Life Is On | Schneider Electric

Integrated control and safety

Assessing the benefits; Weighing the risks

by Grant Le Sueur and Phil Knobel

Executive summary

While best practice has leaned toward keeping control and safety isolated from each other, recent enterprise data integration and cost control initiatives are providing incentives to achieve some level of integration. This paper describes three basic integration models, including an “interfaced” approach, in which separate control and safety communicate via a custom built software bridge; an “integrated but separate” approach, in which the disparate systems sit on the same network but share information only across isolated network channels; and a “common” approach, in which both control and safety systems share a common operating system. The three approaches are then compared according to compliance with safety standards and cost efficiencies.

Table of contents

Introduction

Safety instrumented systems (SISs) are industrial safety nets. They must be available 24/7 to provide backup when something renders a process automation system (PAS) unable to perform its job of controlling a hazardous process. To protect the SISs from faults caused by the same issue(s) that caused the PAS to malfunction, good practice has traditionally dictated strict physical and functional isolation between the two systems. But as increasing business complexity and global competitiveness drive often conflicting needs for greater enterprise integration, improved safety, and reduced costs, officials at some companies are looking at integration and consolidation of safety and control functions as a way out of the dilemma.

Safety and risk managers might see the safety system as a goldmine of valuable data that, if made more accessible, could help identify leading indicators of future problems. Engineering managers see redundant effort that can be streamlined. Operations managers see islands of activity that can be better communicated with each other and with the rest of the enterprise. Maintenance managers see volumes of data on machine and system health that can contribute to improved maintenance and lower maintenance costs. Financial managers see redundant capital expenditures and training costs ripe for consolidation into a single system.

In efforts to address these needs, automation vendors have offered various models for integrated control and safety systems (ICSSs). This paper compares the benefits and risks at four levels of integration: complete physical separation, integration via a custom programmed software interface, integration via isolated subsystems on a client-server control network, and integration across a common control platform.

The difference between a PAS and an SIS

Although both the PAS and SIS are control systems, they are designed for fundamentally different purposes. The PAS, which is also often called a distributed control system (DCS) or basic process control system, regulates production based on values of production variables received from field devices such as pressure and temperature transmitters, via I/O cards terminating in a control room. A PAS also incorporates an engineering environment and tools used to configure and maintain it. Users interact via a human-machine interface (HMI).

SISs also provide control based on signals received from field devices; but unlike PASs, which are optimized to handle high volumes of complex process logic, SISs are applied to provide safe and orderly shutdown of operations that might otherwise fall under the control of the PAS. When applied for this purpose, SISs are also called emergency shutdown systems (ESDs.) For the highly critical ESD function, SISs are optimized for speed and reliability. The control elements are usually redundant, high speed, programmable logic controllers that have been heavily tested and certified for reliability.

Virtually all medium to large companies processing hazardous materials or running otherwise potentially dangerous operations will implement an SIS to back up their PAS. These systems provide independent control of a process operation, typically using dedicated field devices, I/O networks, engineering workstations, configuration tools, and HMIs. This is by far the dominant approach taken throughout the world. And more often than not, the PAS and SIS have been from different vendors.

Efforts to make more strategic use of safety operation information or to save money through consolidation of safety and control functions have led to the emergence of a number of ICSS models. In its 2013 “Process Safety Systems Global Market Research Study,” ARC identifies four levels of control/safety integration: separate, interfaced, integrated but separate, and common. We will look at each option in more detail and evaluate them according to their impact on safety, productivity, and cost control.

Maintaining separate control and safety architectures

Ask most safety engineers for their preferred level of integration and most would opt for no integration at all. That is what Schneider Electric found in a 2010 survey of more than 200 Schneider Electric customers, including 23 of the top 25 petroleum companies and 45 of the top 50 chemical companies in the world. Seventy-eight percent adhered to strict separation of safety and control for safety protection and 74 percent indicated that independent protection layers (IPL) were critical.

