Integrated Control and Safety: Assessing the Benefits, Weighing the Risks

by Grant Le Sueur and Phil Knobel

Executive summary

While best practices have traditionally called for keeping control and safety functions isolated from each other, new integrated control and safety systems (ICSS) can make more strategic use of data and reduce costs. This paper compares three integrated control and safety architectures — interfaced, integrated but separate, common platform — weighing the benefits and assessing the risks according to compliance with safety standards and cost efficiencies.

998-2095-09-12-14AR0

Foxboro
by Schneider Electric

Schneider Electric

Introduction

Safety instrumented systems (SIS) 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 SIS from faults caused by the same conditions that led to the PAS malfunctioning in the first place, best practices have traditionally dictated the two systems be physically and functionally isolated from each other. However in an effort to balance the often-conflicting business drivers of streamlined enterprise operations, improved safety, and reduced costs, some companies are looking at integrating and consolidating safety and control functions.

An integrated approach whereby process control and safety instrumented functions use a common automation infrastructure — with similar hardware and software dedicated for control and safety functions, respectively — offers cost savings and improved productivity benefits across the enterprise. Safety and risk managers 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 an opportunity to streamline redundant effort. Operations managers see islands of activity that can be better communicated with one another and with rest of the enterprise. Maintenance managers see volumes of data on machine and system health that could contribute to improved equipment performance and lower maintenance costs, and financial managers see redundant capital expenditures and training costs ripe for consolidation into a single system.

Table 1

Integrated control and safety systems (ICSSs) offer cost-savings and improved-productivity benefits across the enterprise.

Managerial function	Benefits of ICSSs
Safety & risk	Insight into leading indicators of future problems
Engineering	Streamlined processes
Operations	Improved communications
Maintenance	Insight into machine and system health
Finance	Reduced capital expenditures, lower training costs

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 integrated control and safety system (ICSS) models. In its 2013 “Process Safety Systems Global Market Research Study,” the global industry analyst firm ARC Advisory Group identifies four levels of control-safety integration: separate, interfaced, integrated but separate, and common platform. This paper compares the four approaches and evaluates the risks and benefits of each according to their impact on safety, productivity and cost control.

> *“ARC Advisory Group believes that most companies will seek a balance between cost savings and risk, and take the integrated but separate approach”.*

- **separate control and safety architecture:** complete physical separation between control and safety systems
- **interfaced ICSS architecture:** integration via a custom-programmed software interface
- **integrated but separate ICSS architecture:** integration via isolated subsystems on a client-server control network
- **common platform ICSS architecture:** integration across a common control platform

Which architecture is best for a particular company depends on the organization's business strategy and tolerance for risk. At companies where safety at any cost is top priority, separate control and safety systems are likely to continue remain the preferred approach. Companies looking to maximize cost savings are more likely adopt a common platform ICSS. ARC Advisory Group believes that most companies, however, seek a balance between cost savings and risk, and will increasingly take the integrated but separate approach.

The difference between a PAS and an SIS

Although both the process automation and safety instrumented are control systems, they are designed for fundamentally different purposes.

A process automation system (PAS), also often called a distributed control system (DCS) or basic process control system (BPCS), 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).

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

Virtually all medium to large companies processing hazardous materials or running otherwise potentially dangerous operations 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 the SIS are manufactured by different vendors.

Separate control and safety architecture

Most safety engineers would prefer that there be no integration between safety and control systems at all. That is what Schneider Electric found in a 2010 survey of more than 200 of its chemical, oil, and gas process plant customers, including 23 of the top 25 petroleum companies and 45 of the top 50 chemical companies in the world. A full 78 percent adhered to strict separation of safety and control for safety protection, and 74 percent indicated that independent protection layers (IPL) were critical. (See **Figure 1**.)

