

## ARC WHITE PAPER

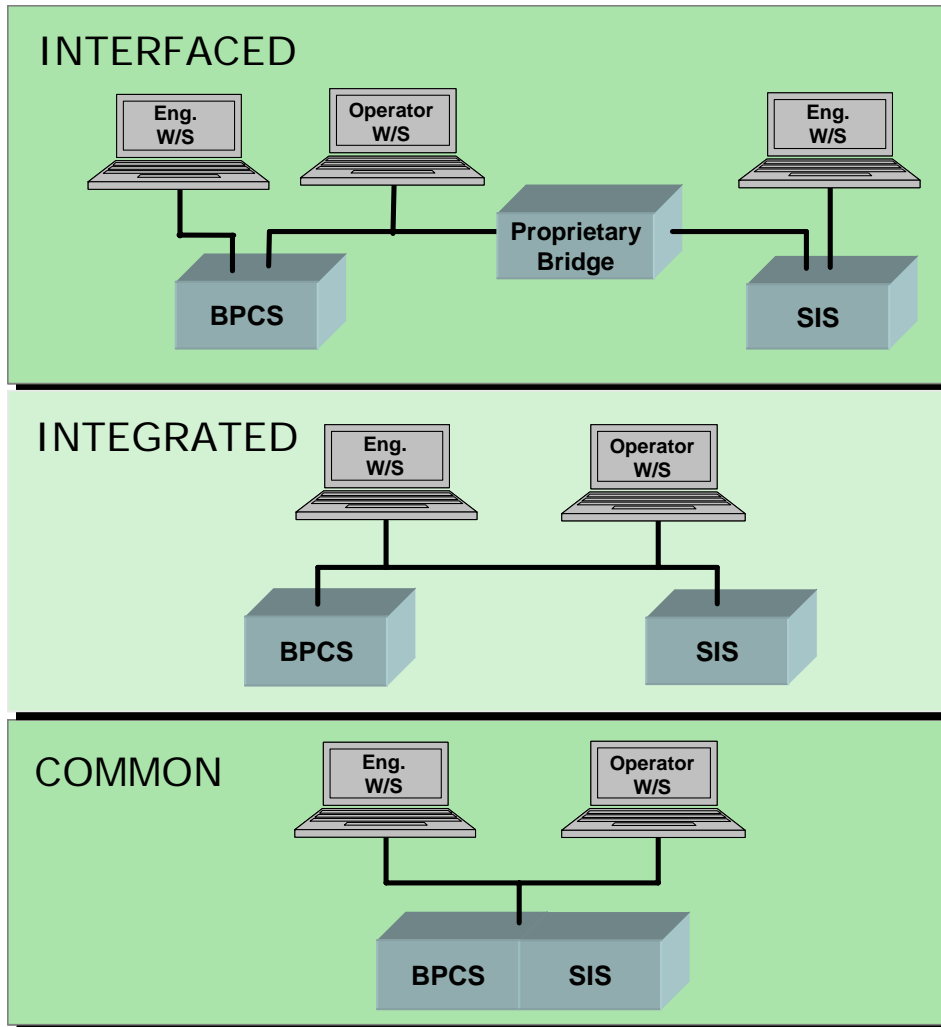
By ARC Advisory Group

FEBRUARY 2006

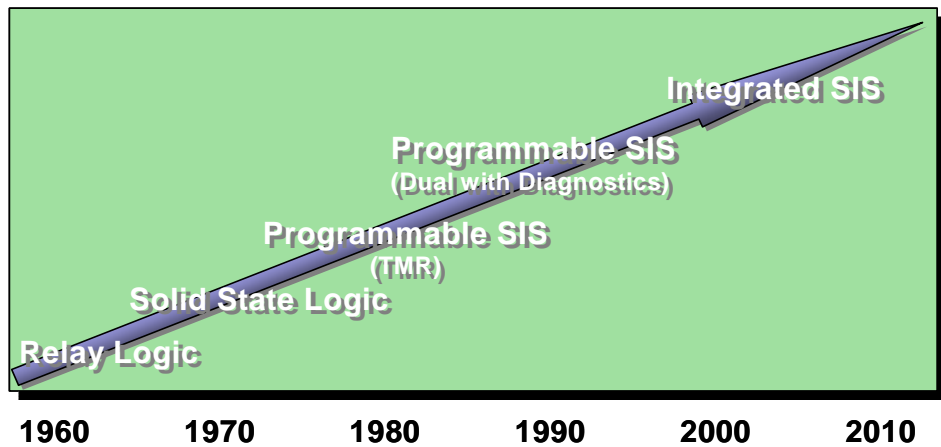
# Business Issues Driving Safety System Integration

