Co-innovating tomorrow™

YOKOGAWA

Control & Safety: Integrate or Segregate?

WHITE PAPER

Table of Contents

Table of Figures

KEY TAKEAWAYS

- ✓ Control system and safety system functions are completely different. The former controls the process under normal circumstances; the latter takes it to a safe state under abnormal circumstances.
- ✓ Safety systems run the gamut from fully segregated, to interfaced, to networked, to fully integrated with control systems. All satisfy IEC 61508/61511 requirements.
- ✓ Today's technology enables users to weigh the benefits and drawbacks of each approach for their particular situations.
- ✓ A tight coupling of control and safety systems can provide advantages in terms of ease of use, cost and information consistency.
- ✓ Today, cybersecurity is a key consideration that drives users to opt for segregated systems.
- ✓ It is critical to simultaneously provide independence for safety integrity and allow interference-free commonality at all other levels of the control and safety systems.

Part 1 Introduction

> *"The international standard for functional safety, IEC 61508 Ed2, 2010, defines the SIS as "a system used to implement one or more safety instrumented functions composed of any combination of electrical, electronic and programmable electronic sensor(s), logic solver(s), and final element(s)."*

The architectures and deployments of logic solvers of Safety Instrumented Systems (SIS) are as varied as the suppliers who design, build and implement these systems. In general, the categorization of SIS architectures can be termed integrated or segregated; the latter is also known as independent.

Safety Instrumented Systems play a critical role in the process industries, preventing personal injury, environmental and equipment damage, and loss of production. These systems must conform to stringent and accredited functional safety, Electromagnetic Compatibility (EMC), hazardous location equipment, marine, and application safety standards.

Two international standards, IEC 61508 and IEC 61511, are the basic global requirements for new Safety Instrumented Systems. The international standard for functional safety, IEC 61508 Ed2, 2010, defines the SIS as "a system used to implement one or more safety instrumented functions composed of any combination of electrical, electronic and programmable electronic sensor(s), logic solver(s), and final element(s)."

Most safety system logic solvers manufactured by SIS suppliers have been certified by TÜV Industrie Service GmbH Business Sector ASI (**http://tuvasi.com**), TÜV Rheinland Group to fulfill the requirements of Safety Integrity Level (SIL)[1] level of the IEC 61508 standard involving the Safety Lifecycle and conditions for building an SIS. Other companies are often involved in evaluation and certification. Frequently, safety system suppliers utilize one company for evaluation and critiquing of equipment and architectures in order to help suppliers correct deficiencies before submitting for certifications. These equipment and architectures must be designed, configured, and implemented, so certification against IEC 61511 Ed2, 2016 is also required for SIS designers, integration firms, and the end users.

1. *Safety Integrity Level (SIL) is a measure of safety system performance, or probability of failure on demand (PFD) for a SIF or SIS. There are four discrete integrity levels associated with SIL. The higher the SIL level, the lower the probability of failure on demand for the safety system.*

> *A Basic Process Control System (BPCS) function is used to control the process safely during normal operation, whereas the SIS is used to place the process into a pre-determined safe state at the time of emergency and/or abnormal condition.*

The IEC 61508 standard provides device manufacturer guidelines for the specification, drafting, and operation of electrical, electronic, and programmable safety systems. It is based on a lifecycle concept in which specific techniques are recommended to ensure that mistakes and errors are avoided from the initial concept, risk analysis, specification, design, installation, and maintenance phase, all the way through to disposal. These types of mistakes and errors could undermine even the most reliable protection.

Much like IEC 61508, the IEC 61511 standard is based upon a lifecycle concept, but provides guidelines and procedures and places responsibility on the end user instead of the supplier.

A Basic Process Control System (BPCS[2]) function is used to control the process safely during normal operation, whereas the SIS is used to place the process into a pre-determined safe state at the time of emergency and/or abnormal condition. Though a BPCS will have interlocking and other capabilities to keep the process out of most trouble and within a defined operating condition, the SIS is an outer layer of protection and often the last resort of protection for process emergencies. Because they have different purposes and functions, the SIS and BPCS are required to be segregated.

