Process industry automation meets maritime needs

KAI HANSEN AND LUIS M. DURAN – Automation systems perform critical monitoring and control at process plants. Such systems may also be used to set safety targets in the maritime, and particularly oil and gas, industries.

Sea travel has always brought with it a certain level of risk. For centuries, navigation was a challenge many thinkers and craftsmen tried to solve. Today, a ship's crew continues to face the dangers of bad weather and loss of propulsion, which can sometimes lead to fatal accidents.

At the same time, modern ships face risks such as accidents involving cargo or problems related to a ship's systems and infrastructure. As more types of vessels are involved in the growing offshore oil and gas industry and in the transportation of hydrocarbons and chemicals, dealing with such potential disasters is crucial.

It is therefore essential to oversee a ship's functions and cargo and to take appropriate action before a situation gets out of control. This requires using computerized systems, which provide users with a high degree of trust. ABB's safety controller ensures a high level of confidence and also acts as an integrated part of the extended automation system 800xA – a complete solution within one framework. This means a ship's crew does not have to access too many different interfaces and hardware; they can rely on the same system, whether handling an emergency shutdown after an accident or simply checking generators or ballast water.

In addition to providing the highest level of safety and control, 800xA can be integrated into a collaborative solution whereby onshore offices and vessels can share information and work tasks in a way that was not possible before. This is already the case for sophisticated oil producing platforms and vessels and is now being used in other parts of the maritime industry, with examples given in other articles in this and the previous edition of *Generations*.

New challenges, new solutions

Oil and gas is, of course, vital to today's industrial civilization as it accounts for a large percentage of the world's energy consumption. The challenges facing offshore oil and gas development have driven innovation. Developing large production facilities, such as the Troll A platform, which stands at a depth of 300 meters, also entails major investments. Other types of offshore platforms, which float using a mooring system to keep them on location, bring their own challenges.

While it may cost less to use a floating system in deeper waters compared with a fixed platform, the dynamic nature of the platforms introduces other challenges for the drilling and production facilities as the ocean can add several hundred meters or more to the fluid column. The additional depth increases the equivalent circulating density and down-hole

pressures in drilling wells, as well as the energy needed to lift produced fluids for separation on the platform. This puts pressure on operations and increases criticality and related hazards.

Offshore manned facilities also present logistics and human resource challenges. They are a small community in themselves with their own sleeping quarters, management, cafeteria and other support functions in addition to the production and storage facility. Today, much effort goes into relocating as many of the personnel as possible on shore, where management and technical experts use remote access technologies and video conferencing to stay in touch with the platform.

Collaborative solutions

One type of floating system is a Floating Production, Storage and Offloading (FPSO) vessel, typically a tanker-type hull with wellheads that sit on a turret, allowing the ship to rotate freely – pointing into wind, waves or currents. Such vessels usually operate in water depths of between 200 and 2,000 meters. The main processing facility is located on the deck, while the hull is used to store and offload to a shuttle tanker or, in some cases, to a pipeline. While offshore operations have the complexity of any production facility, this is increased exponentially by limited space, weight capacity, harsh environments and other factors. While an FPSO needs to have a standard process control and safety system as with other installations, it also requires efficient operations on board and accessibility from a remote, onshore operations center.

The emerging trend is to create a collaborative system instead of segregated control solutions. So-called “integrated operations” are characterized by increased cooperation (independent of location) between operators, maintenance personnel, electricians, production and business management, and suppliers to provide more streamlined operations. For a big oil producing platform, this system is operated from the Central Control Room (CCR) using a combination of graphical process displays, alarm lists, reports and historical data curves. Console displays are often used in combination with a large wall mount display. With modern systems, the same information is available for remote locations such as an onshore corporate operations support center.

The goal is that, regardless of the technology used, CCR operators can access information seamlessly from a multitude of systems to run the facility safely and productively. Under abnormal conditions, timely decision making can prevent hazardous conditions, equipment malfunctions and process downtime.

