

Safety

Demanding Performance Requirements of Oil and Gas Industry Require Careful Safety System Selections



Striking the right balance helps optimize investments, enhance safety and reduce lifecycle costs

A sset and system availability along with process uptime are more critical than ever in the oil and gas industry. At today's high fuel prices, each minute of uptime counts. Any disruption of the supply chain creates a strain in the market and puts companies at risk for incurring substantial downtime losses.

While safety is a concern across all

manufacturing sectors, it is especially critical in the oil and gas industry. In this environment, risks can be far-reaching. The spill of a toxic agent or explosion could harm the entire plant or surrounding community. The inability to respond effectively to hazardous situations can be extremely costly from jeopardizing personnel to diminishing the bottom line, brand reputation, or

consumer and investor confidence.

Role of the Safety System

Oil and gas facilities employ a variety of processes that require continuous operation for practical and financial reasons. For example, a shutdown of a fuel distribution pipeline may take days to restart and cost millions of dollars in lost production. Therefore,



it's essential that critical devices, such as pumps, compressors, motors and instrumentation, continue working if the primary control system fails.

In most production operations, the basic process control system (BPCS) – historically a DCS but increasingly a programmable automation controller (PAC)-based system – continuously monitors the process and controls parameters, including temperature, flow, pressure, weight and viscosity. The BPCS maintains process variables within safe boundaries and therefore can help provide some level of protection, i.e., the control system detects a change in flow or pressure and responds.

However, processes have the potential to create hazardous situations when the BPCS is out of control or unexpectedly fails. This is where the safety instrumented system (SIS) comes into play. The goal of the SIS is to maintain the safety of a facility in the event of a control system failure. This may require an orderly shutdown of the process to help protect the people, equipment and production.

Evaluating the Vendor

In accordance with international standards, independent third parties certify most control systems used in critical safety applications. However,

using a certified system does not automatically make a facility safer. The system must also be implemented properly. Many systems are rendered ineffective by improper specification, design, installation, operation or maintenance. In order to help maintain system effectiveness, selecting the right safety system vendor is key.

As you evaluate safety vendors, you'll likely hear a wide variety of opinions. As you go through your evaluation process, you should avoid over-simplified recommendations like the following:

- "Just use the same vendor that ABC Company uses. After all, they're bigger than we are so they must know what they're doing. Right?"
- "Go with XYZ Company. They're the industry leader."
- "Just deal with the same vendor we've always dealt with."

In reality, too many safety system purchases are based on past purchasing habits. However, with new technologies available to help improve performance, design productivity and safety, look for the most effective system to meet your plant requirements, at a cost-effective price.

Look for a vendor who can deliver the range of control technology required. Also, make sure the vendor has the experience to guide you through the application of those products throughout your plant or process, as well as the required certification processes for each region in which they will be used. In other words, you need a partner who advises you on the best ways to help improve your safety systems, keeps you up to date on changes to regulations and helps you stay in compliance with evolving standards. System selection should also include connectivity with upstream and downstream systems and system applicability across your plant, beyond a single application.

Once the equipment is in place, the supplier should provide ongoing technical and engineering support to keep the systems running properly and cost-effectively. This will help you implement safety measures at plant sites around the world.

Matching the Technology to Application Demands

Selecting the right technology requires in-depth analysis. Just as each project is different, so are safety system needs. A detailed, systematic, methodical, well-documented process is necessary in the design of safety instrumented systems. This process comprises a series of detailed steps, including a safety review of the application, implementation of other safety layers, and systematic analysis, as well as detailed documentation and procedures.

These steps are described in various regulations, standards, guidelines and recommended practices. The intent is to leave a documented, auditable trail, and make sure that nothing is neglected or missed.

Risk assessment processes defined within industry standards, such as IEC 61511, typically take a life-cycle approach in clarifying how to implement an effective process to identify hazards.

A risk analysis is integral to this



process to quantify the level of risk in terms of severity of consequence, frequency of exposure and probability of avoidance. The risk assessment quantifies the performance required of each safety instrumented function into one of four possible safety integrity levels (SILs). SIL represents the amount of risk reduction or performance required of a safety-instrumented function in order to manage the risk of a potential incident outcome to a tolerable level. For example, a SIL 1-rated system offers a probability of failure on demand (PFD) (dangerous failure) of .1 to .01, while a SIL 4 system offers a PFD of .0001 to .00001.