2. *Process Automation Systems (PAS), Industrial Control Systems (ICS) or Industrial Automation and Control Systems (IACS) are other terms used in conjunction with BPCS and may be used interchangeably.*

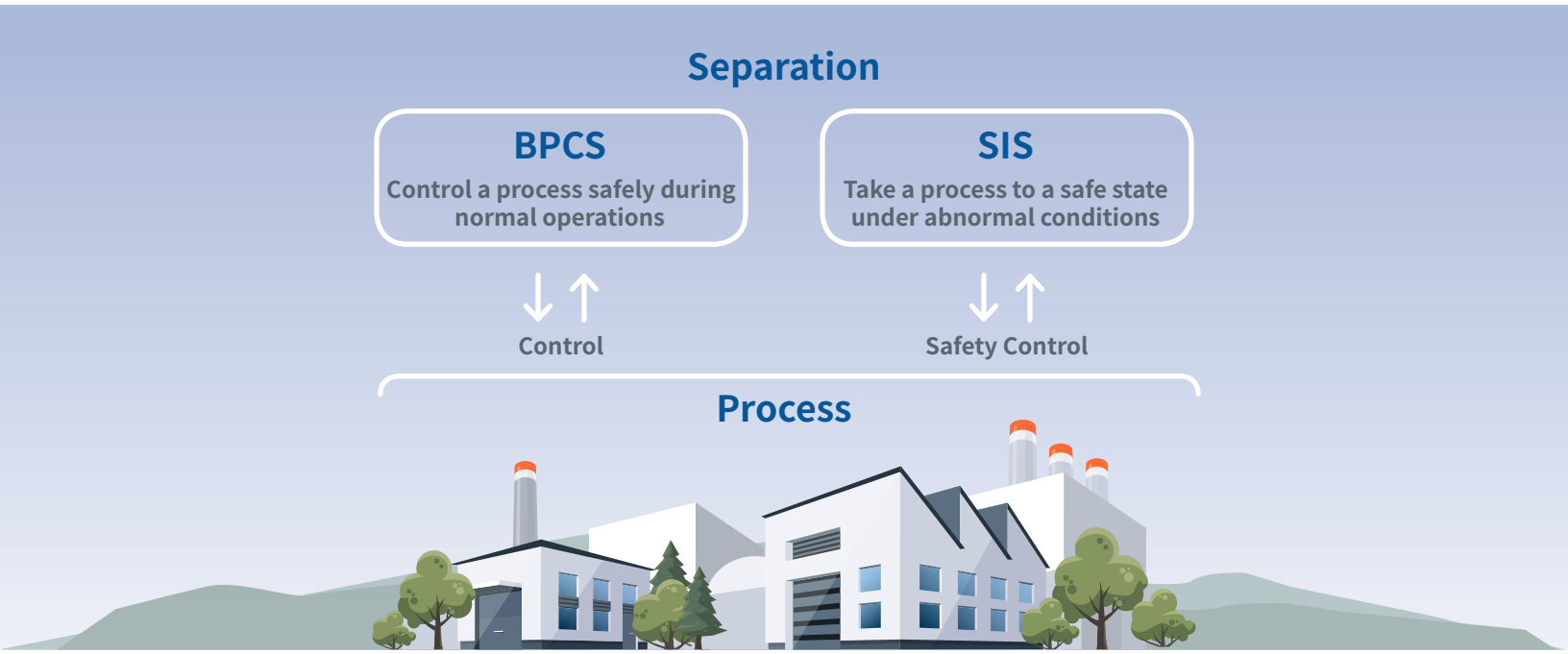


Figure 1 – Basic Process Control System and Safety Instrumented System Relationship to the Process

Part 2 Independent Safety Systems

Independent Safety Systems can be categorized as either stand-alone or interfaced.

