EVOLUTION OF PLANT AUTOMATION

Angela Summers, PhD, PE, President, SIS-TECH Solutions, LP

Published as "The Evolution of Plant Automation, Control Global, February 2007.

Protective Systems

Most owner/operators continue the practice of implementing separate, and often diverse, platforms for the BPCS and SIS.

Within the process industry, control functions are used to achieve production and product quality targets, reduce manpower requirements, reduce human errors, and improve process uptime. In the early years, control functions were mostly pneumatic and were physically mounted on control valves, I-beams, and the walls of plants, it was truly distributed control in the field. By the time the first distributed control system (DCS) was introduced in the late 1970's, control functions had been relocated into central control rooms with their long steel panel boards of controllers, indicators, alarm panels, and switches and lights.

Despite its name, the introduction of the DCS actually caused control to become further centralized by placing multiple control functions into one microprocessor based controller, thus the requirements for redundant controllers was born. Today we have digital "open" control systems that are far more robust and capable in terms of performance and diagnostics than their DCS predecessors, but that doesn't mean they can be relied on to perform control and safety functions.

Understand the Differences:

Control systems execute one or more control functions, which cause the process to operate within the normal operating limits. Control functions can be executed manually or automatically. Operators supervise the process using the control system interface, respond to its indications and alarms, and, when necessary, use it to act on the process.

The control system may be implemented as part of a basic process control system (BPCS), which is separate and independent of the safety instrumented system (SIS). The BPCS may execute control and safety functions when it is designed and managed to achieve the assumed risk reduction or hazard rate. A BPCS may not execute a safety instrumented function with a SIL ≥ 1 (see ISA 84.01/IEC 61511, clause 3.2.3).

Use of the BPCS to perform a safety function is highly restricted, since a dangerous failure somewhere within the system may lead to the loss of control and potentially to a hazardous event. Control functions are often configured to continue plant operation on detected failure rather than failing to a safe state. The dangerous failure rate of a BPCS that places a demand on a protection layer cannot be assumed to be better than 10-5 per hour (see ISA 84.01/IEC 6151l, clause 8.2.2).

The BPCS is generally designed and managed using a less restrictive user approval process than the SIS, thereby allowing for more rapid deployment of new technologies. Validation, access security, and management of change requirements are also typically more flexible and performed on an “as needed” basis within the bulk of the process industry. Some industry sectors, such as those falling under food and drug requirements, do incur rigid administrative controls and validation processes for the BPCS. However, most BPCS are not rigorously designed and managed. Many allow nearly open connection of the BPCS with other data systems internal or external to the facility. The system is therefore vulnerable to unknown impacts of these other systems and the people responsible for them.

The use of the BPCS to perform a safety function should be approved by a hazard and risk analysis team, which considers the initiating cause and any potential common cause or common mode failures within the system. The risk reduction factor for a BPCS used as a protection layer must be assumed to be below 10 (see ISA 84.01/IEC 61511, clause 9.4.2).

When the SIS is independent of the BPCS, it generally operates as a dormant system that takes action only in response to operation outside the normal operating envelope. These process demands are often caused by failures within the BPCS. The SIS is designed and managed to ISA 84.01/IEC 61511 to achieve a specified safety integrity level (SIL). Most SIS’s are designed to fail to the safe state on loss of power or other support systems. SIS devices are also configured to fail to the safe state on detected failure unless compensating measures are available to reduce the risk equivalently to the failed device.

Independence is a fundamental principle in the design of the SIS, regardless of the capability of the BPCS. The systems should be sufficiently independent such that one system can suffer a complete system collapse while the other system remains fully functional. If this criterion cannot be met, the entire system–BPCS and SIS–must be designed and managed as an SIS under the rigors of ISA 84.01/IEC 61511.

Maintaining such rigor dramatically increases the cost of BPCS ownership and significantly restricts BPCS flexibility. However, applying the ISA 84.01/IEC 61511 lifecycle and its associated quality management system to the BPCS can add significant benefits because better managed systems tend to operate more reliably.

