Pedigree ensures reliability in automation

Roger Prew Safety Consultant, ABB Limited, Howard Road, Eaton Socon, St Neots, Cambs PE19 8EU,
Tel: 01480 475 321; Fax: 01480 218 361; Email: enquiries@gb.abb.com; Web: www.abb.com

Roger Prew, Safety Consultant at ABB, argues that the development of international standards underpinning programmable integrated automation systems ensures safety.

AC 800M controllers, field devices, I/O modules and field actuators are SIL rated

Last March an explosion at the Texas City oil refinery killed 15 people on site and injured 100 more. This happened in a society acutely aware of industrial hazards, in an industry that is highly regulated, where modern safety controls are in place, and where competent professionals are employed!

Incidents such as this may mean reviewing the regulations to determine if changes are needed and the investigation will examine this, but more likely the company will need to review its own procedures and systems against the current regulations and standards to ensure they comply. Companies continually need to utilise their experience in ensuring safety considerations remain of paramount importance. However, lessons learned from this sort of incident are enormously costly hence it is essential that the industry develops new techniques and technologies to achieve safe operation of hazardous process based on sound and well considered experience.

Programmable electronic Emergency Shutdown and Fire and Gas protection systems are widely used to reduce the risks of such events to acceptable levels, and the debate about the integrity of different system architectures has been going on since they were first introduced in the 1970s. The current debate about the integration of Safety and Control functionality is just as passionate! Some will find cause to argue against the trend towards integration, but this paper explores one company's approach to the subject. An approach based firmly on experience going back over 20 years.

The existing international standard covering programmable electronic safety systems, IEC 61508, is based on the findings of an IEC committee that was set up in 1995 to produce a truly international standard. This aimed to bring together the DIN standards that were gaining recognition in Europe, Middle East and Asia with the newly emerging SP84 standard in the USA.

The committee recognised the strength of both the existing DIN and ISA standards in addressing the integrity of the programmable system, and set about bringing them together into a single consistent guidance document. The intention was to extend the scope to cover the complete safety loop including field devices and to cover the full life cycle, from design concepts through operations and maintenance to final decommissioning. IEC 61508 was fully approved in 2000.

IEC 61508-2 recognises that safety and non-safety functions can reside in the same system where "functional separation" is maintained. If it can be shown that the implementation of the safety and non-safety applications are independent, ensuring that any action, including failure, of a non safety-related function cannot cause a dangerous failure of any safety-related functions. Physical separation into different systems from different suppliers, with different communications and different programming tools is no longer necessary to meet the requirements of the standards. Modern development techniques involving the use of high integrity computation and firewalls allows higher levels of integrity can be designed in from the out-set. If the new design builds on experience from the previous generations high confidence levels can be achieved.

It is often asked whether new standards mean safer products. The answer has to be yes! The new standard, in addition to explicit definition of the way reliability figures are calculated and used, defines the procedures under which high integrity software is structured, coded, tested, complied and processed. The Functional Management procedure under which a modern system is developed provides greater confidence to the user that the design is sound and totally auditable. If anything does go wrong it can be traced and corrected with the upgrade being fully tested against the Safety Requirement specification and implemented according to the standard. The standard not only relates to the product being developed but also defines the processes under which a safety system is designed in the first place plus the way the specific application is implemented.

A system developed from the outset under an IEC 61508 certificate will attract greater confidence in the market than one that pre-dates the standard.

That's not the end of the story! The IEC 61508 standard not only defines the integrity characteristics of the complete safety function (end to end) but also how it should be implemented, operated, maintained and tested for the full life cycle of the system (design through to decommissioning). A process application implemented on a fully compliant system by competent engineers using compliant procedures must ensure that risks are reduced to an absolute minimum.

Getting to this point has been a process of continual evolution. Programmable electronic systems have been used for control and monitoring application in the process industries since the 1970s and today the use of computers, PLCs, and DCS to control and protect processes is commonplace. Initially the use of programmable systems was confined to control and monitoring functions with solid-state, pneumatic, relay or hard electronic safety back up providing any protection considered necessary.

