Life Is On Schneider Electric

Control and safety integration

Maintaining defense in depth

by Farshad Hendi

Table of contents

Introduction

New digital technology now makes it feasible to integrate process control and SIF within a common automation infrastructure. While this can provide productivity and asset management benefits, if not done correctly, it can also compromise the safety and security of an industrial operation. Cybersecurity and sabotage vulnerability further accentuate the need for securing the safety instrumented system (SIS).

Certainly, a common platform approach using similar hardware and software dedicated for control and safety functions, respectively, can provide the potential for cost savings. However, it is widely acknowledged that utilizing separate, independent, and diverse hardware/software for safety and control is the optimal way to protect against potentially catastrophic common cause and systematic design and application errors.

Different vendors offer varied degrees of integration and solutions. The question is how to provide an integrated control and safety solution with advanced functionality and productivity without compromising safety and security. So where do users draw the line?

A third-party (e.g., TÜV) certification of the hardware/software systems to IEC 61508 specifications carries significant advantages, but should this be the only criterion? How does a third-party certificate extend to the plant's overall assignment of risk reduction credits for all independent protection layers (IPL)? Control system embedded safety logic solvers may actually increase the SIL requirements of the SIF if no credit is allowed for the distributed control system (DCS) as an IPL.

This paper discusses engineering best practices in integrating control and safety in a secure manner while maintaining IPLs. Potential benefits and side effects of the different approaches are highlighted within the paper.

Potential benefits of a tight integration

There is undoubtedly a very good case to be made for tight integration of control and safety from an operations and productivity point of view. Some of the major potential benefits include:

- Seamless integration
- Time synchronization
- Elimination of data mapping duplication
- Common human-machine interface (HMI)
- Compatible configuration tools
- Minimized set of spare parts
- Single operator and maintenance training requirements

All of the above are great benefits for productivity and maintenance. However, merging control and safety too far could outweigh the advantages. What are the side effects of using a common platform? How is the integrity of each IPL guaranteed? Does a DCS embedded safety logic solver pose concerns of side effects and hidden costs?

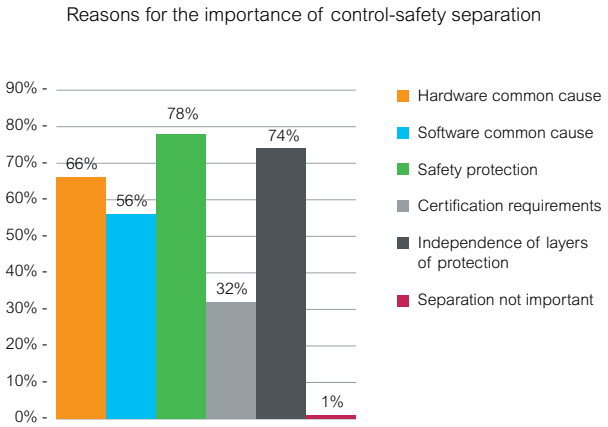
Potential benefits can, at times, become a liability if they are at the expense of safety and security, and increasing life cycle costs.

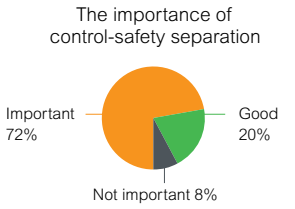
Where to draw the line

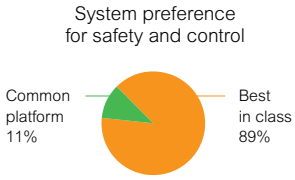
Regardless of the technology implemented, maintaining the basic principle of IPLs is the responsibility of the operating company.

Providing functionality and productivity without compromising safety and security is the responsibility of the end user. So where do plant operators draw the line?

The answer may lie in a recent Zoomerang survey of chemical, oil, and gas process plant operating companies conducted by Schneider Electric. The survey responses revealed that 78% of the over 200 respondents adhered to strict separation of safety and control for safety protection. Additionally, 74% of respondents indicated that IPLs were critical and 66% gave common cause as a major concern. In the same survey, only 8% indicated that diversity was not a concern, while 89% of users said that their ability to choose best in class for both safety and control was important.







The conducted survey included 23 of the top 25 petroleum companies, and 45 of the top 50 chemical companies in the world.

Results of this survey, combined with in-depth discussions with a larger population of process industry end users around the world, clearly indicate that the majority of operating companies draw the line at maintaining IPLs and diversity between their SIS and process control system.