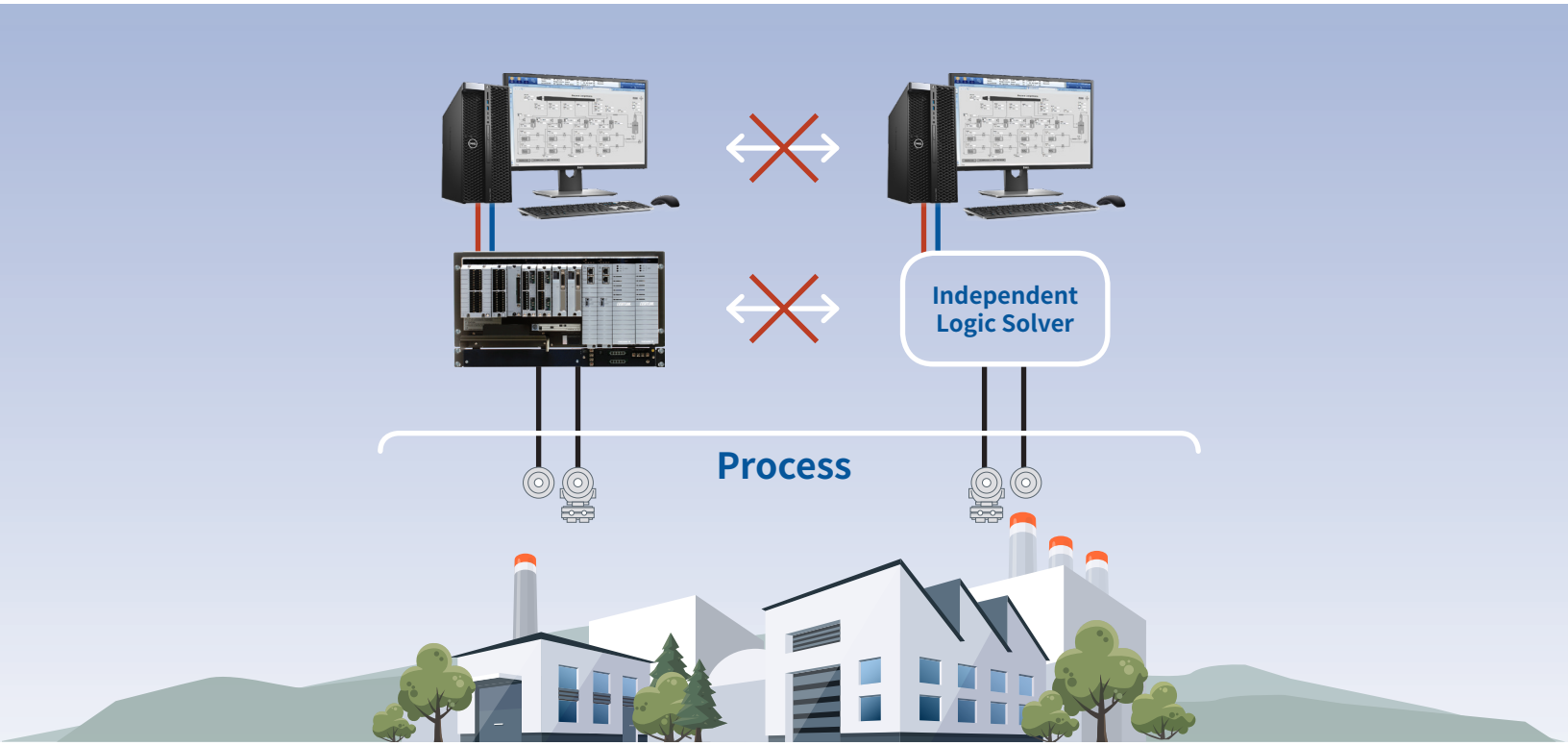


Figure 2 – Independent Standalone Safety System

> *A stand-alone system is configured, deployed and subsequently left alone to provide its function and application.*

1. STAND-ALONE SYSTEMS

A stand-alone system is configured, deployed and subsequently left alone to provide its function and application. The application of the Safety Integrity Functions (SIF) do not change. A SIF is an operation that takes the process to a safe outcome if predetermined conditions are not in compliance. The system involves the three elements of sensor (e.g., temperature, pressure transmitter, and others), logic solver and final element (e.g., valve). There is no need to monitor or otherwise disturb the system. The SIF functions monitor and act, if needed, without intervention. High Integrity Pipeline Pressure Systems (HIPPS) and many Safety Integrity Level 4 (SIL4) rated logic solvers are examples of this type of standalone systems.

Newer systems and architectures on the market require the end user to design processes to require Safety Integrity Level 3 (SIL3) or lower protections; these types of implementations are being seen less often. In fact, Yokogawa's ProSafe SLS and HIMA are the only two SIL4 SIS systems still marketed in the process sector. An example of the difference of the architecture is that Yokogawa's ProSafe SLS is a magnetic-core, solid-state component based system, utilizing circuit boards for all functions; unlike current SIL2/SIL3 systems which use IEC 61131-3 programming languages of ladder logic, function blocks, and/or structured text for programming of the SIF functions. Because of the use of solid-state components and hardwiring, this standalone system generally has low Input/Output (I/O) counts and low number of SIF functions.

