Integrated but separate

Advances in integrated and safety control

Roger W. Prew

End users of older automation systems essentially had to invest in two separate systems: a basic process control system and a separate safety instrumented system. Nowadays, suppliers differ in their opinions about the acceptability of implementing safety and basic process control functions in a single system with common processors. Some argue that integration reduces overall integrity, while safety, which faces ever-increasing regulation, is compromised.

The debate about integration is set to continue but one company that has been more constructive than vocal about this topic is ABB. As an established supplier of safety systems for hazardous processes since 1979, ABB launched the unique 800xA HI (High Integrity) combined safety and control architecture as part of the successful 800xA Extended Automation System. With this architecture, ABB has proven that true integration is possible, and functional separation of control and safety is ensured using modern high-integrity processing techniques, firewalls and active diagnostics. The system also is fully compliant with the requirements of the international functional safety standards.

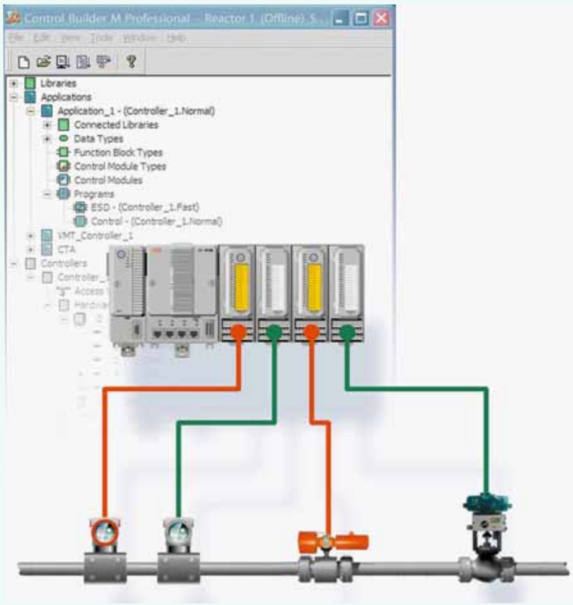
Today's hardware and software technologies, in the hands of professionals operating under rigorous functional safety management procedures, can deliver new system architectures with higher levels of control and management functionality, and safety compliant integrity.

What are the advantages of integrating a safety instrumented system (SIS) and a basic process control system (BPCS)? For one thing, the lifetime cost of ownership of the system is significantly impacted, as are project design, engineering and modification costs. At the system definition phase, the flexibility of being able to transfer inputs and outputs (I/O) and functions between the SIS and the BPCS – without materially altering the system architecture – improves the efficiency of the design process and results in a more cost-effective solution. During system integration, this same flexibility ensures that the split between BPCS and safety matches the actual requirement and has not been forced into an architecture that was ordered many months earlier.

ABB's 800xA HI combined safety and control architecture has proven that true integration is possible, and functional separation of control and safety is ensured.

Cost savings arising from common configuration tools, communications networks, spare parts, maintenance, training, service and upgrades are obvious, but the biggest advantage is an increase in data access among the safety system, the distributed control system (DCS) application and process-management tools. Real-time connection of parameters between safety and DCS applications – only possible if the two applications are executed in a single common controller node – means that expensive field equipment and wiring can be shared, thus optimizing the physical architecture 1.

1 ABB's System 800xA HI enables an increase in data access among the safety system, and the DCS application and process-management tools


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_1
Access
Hardware

Moreover, full integration means that all data associated with the safety instrumented function (SIF)[1], such as the safety integrity level (SIL) calculation, system and field-device diagnostics, trip frequencies, trip responses, valve condition and so on, are available to the BPCS asset management system. In addition, the high-level data collection and analysis tools of a BPCS can be exploited in a common and consistent way by the SIS 2.