As technology has evolved, emphasis continues to be placed on maintaining the independence and separation of the BPCS and SIS functions to reduce system complexity and the potential for systematic errors. While integrated technology often decreases resource needs, it typically demands resources with specific skills, knowledge, and experience. When separation is not provided, the potential for human error increases as system components are accessed more frequently. The approximate ratio of BPCS to SIS input and output signals is more than 90% BPCS to less than 10% SIS. When these systems are combined, the need for access significantly increases. Increased system access results in a greater potential for inadvertent and unintentional changes resulting in an increased need for a more rigorous management system.

Finally, when the BPCS and SIS are combined into a single SIS, the logic solver likely operates in a continuous mode because a dangerous failure within the logic solver may cause a simultaneous loss of control and safety functions. This additional system complexity makes aspects of the lifecycle more difficult, including the assessment of independent protection layers in the risk assessment, development of the fault detection and response strategy, and design verification. However, in some specialized applications, such as turbine controls and shutdown, the greater complexity is frequently justified.

Armed with the knowledge of the differences of the BPCS and SIS, lets now explore some of the advantages and disadvantages of their use.

Understanding the BPCS

In the early days of process automation, the BPCS consisted of pneumatic transmitters and controllers that operated the control valve by adjusting its output air signal to the positioner on the valve. These pneumatic controllers were used to perform relatively simple control functions. Over time, the BPCS evolved into programmable logic controllers (PLC) and distributed control systems (DCS), which are based on programmable electronic (PE) technology. PE technology brought an increased ability to execute more control functions on a single platform. This processing capability allowed the implementation of statistical process control, predictive control algorithms, and other advanced control techniques, resulting in tremendous productivity and quality improvements.

The integrity of the BPCS hardware has steadily improved over the years with increased internal diagnostics allowing these systems to be configured to obtain the desired process reliability. The capability to implement redundant components throughout the system, including input/output modules and main processors, has further enhanced reliability. Extensive internal and external diagnostics have also been incorporated into the field device design, providing more rapid fault detection.

Today, most process units are highly dependent on automated control systems. Operators rely on the BPCS and its operator interface for process information during normal operation, for alarms during process excursions, and for troubleshooting process control problems. The BPCS is now so specialized that typically only a few site personnel are knowledgeable in the control system design details and are responsible for implementing solutions to optimize the BPCS in order to garner improvements in quality, production, and cost. BPCS technology provides significant benefits with its capabilities and flexibility, but it also introduces new and more complex failures. This creates an environment where, if administrative controls are not in place, the BPCS exists in an almost endless state of flux where control loops are routinely placed in manual mode, alarms are disabled or reset by operators based on personal choice, and process control specialists implement the newest in control algorithms while the process unit is in operation.

Understanding the SIS

At a minimum, an SIS consists of a sensor, a logic solver, a final element, and a support system. The SIS includes a combination of hardware and software elements that work in unison to detect process hazards and to take defined actions to achieve or maintain a safe state. Historically, SIS's were implemented using process switches, hardwired electrical systems, and final elements, such as motor control circuits or solenoid operated block valves. Since the SIS was physically separate and diverse from the BPCS, functional independence of the SIS and the BPCS was easily evaluated. The BPCS and SIS were typically designed and maintained by diverse personnel and departments. The two systems shared few, if any, components, technology, or personnel support.

When programmable electronic system (PES) technology became available, there was hesitation concerning its use in safety applications. Incidents were reported in which input and output points stuck in position without warning or the main processor halted. These failures were unacceptable and could not be tolerated when safe operation was at risk. Following years of use in control applications, owner/operators learned the nature of PES failure and how to detect failures through diagnostics. PES's were "safety

configured" to detect known failures including the configuration of input and output signal and main processor diagnostics. Output signals are often pulsed to detect stuck points and watchdog timer circuits are commonly used to detect misbehaving microprocessors.