Even so, Boiler Management Systems (BMS) requiring only SIL2 protection are often standalone as well. However, most SIS systems are used for Emergency Shutdown (ESD) of processes and to a smaller, but just as important extent, Fire and Gas (F&G). These applications have generally been classified as SIL3.

2. INTERFACED SYSTEMS

With the advent of programmable logic solvers in the 1980s, interfaced systems utilizing programming languages became very scalable from low I/O and SIF functions to extensive SIS systems. However, BPCS and SIS implementations were based on different technologies operating independently.

The BPCS and SIS are separated, not integrated. Although sensors are measuring variables in the same process, the information cannot be exchanged smoothly or monitored together unless some communication method is provided.

The need to present the operator with critical information, including information from the safety critical systems, has always been present. Interfaced systems provide for monitoring of the inputs and outputs of the safety system and are interfaced to a BPCS either via a Distributed Control System (DCS), Programmable Logic Controller (PLC), or Supervisory and Data Acquisition System (SCADA) and its Human Machine Interface (HMI) or operator console. The system performs its function without regard to the process automation system, but important variables from the safety system are brought into the process automation system for monitoring on the operator station via graphics or other display means. Engineering is required to bring the desired variables into the process automation system.

> *“Many end users who choose interfaced systems do so because of the inherent nature of separation of process and safety functions.*

Many end users who choose interfaced systems do so because of the inherent nature of separation of process and safety functions. BPCSs and SISs were typically supplied by different vendors and required extra engineering for the individual systems and interconnections. These are two separate systems, with separate networking interfaces, tools, architectures, and engineering teams. Furthermore, these systems were more difficult to master and operate because of these interfaces and environments.

In the early days, the common interface to the DCS, PLC, or SCADA system was proprietary. A gateway or other hardware interface provided the connectivity between the BPCS and SIS even if it was the same supplier. More recently, using some more open standards, that interface is commonly Modbus, either Modbus TCP or Modbus Ethernet. A Modbus type Interface requires poll/response from the Host or Master (DCS, PLC or SCADA) to the Client SIS system. As such, variables that need to be communicated from the SIS to the Host BPCS system for information and monitoring on the operator stations must be engineered. In addition, the Host must be engineered to "map" the locations to create the variables needed to be displayed in the Host system (i.e., create a table of variables of interest in a designated memory location that is available for reading by a Modbus command).