The importance independent protection layers

The basis for the concept of "defense in depth" (D3) and IPLs at the heart of all international safety standards (including IEC 61508 and IEC 61511), is every layer of protection, including both control and safety, should be unambiguously independent. Some of the reasons for this basic requirement are to avoid common cause faults, minimize systematic errors, and provide security against unintentional access, sabotage, and cyberattacks. Merging two layers of protection is a safety incident waiting to happen.

Process safety is based on D3 and the separation of the control and safety systems operating independently. Each IPL is designed to independently protect against the hazard for which it is designed to safeguard.

3.2.43.1 Demand mode safety instrumented function

Where a specified action (for example, closing of a valve) is taken in response to process conditions or other demands. In the event of a dangerous failure of the SIF, a potential hazard only occurs in the event of a failure in the process or the BPCS.

One of the main duties of the DCS is to reduce the number of demands on the SIS. A demand on the SIS implies that the control system has failed to keep the process within the safety range and the process is now relying on the SIS to protect against the hazard.

The IEC 61511-1 definition of demand mode of operation in the process industry demonstrates the intent for the requirement of total independence of the basic process control system (BPCS) and SIS protection layers.

In essence, the function of the IPLs is to ensure that the potential hazard will occur only when both the BPCS and SIS fail.

This leads us to question the following scenario: If the BPCS and SIS are embedded in a way that they might both fail simultaneously due to common cause or systematic failures, the operation is effectively in "continuous mode," with the DCS/SIS combination functioning as a critical control system. In this case, the whole objective of the SIS layer of protection is lost.

Interpreting the safety standards

IEC 61511-1 clause 11.2.4 states that the BPCS shall be designed to be separate and independent to the extent that the functional integrity of the SIS is not compromised. The caution here is that these are minimum benchmark requirements and may not provide adequate risk reduction in many Chemical and Oil & Gas applications.

Several automation vendors seem to have selectively interpreted the above clause to indicate that the standard does not require physical separation or diversity.

However, another section of the same standard, clause 9.4, addresses the requirements for preventing common cause, common mode, and dependent failures. Clause 9.4.2 states that the assessment shall consider (a) independency between protection layers, (b) diversity between protection layers, (c) physical separation between protection layers, and (d) common cause failures between protection layers and BPCS.

The question is how to conform to clause 11.2.4 without physical and diverse separation? Systematic errors, common cause errors, and software errors form an integral component of the overall safety assessment.

ISA TR84.00.04 part 1 is designed to be a guideline for the interpretation and implementation of IEC 61511. This technical report has many good recommendations, including Annex F section F.4, where it addresses physically separate and diverse SIS logic solver as having served the industry well and a way to virtually eliminate common mode failures.

