Value Paper Authors: **Luis M. Duran, Ron Johnson**

Providing independent layers of protection with integrated safety systems

Power and productivity
for a better world™

ABB

Providing independent layers of protection with integrated safety systems

Abstract

Modern automation systems incorporate (Safety Integrity Level) SIL certified Safety Instrumented Systems (SIS) as an inherent part of the system. Phrases such as "integrated but separate" are often used to illustrate the undiminished safety integrity of these fully integrated automation systems. This paper will cover how an Integrated Safety System (one that performs both basic process control in addition to safety protection) can still act as a completely independent layer of protection and enhance safe operation by addressing additional sources of risk

The paper will describe industry requirements throughout the safety lifecycle, and the design requirements on the safety system to provide the most comprehensive platform for process safety management, including safety engineering tools, operation management tools including alarm management, management of change and maintenance.

This paper will discuss the basic requirements of the standard for SIL–1, SIL–2, & SIL–3, which is more than just (Probability of Failure on Demand) PFD, and the potential end-user benefits enabled by a fully integrated system.

Keywords:
Safety Instrumented Systems, Safety Integrity Level, Integration, Independent Layer of Protection, Common Cause Faults

Is integration a novel concept?

The integration of Safety Instrumented Systems (SIS) into a Basic Process Control System (BPCS) is not a new practice, even when the technology was as diverse as relays and process control computers. The plant operators relied on Annunciation Panels to identify process alarms, plant upsets, and critical conditions which were intended to integrate those signals with the rest of the process control operation. As process control systems transformed into programmable electronic systems, both for regulatory control and safety, another integration scheme appeared. These schemes used communication protocols, either proprietary (typically when both were provided by a single vendor) or "open" such as Modbus RTU (when the relationship between vendors was more "loose"). Recently Modbus TCP and OPC substituted the previous communication schemes.

These communication protocols allowed transference of operational data across systems. The type of data varied from

alarms, sequence of events, and diagnostics. The quality of data was also dependant on the communication protocol. Although these integration schemes were perceived to be cumbersome to configure and expensive to maintain, operating companies were inclined to pay the price in order to enjoy the benefits of integrated operations.

What are Independent Protection Layers?

Over the same time period the industry develop standards to document the best practices directed at how to implement a programmable electronic systems (E/E/PES) technology to satisfy the industry requirements. One such practices, independent protection layer (IPL), was particularly critical to the idea of integration.

For years the process industries relied on independent protection layers to reduce process risk. The concept assumes that the Basic Process Control System (BPCS), process alarms, operator actions, safety instrumented systems (SIS), fire and gas (F&G) systems, and any other system intended to reduce risk in the processes are capable of acting independently from each other. This means performing properly without being influenced by one another and without failures that would potentially disable two or more of the protection layers (defined a Common Cause Faults).

What are common cause faults?

Following the safety system design stages according to the standard's safety lifecycle, users are required to perform a Process Hazard Analysis and consider the potential demands on the protection layers. All systems are expected to fail and electronic systems are no exception. An important part of the assessment of a safety instrumented system is the Failure Mode Effects and Diagnostics Analysis (FMEDA) of its elements that will be the basis for identifying the impact of such failures for the plant risk reduction strategy in the case of a given demand.

As documented in the standards and published literature a Common Cause Fault occurs when a single fault results in the corresponding failure of multiple components. An example of such is a miscalibration error on a bank of redundant transmitters[1]. A common cause fault can result in the SIS failing to function when there is a process demand. Consequently the potential impact of Common Cause failures on the SIS functionality must be understood and it must be identified during the design process.

Concepts as "defense in depth (D3)" and "independent protection layers (IPL)" have their basis at the heart of all the international safety standards (ISA S84, IEC 61508 and IEC 61511). They assume that every layer of protection, including both control and safety systems, should be completely independent. Some of the reasons for this basic requirement are to avoid common cause faults and to minimize systematic error[2].

