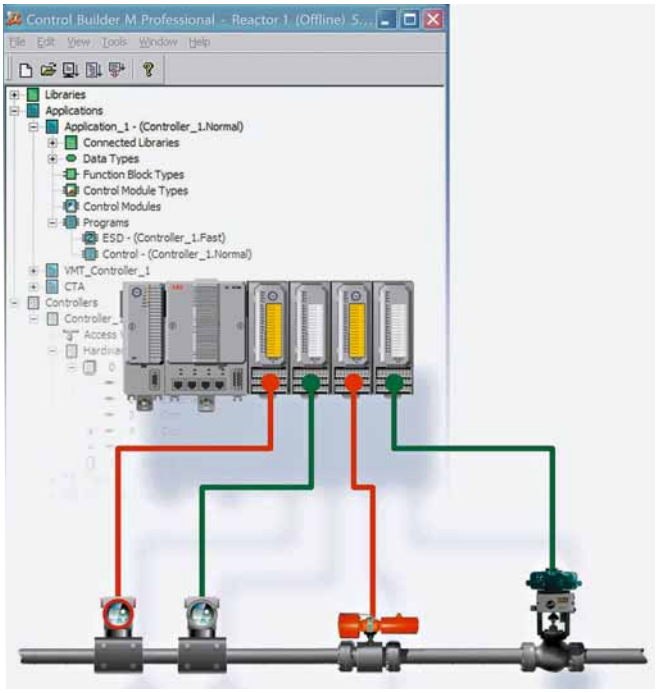
Safety systems were historically designed as completely standalone systems in which risk reduction was ensured by hardware redundancies and the independence of the process control and safety systems. Progress in software and hardware design, as well as manufacturing techniques, provides increased hardware reliability as well as a near 100 percent diagnostic coverage. Safety products can today be designed to achieve reliability levels meeting specifications set by international standards without resorting to complex hardware-redundancy schemes. As a result, simplex and duplex 1 modular and scalable integrated control and safety systems

Footnotes

[1] The V-model is a project management structure for IT-system development. The name derives from the commonly used V-shaped depiction, with definition steps along one leg and the corresponding testing steps on the other.

[2] Safety integrity level (SIL) is a relative level of risk-reduction, with SIL3 being the highest level typically found in the process industry

have been developed that do not compromise safety or continuous plant operation [5]. While still fully compliant to international safety standards, these systems have greater commonalities with regular process-control systems and are hence well suited to integrated solutions. As a result, safety systems are now less likely to be purchased separately but are rather becoming critical and integrated components of complete automation solutions. This market trend is a prime differentiator setting suppliers of integrated safety systems apart from more traditional providers of separate offerings.



Despite increased dependence on ever more powerful process-control and safety systems, the human aspect remains an integral part of any plant's operation. Operators, engineers and maintenance personnel constitute important contributors to overall plant risk reduction [6]. Consequently, the operational aspects of safety systems is an area currently being scrutinized. One business driver for this effort is a focus on reductions in operational costs throughout the system's lifecycle. However, while potential savings in operational cost are substantial, it is often easy to forget that there are also real safety concerns fueling this discussion. In an industry struggling with increasing complexity in its systems, a large number of suppliers contributing to any given plant combined with an aging competence pool, imply an increase in the risk of safety-critical mistakes. An obvious countermeasure is a reduction in both system complexity and the number of systems employed – enter integrated and similar process-control and safety systems.

Many new safety systems offer an increased level of integration and scalability. These are designed to facilitate optimized system design, efficient engineering, operations and maintenance while also allowing the user to tailor system design and integration concepts to meet plant-specific functional safety policies. Properly integrated safety systems can offer ways to not only reduce cost of ownership, but also, more importantly, to ensure safe operation of the system. Engineering efficiencies, improved understanding of the system and support can have a direct impact on bottom-line performance and safe plant operation.

Despite increased dependence on ever more powerful process-control and safety systems, the human aspect remains an integral part of any plant's operation.

Many suppliers of major process control systems offer integrated safety systems to complement their DCS[3] offering. However, there are subtle, but important, differences in the levels of integration that are supported [7]. Some solutions are more integrated than others, offering a differing scope for reduction in cost of ownership.

System 800xA High Integrity

The SIL2-certified 800xA High Integrity controller (logic solver) and associated I/O subsystem was released in late 2004. More than 1,000 controller units have been delivered to date in more than 35 countries.

Based on further developments released during 2008, the 800xA High Integrity platform is now SIL3 compliant, with certification being expected in late 2008. This will further enhance its range of application in the marketplace. Although the majority of safety-system applications only require a SIL2 rating, it is common practice among end-users to nevertheless specify an SIL3-certified system to ensure flexibility should a SIL3 requirement arise in the future. The 800xA High Integrity belongs to the newest generation of scalable and modular safety systems. The latest SIL3-compliant version is based on a system configuration known as a 1oo2D system where the "D" stands for diagnostic, indicating the significant internal diagnostic measures in place to detect failures. The system is SIL3 compliant in a single configuration. Redundant configurations are used to increase availability, and safety is ensured regardless of the configuration.