Under such operating conditions, the control system is designed to allow users to:

- Access alarms and events from anywhere in the process (process control or safety systems)
- React seamlessly to diagnostics
- Assess initiating events from sequence-of-events data from the safety system in the context of other relevant information in the process history
- Create personalized work spaces, from which the operator can respond and make decisions

Within an integrated control environment, the operator can maintain a high level of alertness and understanding of progress through the production cycle. Real-time access to critical information enables operators to make correct decisions as soon as circumstances dictate, or to get remote assistance from experts on shore.

Similar collaborative solutions can also already be used on the bridge today and in the engine control room in more traditional vessels. The main difference is that navigation plays a more central role in a moving vessel and the process control system is much simpler.

Safety automation

Safety applications, such as the Emergency Shutdown (ESD) system, are essential and critical in vessels equipped for hydrocarbon handling or storage. The system kicks in when a process malfunctions or reaches a dangerous level.

A Fire and Gas System (F&G) automatically mitigates the consequences of a potentially hazardous occurrence (rather than preventing the hazard) and is normally implemented using certified controllers. The F&G is not generally related to any particular process for a vessel with oil or gas processes. Instead, it is divided into fire areas according to the location in the vessel.

Each fire area should be self-contained; that is, it should detect fire and gas by using several types of sensors, as well as control fire protection and fire-fighting devices to contain and fight a fire within the fire area. In case of fire, the area will be partially shut off by closing ventilation fire dampers.

In a more traditional vessel, fire zones in the ship and a fire detection system detect and warn of a dangerous situation. The Emergency Shutdown systems are then activated, closing fire dampers, etc., and ensuring that other systems take appropriate actions. In contrast to a processing facility on a production vessel, the ESD will normally not automatically execute the actual firefighting, but leave this to the crew.

Safety standards

Governments in many countries now enforce compliance to the safety standard IEC 61508 for the critical safety standards in the oil and gas industry, including floating units. This is a generic standard, which has a "functional safety" approach. There are also application-oriented standards that are based on this standard, implying that it not only addresses the technical solution but also takes a complete life-cycle approach to the system and its use.

The Safety Integrity Level (SIL) concept is the core of the standard. Levels are numbered from one to four and must be approached from two directions: the risk-and-consequences approach determines the required SIL, while the technical solutions approach fulfills the SIL requirement. The first approach involves evaluating what kind of incidents can happen and their consequences for people and the environment.

From this consequence analysis, an overall safety integrity requirement is determined. After taking into consideration how to reduce risk through mechanical and physical means, and by procedural and similar methods, the remaining requirements decide which SIL level the computer control system still needs to fulfill. This generic standard looks at several different models that can be used to determine a SIL level.

Finding out which methods to use, how a situation should be analyzed and the right SIL level must be done for each type of application according to the accepted risk level in a given case.

Even if it is difficult to come up with absolute numbers for such calculations, the standard does define numerical values for the SIL levels. For applications where an ESD system is triggered very infrequently (eg, once a year), safety standards in the table below apply. This shows how frequently a dangerous failure is accepted if the ESD function requires the system to take action. This refers to complete failure probability, including sensor, communication, electronic, software and actuator failures. For example, a SIL 3 cannot face a dangerous failure more than one out of 1,000 times.

Table 1 Numerical values for SIL

Safety integrity level	Average probablility of dangerous failure on demand of the safety function
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Even if the standard gives quantitative numbers as in Table 1, qualitative methods must also be used because it is difficult to make exact calculations.