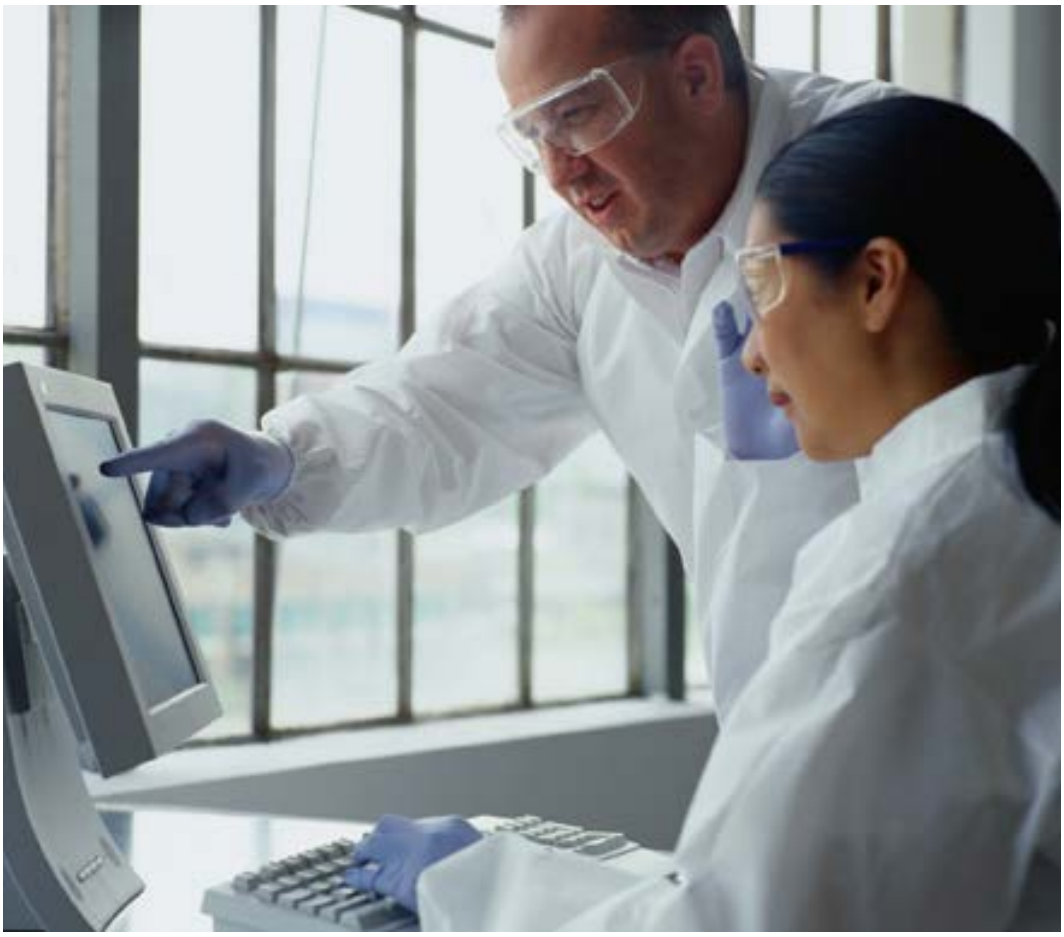
The AIChE Center for Chemical Process Safety book **Guidelines for Safe and Reliable Protective Systems** (ISBN 978-0-471-97940-1) cautions that the international safety standards are performance benchmarks for minimum requirements. It further defines in section C, on page 301, that independence, functionality, integrity, reliability, auditability, access security, and management of change are fundamental characteristics of an IPL.

- C.1 Independence
  For a protection layer to be considered independent, its performance should not be affected by the occurrence of the initiating cause, its consequences, or by the failure of another protective function used to reduce the risk of the same hazardous event. The correct operation of the protection layer should not be conditional on any other layer and its separation from other layers should be unambiguous.

- C.2 Functionality
  The protection layer must be capable of responding effectively within the time required by stopping the propagation of the initiating cause, even in the presence of other protection layer failures. This requirement along with the core attribute of independence generally results in the use of separate equipment and management systems for each protection layer. The reduction of the system to its individual functions allows function classification and provides traceability between the design and management of the function and the required risk reduction.

"Integrated functionally separate safety and control" is marketing terminology that requires an in-depth assessment of its implications.

A safety logic solver that is embedded within the same platform as the control system, using separate modules, does not meet the requirements of an IPL.



Is a third-party certificate enough?

Some may think that a third-party certificate of compliance of the equipment is sufficient. However, the ultimate responsibility is with the plant operating company's management, not the vendor.

International safety application standards require that manufacturers document compliance of SIS logic solvers to IEC 61508. A TÜV certificate of compliance goes a long way, but, as a user, is this all you need? Most all safety practitioners and process plant operating companies will definitely say that, although essential, product certification should not be the only criterion.

The compliance to all phases of the IEC 61511 safety life cycle, the assignment of safety integrity requirements to all the IPLs, as well as verification, validation, audits, and management of change are only some of the requirements for a successful risk reduction implementation.

A third-party certificate of compliance for the SIS logic solver will validate the design and fail-safe suitability for use in an SIF up to the SIL claim limit. It does not say anything about the spurious trip vulnerability, which is an issue that the end user needs to evaluate based on the specific application.

Furthermore, and extremely critical, is the fact that when an SIS logic solver receives certification, it is done in isolation of the application with an additional review of safe communications to external equipment and protection against interference with the integrity of the safety functions.

For systems where the SIS logic solver is embedded within the platform of a DCS, the certification will validate the noninterference of failures in the DCS affecting the SIS safety functions. Is this enough?

The first problem is that the certification does nothing to avoid the common cause failures of the SIS and DCS, which are based on the same hardware/software platform. Neither does it say anything about the systematic errors inherent in using the same platform for SIS and DCS. The certification validates the functional separation and noninterference of control system failures on the SIS, firewalls, and password-based access protection.

What about independence of the layers of protection in the plant? This is not part of the SIS logic solver certificate. This is a responsibility of the operating plant company. Compliance to the functional separation requirements of IEC 61511 is enough to obtain a TÜV certificate, but when the SIS is embedded in the control system (even if it uses separate modules), this eliminates the credit that could have been taken for a DCS as an IPL.