Regulations and standards

Process safety has gained corporate importance especially since the catastrophic incidents that occurred at Flixborough[2] (UK), Serveso[3] (Italy), Bhopal[4] (India) and on board the Piper Alpha[5] North Sea production platform. Now process safety expertise has extended into the general skill set of engineers and operators, and many industry-wide guidelines for process safety have been developed. The current industry standard for electronic and programmable systems, IEC 61508[6], is the result of concerted efforts by industry and regulators over the past 30 years. The global objective of such a standard is to ensure that proper risk reduction strategies are adopted by all industries with hazardous processes so that the incidents mentioned above can be prevented. This generic standard and the process industry's specific standard, IEC 61511[7], are essentially advisory. However, they are now considered "good practice" by regulators in the United Kingdom and other industrial countries, and also as a means of determining whether a reasonable practical level of electrical, electronic and programmable electronic safety (E/E/PES) has been achieved. The standards are used to benchmark installations and are, for all intents and purposes, considered mandatory.

IEC 61511 defines methods of assessing risks associated with a particular hazardous process and it determines the risk reduction the safety system(s) must achieve. The standard is prescriptive in that risks must be assessed and reduced to "as low as is reasonably practicable." It does not however prescribe what technologies and architectures should be used to achieve the reduction.

Footnotes

[1] A safety instrumented system (SIS) contains many safety loops or safety instrumented functions (SIFs), each with its own safety integrity level (SIL).

[2] See http://www.hse.gov.uk/comah/sragtech/caseflixboroug74.htm (Retrieved October 2, 2008)

[3] See http://www.chm.bris.ac.uk/motm/245t/245th/seveso.htm (Retrieved October 2, 2008)

[4] http://www.bhopal.org/whathappened.html (Retrieved October 2, 2008)

[5] http://www.answers.com/topic/piper-alpha (Retrieved October 2, 2008)

[6] IEC 61508 is the international standard for electrical, electronic and programmable electronic safety (E/E/PES) related systems. It sets out the requirements for ensuring that systems are designed, implemented, operated and maintained to provide the required SIL.

[7] The IEC 61511 standard refines the functional safety requirements laid down by IEC 61508 specifically for the process-industry sector. It provides guidance in the proper application of a safety instrumented system (SIS).

Current technologies

Many of the stand-alone safety systems currently available on the market predate the new IEC standards and employ a variety of technologies to achieve the high-integrity control required for safety applications. "High integrity" normally suggests a combination of fail-safe and fault-tolerant operation. Fail-safe ensures that if a fault occurs the system will react in a predetermined and safe way, whereas fault tolerance minimizes the likelihood of a failure that would prevent the system from performing its functions. These two terms often get confused! A fault-tolerant system may not be fail-safe. Just because it may be redundant or triple-modular redundant doesn't automatically make it suitable for safety applications. Also, a fail-safe safety system does not require redundancy to achieve its SIL. Redundancy is built in solely to improve system reliability and availability.

The 800xA HI safety system shares a common processing unit and other components with the DCS, and brings a number of significant enhancements to the overall BPCS package.

The 1oo2 dual, 2oo3 triple and 2oo4 quad systems available on the market today come from a design era that used redundancy and fault tolerance as a means of reducing the probability of a dangerous failure occurring. Today, dangerous failure modes can be completely eliminated and 100 percent diagnostic cover can be provided to protect integrity without resorting to duplication. The requirements of "fail-safe" for "safety integrity" and "fault tolerance" for "availability" can now be considered independently and used when and where they are applicable 3.

There is always much debate about the hardware reliability of electronic and programmable systems. However, modern surface mounted, high-integration electronics is considered extraordinarily reliable. In an SIS, the logic solver hardware is the most reliable element in the entire safety loop! More evidence can be found in some modern simplex systems where the mean time between failure (MTBF) figures are better than the last generation dual or triple systems. In fact, the triple and quad systems suffer from the law of diminishing returns on reliability in that the inherent failure rate rises in proportion to the increase in components and complexity.

