

Optimized Performance Throughout System Lifecycle With Integrated Safety Systems

Kristian Olsson
Global Sales – Safety Center of Excellence
ABB AS
Ole Deviksvei 10, PO box 6359 Etterstad
0603 Oslo, Norway
Tel:+47 22872386
E-mail: kristian.olsson@no.abb.com

Abstract

Amidst the continued heated discussion on the pros and cons of integrated safety systems market demand - driven by the pursuit of reduced cost, operational excellence and engineering efficiencies - continue to fuel the inevitable integration efforts.

Advances in software and hardware design as well as manufacturing techniques enable near 100% internal diagnostic coverage and increased hardware reliability in turn removing the need for redundancy schemes to achieve sufficient reliability and Safe Failure Fraction levels. As a result, modular and scalable integrated control and safety systems have been developed without compromising safety performance. These systems do, while still fully compliant to international safety standards, have greater commonalities to regular control systems and are ideally suited to integrated solutions.

Having delivered safety systems for more than 25 years and with an extensive installed base ABB is a leader in the safety market. Through its System 800xA portfolio and more specifically the 800xA High Integrity offering, ABB continue to focus on delivering integrated safety systems solutions. System 800xA offers the truly integrated solution to facilitate an optimized system design, efficient engineering, operations and maintenance while also allowing the user to tailor system design and integration concept to meet plant specific functional safety management requirements. But while integrated safety systems surely are here to stay, the level of integration is not a black and white decision.

1. Introduction

Amidst the continued heated discussion on the pros and cons of integrated safety systems market demand continues to fuel the inevitable integration efforts. End-users, in pursuit of reduced cost of ownership, improved operational excellence, increased engineering efficiencies and more, are driving a re-think from traditional stand-alone safety systems.

Advances in software and hardware design, as well as manufacturing techniques, provide increased hardware reliability as well as near 100% internal diagnostic coverage. Safety products can be designed to achieve reliability levels meeting specifications set by international standards without resorting to hardware redundancy schemes. As a result, simplex and duplex modular and scalable integrated control and safety systems have been developed without compromising availability or continuous plant operation. These systems do, while still fully compliant to international safety standards, have greater commonalities with Basic Process Control Systems (BPCS) and are well suited to integrated solutions.

Despite increased dependence on increasingly powerful BPCS and safety systems the human aspect remains an integral part of any plant operation, for better or for worse. Operators, engineers and maintenance personnel constitute important contributors to overall plant risk reduction. Many new safety systems offer an increased level of integration to facilitate optimized system design, efficient engineering, operations and maintenance while also allowing the user to tailor system design and integration concept to meet plant specific functional safety policies. But while integrated safety systems surely are here to stay, the level of integration is not a black or white decision.

1.1 Market Drivers

Not surprisingly, the continued development of safety systems, is mainly market driven. In addition, the influence from international standards and a growing safety concern among various third party interest groups, is driving safety products and system suppliers to incorporate new ideas and requirements while maintaining a vigilant approach to compliance issues.

Despite a recently booming market a strong pressure to reduce capex expenditure and cost of ownership has been prevalent, very much setting the tone for development trends such as the emergence of integrated safety systems.

Another area coming under increased scrutiny is the operational aspects of safety systems, viewed by many as a strictly financially driven focus area which focuses on reducing operational cost throughout the system lifecycle. While potential savings in operational cost are typically substantial one often forgets that there are also real safety concerns fueling this discussion. In an industry struggling with increasing system complexities, a larger number of system suppliers in any given plant combined with an ageing competence pool the risk of safety critical mistakes is growing. An obvious counter-measure to negate this risk is a reduction in both system complexity and number of systems employed.

Integrated safety systems could offer ways to not only reduce cost of ownership, but also, more importantly, to ensure safe operation of the system. Engineering efficiencies, improved system understanding and support can have a direct positive impact on bottom line performance and safe plant operation.

2. Less Complex Solutions

Following the general trend of developing simpler, modular and more standardized systems many safety system suppliers have today shifted from Triple Modular Redundancy (TMR) type solutions, either own products or third party supplied, and are now mainly focusing on own simplex or dual solutions (typically 1oo1D or 1oo2D).