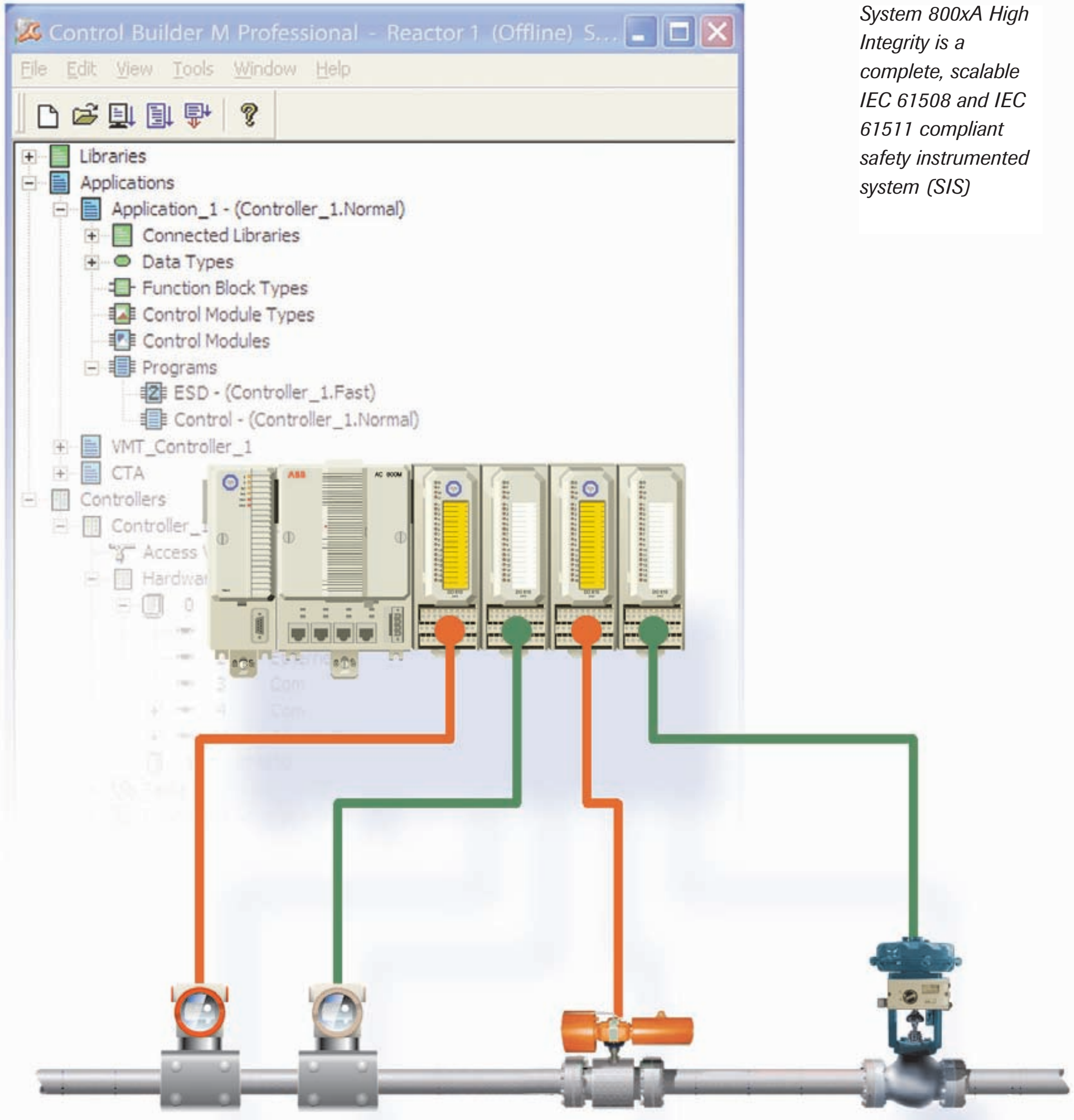
As confidence in the new technology grew and the tremendous advantages and flexibility of programmability became clear, the industry started to look to the regulators for some guidance on how these systems should be used, especially for safety applications. The regulations have developed from that point to date where IEC 61508 extends the standard requirements beyond programmable electronic systems to include the complete control loop. It includes field equipment and establishes fundamental requirements for the processes and competencies needed to design, implement, support and maintain such systems during their complete lifecycle.

High Integrity Control requires two main characteristics – High Availability (reliability) and Fail Safe Action (deterministic failure action). These two requirements remain core components of today's systems.

