Distributed Safety Instrumented Systems

Angela E. Summers, PhD, PE, President, SIS-TECH Solutions
12621 Featherwood Drive, Suite 120, Houston, TX 77034
asummers@sis-tech.com, 281-922-8324

In the beginning, control was distributed in the field within the process unit. Most control was manual with pneumatic systems in production-critical areas. Then, new systems became available that were inaccurately named distributed control. The reality was that they were not distributed at all. Instead, control was centralized in a special room with proprietary controllers and associated I/O. Today, smart instruments, local valve controllers, digital fieldbus networks and other new technologies are moving control back into the field—closer to the process and field operations personnel.

The advantages of distributed SIS are similar to those realized with distributed control. The system provides independent operation and safe shutdown in the event of failure of the control system whether distributed or centralized. A distributed SIS has significantly less common-cause failure potential compared to centralized PLCs. Each function is operated, inspected, maintained and tested independently, and the performance of each SIS impacts only the equipment it's designed specifically to protect. In many cases, a distributed SIS is less complex, easier to implement and maintain, and significantly more cost-effective.

Introduction

Process plant safety systems can either be centralized, distributed or a combination of both. Each approach has its advantages and challenges, with selection of the best option dependent on a variety of factors.

This article will examine various safety system architectures, and will show process plant users how to pick the best solution to fit their specific needs.

Key points

- Picking the best safety system architecture cuts risk and cost while simplifying implementation and maintenance
- Safety systems can be implemented in a centralized or a distributed fashion
- Centralization is the more traditional approach, but distributed safety is gaining momentum
- Process plants should consider both approaches to meet their safety needs, and may need to mix and match centralized and distributed safety for best results

Centralized Safety

Some process plants employ a single monolithic safety system across their entire facility. These systems use a centralized logic solver, typically a large programmable unit and probably

featuring internal redundancy and extensive diagnostics, all housed in an environmentally controlled area.

Use of a single safety logic solver gained popularity as a means to lower the cost per I/O point by connecting increasing numbers of I/O to the logic solver central processing unit (CPU).

At many sites, the safety logic solver provides oversight for thousands of I/O points, with the result that facility safety and production reliability is dependent on the performance of a single safety logic solver. Consequently—software upgrades, application program changes, hardware failure, maintenance, and function checks can affect the entire safety system.

With centralized safety, decisions about CPU and I/O placement must be made during initial project design. The safety system I/O modules may be located in the central area, or remotely located near the field devices with secure digital communication back to the logic solver. The communications between the CPU and remote I/O must be vendor certified to IEC 61508. Because of their importance, these remote I/O links are often installed along different and redundant paths so that damage to one area of the plant doesn't bring down the entire system.

Conformance to IEC 61511 requires that individual field devices be hardwired directly to the safety system I/O. Remote safety I/O allows the designer to reduce the length of these individual wire runs, potentially lowering the project cost.

With centralized systems, users only need to master one software product, although it can be quite complex. Programmable systems require an engineering interface with access security controls to troubleshoot performance degradation. The centralized system does not provide local interfaces or panels in the field, so these must be designed and installed separately, adding additional cost and complexity.

Manufacturer selection constitutes a long-term commitment for training and spare parts. Once the selection is made, the number of different hardware components is minimized, lessening the learning curve and reducing stocking requirements. Small addition and upgrade projects must adapt to the existing system, so additional connection points need to be implemented with hardware compatible with the original installation.

Since a single logic solver manages many safety functions, the application program execution must be fast enough to address the shortest required process safety time. Changes to the application program, such as the addition of a new safety function, must be evaluated for their impact on other safety functions. Problems during download of a new application program or during loss of CPU environmental control may impact multiple plant process units, potentially affecting the safety and uptime of many pieces of equipment.

Perhaps, the greatest problem with centralized systems is that failure of the main controller can cause the entire safety system to cease functioning. While hardware redundancy can reduce the probability of this occurrence, systemic errors in software and the need for firmware updates

remain as potential threats, and the need to shutdown the entire system to perform updates can impact process uptime.

On the plus side, integration issues are virtually eliminated because the hardware components and software are supplied by one vendor, and there is a clear single source responsibility in case any issues arise. Table 1 summarizes the benefits and drawbacks of centralized safety systems.

Distributed Safety

Distributed safety systems are perhaps less familiar, but are nonetheless used extensively in process plants worldwide. Main distributed safety components include trip modules or relays, and/or small programmable electronic controllers with limited I/O capability, each designed selected to fit the needs of a single safety function.

A distributed safety system is often designed to provide safe operation of a limited plant area, a particular plant process, a single piece of equipment, or a single safety function. For example, a compressor skid might be supplied with its own control and safety system, separate and apart from the plant's main control and safety system.

In another case, a particular plant process might have its own safety system. For example, our company supplied a distributed safety system for a distillate hydrotreater unit at a refinery. The system used four separate trip modules to monitor four scenarios involving low level and low flow that could lead to overpressure of equipment within the unit.

Distributed safety systems have benefits and drawbacks as summarized in Table 2. Perhaps, the greatest advantage of the distributed safety system is independent operation and shutdown. Simply put, the locally controlled system will operate as designed even if other safety systems fail, or if communication links among the systems fail.