Figure 3 – Gateway/Bus Converter Interfaced Safety System

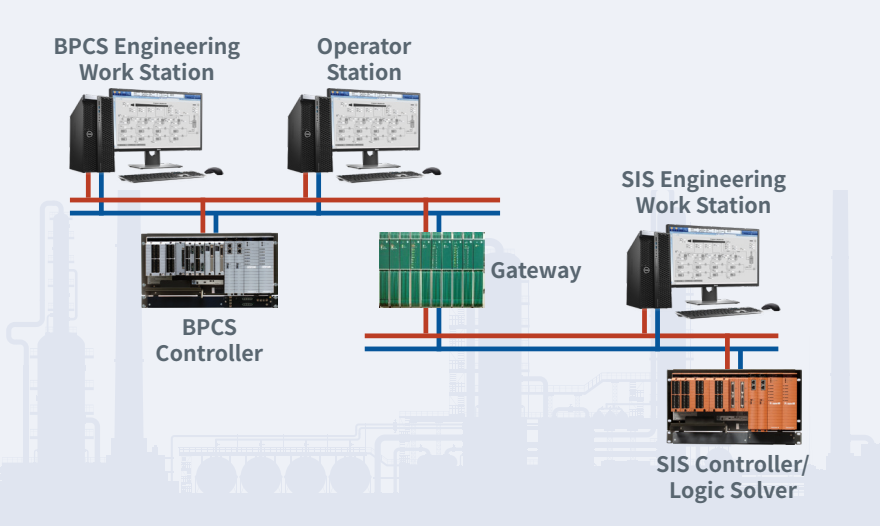
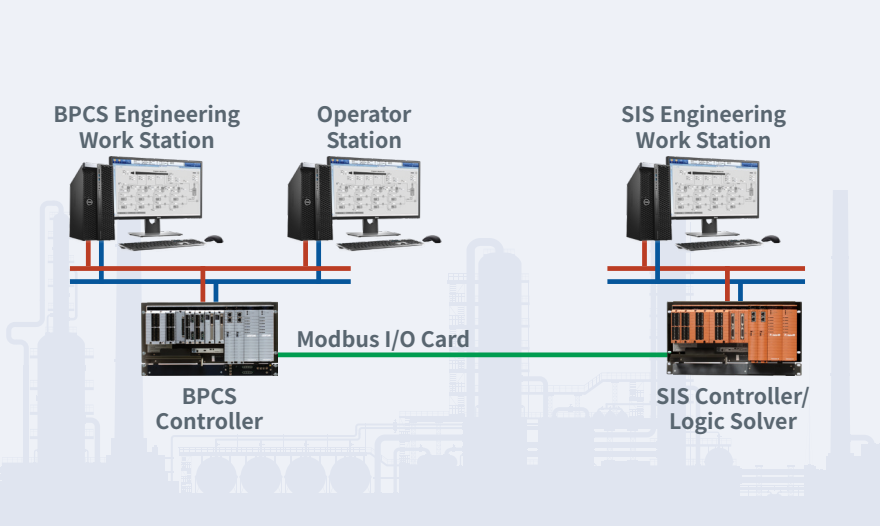
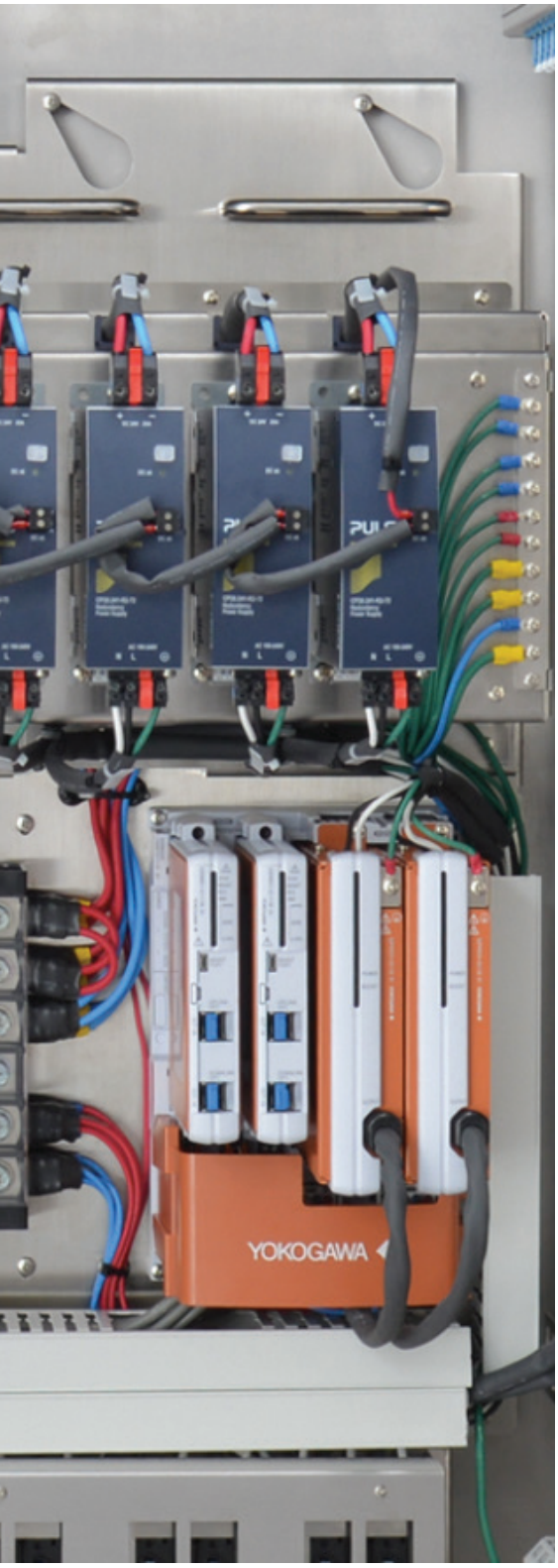


Figure 4 – I/O Card Interfaced Safety System



Part 3 Integrated Safety Systems



Interfaced systems based on Modbus or proprietary protocols and hardware were the only method until the adoption of open network protocols and Windows operating systems on industrial automation and control systems. This increased the connectivity to business systems and at the same time (at least in theory) exposed them to the same issues (malware, viruses, cyberattacks, etc.).