A new generation of system

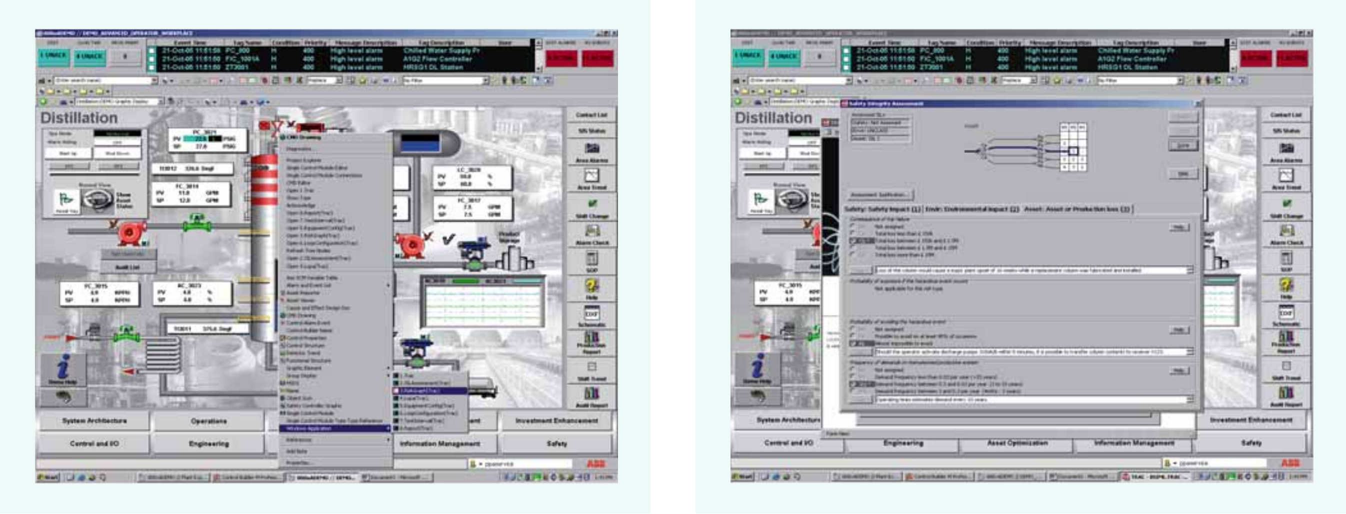
The new-generation 800xA Extended Automation System from ABB is flexible enough to either combine the control and safety functions within the same controller or keep the functions separate but within the same integrated network. Known as the 800xA High Integrity (HI), it is definitely not a "modified DCS" or a DCS with added safety functionality. Instead it is a system designed from the outset to meet the requirements of the safety market and the current safety standards.

Safety-related programs are compiled using a limited instruction-set compiler certified for 800xA HI safety programs.

Many people erroneously believe that as long as the calculated probability of failure on demand (PFD) is within the right band, the system complies. There are four key requirements that must be met for a safety-related system to meet the aforementioned standards:

- Reliability (PFD) is of course important and the figures for all subsystems that make up the safety function must form part of the certified data set so that the overall loop SIL can be assessed.
- The safe failure fraction (SFF), which is a measure of the ability of the system to detect and avoid dangerous failure modes, is also part of the certified data set.
- Any constraints or integrity advantage resulting from the complete system architecture must be assessed and the implications on the SIL rating documented.

2 Risk graph for a related safety function to protect against a hazardous event



- Finally, the systematic integrity of the system including the development processes utilized, the lifecycle safety management of the system, and the methods used to develop and prove high-integrity software must also comply with the letter of the standard.

A fault-tolerant system may not be fail-safe. Just because it may be redundant or triple-modular redundant doesn't automatically make it suitable for safety applications.

The development of the 800xA HI safety system addressed the above issues. The design teams operated under audited functional safety management processes and the design concept and detail was approved at every stage by TÜV (the TÜV Product Service is considered to be the foremost independent certification authority in the business) 4. A certification specialist on the team, helped by third-party consultants, steered the detail design continuously, confirming compliance with the requirements and the standards.