Although the leading standards influencing process safety, IEC 61508 and IEC 61511, have been somewhat ambiguous regarding integrated control and safety, there is no doubt that implementing systems separately satisfies requirements for the independent layers of protection necessary to ensure that a potential hazard could not occur unless both the DCS and SIS fail.

Separate systems also comply most completely with IEC 61511-1 clause 11.2.4 sections that dictate that the PAS shall be designed to be separate and independent to the extent that “the functional integrity of the SIS is not compromised” and IEC 61511-1 clause 9.5, which addresses the requirements for preventing common cause, common mode, and dependency failures, suggesting consideration of the following criteria:

- Independency between protection layers
- Diversity between protection layers
- Physical separation between protection layers
- Common cause failures between protection layers and the DCS

But, because separation does require implementing, operating, and maintaining two different systems, it can also be the most costly route. Also, because operating data is so strictly isolated, there may be lost opportunities for improvements in maintenance, troubleshooting, and trend analysis.

Interfaced ICSS architectures

Interfaced systems still maintain a high degree of separation, but the DCS and SIS exchange information through custom-designed interfaces using standard integration protocols such as OPC, modbus, Profibus®, Profinet, TCP, and HART. These are used most commonly when control and safety systems are from different vendors and the end user needs the systems to share data for a specified purpose.

Assuming that the systems integrators who build the interface have adequate expertise in working with safety systems, this could be a very safe approach. However, the information that it yields will be limited to the specification. Additional ongoing maintenance and subsequent change could be costly. And the integrity of the gateway will not likely have been subjected to third-party validation.

Integrated but separate ICSS architecture

In the third model, which ARC has labeled “integrated but separate,” the safety and control logic solvers are deployed on independent buses of the control network. Clients can share process data across isolated sub networks but do not share control functionality. In the Schneider Electric Foxboro™ Evo PAS, for example, the safety controllers are deployed as peers on a Foxboro Evo MESH control network (Figure 1).

This model formats all data to flow natively between network channels that are physically isolated with one-way communications maintained by a communications module (Figure 2). This example is “integrated” in that companies that want to integrate control and safety data or that want to take advantage of other productivity and cost efficiencies can do so safely. But it is “separate” in that all functionality is implemented on separate devices and the system can be configured as an entirely separate system.