Improvements in safety PES performance have been gained through implementation of extensive self-diagnostics. For SIS applications, the diagnostics are configured to take failed components and/or a single output channel to pre-defined safe states. This philosophy supports safe operation, but results in impact to plant uptime resulting from possible spurious trips. When SIS reliability is paramount, designs will likely employ redundant channels with appropriate voting and enhanced diagnostics, such as channel value comparisons.

Eventually, complex functions migrated into safety PES while simple functions remained in electrical systems such as relays or trip amplifiers. For low input/output (I/O) systems, electrical systems are very cost effective and easily implemented. Large I/O signal requirements often make a safety PES more cost effective than a comparable electrical system, but larger safety PES's also increase the number of potential failures in the hardware and software making analysis and design more costly.

The safety PES brings the ability to implement more complex and extensive logic with greater flexibility for modification. With these benefits comes an increased potential for systematic faults resulting from human error as well as the introduction of common mode faults in which the random hardware failure of the safety PES can result in the loss of multiple safety functions. The use of application software incurs an additional security risk since changes are so easy to make. A dedicated safety PES engineering interface should be used to facilitate administrative control of SIS logic and to reduce the potential impact of routine BPCS changes on the SIS. Software modifications should be controlled through a software management of change (MOC) procedure with version tracking. Access security should include:

- Restricting access to the engineering interface such as placing the engineering interface computer in a locked cabinet;
- Applying robust password administration policy within the programming interface; and
- Restricting hardware access in order to prevent unauthorized downloads of a new or revised application program to the safety PES.

To reduce the potential for data corruption, communication between the BPCS and SIS should be highly restricted. In most cases read-only communication should be applied, with the BPCS allowed only to read information from the SIS. If communication from the BPCS to the SIS is absolutely necessary, the communication technique must be evaluated for potential failures and steps must be applied that reduce the potential that a communication failure will result in an SIS failure.

A Peek Into the Future

BPCS field installation and commissioning keeps getting easier. The evolution from mainframes to integrated servers is being mirrored in the process units as systems are migrating from large, centralized control systems to small, digital plant architectures. Moving the equipment back into the process unit substantially reduces installation costs, but it also exposes the system to a more hostile and hazardous environment.

The amount of required wiring continues to decrease. Communication buses, such as Modbus, FOUNDATION fieldbus, Profibus, and Ethernet, are positioned to become the replacement for standard field wiring in control system applications. While this technology can significantly reduce the costs associated with the installation of such systems, the potential for common cause failure and loss of concurrent signals is significantly higher. For this reason, communication buses, even those certified to IEC 61508, have not yet received widespread acceptance for SIS applications within the process industry.

In some systems, the BPCS and SIS are implemented on a common system backplane, eliminating the need for physical hardwired or soft-linked communication pathways between the BPCS and the SIS. To maintain independence, the BPCS and SIS have their separate I/O modules and main microprocessors. They share the backplane, allowing user configurable communication without additional wiring or communication equipment. This enhanced capability should not be overused. Communication from the BPCS to the SIS should remain as limited as possible to reduce the potential for data corruption. Any potential failures of the communication should be assessed to determine how the failure affects the SIS operation and the impact should be addressed during design.

Some systems provide common configuration or programming tools for the BPCS and SIS. Although a common tool reduces resource and training requirements, one tool can mean one access point to both systems. This presents a significant challenge to administratively control access and changes to the SIS. It's recommended that separate engineering interfaces be provided to the BPCS and SIS to reduce systematic errors and support access security.

Most owner/operators continue the practice of implementing separate, and often diverse, platforms for the BPCS and SIS following the well proven, "defense in depth" 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 also allows the owner/operator to implement a less rigorous management system for the BPCS.

Within the process industry, control functions have always existed to help achieve production and product quality targets, reduce manpower requirements, reduce human errors, and improve process uptime. Those are the duties of the BPCS. The duties of the SIS are to protect the people, environment, and assets against unsafe conditions. Savvy automation professionals understand and respect the different purposes of control and safety systems and thus are able to optimize each in terms of design, installation, operation, and maintenance.