Availability is a measure of reliability (how long will it run before going wrong) and can be assessed from the reliability data produced for each component part or from statistical field returns data. Fail Safe Action is a system's ability to shut down in a pre-determined way under any failure mode. True Fail Safe action was quite easy to achieve in relays and even hardwired electronics, but became more difficult when software based programmable systems were introduced.

Early dual redundant and TMR (Triplicated) systems used

ABB's distributed control system (DCS) gives personnel from all areas of manufacturing or process plant access to customised information according to their job functions


Control Builder M Professional - Reactor 1 (Offline) S...
File Edit View Tools Window Help
Libraries
Applications
Application_1 - (Controller_1.Normal)
Connected Libraries
Data Types
Function Block Types
Control Module Types
Control Modules
Programs
ESD - (Controller_1.Fast)
Control - (Controller_1.Normal)
VMT_Controller_1
CTA
Controllers
Controller_
Access
Hardwar
ABB
AC 800M

System 800xA High Integrity is a complete, scalable IEC 61508 and IEC 61511 compliant safety instrumented system (SIS)

duplication and triplication of the electronics to enhance both Availability (by adding fault tolerance) and Fail Safe action (by adding voting). The architectures were often presented as fulfilling both requirements, but unfortunately, they are mutually exclusive. A redundant system that uses its duplication for voting is NOT fault tolerant and likewise if duplication is used to achieve fault tolerance it does not enhance the determinism of the system. Today's generation of integrated safety and control system separates these two features by addressing Fail Safe action by rigorous "failure modes and effects" analysis during the design stages and electronic design that is effectively covered 100 per cent by diagnostics. Availability (which is inherently extremely high in modern electronics) can then by increased by conventional fault tolerant structures.

Process systems are now selected on their ability to "manage assets" in an efficient and cost-effective way. Asset management and optimisation requires the collection, management, storage and analysis of vast amounts of data collected from sources such as direct measurement, fieldbus links to field devices, and vibration and health monitoring devices. This data is then used to make decisions that will improve process efficiency, reduce waste, minimise maintenance time, reduce carbon emissions or whatever happens to be the primary issue at the time.

Systems such as System 800xA from ABB can integrate information from a multitude of different sources and in many formats. Because it can do this, and organise that data in different ways, depending on the most relevant factors this puts the system at the leading edge of asset management technology.

Safety is "just another asset" that needs management. It is equally valid to monitor the characteristics and diagnostics of a shut down valve to determine its servicing requirements as it is to collect trip data alarm data to maximise its proof test cycle and ensure full compliance with safety standards.

On-line Functional Safety Management (FSM) tools, that form part of the Asset Management suite analyse and document data, collected on all aspects of every safety function. It can store the detail of the SIL assessment for future review, recalculate test cycles against changing duty and updated the database with new more accurate reliability data as it becomes available. Analysis of actual trip and alarm data enables the Safety requirements and performance of each safety function to be used in the optimisation calculation. More importantly they are recorded, documented and presented in a way that references the clauses of the standard, making compliance easy for the regulator to audit. An automated FSM system enables you to sleep easy.

The ABB System 800M HI receives its pedigree from a range of different architectures and technologies supplied by ABB since the first ASEA safety PLCs supplied to the North Sea in 1979. ABB's experience encompasses dual redundant architectures (Master Safeguard) Triple Modular Redundant (August Triguard) plus inputs from H&B, Satt and Elsag Bailey high integrity technologies spanning more than 20 years, and with several thousands of applications worldwide. 800xA HI successfully moves the architecture from "separate systems with common parts" to "full integration into a single system". This has been achieved only because System 800xA was designed from the outset to meet the requirements of the safety market place and the current safety standards. It definitely is not a "modified DCS" or a DCS with added safety functionality. It is a SIL certified control system that can combine Safety and control in a single node, and maintain full functional separation.

To complete the package all of ABB's Safety Execution Centres have embarked on a competency program aimed at certifying the projects organisations to meet the standard and ensuring properly qualified engineers carry out 800xA HI systems designs. ABB's System 800xA design teams operate under audited Functional Safety Management processes.

Experience is important but it is essential that we continue to build on what we already know, develop better methods, understanding and higher levels of professionalism. We cannot afford mistakes like Texas City!