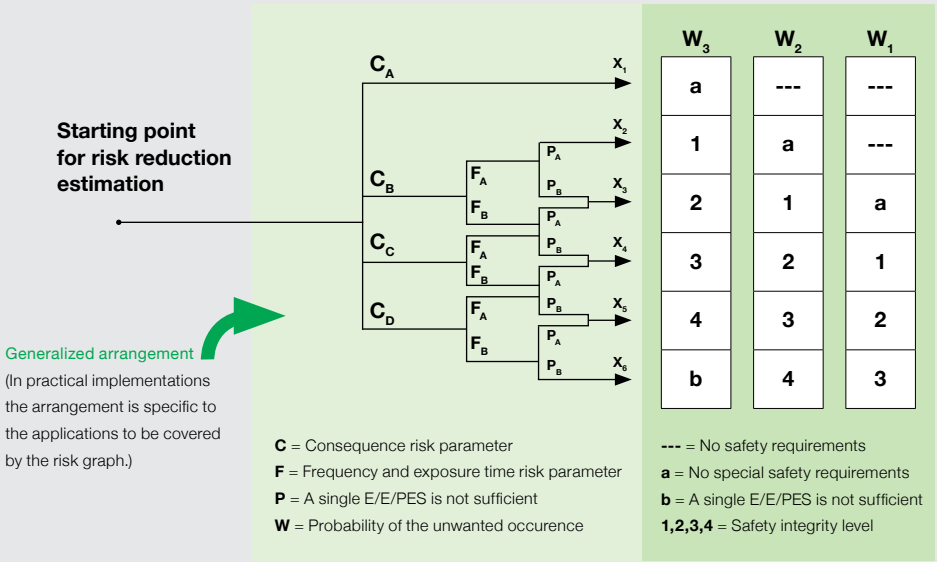
In order to determine the necessary SIL, the concrete case must be evaluated. There are several ways of doing this. Figure 1 shows an example of a risk graph method, which basically evaluates the consequences and probability of an unwanted incident. By following the arrows, we can find out which systems do not need a special safety requirement, which systems need SIL 1, SIL 2, SIL 3 and SIL 4, and which systems should be redesigned because of unacceptably high risk. In the process industry, solutions that require SIL 4 as a control protection would be redesigned to reduce the computerized safety system to a SIL 3 level.

When the required SIL level is determined, the next question is how to reach this SIL level with the electronic components and the software. This is done by combining a number of well-known techniques proven to improve the reliability of the system so that it works as intended. The safety standard has long lists of these techniques, but to put it simply: hardware is made with redundant components, while system design and software is developed in accordance with state-of-the-art methods. It is also important that good safety requirements are in place and that they are tracked throughout the lifecycle of product development. Higher SIL levels require the use of more methods and stricter development processes.

High Integrity

For years, process industries relied on independent protection layers to reduce risk. The concept assumes that the Basic Process Control System (BPCS), process alarms, operator actions, safety

1 Risk Graph Method



instrumented systems (SIS), Fire and Gas Systems, and any other system intended to reduce risk in the processes are capable of acting independently from each other. This means each layer must perform properly without being influenced by others and without failing, which would potentially disable two or more of the protection layers (defined as Common Cause Faults).

Traditionally, common cause was reduced by using totally different systems for the BPCS and the SIS and by using different hardware and software to reduce common cause failures. If these systems are purchased from different automation providers, common cause failures can probably be excluded; the user can assume that different development organizations, knowledge and manufacturing processes, as well as different installation, operation and maintenance procedures were used in the logic solver's manufacturing process. All of these, however, work against the idea of integrating solutions into a collaborative solution for marine applications.

Diversity of Design

This new degree of integration challenges the commonly accepted practices of satisfying and demonstrating that the SIS is not subject to common cause failures. Furthermore, even though the safety system and the normal process systems are integrated, both systems can provide independent protection layers and meet the safety standard's requirements. ABB chose an alternative approach while designing 800xA High Integrity, which is to build such independence into the design process of the Integrated System. It is possible to achieve independence by using diverse design engineering and programming teams who are provided with different software architecture specifications and guided by an overall concept for diversity from the start of the detailed design specifications.

In this way, dangerous failure modes can be designed out and more than 99 percent diagnostic coverage can be provided to protect safety integrity without resorting to duplication. Technology has evolved to the point where multiple options can address similar technical problems. For example, by using two or more of these technologies, diversity is embedded in the system design. Diversity can be achieved in the embedded software by using different operating systems and then by using different teams to develop the software on multiple compatible modules.

2 The 800xA High Integrity controller.

Security does not become an isolated activity after product development is complete, but is part of the design considerations early on in the process.