Executive Overview .....	3
Business Issues are Driving towards Safety System Integration .....	4
The Importance of Risk Reduction .....	4
The Need for Cost Effective Safety Systems .....	5
Separate Safety and Control.....	5
Integrated Safety and Control .....	7
Suppliers are Offering Integrated SIS.....	8
Recommendations .....	10





SIS and BPCS Integration Levels



From Relay Logic to Integrated SIS

## Executive Overview

---

Manufacturers today are under pressure to contribute value to a company's bottom line by continuously improving the performance of their assets. Also, in industrially developed countries the difficulties in getting approval for the addition of new plants or major units 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). The nemesis of all manufacturers is unscheduled downtime - unexpected stoppage resulting from equipment failure, operator error, or the most exasperating nuisance trips. Safety solutions available today offer improved diagnostics that minimize the chance of nuisance trips. They integrate directly into standard control architec-

Manufacturers are under pressure to enhance the performance of their assets. For them, integrating safety and control is a cost effective way to improve their bottom lines.

tures, allowing improved asset and event management thus minimizing the chances of failure.

Stand-alone safety systems have been the traditional method of choice, which meant separate design and operation requirements for basic process control systems (BPCS) and safety instrumented systems (SIS). 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. That adversely affected the cost of infrastructure acquisition, plant systems integration, control and instrumentation hardware, wiring, project execution, installation, and commissioning, as well as ongoing expenses such as training, spare parts holding, and support contracts.

Until recently, users 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. Today, integrating safety and control has become a cost effective way for manufacturers that could not justify a separate SIS in the past. As a process manufacturer, you need to perform rigorous hazard and risk analysis based on IEC 61511 or ANSI/ISA-84.00.01 safety standards to decide on the right level of protection required for your manufacturing plants. You may follow that by selecting an SIS that provides close integration with the software tools of your BPCS while still providing the required degree of separation.

## Business Issues are Driving towards Safety System Integration

Process safety in the traditional sense refers to add-on components that protect personnel working in or near hazardous manufacturing processes from injury or death and from economic loss. However, modern safety solutions go far beyond this notion. Many end users now recognize that the deployment of intelligent, integrated safety solutions can directly affect their bottom line, while simultaneously improving process and personnel safety.

Manufacturers today are under pressure to contribute value to a company's bottom line by continuously improving the performance of their manufacturing assets. 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). The nemesis of all manufacturers is unscheduled downtime - unexpected stoppage resulting from equipment failure, operator error, or nuisance trips. 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 thus minimizing the chances of failure.

### The Importance of Risk Reduction

Risk is usually defined as the combination of probability and the severity of a hazardous event. That is, how often can it happen and how bad are the consequences when it does. Examples of events and their associated risks in manufacturing operations include loss of life or limb, environmental impact, loss of capital equipment, and loss of production. For many manufacturers, loss of company image can also be a significant risk factor. Add to these issues

Operating plant & machinery close to their limits
Transient operation states (startup, shutdown, shift change, work force transitions)
Use of hazardous raw materials
Manufacture of hazardous intermediates
Presence of untrained personnel
Absence of safety culture

#### Factors that Increase Risk

the realities of increased environmental awareness, regulatory concerns, and threat of litigation and it is easy to see why risk reduction is becoming increasingly important to most manufacturers.

The best way to reduce risk in a manufacturing plant is to design inherently safer processes. Risks exist wherever risky equipments are used and hazardous or toxic materials are stored, processed, or handled.

Since it is impossible to eliminate all risks, a manufacturer must agree on a level of risk that is considered tolerable. After identifying the hazards, a

Higher environmental awareness

Increased regulatory considerations

Emergence of safety standards

Maintaining company image

**Forces Driving Lower Risk**

hazard and risk study should be performed to evaluate each risk situation by considering its likelihood and severity. Site-specific conditions, such as population density, in-plant traffic patterns, and meteorological conditions should also be taken into consideration during risk evaluation.

Once the hazard and risk study has ascertained the risks, it can be determined whether they are above tolerable levels. Basic process control systems (BPCS), along with process alarms and facilities for manual intervention, provide the first level of protection and reduce the risk in a manufacturing facility. Additional protection measures are needed when a BPCS does not reduce the risk to a tolerable level. They include safety-instrumented systems (SIS) along with hardware interlocks, relief valves, and containment dikes. To be effective, each protection subsystem must act independently of all others.