Based on these open network protocols, integrated safety systems came onto the scene in the mid-2000's and have continued to gain more traction in many applications in recent years. These systems provide tools where engineering time to configure and interface a SIS system to a BPCS system is greatly reduced, in some cases to the point of requiring no time. To do this there must be tight coupling of the architectures, the software, and networking. Information received by the BPCS from the safety system must traverse from the logic solver to the HMI of the BPCS.

In the Independent Safety System method, there is extra configuration for the points to be transferred to the BPCS. Additionally, the BPCS system requires configuration to input variables to create the BPCS tags required to display them. However, with the integrated system, the BPCS tag names are created when the safety system tags are configured and communication protocol subsequently relays them to the BPCS system. Here, no BPCS system configuration is required.

Operators can access both BPCS and SIS data from the control system's human-machine interface (HMI) station. This one window on the two systems simplifies the task of handling their data. Not only are these tags available to the HMI, but also to asset management systems, whereby smart SIS instrumentation and SIS final control elements can be monitored and evaluated for health. This same safety tag information can also be accessed by historical data systems whereby historization and data aggregation can be performed. Architectural vertical integration is achieved with a minimum of configuration of all systems.

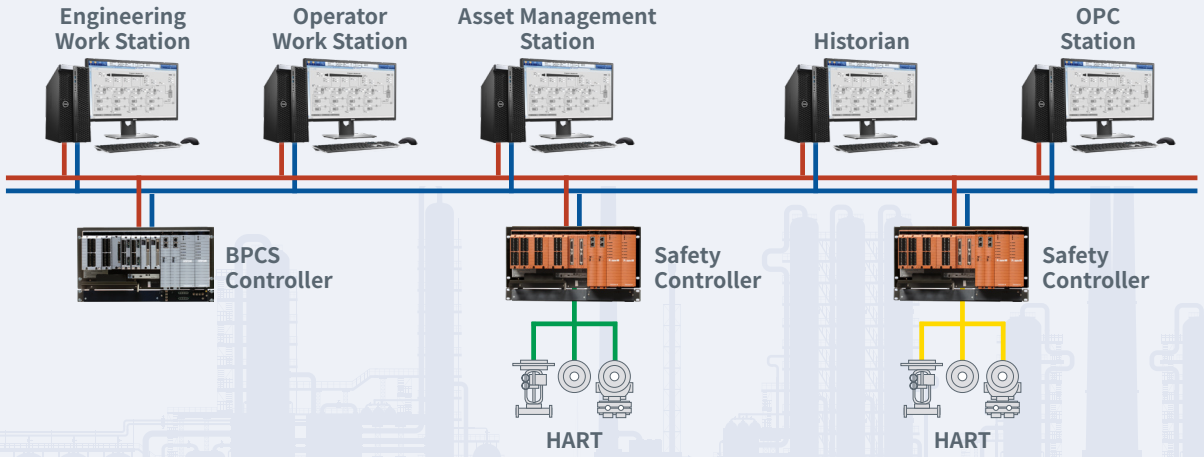


Figure 5 – Integrated Control and Safety System

The one-window integration of the BPCS with the SIS creates an operating environment with a unified user interface, integrated field device management, and remote engineering. Increased functionality from field device management includes smart digital communications like HART which has become SIL approved. Integrated field device management with HART protocol provides for additional functionality. For example, Partial Stroke Testing[4] (PST) of valves using HART[3] provides additional value. The SIS must still meet the control and safety segregation requirements specified by IEC 61508 when integrated with a BPCS and be accredited as an IEC 61508 designed and integrated certified system.

However, care must be taken to provide differentiation of the tag or instrument to the operator, and integration systems inherently provide this. Is the tag a BPCS tag or is it a SIS tag? Does the logic associated with the tag that is monitoring to a SIF function or BPCS function need to be known? And does it matter to the operator or only to the control or safety engineer?

On the communications side, the physical layer of the network can be the same. Hardware (cables, and network switches) are the same. Therefore, integration facilitates one network design.

The disadvantage and risk are to cybersecurity – shared common networking components or shared hardware components create a commonality that can be exploited if only one is known.

