ARC INSIGHTS

INSIGHT# 2006-17MPH
APRIL 13, 2006

Need for Cost Effective Systems Drives Safety and Control Integration

By Asish Ghosh

Keywords

BPCS, Integration, Process Control, Safety, SIS

Summary

Manufacturers today are under pressure to contribute value to a company's bottom line by continuously improving the performance of their assets. In addition, difficulties in getting approval for the addition of new plants or major units in industrially developed countries are making existing assets more valuable and important to protect. Today's business drivers focus on metrics such as Return on Assets (ROA) and Overall Equipment Efficiency (OEE), both of which are critical contributors to the overall goal of achieving Operational Excellence (OpX). Unscheduled downtime – unexpected stoppages resulting from equipment failure, operator error, or nuisance trips - is the nemesis of all manufacturers. Safety solutions available today offer improved diagnostics that minimize the chance of nuisance trips. They integrate directly into standard control architectures, allowing improved asset and event management and thus minimizing the chances of failure.

Integrating safety and control is a cost effective way to improve your bottom line.

Analysis

Standalone safety systems have been the traditional solution of choice, which meant different design and operation requirements for Basic Process Control Systems (BPCS) and Safety Instrumented Systems (SIS). The primary function of a BPCS is to hold specific process variables to predetermined level in a dynamic environment. An SIS, on the other hand, is static, waiting to take action to bring the process to a safe state when it is out of control and the BPCS is unable operate within safe limits. As a result, separate systems were developed for process control and safety with separate operator interfaces, engineering workstations, configuration tools, data and event historians, asset management, and network communications.

Lifecycle costs, such as spare parts, support, training, maintenance, and service are higher with this approach. Added costs are incurred because these interfaces are engineering-intensive and expensive to maintain and synchronize. An SIS is also a costly solution for end users, considering that it has no definitive return on investment unless something goes wrong.

Until recently, users have had little choice other than to use completely different systems for control and safety. Some users even mandated that the BPCS and SIS be supplied from different manufacturers. There continue to be many other good reasons to put safety and control functions in different controllers. They include:

- Independent failures: minimizing the risk of simultaneous failure of a BPCS along with the SIS
- Security: preventing changes in a BPCS from causing any change or corruption in the associated SIS
- Different requirements: an SIS is normally designed to fail in a predictably safe way, whereas a BPCS is usually designed for maximum availability
- Special features for SIS: extended diagnostics, special software error checking, protected data storage, and fault tolerance

Benefits:
No need for data mapping
Single set of engineering tools
Significant reduction in integration efforts
Lower life-cycle cost
Challenges:
Putting hardware and software barriers between safety and control systems
Ensuring proper access protections
Ensuring visual differentiation between control and safety environments

Benefits and Challenges: Integration of Safety and Control Systems

Integrated Safety and Control

Integrating both safety and control in the same controller has become a cost effective way for manufacturers to implement an SIS. This has become a consideration because the safety standards for process industry applications are somewhat ambiguous on the issue of separation, which is mandated only in nuclear power industry applications (IEC 61513).

Today, many users are finding logical reasons to justify using similar systems for control and safety functions, such as reducing the problems associated with different programming procedures, languages, installation requirements, and maintenance. Other financial benefits include reduced hardware, configuration, training, and inventory costs. In addition, the burden of different service and support help associated with disparate systems is reduced.

The degree of integration between SIS and BPCS may be categorized into four levels: separate, interfaced, integrated, and common. Some BPCS and SIS suppliers now offer similar systems for either function that incorporate similar HMI, configuration procedures, programming languages, and maintenance procedures.

Level of Integration	Engineering Tools		Systems and Networks	
	Advantages	**Drawbacks**	**Advantages**	**Drawbacks**
Separate		Higher installation, engineering and training costs because of need to implement two separate systems Higher lifecycle costs due to the need to manage and maintain two separate databases	No common cause failure Better protection against cyber attacks Failure of BPCS has no impact on SIS Fewer management challenges	Higher lifecycle costs due to the need to manage and maintain two separate systems
Interfaced		Higher installation and engineering costs Additional training and maintenance	Reduced common cause failures	Gateway issues; unknown failure modes of the gateway, and potential throughput issues
Integrated	Lower engineering & life-cycle cost Lower training and maintenance expenses Easier time synchronization Improved asset & event mgmt.	Requirement for very rigorous user management capability	Lower cost of hardware through common backplanes and communications	Increased risk of common cause failures Some BPCS failures will impact SIS Greater management challenges Need careful design to ensure that BPCS failure modes do not lead to dangerous conditions
Common	Lowest system & life-cycle expenses Significantly lower installation and engineering costs Little need for additional training and maintenance. Improved asset & event mgmt			Reduction in the number of layers of protection Failure due to common cause can be a significant issue Increased expenses and mgmt. challenges as whole system may need to be treated as SIS

INCREASING ADVANTAGES

INCREASING ADVANTAGES

Levels of SIS Integration with Control Systems

The key is to ensure that the two systems are separate with different hardware, software, and networks, even though they share a common configuration, operations, and maintenance interface. This allows users to achieve the operational benefits of integration while meeting the safety requirement for separation.

Suppliers Are Now Offering Integrated SIS

A number of BPCS system suppliers, such as ABB, Emerson, Siemens, and Yokogawa, are offering integrated control and safety systems. Some of them, like ABB and Yokogawa, have updated or modified their process controllers for safety applications. Emerson, on the other hand, chose to develop an entirely new controller module for safety applications with a higher degree of scalability than their process control modules.

Integrated systems pose greater management challenges since they need careful design to reduce risks from common cause failures.

The new distributed safety concept offered by some suppliers enables programming of safety functions in the same graphical environment used to configure non-safety functions, but in distinctly different organizational units within the project. Safety functions are color-coded so that they are readily distinguishable from non-safety functions. This allows safety functions to be designed, reviewed, commissioned, and locked in, while non-safety related code could be edited with lesser restrictions. In addition to stand-alone SIS, suppliers are now offering TÜV certified systems for the three levels of integration.

Recommendations

- Adopt IEC 61511 or ANSI/ISA-84.00.01 as your safety implementation standard and perform rigorous hazard and risk analysis to decide on the right level of protection for your manufacturing plants.

- Based on the analysis, make a short list of certified SIS suppliers that meet all of your risk management needs, offer state-of-the-art tools for safety lifecycle management, scaleable solutions, and global support.

- Choose a system from the list that will provide tight integration with the software tools of your BPCS while still providing the required degree of separation between the control and safety hardware platforms.

For further information or to provide feedback on this Insight, please contact your account manager or the author at aghosh@arcweb.com. ARC Insights are published and copyrighted by ARC Advisory Group. The information is proprietary to ARC and no part of it may be reproduced without prior permission from ARC.