Suppliers of simplex/dual solutions argue that system reliability is guaranteed by improved and to some extent different mechanisms than was typically the case with previous generations. Improvements in manufacturing techniques mean that the surface mounted circuitboards of today are considered extremely reliable when compared to what was available a number of years ago. This, together with improved software based diagnostics, has reduced reliance on redundancy schemes to achieve required reliability. The improved hardware reliability is of course beneficial to any system regardless of complexity. However, TMR systems, with an inherently larger number of components, suffer from the law of diminished return proportionate to the increase in component count. A simplex or dual system on the other hand face the opposite where less components reduce the number of potential sources of hardware failures.

Implementation of internal diversity schemes have resulted in a reduction of dangerous undetected failures in favour of safe failures. Improvements in software design allow internal diagnostics and watchdogs to effectively provide near 100% diagnostic coverage to protect integrity without resorting to duplication or triplication.

Development techniques utilizing the V-model, strict coding guidelines, separate development teams and diverse implementation ensure a structured approach to avoid common mode failures throughout the entire development process. Supervision and guidance by third party independent certification organizations throughout complete development projects provide additional end-user confidence.

3. The Human Factor

Many of the debated pros and cons of integrated safety systems are “soft” and are often not easily quantifiable. Nevertheless, they constitute an important consideration when evaluating the overall performance of a safety system. A fact further compounded by the increasingly depleted competence pool which is due to an ageing and retiring workforce.

A commonly referred to publication¹ by the UK Health and Safety Executive summarizes primary causes of failure of safety systems as follows:

- Inadequate specification: 44%
- Changes after commissioning: 20%
- Design and Implementation: 15%
- Operation and Maintenance: 15%
- Installation and Commissioning: 6%

The publication points out that close to three-fifths of all sources of failure are built in before operation of the system has commenced. Improvements during specification and design stages of projects are required to reduce the number of failures.

However, according to these numbers, human error unquestionably plays a significant role in a majority of failures occurring during system installation, commissioning, operation, maintenance and subsequent upgrades or modifications. Safety systems with tools and functions supporting operators, engineers and maintenance personnel should therefore have a considerable potential to reduce the number of hazardous events and accidents.

4. Lifecycle Management

Most existing process automation systems were originally introduced as critical components of manufacturing infrastructure. End-user expectations on system lifetime have typically been in the range of 20-25 years. Due to the

¹ Ref: “Out of Control: Why Control Systems go Wrong and How to Prevent Failure”, UK, Health and Safety Executive

convergence of automation systems and commercial off-the-shelf technology the lifecycle cost and system lifetime have become increasingly difficult to predict and control.

The lifecycle management policy of a system or product supplier, while often forgotten, has therefore become an ever more important consideration when selecting a safety system. With the increasing pace of development resulting in increased R&D expenditures and higher profitability pressure in the corporate arena real concerns have been raised about long-term sustainability of system support not to mention continued system development. Suppliers, able to leverage from larger business volumes typical of BPCS systems, should be able to offer better long-term support and, perhaps more importantly, forwards and backwards compatibility as newer safety system generations are introduced.

This is also an area of increased importance considering today's modular system architectures where seamless system expansions, upgrades and retrofits should ideally be possible without compromising the intellectual property of the end-user, i.e. the process knowledge and application software.

Few suppliers today have a published corporate-wide lifecycle policy stating clear long-term guarantees in terms of support, availability of components and forwards/backwards compatibility, a fact that should be carefully considered during any supplier qualification process.

To compound the matter further, increased drain of the talent pool, i.e. retirement of skilled and experienced engineers, is placing end-users in a precarious situation. By minimizing the number of systems in use as well as system complexities the amount of training and skilled staff can be reduced resulting in improved operational performance and lower cost of ownership.

5. Integration Levels

Significant energy is being spent on debating the question of integrated safety systems or not, interestingly enough much less attention is devoted to closer inspection of the different levels of integration available with existing technology.

With current technology and systems a wide variety of separate, interfaced or integrated solutions are possible. Tailored solutions can be devised to meet plant and system specific requirements.