The traditional approach for reducing common cause is to use totally different systems for the (BPCS) and the (SIS), using different hardware and software to reduce common cause failures. If these systems are purchased from different automation providers common cause failures can probably be excluded because the user can assume that different development organizations, knowledge, manufacturing processes, as well as different installation, operation, and maintenance procedures were used in the logic solver's manufacturing process.

Additionally the SIS provider will be required to have a third party certification of their products according to applicable safety standards. For example, a certification provided by TÜV includes a complete assessment of the hardware and software of the product including failure modes, installation requirements, operating restrictions in case of a failure, design and verification process, and many others.

Obviously the disadvantage is that two totally different systems need to be engineered, commissioned, operated and maintained throughout the lifetime of the plant. Engineers, operators and maintenance personnel need to be trained on and maintain knowledge about different systems.

The Automation industry has changed

Within the past decade the automation market has consolidated vendors and started to develop BPCS and SIS using similar hardware and software for both sequential logic control and regulatory process control. Integration became more than sharing the process network.

As the advances in technology continued, the industry benefited from improvements in the reliability of hardware and software, including embedded software. The 1oo2 dual, 2oo3 triple, and 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 designed out and more than 99% diagnostic coverage 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].

Other advances are in the form of the design process. Safety standards recommend product life cycle design processes which include product development or "validation and verification" to ensure proper care is taken in the development of the product.

This new degree of integration challenges the common accepted practices of satisfying and demonstrating that the SIS is not subject to common cause failures with the BPCS. Furthermore, even though they are integrated, both systems can provide independent protection layers and meet the safety standard's requirements.

The debate about the separation of the safety function from the BPCS will no doubt continue. However the IEC 61508 and IEC 61511 standards 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 (i.e. that the failure of a non safety related function does not cause a dangerous failure of the safety related functions)"[4]. Additionally the standards also require that the possibility of common mode dependent failures is reduced to an acceptable level. [5]

Is it possible to comply with the standards and be integrated?

Safety Standards have been quoted before to answer this question. IEC 61511-1 clause 11.2.4 states that the basic process control system (BPCS) should be designed to be separate and independent to the extent that the **functional integrity of the SIS is not compromised**[6]. ISA-84.00.01-2004 Part 2 Clause 11.4.2 adds "Physical separation between BPCS and SIS **may not be necessary** provided independence is maintained, and the equipment arrangements and the procedures applied ensure the SIS will not be dangerously affected by:

- Failures of the BPCS;
- Work carried out on the BPCS for example: maintenance, operation or modification."[7]

The same reference suggests that "In order to safely use a single platform for both Basic Process Control and Safety, you need to effectively separate the BPCS from the SIS. They need to be as independent as possible to ensure interference is eliminated. This is managed by a strong Operating Discipline (OD) program."

How can Independence between protection layers exist within an Integrated System?

As mentioned earlier the traditional approach was to use systems from different automation providers. This assumed that common cause failures were probabilistically impossible because the two companies would use different development organizations, knowledge, manufacturing processes, as well as different installation, operation and maintenance procedures during the design process.

An alternative approach is to build such independence in the design process of the Integrated System. Independence is possible using diverse design engineering and programming teams provided with different software architecture specifications and guided by an overall concept for diversity from the start of the detailed design specifications.

The use of different toolsets in the development process provides even further diversity and facilitates reduction of common cause faults. Development techniques utilizing formal methods, the V-model (as defined in the safety standards), strict coding guidelines, separate development teams, and diverse implementation ensure a structured approach to avoid common mode failures throughout the entire specification, design and development process. When supported by a structured approach to test and formal verification at different levels, performed by an independent team, the system reliability can be enhanced even more.

How to build diversity between protection layers in an integrated system?

As previously mentioned, dangerous failure modes can be designed out and more than 99% diagnostic coverage can be provided to protect integrity without resorting to duplication. Technology has evolved to points in which there are multiple options to address a similar technical problem. For example by using two or more of these technologies, diversity is embedded in the system design. Diversity can be achieved in the embedded software by using different operating systems and then using different teams to develop the software on multiple cooperating modules.