It should be noted that while 800xA High Integrity is an integrated safety system, this is only one of several possible configurations. The system has been designed from the outset to be able to operate as a standalone safety system, and integration to a process-control system is only one of the possible options available to an end-user. Based on current market trends, more and more end-users are moving towards integrated systems and looking to tap into the potential benefits. Based on the large commonalities to – and true integration with – the process-control portions of the overall System 800xA product family, end users of 800xA High Integrity are able to enjoy significantly reduced cost of ownership as several key cost drivers are removed or reduced when implementing integrated safety systems.

Footnote

[3] DCS: distributed control system

Engineering time and cost is lowered through a common engineering environment for process control and safety, enabling more efficient work procedures throughout the system's life cycle. These range from initial system and application engineering to commissioning and subsequent modifications as the system is tuned and possibly expanded to meet future requirements.

Supported by a common sequence of event- and alarm-handling functions, operators are able to analyze hazardous events as they unfold and make key decisions that can potentially prevent or significantly mitigate the consequences thereof. Should an event actually take place, the same functionality, with its millisecond accuracy, constitutes a powerful tool during post-mortem analysis.

An extensive array of built-in and configurable access and by-pass management functionalities allows tailored solutions for any plant to manage the interaction of both operators and maintenance crews with the safety system, without unduly influencing safe plant operation or causing unwanted tripping.

With largely similar equipment and software tools being in place for process control and safety systems, overall training required is reduced, understanding increased and complexities removed – again resulting in reduced total cost of ownership throughout the lifetime of the system.

Factbox Safety-related areas covered by ABB Global Consulting

- Process safety
- HAZOP
- Process hazard review (PHR)
- Hazardous area management – ATEX/DSEAR
- Human factors
- Alarm management
- Functional safety
- Functional safety management systems (certified by TÜV)
- SIL determination and achievement
- Legacy system evolution
- Safety instrumented systems (SIS) implementation

An area increasingly being explored is the possibility of leveraging top-level capabilities such as the information management or asset management functionality on System 800xA, and implementing these powerful tools in a safety context. Furthermore, it should not be forgotten that safety is part of any automation life-cycle plan where an existing process-control system is gradually upgraded and evolved to use more System 800xA components. Many existing plants are coming under pressure to implement risk-reduction measures in line with current standards, or can benefit from lowered insurance premiums by including safety systems into their overall automation solution. 800xA High Integrity is ideally suited to be added to existing plant automation solutions whenever System 800xA is introduced.

A one-stop shop

While controllers and I/O subsystems typically come to mind when discussing a safety system, it is important to remember the many other components that are involved in any safety-critical loop; from the initiating element (the instrument) to the final element (the actuator) and everything in between.

ABB's total offering includes safety-certified instruments, positioners as well as expertise built during decades of safety-system implementations.

ABB can provide a wide range of SIL-rated sensors, valve positioners and actuators. Various solutions are available: These range from high-integrity transmitters with full redundancy designed and certified by TÜV according to IEC 61508 requirements, to standard transmitters with enhanced internal diagnostics to improve reliability. The positioners are available with a shutdown module allowing the control action to be overruled if required. All of these possibilities include third-party calculations and evaluations of safety performance to enable loop risk reduction assessments.

The growing ABB Global Consulting organization considers safety consulting a key offering and is continuously working to meet customer requirements, addressing industrial plants and processes in all phases from planning, through operation to decommissioning. Consulting capabilities cover all project and product phases and the full scope of safety issues from the management level to the shop floor Factbox.

A truly integrated solution

ABB, with its almost 30 years of experience in the industry and a highly competitive safety systems offering, is ideally placed to meet customer requirements and expectations for the new generation of integrated safety systems. System 800xA, featuring the 800xA High Integrity safety system constitutes a comprehensive and cohesive plant automation solution for all applications; a truly-integrated safety system where functionality and safety have been perfectly balanced to allow end-users to minimize overall cost of ownership without compromising safety.

Kristian Olsson
ABB AS, Safety Center of Excellence
Oslo, Norway
kristian.olsson@no.abb.com

References

[1] Safety and Critical Control System Worldwide Outlook, Market Analysis and Forecast Through 2012, 2008, ARC Advisory Group.

[2] Complete Control And Safety For Statoil Sleipner Platform, ABB Project Profile 3BNP000565R0001.

[3] **Nunns, S. R., Prew, R. W.** (2008). Safe and sound. *ABB Review Special Report Process Automation Services & Capabilities*, 30–34.

[4] Business Issues Driving Safety Systems Integration, 2006, ARC White Paper, ARC Advisory Group.

[5] Reduce Risk With A State-of-the-Art Safety Instrumented System, 2004, ARC White Paper, ARC Advisory Group.

[6] Out Of Control: Why Control Systems Go Wrong And How To Prevent Failure, UK Health and Safety Executive.

[7] Business Issues Driving Safety Systems Integration, 2006, ARC White Paper, ARC Advisory Group.