While the curve representing the level of integration between BPCS and safety systems is approaching the linear this paper will, for simplicity, look further into four basic system architectures and the inherent pros and cons of each system solution.

5.1 Different Suppliers and Systems - Separated

A system architecture based on completely separate BPCS and safety system from different suppliers, typically with no or very limited communication between the two systems, is considered by many as the original way to incorporate safety systems into the overall plant automation scheme.

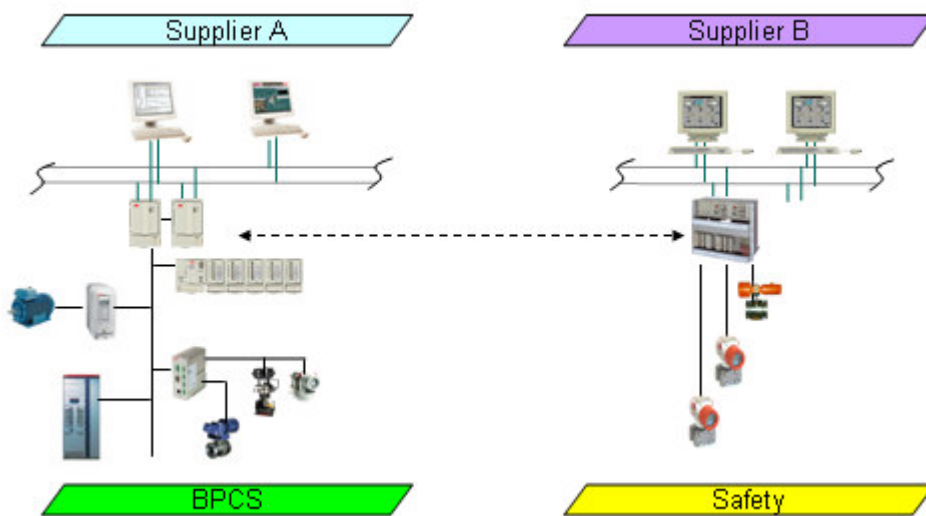


Figure 1 Non-Integrated system architecture.

Historically the main advantage of this approach has been the near total avoidance of common mode failures through physical separation. Furthermore, different suppliers ensure that the likelihood of a common mode failure is approaching zero as development of each system has been completely independent. By implementing BPCS and safety as two essentially separate systems there is little risk of systematic failures on a system level. However, it should be remembered however that every system in existence does have some form of common mode failure, e.g. through process/system design, environmental factors and maintenance procedures.

Safety systems used in this configuration are sometimes small and basic, constituting a “black box” to the user. This typically results in limited system understanding, trouble-shooting capabilities and operational performance.

Communication, if existing, between BPCS and safety systems can be non-standard or proprietary which may introduce unknown factors, that could potentially compromise safety performance unless properly analyzed and evaluated on a plant by plant basis.

Due to their different origins, operation and engineering of the two systems (BPCS and safety) are completely different, further ensuring the avoidance of common mode failures. However, this separation does mean that operators and engineers must work on two systems throughout the system lifecycle, in effect resulting in unnecessary double work. Engineering times would most likely be relatively long during upgrades and system modifications. Depending on the application the demand for operators to analyze information from several sources,

presented in various formats could give cause for operational concerns. Time to decision could increase and potentially reduce the operator's ability to prevent hazardous events from taking place or subsequently mitigate the impact of such an event. Training programs would have to encompass two completely different systems, demanding additional time and resources.

A final factor to be considered is lifecycle management and support. Increased efforts spent on maintaining two separate systems typically results in higher cost of ownership over system lifetime. Different suppliers of BPCS and safety systems present the user with the age-old problem of discerning areas of responsibility between several suppliers, a frustrating process, especially in time-critical situations, often resulting in slow and poor technical support.

5.2 Single Supplier with Different Systems - Top-level Integration

Another typical architecture is the result of an overall automation system delivery from a single supplier but with different BPCS and safety systems. Both systems are based on in-house products, but have been developed separately (or added to the product portfolio through external acquisition) without any significant commonalities. This offer advantages associated with a common supplier while keeping concerns regarding common mode failures at a reasonable level.