Failures and degraded conditions within the local and distributed safety system can be diagnosed and presented to the operator for appropriate response. For a simple trip module system, the required diagnostic is probably a periodic proof test, and any necessary repair is performed by an electrician with a screwdriver. Contrast this condition with a centralized safety system running continuous hardware diagnostics, and requiring an engineering interface with diagnostic tools and an engineer or a highly-skilled technician for troubleshooting and repair.

Because distributed safety systems only address a limited number of functions, the safety system can be modified or upgraded without disturbing other parts of the process. For plant retrofits and expansions, it's often easier to install a distributed safety system instead of integrating the new functionality into the centralized safety controller. The addition of a new safety function is relatively simple because the new function does not have to interact with the existing safety hardware or fit in an existing enclosure. New field hardwired safety connections can be relatively short in length since the logic solver can be mounted in close proximity to the protected unit.

If the distributed safety system uses only trip modules and relays instead of programmable electronics, several other advantages are realized. No software programming is required, and the

system can easily be designed to fail-safe. Speed of execution is unmatched by a programmable system, as is the ease of design and maintenance. Trip modules and safety relays can be selected to withstand the field operating environment, and can be mounted in simple waterproof enclosures in close proximity to the protected equipment, with no operational dependence on environmental controls such as air conditioning.

As with centralized safety systems, conformance to IEC 61511 requires that individual field devices be hardwired directly to the safety system I/O. The field sensors may be shared with the regulatory control system and operator HMIs through isolators or through a digital communication bus. All of the safety actions are performed locally by the distributed safety system. If a local operator interface is required, the distributed safety system panel can be modified to provide lights, push buttons, and/or an operator interface terminal.

The main challenge of implementing distributed safety is the need to implement and integrate products from a number of different suppliers. Although each distributed safety system may be relatively simple itself, the sheer number of different systems can add complexity. Parts from different suppliers need to be stocked, and plant personnel need to be familiar with the operation of each system. Just gathering the right tools for field troubleshooting can become a challenge, as these tools are often specific to each safety system.

Many process plants want to combine the benefits of centralized and distributed safety while minimizing the drawbacks of each, and one way to do this is with a hybrid safety system architecture.

Hybrids May Improve The Breed

Newer technologies such as distributed and networked safety controllers, safety-rated digital communication networks and safety-rated remote I/O are allowing some process plants to combine many of the advantages of both centralized and distributed safety in a hybrid safety system architecture.

In this type of a system, a central safety controller communicates to one or more distributed sub-controllers located throughout the plant via a high-speed digital network. Each sub-controller has its own local I/O, and can control its local process on a stand-alone basis. The communications among the safety CPUs must be covered in the logic solver vendor product certification to IEC 61508. This requirement implies that that the hybrid safety system will be purchased from a single vendor, much like the centralized system.

With this approach, there is only one software programming environment for the entire safety system, and only one supplier. This virtually eliminates integration issues, and simplifies design and maintenance. Control room personnel are presented with a unified operator interface, and this interface can display complete information from each distributed safety sub-controller.

On the negative side, these systems are often the most complex of all to design, program and maintain because there are many separate safety controllers. A high-speed network must be

designed, installed and maintained—and access security and cybersecurity must be tightly controlled.

Selecting The Best Option

For a new Greenfield plant, a centralized safety system architecture is often the initial approach. If the selected regulatory control system supplier also offers distributed safety, as most of the major automation vendors do, then the plant can realize the benefits of a single vendor approach with a hybrid system.

Reliance on a single vendor is often more costly in terms of purchase costs, but this approach should reduce other life cycle costs. The main risk is complete dependence on one supplier, as well as sometimes overwhelming complexity in initial design, often requiring extensive supplier support at considerable cost.

Centralized safety systems are installed and running in many process plants, and most users can't justify a wholesale change of approach. In this situation, it's often more cost effective and simpler to perform additions and upgrades with distributed safety systems.
These distributed systems can networked back to the regulatory control system and its operator interface via either hardwiring or a digital network, providing the operator with a system that looks and feels much like a centralized safety system at a lower cost.

Distributed safety systems are often present in process skids, compressors, packaging machines, and other subsystems purchased from OEMs. The OEM safety systems are usually linked back to the central regulatory control system via either hardwiring or digital networks, although the safety systems may be completely standalone.

Most new facilities will select either a centralized or a hybrid safety system architecture. Existing plants need to make sure that newer safety systems fit into their existing safety system architecture. In many cases, this means that distributed safety systems will be used, and that these systems will be integrated into the existing safety system architecture.

Table 1: Benefits and Challenges of Centralized Safety

1. Only one system to learn and support
2. Common operator interface
3. No integration required
4. Single point of supplier responsibility
5. Significant wiring requirements for field I/O
6. Higher installed cost
7. Slower speed of execution
8. Failure of central controller brings down entire plant safety system
9. Programming can be very complex

Table 2: Benefits and Challenges of Distributed Safety

1. Independent operation and shutdown
2. Easier to modify and upgrade without disturbing other functions

3. Easier to install and start up for retrofits and expansions
4. Reduced wiring
5. Simpler to design, program, install and maintain
6. Improved overall speed of execution
7. Easier to provide local operator interfaces and local control
8. Typically less expensive
9. Multiple systems to learn and support
10. Integration among systems required
11. No common engineering interface
12. No single point of overall supplier responsibility