By combining two different technologies (such as Micro Processor (MPA) or Micro controllers and Field Programmable Gate Arrays (FPGA)) to perform the same functionality in parallel to each other the design achieves a truly redundant and diverse implementation with a minimum of possible common cause failures. To eliminate the potential sources for common cause failures originating from design, development and test, this

approach requires different development and test tools, as well as different programming languages for implementing the functionality,. Additionally, by using two different development teams for creating system overheads in these two technologies, common cause failures can be minimized.

Is logical separation acceptable as a substitution for physical separation?

In addition to the implementation of access control, password protection and firewall, logical separation can be added in the form of memory management. A memory management unit (MMU) will can provide independency between different partitions of memory areas. These memory partitions are then connected to different executing processes of the CPU such as regulatory process control or safety instrumented function. This approach ensures that only the memory area belonging to that process is accessible while the CPU is executing one of its processes.

However in order to fully answer the question, each user should seek for their answers by applying the ISA standards to assess the independence of both systems.

What are the Benefits of Integration?

The operational aspects of safety systems are under increased scrutiny. Beyond the purely financially benefits (which focuses on reducing operational cost throughout the system lifecycle) the real driver is safer operations.

The industry is struggling with increased system complexities. A larger number of systems in any given plant combined with a competence pool that is depleting through retirement increases the risk of safety critical mistakes. An obvious counter-measure to negate this risk is a reduction in both system complexity and number of systems employed.

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. The benefits can be categorized in the following areas:

- There is only a single process automation computer platform in the facility.
- This means there is only a single operator interface for operations to learn and operate.
- There is only one computer language for programmers to learn.
- There is only one platform for maintenance personnel to maintain.

All field instruments are wired to the common system, meaning there is less field splitting (optical isolators) or less communication required between two separate systems.

- Easier instrument design and field wiring because all the I/O for a given unit operation are wired to the same logic solver, regardless of whether it is Safety I/O or not.

The complete pool of plant information is available for both the BPCS and the Safety System because all the facility’s I/O is wired to the same logic solver. This allows for easy and safe communication of information between the SIS and the BPCS by utilizing the platform’s certified safeguards to maintain “non-interference” and “functional independence”.

- The SIS operating window can be made flexible since it can intimately know what is going on with the BPCS. For each unit operation the boundaries of the operating window change as the plants start up and shut down. This is much more difficult to manage with independent BPCS/SIS systems because there is only one SIS trip setting which forces operations to sometimes by-pass these restrictive trip setpoints (for example during start-up activities). This introduces the need to by-pass, and consequently the chance of leaving these hardware and software bypasses in place after startup.
- With an integrated system, manual SIS bypasses and enables can be automated by coordinating with process operations and thereby eliminate the issues associated with having to remember to re-enable the safety systems.
- In a more abstract way, signals are not simply used, but rather the data they represent is used. The data is put in the data pool and validated first. This allows the use of multiple information sources as well as more final elements to execute decisions.

A commonly referred to publication by the UK Health and Safety Executive[8] 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%

Although these problems are compounded by the depletion of the competence pool due to a retiring workforce, the publication points out that close to three-fifths of all sources of failure are built in before operation of the system has started.

Improvements during specification and design stages of projects are required to reduce these types 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. ISA-84.00.01-2004 part 2 says in clause 11.4.2: “Identical separation1 between the SIS and BPCS may have some advantages in design and maintenance because it reduces the likelihood of maintenance errors.” additionally systematic trips may also be minimized.

The use of Integrated Safety Systems offer ways to enhance safety and, as an added benefit, reduce the cost of ownership.

1 Identical separation as defined on IEC 61511-2 refers to using the same technology for both the BPCS and SIS

Additionally Engineering efficiencies, improved system understanding and support will have positive impact on safe plant operation and bottom line performance.

Conclusion

When the safety standards and best engineering practices are used from the initial design, it is possible to develop an automation system that integrates the basic process control system (BPCS) and safety instrumented systems (SIS) function within the same operational, maintenance and engineering environments.