3. *HART (Highway Addressable Remote Transducer) Protocol is a bi-directional communication protocol that provides data access between intelligent field instruments and host systems. It is the global standard for sending and receiving digital information across the 4-20mA analog.*

4. *Partial stroke testing (or PST) is a technique used in a safety system application to allow the user to test a percentage of the possible failure modes of a shutdown valve without the need to physically close the valve. PST is used to assist in determining that the safety function will operate on demand. PST is most often used on high integrity emergency shutdown valves (ESDVs) in applications where closing the valve will have a high cost burden yet proving the integrity of the valve is essential to maintaining a safe facility. Thus, PST assists in proving longer interval before a full stroke is required for proof testing.*

> *...the benefit of a unified operation and monitoring environment allowing operators to watch and utilize the integrated information is the improvement of operational speed in case of unexpected circumstances*

In interfaced systems, there is a natural barrier, a subsystem interface as previously shown in figure 4 as another piece of hardware like a bus converter or gateway box or as shown in Figure 5 as an Input/Output (I/O) card in the BPCS. In integrated systems this is most often an Ethernet Switch. In some cases, a layer-2 switch as shown in figure 5 but more often a layer-3 switch that segregates the Internet Protocol (IP) addressing between BPCS and SIS networks as shown in Figure 6. In either instance, whatever malware can infiltrate the network may have access to both the BPCS and SIS system; however, a layer 3 switch can be configured to make it more difficult.

Additional hard security must be present in the safety logic solver in the manner of protections of downloading and changes to a logic solver. This may involve a hard-key position or even a soft security level with separate password protection for download authorization.

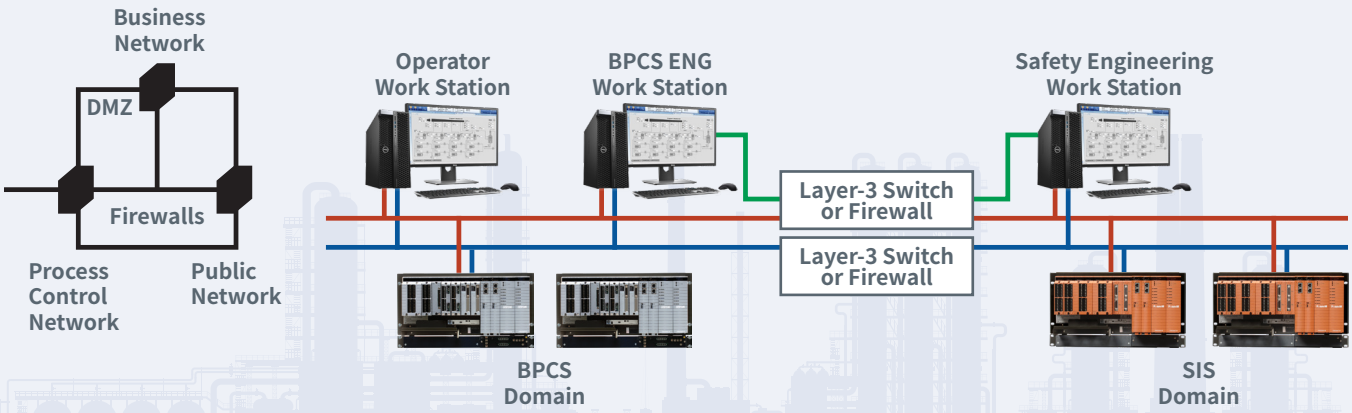


Figure 6 – Integrated Control and Safety System with segmented networks

However, the benefit of a unified operation and monitoring environment allowing operators to watch and utilize the integrated information is the improvement of operational speed in case of unexpected circumstances. The simple architecture allows use of a common network for both BPCS and SIS while keeping the safety integrity level (SIL). A Lower Cost of Ownership is achieved because of common standards for the control and network architecture that allows for users to implement projects more quickly, while engineering and maintaining the plants effectively.

Part 4 Lessons Learned From Project LOGIICS

The Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC) program, a collaboration of five (5) major oil and natural gas companies and the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) Cyber Security Division (CSD) was formed in 2004 to facilitate cooperative research, development, testing, and evaluation procedures to improve cybersecurity in petroleum industry process automation systems. The program undertakes collaborative R&D projects to improve the level of cybersecurity in critical systems of interest to the oil and natural gas sector.