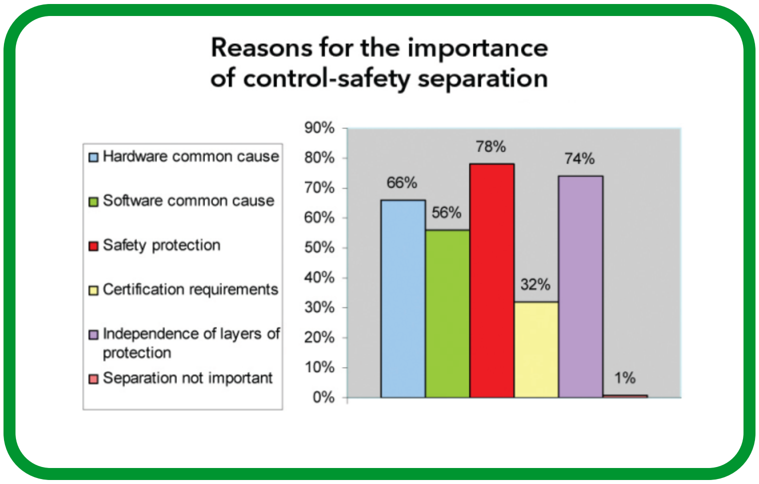

Figure 1
Some 78% of 200 chemical, oil, and gas process plant companies surveyed adhered to strict separation of safety and control functions.

Glossary

BPCS basic process control system
DCS distributed control system
ESD emergency shutdown system
HMI human machine interface
ICSS integrated control and safety system
IEC International Electrotechnical Commission
I/O input/output
IPL independent protection layer
PAS process automation system
PLC programmable logic controller
SIS safety instrumented systems
SOE sequence of operations

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 11.2.4 sections dictating that the process automation system 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

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

Interfaced ICSS architecture

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 made by different vendors and the user needs the systems to share specified data for a specified purpose.

Assuming that the systems integrators who build the interface have adequate expertise in working with safety systems, this can be a very safe approach. However, the information that it yields is limited to only what was specified. Additional ongoing maintenance and subsequent changes may be costly, and the integrity of the gateway likely has not been subjected to third-party validation.

Integrated but separate ICSS architecture

In the third model, which the ARC Advisory Group calls “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. For example, safety controllers are deployed as peers on a MESH control network (**Figure2**).

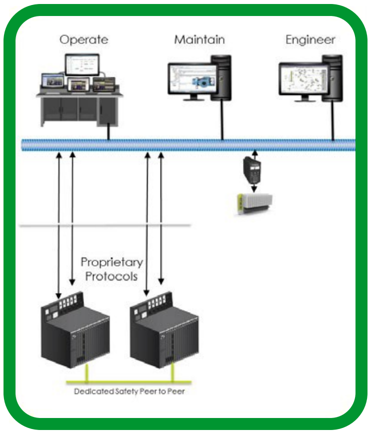

Figure 2
An integrated but separate control and safety system shares process data but not control functionality.

The integrated but separate approach 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 approach is "integrated" in that companies wanting to integrate control and safety data or wanting 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.

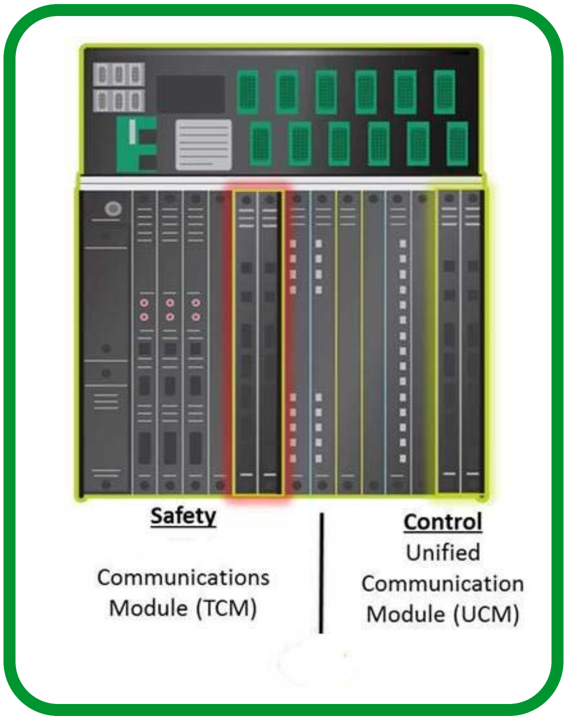
Safety
Communications Module (TCM)
Control
Unified Communication Module (UCM)

Figure 2
The system may be "separate" by physically isolating network channels, but "integrated" with one-way communications maintained by a communications module.

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

"The fully integrated user experience enhances safety, productivity, and cost savings."