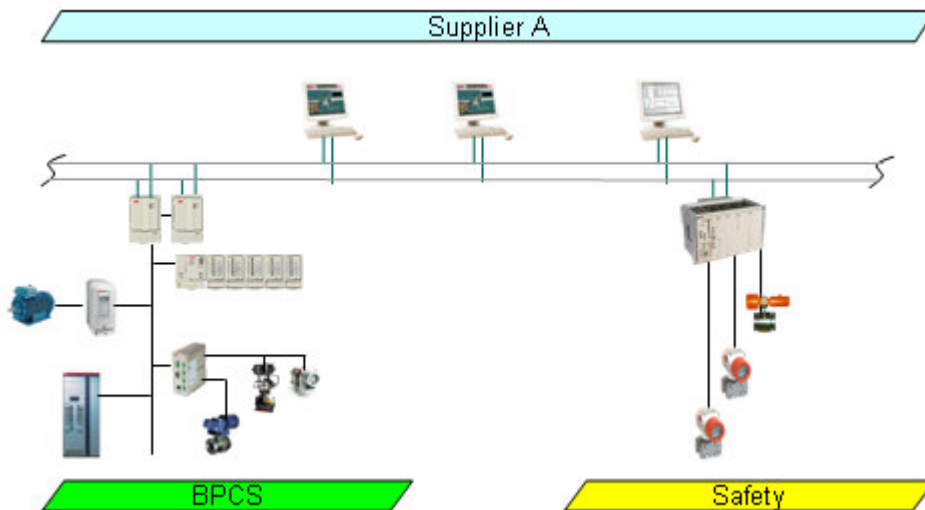


Figure 2 Top-level integrated system architecture.

The supplier use completely different hardware, software and system design for BPCS and safety on the logic solver level, while still providing some common overall system level tools and support. This negates some of the disadvantages of the previous system example (separated systems) while, at the same time, enabling the advantages associated with a common overall system strategy and top level structure typical of a single supplier. As always, benefits come at a price, as the closer top-level integration between the BPCS and safety systems theoretically increase the likelihood, however remote, of interference with safety functions.

Common HMIs can be expected as they are relatively easy to integrate, in most systems. Common HMIs offer some significant advantages from an operational point of view, improving operator system familiarity and potentially reducing time to decision. The relatively more complex engineering tools typically remain different for the BPCS and safety systems, effectively removing any real potential for engineering efficiencies. Unfortunately this means that the double training requirements remain largely intact due to differing hardware and engineering tools thus providing little potential for reduction.

With both systems delivered by the same supplier it is reasonable to expect that communication protocols are standardized and hence not a major cause for concern. Furthermore with a single overall supplier the support organization should be well defined and hopefully efficient.

5.3 Single Supplier with Similar but Separate Systems - Interfaced

A system architecture based on the same technology, but where the BPCS and safety systems are implemented as two separate systems, would ensure separation between BPCS and safety functions. There will inevitably be some differences between BPCS and safety hardware and software, but if developed as part of the same product family one can assume enough similarities from a user perspective to consider them common.

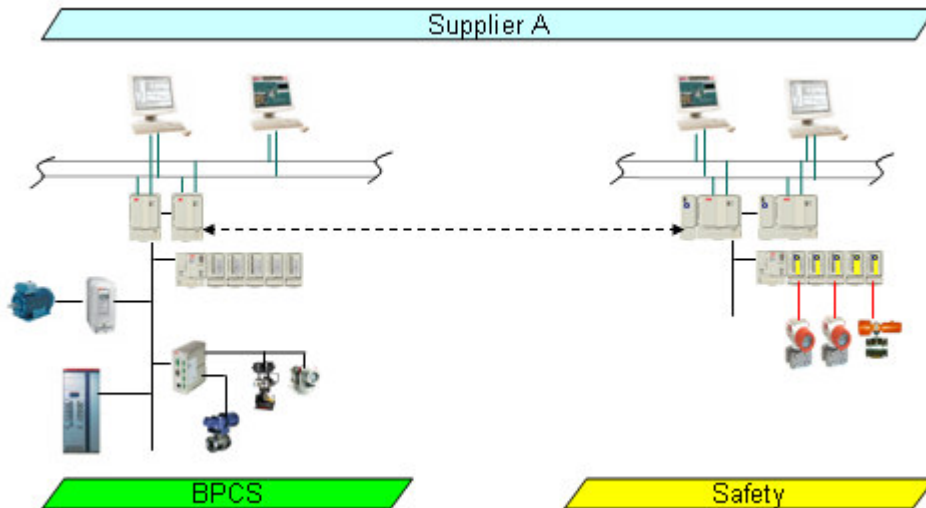


Figure 3 Interfaced system architecture.