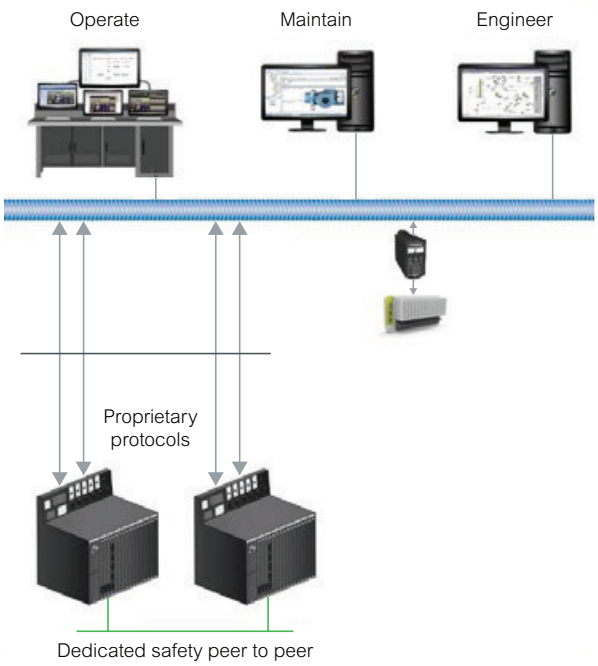

Figure 1

Foxboro Evo integrated but separate control and safety system

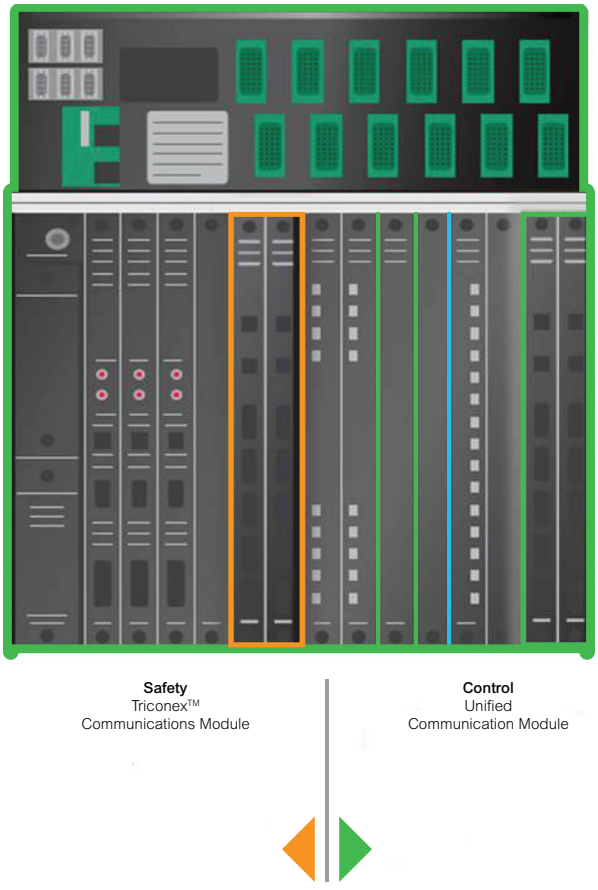

Figure 2

In the Schneider Electric Foxboro Evo implementation of integrated but separate control and safety, network channels are physically isolated with one-way communications maintained by a communications module. Users can choose the level of integration that meets their needs, from fully integrated to complete and total separation.

Generally, integrated but separate control and safety systems are viewed as compliant with IEC standards for IPLs because the network channels are independent and threats to one system will not affect the other. Safe access to data enhances safety, productivity, and cost savings by providing a fully integrated user experience, including sequence of events (SOE) recording, system management, engineering, and maintenance.

- **Integrated SOE repository.** Seamless integration of PAS and the SIS enable shared SOE logging. In the Foxboro Evo integrated but separate implementation, for example, SOE logs and system diagnostic logs are recorded into the same data repository managed by the Foxboro Evo enterprise integration control software platform. Logging all SOE events into the same repository provides end users with a more convenient way to perform a post trip analysis. They can use common tools to review them and identify the true root cause of a trip event more effectively.

- **Integrated system management.** In integrated but separate architectures (Figure 3), all of the capabilities of field diagnostics and asset management, including partial stroke testing, can be implemented more effectively, simplifying actuator testing and avoiding false trips. Such extensive system diagnostics and system management capabilities provide end users with a single application point of view from which they can view the state of the entire system and, if required, acknowledge system alarms. It also minimizes the number of steps it takes to get information from the safety system to the operator; and the fewer the number of steps, the less likely that mistakes will occur. This also simplifies operator training.

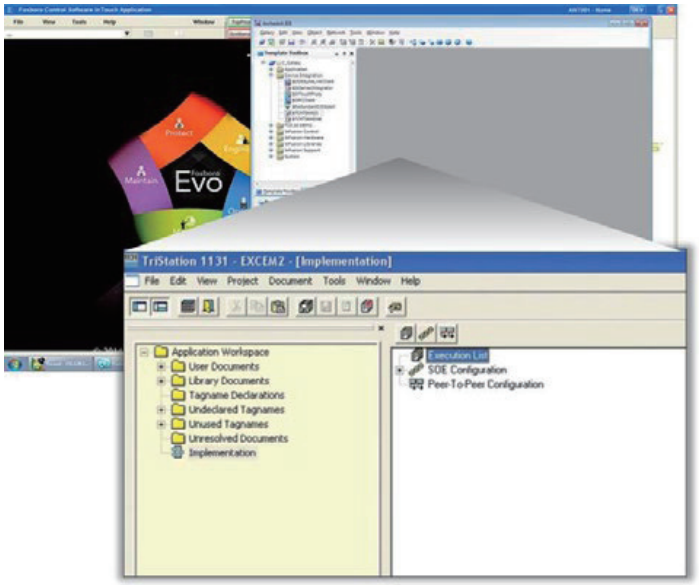

Figure 3

The Foxboro Evo integrated but separate architecture provides end users a single application point of view from which they can view the state of the entire system.