By combining two different technologies – such as Micro Processor (MPA) or Micro controllers and Field Programmable Gate Arrays (FPGA) – to perform the same functionality in parallel to each other, the design becomes truly redundant and diverse with minimum possible common cause failures. This diverse implementation with the System 800xA integrated control and safety system makes it a great solution for the challenging requirements of the offshore marine and oil and gas industry. Using an integrated system not only meets the safety standards for diversity in terms of layers of protection, but also brings significant benefits in operations and maintenance over the system's lifecycle.

Security in integrated control

With the advent of Integrated Control and Safety systems, security and safety have become inseparable. In addition to the implementation of access control, password protection and firewall configuration, logical separation can be added in the form of memory management. A memory management unit (MMU) allows different partitions of memory areas to be independent. These memory partitions are then connected to different execution processes of the CPU, such as regulatory process control or safety instrumented function. This approach ensures that only the memory area belonging to that process is accessible while the CPU is executing one of its processes.

As such, security does not become an isolated activity after product development is completed, but is part of the design considerations early on in the process. This includes not only threat modeling but also security checkpoints in the code design and review. In a similar fashion, testing does not become an isolated activity after the fact, but is embedded with functional testing. Independent teams, third-party assessors or both can perform tests and issue certification as applicable.

The option of taking an interfaced approach, instead of an integrated control and safety approach, will push the user to perform the following activities to satisfy security requirements:

- Perform a full vulnerability assessment/threat modeling and testing of the different subsystems
- Define the best security mechanism for each of those subsystems to cover any identified gaps
- Perform a full vulnerability assessment/threat modeling and testing of the entire interfaced architecture

- Implement and maintain the security mechanisms throughout the system lifecycle

Based on these, the challenge most users face is establishing a Security Management System of the interface architecture and supporting it over the system's lifecycle. Installing an integrated solution can help reduce the complexity of securing the control and safety systems, while also making it easier to maintain over time.

Peregrino FPSO

In 2008, with only one commercial voyage on its log books, the *Nova* returned to the shipyard for its conversion from a Very Large Crude Carrier (VLCC) to an FPSO vessel. At a cost of more than $1 billion, the conversion was the largest investment in a single vessel in the history of the ship's owner.

With a daily production capacity of 100,000 barrels of oil, 350,000 barrels of liquid, and 7.3 million standard cubic feet of gas, the FPSO *Peregrino* has a storage capacity of 1.6 million barrels of oil, equivalent to 16 days of round-the-clock production. The topside consists of two identical production trains and 15 modules for crude oil separation, water treatment, chemical injection, metering, power generation, power distribution, power and process control, and accommodation for 100 staff.

On the electrical side, the ABB solution for the FPSO and wellhead platforms distributes power for the entire production process, including the electric submersible pumps in the production wells below the seabed.

A multisystem automation solution, including field instrumentation and telecommunications systems, was supplied by ABB. The solution includes systems for process control, power management, production information management, condition monitoring, fire and gas, and emergency shutdown. These are all integrated within the same System 800xA Extended Automation platform and operating environment.

Each system is operated from a System 800xA Extended Operator Workplace (EOW-x) control room on board the FPSO. EOW-x offers an ergonomic operator environment that facilitates operator decision making and produces measurable improvements in plant productivity, safety, information flow, and operator job satisfaction. Some 14,000 I/O on the vessel and platforms are controlled by AC 800M process controllers and AC 800M high-integrity controllers.

Conclusion

As shown in the example of the *Peregrino* FPSO vessel, technology has played a crucial role in addressing the challenges facing offshore oil and gas production facilities, including seamless access to information, independent secure layers of protection, and an optimal footprint. This example describes how an Integrated Control and Safety System (ICSS) can address operational challenges by supporting both local and remote operations seamlessly using System 800xA.

ABB has not only addressed the fundamental design elements needed to maintain independent protection layers but has also fully integrated safety systems into the 800xA control and operations environment. By providing the technology for integrating safety into the core of a company's operations, ABB is delivering a safe and reliable integrated operations solution that is perfectly suited to meet the challenges facing today's marine and oil and gas industry.

Kai Hansen
Technology Manager, ABB Vessel Information and Control Center of Excellence, Norway
kai.hansen@no.abb.com

Luis M. Duran
Product Marketing Manager Safety Systems, ABB USA
luis.m.duran@us.abb.com