Since today's safety-instrumented system standards are performance-based, not prescriptive, they do not mandate technologies, levels of redundancy, test intervals, or system logic. Essentially they state "the greater the level of risk, the more robust the safety system needed to control it." That said, choosing a safety system is not as intuitively obvious as it may seem - for example, dual is not always better than simplex and triple is not always better than dual.

Specifying a SIL 3-rated logic solver is often viewed as a conservative and safe choice, even if you don't have any SIL 3 requirements. This may give system designers an added level of comfort, but not necessarily any distinguishable increase in safety. Meanwhile, over-specifying may mean over-spending and possibly overly complicating the system. In this case, it may make more sense to consider cost-effective methods that meet SIL 2 requirements.

If a SIL 3 logic solver is desired, more than a dozen manufacturers exist to choose from, along with five basic configurations (e.g. - 1oo1D, 1oo2, 1oo2D, triplicated and quad). As follows, several important hardware and software issues should be considered

before determining which system is best suited for an application.

Hardware Considerations

Architecture/Fault Tolerance : Most users in the oil and gas industry specify SIL 3 certified triplicated systems. Plant uptime is critical and triplicated logic systems help protect against nuisance shutdowns and the resulting lost production costs. Triplicated systems offer the highest level of fault tolerance. These systems are designed with three parallel systems running in a redundant design. All three systems process the input information and vote to affect a result - meaning that a two out of three vote is required to effect a change or stop a process. Multiple modules can all have single slice failures, and the modules and the system will continue operating.

The redundancy requirements encompass more than the logic solver. They include all of the elements that make up the SIS, including input devices (sensors, switches and instrumentation) and output devices (pumps, motors, valves and other actuators). All must be selected to meet the required SIL level for the safety loop.

System Size : The physical size of the safety system also can be crucial in applications where space is limited, such as offshore platforms and offloading vessels. In general, the more redundant a system is, the larger it becomes.



Most dual redundant systems require identical redundant chassis, even if only a few modules are in a chassis.

Not all triplicated systems are the same size. Some configurations include a spare slot for each module in the system, which allows users to quickly replace an active module online without affecting the process. Other systems offer a much more compact arrangement with only a few empty slots needed to replace any I/O module in the system. This can result in a 50 percent reduction in system size.

Sequence of Events : When something shuts a process down, you want to know what happened and in what order. This is especially critical in high-speed processes. To provide this data, most systems offer some form of sequence of events (SOE) recording. Some systems time-tag the events at the I/O modules with true one millisecond resolution. Other systems time-tag the events at the main processor, and therefore only have the resolution of the processor scan time. Be sure to check the hardware capabilities and make sure the scan time meets the speed requirements of your application.

Key Software Capabilities

Number of Languages : The IEC 61131-3 standard defines five control system programming languages - ladder logic, function block, structured text, instruction list and sequential function chart. Some systems offer only one language, some offer several, while some offer a hybrid language and others offer all five. Different languages are suitable for different tasks.

Using the one that's best suited for the application helps reduce development and testing time, as well as make the program easier to read, understand and maintain. Force-fitting functionality into the wrong language can be problematic.

Case in point : On one particular control system project, the vendor was responsible for the hardware only, while an engineering construction firm was responsible for the human-machine interface (HMI) and application programming. The software developer, having an understanding of what the HMI needed to do, worked himself into a conundrum over how to make it interact properly with the control system.

Unfortunately, the programmer was not an expert in all the languages. In this case, structured text language could have easily handled nested, indented “IF-THEN-ELSE” commands. The programmer, however, used function blocks, a graphical language not ideally suited to nested, conditional execution flow conditions. The result was an extensive use of jumps and labels, which made it extremely difficult to understand and troubleshoot.

Problems were encountered within the first hour of the factory acceptance test when the system shut down unexpectedly. In the end, the vendor had to re-write the application in structured text encapsulating all the required functionality.

Ease of Programming : Most systems today offer a Windows-based development station and at least one of the IEC 61131-3 programming languages. However, this does not mean all systems offer the same ease of configuration and programming, or the same level of design productivity. It’s important to test drive the software and walk through basic configuration tasks. If possible, make head-to-head comparisons of the time required.

Ease of Connectivity. Find out what connectivity choices are available for your control system, HMIs and other third party equipment. Is your control system compatible with Ethernet, serial, OPC, or Modbus network connections? How many connections do you need

and what can the system support? Are redundant communications possible? Are separate gateways required? Does the safety system have a direct highway connection to the control system?