The 800xA HI safety system shares a common processing unit and other components with the DCS, and brings a number of significant enhancements to the overall BPCS package including:

- Higher BPCS reliability through:
  - Diagnostics – extensive diagnostic cover is a prerequisite for integrity.
  - Determinism – the safety model brings with it a deterministic execution model.
  - Integrity – this brings greater reliability and accuracy of measured values and control action.
- Faster communication between BPCS and SIS functions allows a higher degree of process-control optimization with respect to the actual safety boundaries (or safety distances).

Integrated but separate

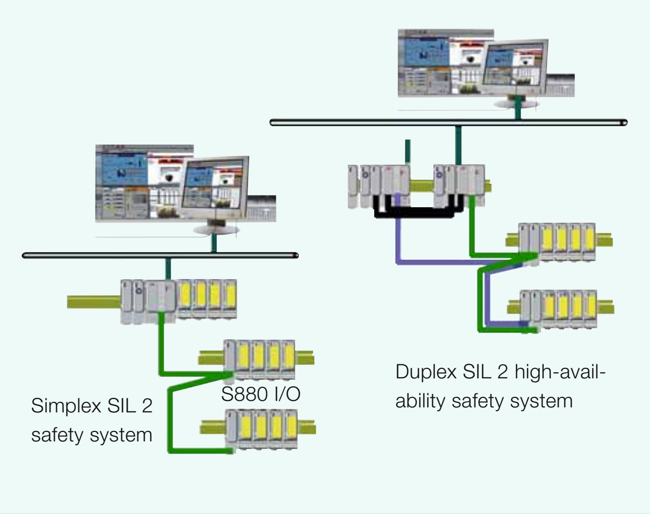
The debate about the separation of the safety function from the BPCS will no doubt continue. However, the IEC 61508 and IEC 61511 standards do actually recognize that safety and non-safety functions can reside in the same system if "it can be shown that the implementation of the safety and non-safety functions is sufficiently independent (ie, that the failure of a non-safety-related function does not cause a dangerous failure of the safety-related functions)" (IEC 61508-2 clause 7.4.2.3). The standards also require that the possibility of common mode-dependent failures is reduced to an acceptable level (IEC 61511 Part 1 clause 9.5.1/2).

ABB's new-generation System 800xA is faithful to these requirements. The modular nature of the new system meets the standard requirements for functional separation and common mode failures. Memory partitioning, separate execution contexts, firewalls and stack management techniques that come from the defense and high-integrity data-processing worlds ensure that safety and non-safety programs running in the same processing environment are actually separate and non-interfering. The integrity of the safety function is assured by limiting general communication with the man-machine interface (MMI) to read-only, and instituting a "safe write" function for overrides that can only be enabled by manual intervention at the controller. Peer-to-peer communications between safety and non-safety functions is strictly controlled to ensure integrity of the safety function. Additional cyclic redundancy checking (CRC) and relevance checking means the peer-to-peer network can be considered a gray channel.

The 800xA HI is a system designed from the outset to meet the requirements of the safety market and the current safety standards.

Detailed analysis was carried out against the layers of protection analysis (LOPA)[8] method of risk reduction. This analysis confirmed that the LOPA credits for protection functions, which are implemented in the DCS application and operate in either a combined control and safety node or a separate

3 System 800xA HI safety-system architecture



4 ABB's 800xA HI safety system is certified to the IEC 61508 and IEC 61511 safety standards, and approved by TÜV.

CERTIFICATE
No. Z10 04 12 29902 002

Holder of Certificate: ABB Automation Technologies AB

Factory: 51752

Certification Mark:

Product:

Model(s): 800xA Safety

Parameters:

Tested according to:

800xA node, are equivalent to those implemented in systems with totally different control and safety systems 5. The additional integrity gained from running BPCS applications in the 800xA HI controller outweighs the additional risks from possible common mode failures.