## The Need for Cost Effective Safety Systems

Since the publication of general safety standards such as IEC 61508 and process safety standards IEC 61511 and ANSI/ISA-84.00.01, manufacturers worldwide are becoming more knowledgeable about safety issues. They are now performing more thorough hazard and risk analysis and are looking for cost effective safety systems that protect them from their residual risks.

### Separate Safety and Control

Stand-alone safety systems have been the traditional method of choice, which meant different design and operation requirements for BPCS and 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 a process 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. That adversely affected the cost of infrastructure acquisition, plant systems integration, control and instrumentation hardware, wiring, project execution, installation, and commissioning.

Lifecycle costs, such as spare parts, support, training, maintenance, and service are also higher with this approach. Added costs are incurred because these interfaces are engineering intensive and expensive to maintain and synchronize. It is a costly solution for end users, considering that an SIS 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.

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

**Benefits and Challenges:  
Integration of Safety and Control Systems**

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 for safety controllers - an SIS is normally designed to fail in a predictably safe way, whereas a BPCS is usually designed for maximum availability. An SIS also has special features like extended diagnostics, special software error checking, protected data storage, and fault tolerance.

features like extended diagnostics, special software error checking, protected data storage, and fault tolerance.

### 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).

Level of Integration	Engineering Tools		Systems and Networks	
	Advantages	Drawbacks	Advantages	Drawbacks
<b>Separate</b>		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
<b>Interfaced</b>		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
<b>Integrated</b>	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
<b>Common</b>	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

Levels of SIS Integration with Control Systems

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.

The financial benefits of using similar systems are also quite apparent; reduced hardware, configuration, training, and inventory costs result from the reduced range and quantity of equipment that is required. In addition, the burden of different service and support help associated with disparate systems is removed.

Integrated and common platforms for control and safety need very rigorous user management to ensure that only the right people have access to the right functionality.

In addition to separate SIS and BPCS, the degree of integration between them may be categorized into three levels: interfaced, integrated, and common. Some BPCS and SIS suppliers now offer similar

systems for either function, which incorporate similar HMI, configuration procedures, programming languages, and maintenance procedures. The key is to ensure that the two systems are separate with different hardware, software, and networks, even though they have a common configuration, operations, and maintenance interface. This allows users to achieve the operational benefits of integration while meeting the safety requirement for separation. The BPCS and SIS communicate transparently with each other, but have adequate protection from corruption of one by the other.

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 also 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, providing wider choice to the users.

## **Suppliers are Offering Integrated SIS**

---

Today, 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.

ABB's 800xA system architecture allows putting control and safety in one box, if needed. The AC800M HI (High Integrity) controller offers a TÜV certified control environment for combining safety and business critical process control in one controller. The AC 800M HI, in combination with a diverse co-processor, performs diagnostics and monitoring of application execution and I/O scanning. Certified firewalls isolate safety and process control applications from one another, enabling them to reside in the same controller and run concurrently. It is certified by TÜV for up to SIL 2 applications. ABB's objective is to get it certified for SIL 3 applications in the

Integrated control and safety reduces engineering, commissioning, and maintenance costs, lowers training and inventory costs, and reduces the burden of different service and support help associated with disparate systems.

near future. **ABB's 800xA SIS offers integrated control and safety hardware and networks with a single set of engineering tools.**

Siemens has developed an integrated safety solution for its process safety customers. The SIMATIC S7 safety system is tightly integrated into SIMATIC PCS7. Additionally, the SIMATIC S7 safety system can be configured as a common solution for both control and safety functions. Siemens' solution is to have a safety-rated controller running both control and safety code and using a common network to communicate with both safety and control I/O modules. Separation is achieved in software through time and calculation diversity. This is certified by TÜV for up to SIL 3 applications. **Siemens' SIMATIC S7 SIS offers common control and safety hardware and networks with a single set of engineering tools.**

Yokogawa's ProSafe-RS safety controllers are built on the same basic packaging as their downsized process controllers. They connect directly to Yokogawa's V-net, which means they communicate directly with the DCS system and workstations, as well as other safety controllers. Yokogawa's BPCS can operate and monitor their SIS since they share the same control network, human interface, and data. Yokogawa claims that, since operators can perform safety monitoring in an operation and monitoring environment that they are already familiar with, overall plant safety is greatly improved. In addition, alarms reported by the BPCS and the SIS can be simultaneously displayed on a single screen for quick response. **Yokogawa's ProSafe-RS SIS offers integrated control and safety hardware along with common control and safety networks but separate engineering tools.**