Common basic hardware and software typically ensures that a common long-term development plan is in place as the lifecycle plan of the safety system would undoubtedly be closely linked to that of the BPCS system. Depending on the lifecycle policy of the supplier this should ideally include a forwards/backwards compatibility guarantee and offer increased confidence of continuous support over the system lifetime. This also applies to technical support where greater similarities between BPCS and safety allow a common support organization.

Over time, similar and common hardware should, as volumes of produced equipment increase, enable reduced hardware and spare parts prices. System components are tested and certified not only on a component level, but also, through integration tests, on a system level to ensure systematic integrity, e.g. by ensuring that non-safety critical components do not inadvertently interfere with safety critical functions.

Common engineering and top-level tools increase system familiarity for engineers and operators thereby significantly reducing training requirements while also improving operational performance. Similar HMI, while still separate, will also support operators by presenting information in a consistent manner allowing straight forward data comparison and analysis. Obviously the lack of complete integration means that the HMIs and engineering tools are run as separate entities with all that entails resulting in good, but less than optimal, engineering times and reduced operational efficiencies compared to an integrated solution.

Naturally the concern of common mode failures is a frequent topic of discussion when similar hardware and software tools are introduced into the system design. However, most suppliers today argue that distinct measures and safeguards are in place to ensure that potential common mode failures are identified during the development process. Working in strict adherence to development guidelines these potential failures are then either engineered out of the system design or otherwise addressed and managed.

5.4 Single Supplier with Integrated Systems - Integrated

Following the prevailing trend of integration, the final example and the currently most integrated system design is a “completely” integrated BPCS and safety system. Based on, in principle, common hardware and software and implemented as one system including both bottom and top level integration to the extent possible.

Today there are even certified safety controllers capable of simultaneously running both Process Control and safety applications, a feature that might be of interest in certain applications and systems to optimize system design and minimize capital expenditure. For instance in highly distributed systems, where the amount of hardware could be reduced, or for safety applications benefiting from very fast communication with process control applications executed in the same controller.

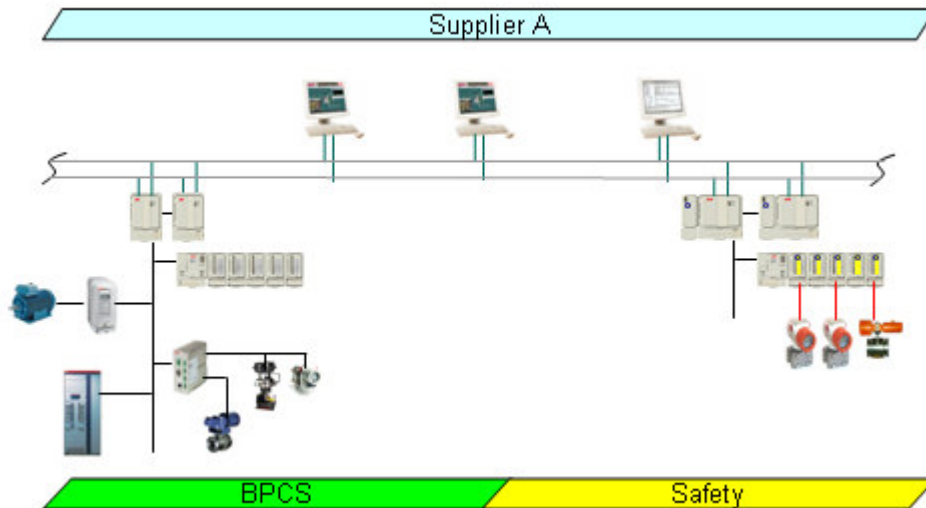


Figure 4 Integrated system architecture.