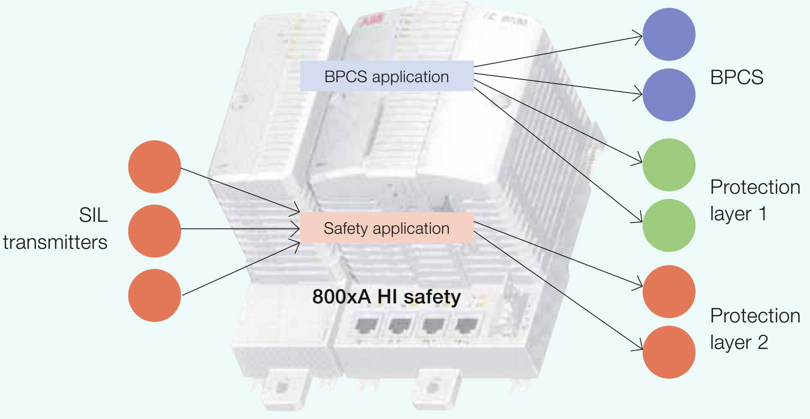
To the oil & gas markets, System 800xA HI offers a redundant architecture that can be independently implemented at the I/O level and at the operator level to add fault tolerance.

Safety-related programs are compiled using a limited instruction-set compiler certified for 800xA HI safety programs. During the compiling process, additional compiler test suites and CRC ensure the integrity of the compiled safety program. The block execution of the application during run time is verified for order, timing and discrepancy. Internal communications between processing elements and I/O are duplicated and double checked using proven techniques to ensure that all erroneous or unexpected messages are ignored. The use of diverse and dissimilar hardware in the I/O and processors, and a TÜV-certified real-time operating system (RTOS) in the safety module ensure that the System 800xA HI meets the integrity requirements of IEC 61511 on all counts.

Highest reliability and availability

The 800xA HI design is inherently fail-safe with near 100 percent diagnostic coverage even as a simplex application (ABB claims 99.9 percent SFF and there are actually no known dangerous undetected failure modes in the system). This is achieved by virtue of an initial hardware design intended to fully meet the requirements of SIL3 (Four SIL levels are possible, with SIL4 being the most dependable and SIL1 being the least)[9]. Hardware diversity in the I/O, local CRC and shutdown control, together with the unique processor/safety module architecture, eliminates common mode faults. In addition, audited failure mode and effects analysis (FMEA) and failure rates place the product within the top 6 percent of the SIL3 band. Audited PFD figures are published and based on a proof-test interval of eight years.

5 Functional separation



LOPA credits 1000 for the protection layer 2 implemented in SIL2 application, and 10 for protection layer 1 implemented in non-SIL2 application.

NB. This data is provided as an example. Actual LOPA credits achieved are dependent on the detailed architecture and function.

- Real and intermediate safety variables are internally transmitted to the BPCS application for control and display.
- Field transmitters may be optimized.
- Real-time BPCS control functions achieved using safety transmitter are data.

Audited FMEA and failure rates place ABB's 800xA HI SIS within the top 6 percent of the SIL3 band.

In the oil & gas markets, safety-logic solver systems are expected to (a) run without interruption for at least 15 years and (b) endure all sorts of upgrades, modifications and changes during that time. System 800xA HI offers a redundant architecture that can be independently implemented at the I/O, the processor and the operator-workplace levels to add fault tolerance – and hence high availability – to an already high-integrity system wherever it is required. This redundant system can also safely upgrade the system application online.

The debate about grassroots principles is set to continue, but history has shown that progress is being made by challenging the accepted view – addressing the problem from a different direction whilst complying with the standards.

Roger W. Prew
ABB Process Automation
St Neots, UK
roger.w.prew@gb.abb.com

Footnotes

[8] LOPA is a simplified risk-assessment method for evaluating the risk of hazard scenarios and comparing it with risk tolerance criteria to decide if existing safeguards are adequate, and whether additional safeguards are needed. See Primatech Inc. (2005). FAQ sheet – layers of protection analysis (LOPA). Retrieved October 2, 2008, from http://www.primatech.com/info/faq_layers_of_protection_analysis_(lopa).pdf

[9] For a more comprehensive explanation of SIL, see "Safe instruments" on pages 96–99 of *ABB Review Special Report Automation Systems* (2007).