Integrated sequence of events repository Seamless integration of PAS and the SIS enable shared sequence of event (SOE) logging. Sequence of events logs and system diagnostic logs are recorded into the same data repository managed by an enterprise integration control software platform. Logging all SOE events into the same repository provides 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 architecture, all of the capabilities of field diagnostics and asset management — including partial stroke testing — are implemented more effectively, simplifying actuator testing and avoiding false trips. Such extensive system diagnostics and system management capabilities provide users with a single application point of view from which they can view the state of the entire system (**Figure 3**) 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. The fewer the number of steps, the less likely that mistakes will occur. This also simplifies operator training.

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

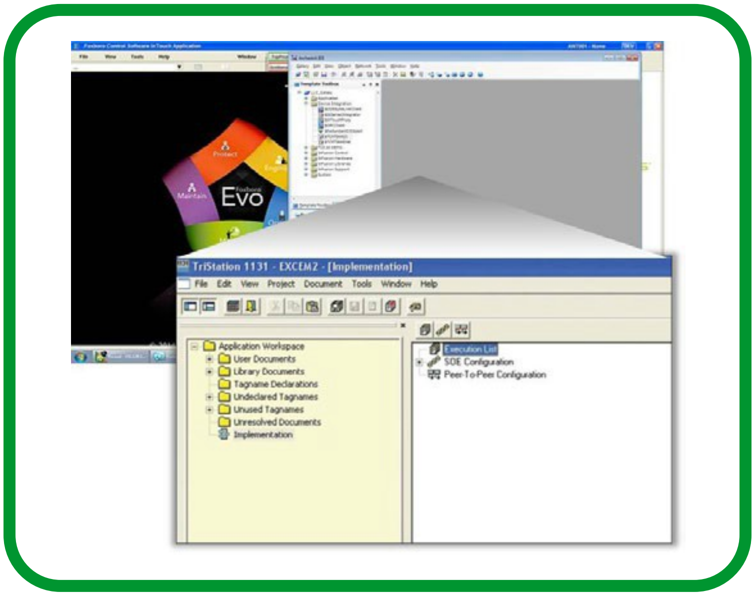

Figure 3

A single application point of view lets users monitor the state of the entire system.

Integrated engineering workflow Integrated workflow ensures 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 also benefit from a single point of entry and 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 also see improvements in alarm handling, time synch, user access. and authorization management. And it is no longer be necessary to map data.

Integrated compliance The repository, system management, and workflow functions of integrated but separate architecture 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 are easier.

“The greatest financial benefits are in information-attainment, configuration, asset management, and HMI efficiencies.”

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 realized in communications technology. The greatest financial benefits, however, are in information-attainment, configuration, asset management, and HMI efficiencies, without jeopardizing safety.

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

Common platform ICSS architecture

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

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

Some common platform ICSS architecture has received third-party Safety Integrity Level (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 when using the same hardware platform.

Conclusion

In its 2013 study, the ARC Advisory Group notes that continued pressure to reduce both project risk and total costs are driving more users to seek closer integration between the control and safety systems. For new projects many companies prefer the same supplier for both systems. Choosing vendors who offer the flexibility to integrate systems according multiple risk levels gives companies maximum ability to protect their plant and people as their risk level changes with their business needs and external events.

Whether to choose interfaced, integrated but separate, or common platform integration depends largely on each company's business strategy and tolerance of risk. Companies that are looking to optimize safety at any cost are likely continue to maintain separate systems. At the other extreme, adventurous companies willing to gamble in exchange for maximum cost savings may opt to run the process automation and safety systems on the same platform. Those looking for a balance between cost savings and risk are more likely to take the integrated but separate approach, which is what the ARC Advisory Group believes is gaining traction as the preferred architecture.

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

About the authors

Grant Le Sueur is the Director of Product Management for Schneider Electric Foxboro control and safety software offerings, including external marketing, product planning, and development. He has more than 28 years of industry experience. He began his career in the pulp and paper industry serving as an instrument engineer at Tasman Pulp and Paper Company in New Zealand. He has served as process control engineer at Siemens AG, where he was responsible for DCS and PLC implementations. He is also certified as a functional safety engineer.

Phil Knobel is a Product Management Director within Schneider Electric's Industry business. He holds a BSEE degree from Rensselaer Polytechnic Institute and a MSEE degree from Northeastern University. He has over 30 years' experience in the industrial applications field.