An IPL must be unambiguously independent. If a common cause error can affect both the DCS and the SIS, then no credit can be taken for the control system as an IPL.

Therefore, although a TÜV certificate for a certain SIL capability limit for the SIS logic solver validates the use of a functionally separate but common platform DCS-SIS, great caution must be taken in the overall implementation of the plant risk reduction requirements.

A recent study by a major refining and energy corporation determined in its review of a TÜV-certified DCS embedded safety system (which actually did use separate modules), that although noninterfering, the BPCS-SIS separation could not be adequately satisfied as an IPL. This operating company concluded that because both the BPCS and SIS equipment on the same carrier used common communication traces, no credit could be gained for the BPCS as an IPL.

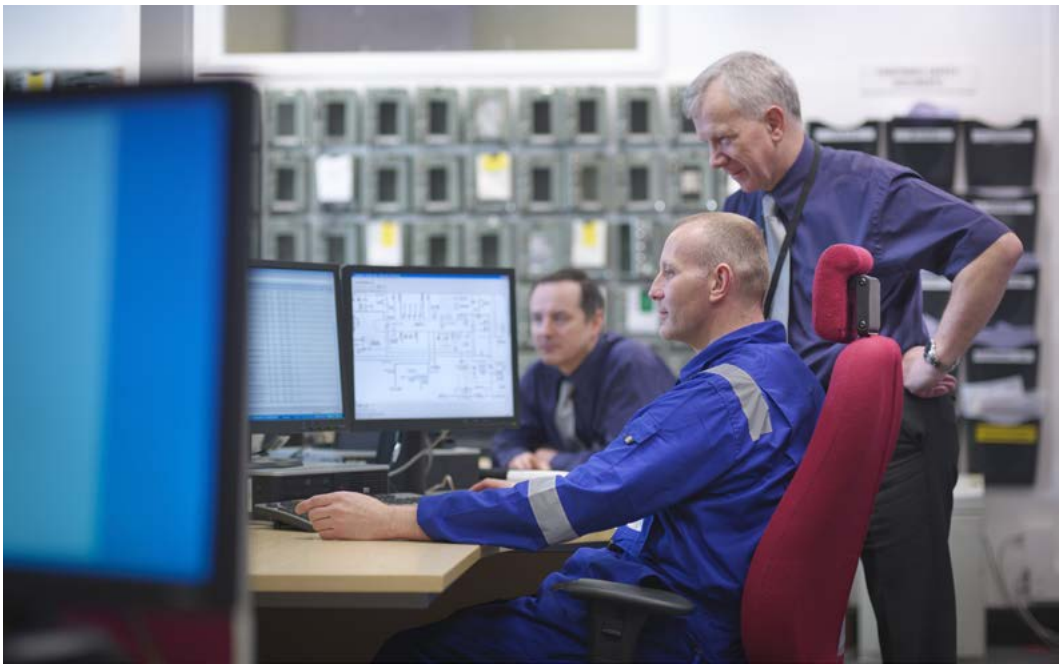
Credits for independent protection layers

In the initial stages of the SIS design, hazards are identified and safety integrity requirements are assigned to each layer of protection. Layers of protection analysis (LOPA) are one of the most popular methodologies used in the assignment of the SIL requirements for each SIF.

LOPA takes credit for all available IPLs that qualify per the IEC 61511 requirements. During the LOPA evaluation, the DCS is considered many times as an IPL and a credit up to the maximum allowable by the standards taken (10-1 or a risk reduction factor (RRF) of 10).

Taking a RRF of 10 for the DCS as an IPL has considerable weight in the final SIL requirement for the SIF. A control system that qualifies as an IPL will substantially reduce the demand rate on the SIS. Actually, the SIL of the SIF will be one whole order of magnitude higher if the DCS does not qualify as an IPL.

Considering the above, during the detail design phase of an SIS, it is very important to verify the assumptions made during the SIL assignment phase.



For example, when a LOPA study determines the need for an SIL 2 SIF, based on credit taken for all IPLs including a RRF of 10 for the control system, the verification phase should verify that all assumptions are still valid. If, however, the SIS logic solver is embedded in the same hardware/software platform as the DCS, then the control system will no longer qualify as an IPL and the RRF credit taken will need to be nullified. Consequently, the resulting SIF requirement will be increased by one order of magnitude to an SIL 3.