Management of safety instrumented functions would be easier because diagnostics can be sent from sensors to control elements. HART device alerts, for example, can be sent to operators and maintenance personnel as early warning of problems with the device or surrounding process. Predictive testing can help avoid spurious trips on demand.

- **Integrated engineering workflow.** Integrated workflow would ensure that changes in any new tags that might be created in SIS user logic become immediately available to the PAS for use with linking to graphics or historization functions, or to drive interlocking permissions that the PAS might use in a broader control scheme.

  Project engineers would also enjoy a single point of entry and the use of common tools to configure both safety and process control systems, reducing time to start up new installations. Common programming procedures, languages, and installation requirements boost productivity further. Systems engineers would also enjoy improved alarm handling, time synch, user access, and authorization management; and mapping of data would no longer be necessary.

- **Integrated compliance.** The repository, system management, and workflow function of integrated but separate architectures can also assist with compliance with regulations and standards. Integrated systems provide better device audit trails, including calibration history, process and safety configurations, and process and event histories. Both document and change management will be easier.

Because the integrated but separate approach still requires installing, maintaining, and configuring what are essentially separate systems, there would be minimal cost reduction on the technology end, although there might be some economies in communications technology. The greatest financial benefits, however, are in attainment of information, configuration, asset management, and HMI efficiencies, without jeopardizing safety.

It has been widely accepted that the integrated but separate ICSS architectures can meet the IPL requirements of IEC 61508 and IEC 61511. These standards, and particularly their guidance on requirements for maintaining IPLs, are now in revision.

Common platform ICSS architecture

In a common ICSS integration architecture the SIS logic solvers are embedded into a control platform. Many of the information integration benefits possible with the integrated but separate architectures can be achieved in a common model. And, because there is only one control system platform to install and one user environment to manage, this would likely have the lowest system and life cycle costs. But because the number of protection layers is reduced, this is also the highest risk option.

Because the logic solvers are embedded into the same platform as the PAS and the same backplane, an event which causes a problem to the PAS platform would also bring down the SIS, defeating the purpose of an IPL. And it is indeed questionable as to whether a common platform approach could meet the above mentioned IEC criteria for avoiding common cause, common mode, and dependency failures.

Some common ICSS architectures have received third-party SIL 3 certification, which proves that the logic solvers would perform reliably on demand. SIL testing does not, however, address the eventuality of a common cause failure. It is done independently of the application. Furthermore, it does not address issues related to systematic errors inherent in use with the same hardware platform.

Conclusion

In its 2013 study, ARC notes that continued pressures to reduce project risk and total cost are driving more users to seek closer integration between the control and safety systems, thus they are choosing the same supplier for both in new projects. Suppliers that offer the greatest flexibility to integrate systems to multiple risk levels increase ability to protect both plants and people as risk level changes with business needs and external events. So whether a company chooses interfaced, integrated but separate, or common integration, the choice will depend largely on each company's business strategy and tolerance of risk. Companies optimizing on safety at any cost will likely continue to maintain separate systems. On the other extreme, adventurous companies willing to gamble in exchange for maximum cost savings might opt to run the PAS and safety systems on the same platform. Those looking for a balance between cost savings and risk will likely take the integrated but separate approach, which is what ARC believes is gaining traction as the preferred architecture.

Architecture, of course, is only part of the story. The success of any control and safety architecture rests also with the design and quality of the control hardware itself as well as with the expertise of those who implement, operate, maintain, and manage it.

For more information visit **www.foxboro.com/foxboroevo**

About the author

(Grant Le Sueur) Director, Product Management, Schneider Electric
(Phil Knobel) Director, Product Management, Schneider Electric