In 2011, the consortium, with the Automation Federation (AF) serving as the host organization, tested various configurations of BPCS and SIS systems. The goals of the project were to determine what, if any, current or emerging cybersecurity issues exist within integrated BPCS and SIS architectures, determine their impact, and develop recommendations to help reduce the cyber risk introduced by integrating SIS solutions. The project sought to identify applicable and relevant security concerns regarding SIS's in several areas of interest, such as access control, functional integrity of safety operations, and integration with basic process control systems. Called LOGIIC Safety Instrumented Systems Project, the project had the support from the major industrial automation BPCS/SIS suppliers and two industrial cybersecurity companies. Together with the DHS S&T CSD contracting the nonprofit research center SRI International, testing was performed on various integrated configurations in order to make cybersecurity recommendations regarding SIS architectures. The objective was to assess representative architectures and to what degree the safety function could be interrupted by an attacker with a foothold in the BPCS.

> *"The project sought to identify applicable and relevant security concerns regarding SIS's in several areas of interest, such as access control, functional integrity of safety operations, and integration with basic process control systems.*

The main conclusions were that first and foremost the technical integrity of the safety function was not detected under a variety of cyberattacks. The LOGIIC SIS project did identify a set of vulnerabilities associated with standard types of contemporary integrated safety systems. Fortunately, those vulnerabilities may be managed or avoided with updated equipment, architectures, and compensating controls. The project demonstrated that these contemporary integrated safety systems have a significant amount of resiliency inherent in them. The systems operated and maintained a safety function for the systems being protected regardless of activity from peripheral and integrated technology.

However, some vulnerabilities could impact the availability of the mechanisms for operator interaction. Several notable susceptibilities related to versions of hardware and software being used in standard deployments were exposed. Several years later in 2017, the custom malware generally known as TRITON or TRISIS, was the first documented attack designed to target a specific vendor's SIS controller; it caused the process to "trip" to a safe condition. One of the findings was that the hardware key for downloads was left in the improper position. While, the SIF function was not compromised, it did execute as a false trip of the process.

Though the LOGIICS test was not widely known, those lessons have largely been adopted by SIS suppliers. Proprietary networks and even enabling firewall capabilities in the layer 3 switch in between the BPCS and the SIS are becoming common practice due to cyberattacks. This increases cybersecurity between vendor specific product platforms and provides the ability to be separate.

Today, many end users are adding firewalls into their internal architectures which were streamed-lined for years. It has added cost back into SIS projects, but cybersecurity is a main safety consideration and like the cost of the SIS themselves, cost is relative against potential catastrophic events.

Part 5 Summary

> *A key element for successful operations and maintenance is the level of integration between the Safety Instrumented System(s) and the Basic Process Control Systems.*

Deployments of SIS systems run the gamut from fully segregated, to interfaced, to networked, to fully integrated within the same control hardware. All satisfy IEC 61508/61511 requirements for compliance and human and environmental safety.

All hazardous process plants require control, coupled with some element of an independent safety layer. When designers decide that an independent safety system should be programmable, there needs to be further consideration about the level of interaction between the control systems and the safety systems.

In the past, so much has been focused on independence that factors which affect operations and maintenance are forgotten. A key element for successful operations and maintenance is the level of integration between the Safety Instrumented System(s) and the Basic Process Control Systems. A tight coupling of these systems can provide large advantages to the end user in terms of ease of use, cost, and even plant safety, but its cybersecurity must be closely and consistently managed. The key is to provide independence for safety integrity but allow interference-free commonality at all other levels of the BPCS and SIS.

Acceptance of integrated control and safety systems is now commonplace, such that it is being considered more and more in deployments, though a significant number of proponents still deploy interfaced systems. Since 2017, there has been a movement in the industry to review the roots of the IEC 61508 Logic Solver requirements and the IEC 61511 user procedures. As a result, platform independence is becoming popular once again.

Now that some of the advantages and disadvantages of independent and integrated safety instrumented systems have been discussed, what is your preference?

YOKOGAWA

Co-innovating tomorrow™

www.yokogawa.com

Yokogawa Corporation of America

12530 W. Airport Blvd.,
Sugar Land, TX 77478

Yokogawa Canada, Inc.

Bay 4, 11133 40th Street SE,
Calgary, AB T2C 2Z4

Yokogawa de Mexico, SA de CV

Urbina No. 18
Parque Industrial Naucalpan
Naucalpan de Juarez, Estado de México
C.P. 53370

[Ed:01] Printed in USA PROD#:YWP29062018E