Emerson's DeltaV SIS uses the same workstations for operations, engineering, and maintenance, with a rigorous user manager to ensure that only the right people have access to safety functions. The use of a common software

platform gives the operational benefits of a high level of integration of control and safety. At the same time, the hardware and networks of the SIS and BPCS are kept separate, using entirely different technologies, software, and protocols. This architecture allows each SIS controller to be a stand-alone, self-contained logic solver with its own pair of redundant CPUs,

Emerson's DeltaV SIS offers a high level of integration with control while maintaining a clear separation from BPCS. This architecture allows each safety controller to be a stand-alone, self-contained logic solver with its own pair of redundant CPUs, redundant power supply, and separate I/O processor.

power supply, and I/O processor. If required, it can be installed on the same carrier as standard BPCS modules, while maintaining complete independence of power supplies, communication networks, hardware, and operating systems. Non-safety related communications between SIS and BPCS are automatically implemented on the control network without the need for mapping of tags between SIS and BPCS. All alarm handling, configuration, time

synchronization, security, and device health monitoring are provided invisibly and automatically. All of the data in the SIS is available to BPCS on a read only basis. **Emerson's DeltaV SIS offers separate control and safety hardware and networks along with a single set of engineering tools**

## Recommendations

---

- Adopt IEC 61511 or ANSI/ISA-84.00.01 as your safety implementation standard.
- Perform rigorous standards-based hazard and risk analysis to decide on the right level of protection for your manufacturing plants.
- Based on the hazard and risk analysis, make a short list of certified SIS vendors that meet all of your risk management needs and offer state-of-the-art tools for safety lifecycle management, scaleable solutions, and worldwide support.
- Reduce the engineering life-cycle and training costs by choosing 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.

**Analyst:** Asish Ghosh

**Editor:** Dave Woll

**Acronym Reference:** For a complete list of industry acronyms, refer to our web page at [www.arcweb.com/Community/terms/terms.htm](http://www.arcweb.com/Community/terms/terms.htm)

<b>ANSI</b> American National Standards Institute	<b>OEE</b> Overall Equipment Efficiency
<b>BPCS</b> Basic Process Control System	<b>OpX</b> Operational Excellence
<b>DCS</b> Distributed Control System	<b>ROA</b> Return on Assets
<b>HAZOP</b> Hazard & Operability	<b>SIL</b> Safety Integrity Level
<b>HMI</b> Human Machine Interface	<b>SIS</b> Safety Instrumented System
<b>IEC</b> International Electrotechnical Commission	<b>TMR</b> Triple Modular Redundancy
<b>ISA</b> Instrumentation, Systems, and Automation Society	<b>TÜV</b> Technischer Überwachungs-Verein (Technical Inspection Association)

Founded in 1986, ARC Advisory Group has grown to become the Thought Leader in Manufacturing and Supply Chain solutions. For even your most complex business issues, our analysts have the expert industry knowledge and firsthand experience to help you find the best answer. We focus on simple, yet critical goals: improving your return on assets, operational performance, total cost of ownership, project time-to-benefit, and shareholder value.

All information in this report is proprietary to and copyrighted by ARC. No part of it may be reproduced without prior permission from ARC. This research has been sponsored in part by Emerson Process Automation. However, the opinions expressed by ARC in this paper are based on ARC's independent analysis.

You can take advantage of ARC's extensive ongoing research plus experience of our staff members through our Advisory Services. ARC's Advisory Services are specifically designed for executives responsible for developing strategies and directions for their organizations. For subscription information, please call, fax, or write to:

ARC Advisory Group, Three Allied Drive, Dedham, MA 02026 USA  
 Tel: 781-471-1000, Fax: 781-471-1100, Email: [info@ARCweb.com](mailto:info@ARCweb.com)  
 Visit our web page at [ARCweb.com](http://ARCweb.com)



3 ALLIED DRIVE DEDHAM MA 02026 USA

---

BOSTON, MA | PITTSBURGH, PA | PHOENIX, AZ | SAN FRANCISCO, CA  
CAMBRIDGE, U.K. | Düsseldorf, GERMANY | MUNICH, GERMANY | HAMBURG, GERMANY | TOKYO, JAPAN | BANGALORE, INDIA