This approach changes the paradigm from building robustness and reliability around multiple redundant paths to the use of the technology options available today to creatively satisfy the core design principles of independence, diversity and separation.

Case Study from Dow Chemical

Dow Chemical has had a long history of utilizing a combined BPCS/SIS logic solver platform. Dow’s proprietary home grown computer system is TÜV certified for SIL-3 plus BPCS control (providing the Safety Manual is followed). It has been used successfully this way since the mid-1990’s. Currently Dow has hundreds of installations utilizing this concept.

Today there are a number of integrated SIS/BPCS logic solver platforms available in the marketplace. Since the early 2000’s, Dow started using the SIL certified ABB platform – the AC800M family of products – in much the same way as their own home grown computer system. One example is a facility in Michigan that uses toxic chemicals and a gas fired curing oven. This 1500 I/O facility uses multiple dual certified ABB safety controllers to perform all of the normal process control plus roughly 75 Safety Instrumented Systems (SIL-1 & SIL-2).

In some cases Dow has gone one step further and utilized this common pool of field data to enhance both the basic process control and the Safety Systems by sharing sensors. One example is where the same two temperature signals are used by both (1) the oven’s fuel gas controller (for temperature control) and (2) by the high temperature SIS trip that shuts the fuel block valves.

Conventional thinking would wire one sensor to the BPCS computer for temperature control and the other sensor to the SIL certified computer for the SIS. But by sharing these sensors the temperature control becomes more robust and fault tolerant thereby decreasing the probability of control failure. At the same time the SIS with 2 sensors is more robust and fault tolerant resulting in a lower failure probability. Dow recognizes the potential common cause issues associated with sharing sensors and consequently calculates proof test intervals with fault tree based tools.

In another recent example a 1300 I/O European Polyurethanes expansion with over 100 SIS loops utilized multiple dual certified ABB safety controllers. The safety systems and the normal process control are fully integrated within this single platform. Roughly 25% of the safety loops also share sensors with the basic process control. Although the front end design is more complex to ensure that safety is not compromised, the long term benefits are worth the effort.

The integration of safety and basic process control has proven itself with safer and less complex operating environments. Within the last 5 years Dow has installed over 20,000 I/O on commercially available dual certified logic solver platforms. Dow’s history with over 1,000,000 I/O on Dow’s proprietary dual certified platform ensures that this is the direction Dow plans for its future. History within Dow has demonstrated that when properly designed and implemented, safety and basic process control can be integrated in a safe and cost effectively manner.

These can then enable Independent Protection Layers that integrate the user work functions. These systems are certified by TÜV without the need of certifying the complete Automation Infrastructure, and without the need of ensuring the non-interference nature of the Process Control System.

Users can enjoy the benefits of integration without compromising safety and be in compliance with the safety standards. More importantly plant operators are able to detect and react promptly to process conditions before they develop into near misses or incidents. Additionally, operations have the ability to track, analyze and report within the environment used to perform those functions for all other plant operations.

Endnotes

1. Common Cause and Common Sense Designing Failure Out of Your SIS
   Angela E. Summers, Ph.D. and Glenn Raney
2. Integrating Control and Safety: Where to draw the line.
   Robin McCrea-Steele, TÜV FSExpert, Invensys-Premier Consulting Services
3. Integrated but separate, Advances in integrated and safety control
   Roger Prew, ABB
4. (IEC 61508-2 clause 7.4.2.3
5. (IEC 61511 Part 1 clause 9.5.1/2)
6. IEC 61511-1 clause 11.2.4
7. Integration of Safety and Control
   Ronald Johnson, Dow Chemical SIS SME
8. Out of control: Why control systems go wrong and how to prevent failure
9. HSE Books ISBN 0-7176-2192-8 [9] Information supplied by Ronald Johnson, Dow Chemical SIS SME

Contact us

ABB Ltd
Affolternstrasse 44
CH-8050 Zurich, Switzerland
www.abb.com

3BUS095014 en ABB USCS 1730

Power and productivity
for a better world™