Drawing from the previously covered advantages of a common supplier, long-term lifecycle management, common support organization, reduced training, hardware costs and spare part requirements, the integrated solution offers an attractive long-term solution. While some of the above listed advantages are shared with one or several of the previous examples it is only the “completely” integrated solution that covers the full list and is capable of fully utilizing each benefit.

In addition to the obvious advantages of the previous example of separated but similar BPCS and safety systems, the integrated solution can leverage further on commonalities between the two systems.

Common engineering tools and HMI should result in reduced engineering times as well as significant advances towards operational excellence. The integrated approach will allow functions such as information management, asset management and production management to be operated across the entire automation system, including the safety system, fully leveraging their functionality. Operators can utilize the powerful top-level tools inherent in many major BPCS Systems (that may or may not be available in stand-alone safety systems). E.g. enabling common alarm management or highly accurate and reliable sequence of events handling, which are powerful tools when trying to avoid or mitigate the impact of hazardous events or unwanted process shutdown by simplifying data analysis and reducing time to decision.

As always, the topic of common mode failures and system independence are areas being heatedly discussed, but while this particular discussion is unlikely to arrive at a definite conclusion anytime soon, the trend is clear; integration between BPCS and safety systems is set to increase. Furthermore, as more and more reliable reference data becomes available over time, confidence levels are likely to improve, which in turn will support continued integration efforts.

The integrated and complete system overview supports highly controlled and safe plant operation and maintenance work procedures. Risk and unwanted shutdowns are reduced as operators and maintenance staff are constantly provided with a comprehensive and immediate understanding of the overall plant status.

6. Summary

The continued development of integrated safety systems is being driven by market demand. With the dawn of integrated safety systems a different set of system characteristics has come under increased scrutiny. Systematic integrity remains uncompromised throughout the development process, ensured by strict compliance with international standards and certification by independent certification bodies.

Historically, and not without reason, the safety community has been advocating strict independence between BPCS and safety systems. However, as more reliable technology is becoming available this view is increasingly being re-evaluated.

Closer integration between BPCS and safety system has resulted in increased commonalities, with hardware and software being developed as part of a common product family. Traditional BPCS tools and functions, such as common HMIs, engineering tools and sequencing of events, are being applied to safety systems to improve overall plant performance.

A proactive approach to management of the human factor is an essential part of risk management. Total independence between BPCS and safety systems will ensure a minimum probability of overall system failures, but would also with all likelihood require additional operator safety competence and possibly have a negative impact on operational performance. However, integrated systems could offer operator support to manage risk through a homogenous interface giving access to all vertically integrated system functions, e.g. common HMIs, information management, asset management, sequencing of events, force control and engineering tools. An interface that, if properly utilized, has the potential to improve both operational performance as well as reduce the number of unwanted shutdowns without compromising safety.

The answer to the question of integrated safety systems or not is far from absolute however. Subject to plant specific requirements and corporate safety traditions a wide range of levels of integration exist through an array of system solutions.

As new options are being introduced a new approach to evaluating safety system requirements is required. Apart from the always paramount question of safety there are a new set of questions to explore:

- What is the lifecycle policy of the supplier? Is it a written commitment or a verbal policy?
- Does the supplier guarantee forwards and backwards compatibility? Is it a written commitment or a verbal policy?
- How can the human factor best be managed? Through clear and distinct separation between BPCS and safety systems to avoid systematic failures? Or through an integrated system supporting operators in managing the overall safety of the plant through a homogenous interface?
- Would common alarm management and sequence of events analysis reduce time to decision in the event of a hazardous event? Hence reducing the number of accidents and unwanted shutdowns?
- How are system modifications engineered for BPCS and safety systems?
- How is risk managed during system modifications and extensions?
- Would integrated HMIs and information management support operators in day-to-day operation?
- Would maintenance routines be supported by overall system management and control? Could risk be reduced while improving plant uptime?
- How is cost of ownership affected by choosing independent BPCS and safety systems?

While the overall discussion on integrated safety systems is set to continue there is also increasing interest for the details of integration. Above set of questions are worth further consideration before a new safety system specification is finalized.