Selecting a Design Approach

There are three types of safety system



designs that allow users to share information between systems – interfaced, hybrid, and integrated. Each design philosophy offers advantages and disadvantages. The most suitable option for a particular application will vary based on factors such as size, level of risk, location, expertise of staff, availability of support, and cost.

Interfaced Safety

The primary function of a BPCS is to hold specific process variables and parameters to predetermined levels 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 the process is out of control and the BPCS is unable to do so. Manufacturers traditionally have implemented BPCS and SIS as separate systems. In fact, certain guidelines, recommended practices and standards suggest and sometimes mandate separating standard control and safety systems, particularly for process applications.

In this configuration, separate BPCS



and SIS systems communicate with each other using hardwired signals, an industry standard protocol or on the same proprietary highway as the control system (often using some form of a gateway). There are several reasons some prefer to keep safety and standard control functions separate in process applications:

- Reduced common cause problems – using diverse hardware and software may mean that any potential single problem would be less likely to negatively impact both systems.
- Physical separation – designed to guard against changes in a PAC or BPCS causing any change or corruption in the associated SIS.
- Different requirements – an SIS is normally called on only in the event the PAC or BPCS fails. An SIS needs to have higher levels of security and typically doesn’t change much once it’s implemented, unlike a PAC or BPCS, which is usually designed for accommodating changes.

The primary benefit of this interfaced approach is you can select the best-in-class of each individual system for any particular application. It doesn’t require you to use the control system vendor’s preferred safety system, but it often influences the decision.

This type of design also has drawbacks. It requires contractors,

integrators and end users to learn two separate systems – hardware and software – which typically also means higher costs for training and spare parts. In addition, getting diverse systems to communicate tends to be more challenging and more expensive.

The Common or Hybrid System

Common, or Hybrid is when one vendor offers two distinct systems, yet they are similar (though not interchangeable) in design. There are varying degrees of compatibility with these types of systems depending on the vendor. The systems may share some hardware, or may communicate on the same highway without gateways and may be programmed in the same software environment. The benefits of this approach are lower costs than interfaced systems, common components, and ease of communication between systems.

The drawback is the potential increase in common-cause problems. In addition, while the programming environment may be the same, the actual hardware modules are often different,

so each system requires its own set of spare parts.



Integrated Safety

Integrated safety entails both functions occurring in a single control platform.

Integrated safety systems are becoming increasingly popular. They may cost more than general-purpose control systems, yet are typically significantly less than separate systems. The benefits of this approach, like common/hybrid systems, are lower

costs associated with learning only one system, simplicity of programming, common components, and ease of integration.

At this time, integrated safety systems are increasingly seen in machine control applications.

However, more widely available process-specific hardware components are needed before these systems come into wider use in process safety.

Achieving the Optimum Balance

Significant business value can be gained from an intelligently designed and properly implemented safety control system. It is important to remember that not all safety systems are created equal and each project has different performance, risks and cost goals. Striking the right balance from the range of technology options requires careful consideration of the specific capabilities, limitations and advantages of each one. ■

Article Courtesy: Rockwell Automation

ESOL Wins First Contract Outside India

New Delhi: Essar Oilfields Services Ltd (EOSL), a wholly owned subsidiary of Essar Shipping Ports and Logistics won its first contract outside India, valued at USD 40 million.

The contract from Vietsovpetro JV (VSP), an oil exploration and production company in Vietnam-is for drilling a 4,800-meter offshore well. The company has deployed its semi-submersible rig Wildcat for drilling the well and the deal is valued at approximately USD 40 million.

“This contract demonstrates the confidence of international companies in the capabilities of Wildcat in meeting their HPHT drilling requirements. A six-member

team from Vietsovpetro JV (VSP) visited the Essar Wildcat in March and found the rig meeting its stringent requirements,” said Ankur Gupta, CEO, EOSL. The Essar Wildcat has recently completed drilling in Gujarat State Petroleum Corporation’s (GSPC) oil and gas block in Krishna-Godavari basin. The rig has the capability to negotiate water depths of 600 metres and drill up to 7,500 metres.

The Essar Wildcat is also being offered to ONGC for its upcoming three-year charter hire tender. Currently, the EOSL owns and operates one semi- submersible rig and 12 land rigs and it has also placed orders with ABG Shipyard Ltd for two jack up rigs.