A TÜV certificate for an SIS logic solver embedded in a DCS platform validates the functional separation and noninterference of the control system on the safety functions. However, no credit can be taken for the DCS as an IPL and the potential for all SIL requirements to be increased by an order of magnitude is real. A plant with requirements for SIL 1 and SIL 2 SIFs will mostly have SIL 2 and SIL 3 requirements. This means incremental costs in field redundancy, installation, maintenance, and testing.

Unfortunately, if an SIL 3 requirement was determined during the LOPA with credit for the DCS as an IPL, using an SIS logic solver embedded in the DCS will render a requirement for an SIL 4, which means going back to the drawing board.

Cybersecurity concerns

We are all well aware of how hackers, viruses, trojans, and worms can penetrate firewalls, break password securities, and generally create havoc in a computer network system.

The vulnerability of a safety system integrated with a control system that in turn is connected to a site LAN and/or corporate WAN is increased exponentially. Remote process monitoring as well as remote diagnostics, maintenance, and asset management through web connectivity have become an efficient operating tool. However, firewalls and passwords are only another challenge to hackers. In time and with focus they are routinely broken. The safety system, as a last line of defense, needs to be secured.

A computerized waste treatment plant in Queensland, Australia, was hacked by an individual who had worked for the contractor that installed the system and who was angry over a rejected job application. The hacker managed to divert millions of gallons of raw sewage to city waterways and rivers.

Insiders, disgruntled employees, web hackers, and terrorists are all real threats to the process industry. Media Corp-News Asia reported on October 4, 2005, that 500 computer hackers in North Korea were given a five-year military university training program with the objective of penetrating the computer systems in South Korea, the USA, and Japan.

Even multiple firewalls and intrusion detector systems are not enough. All systems are vulnerable. There is no such thing as absolute security, only layers of protection.

The solution: Smart integration

The supposed advantages of seamless integration, elimination of data mapping, and lower hardware and training costs for using a common embedded platform come at the expense of safety and security. Actually, life cycle costs are higher, both economically and in safety of personnel, the environment, and the community.

An additional concern is the long-term management of an embedded SIS, where day-to-day activities become more prescriptive and less flexible than with independent and diverse systems. Management of change validations will encompass much larger and complicated processes. This approach has too many downsides.

The AIChE Center for Chemical Process Safety book **Guidelines for Safe and Reliable Protective Systems** (ISBN 978-0-471-97940-1) states in section F.2.3 related to future technology:

Most owner/operators continue the practice of implementing separate, and often diverse, platforms for the BPCS and SIS, following the well-proven, D3 strategy that supports both safety and reliability. With a physically separate BPCS controller and SIS logic solver, independence is easier to assess and manage over the process equipment lifetime. Independence allows the owner/operator to implement different management systems for the BPCS and SIS; the BPCS management system may be more flexible and less rigorous than the SIS management systems.

In section F.3.5, Logic Solver Separation, the AIChE guidelines state:

The interaction between the BPCS and SIS is now much more complex. Field devices are often shared as discussed in Section F.4, and there may be extensive communication between the systems as discussed in Section F.6. However, experienced engineers and many good engineering practices continue to recommend implementing the SIS in a physically separate logic solver from the control functions.

A major justification for separation is reduced long-term administrative costs. When layers are combined the management systems of the highest layer applies. Means should be provided to restrict access, limit communication to other systems, and control system changes. Generally the cost of separation is significantly less than the administrative cost to maintain the required rigor. The administrative rigor must be maintained for the life of the system, including the provision for necessary resources to verify and audit compliance.

Adequate separation is achieved by administrative controls and physical means. Physical separation is provided at the system level by executing the functions in separate and often diverse logic solvers. Access security and management of change is enhanced by physically separate systems. When the BPCS is physically separate from the SIS, the need to access the SIS is reduced and the BPCS can be managed under a less rigorous management system.

Separation ensures that the BPCS and SIS are not dependent on each other to operate. It also provides a clear and unambiguous distinction between the BPCS and SIS, which supports long-term access security and management of change. Separation also ensures that when maintenance and testing is conducted on one system the other remains available.

Conclusion

It is safer, renders a lower SIL requirement, and is less expensive to implement physically separate and diverse independent safety and control systems with smart integration at the information, configuration, asset management, and HMI levels. All the capabilities of field diagnostics and asset management, including partial stroke testing, can be implemented effectively through smart integration.

About the author

(Farshad Hendi) Safety Services Practice Lead Americas and Europe, Schneider Electric