A Practical ‘Live’ Migration Strategy for Upgrading Safety Systems in the Oil and Gas Industry

Recent events in the oil and gas industry have substantially increased interest in maintaining the highest standards of safety at all times.

By Adam Howard, EPC operations manager, Rockwell Automation
Introduction

Recent events in the oil and gas industry have substantially increased interest in maintaining the highest standards of safety at all times. These events have spotlighted the potential worker, environmental and business ramifications of a significant safety event. Oil and gas producers and the operators who manage their production facilities demand the highest level of safety in order to protect personnel, the environment and production assets while maintaining maximum uptime and minimal operational disruption.

Balancing these critical requirements often comes to a head when an oil and gas producer needs to upgrade a facility’s safety system. As safety systems age and become outdated or obsolete, they not only increase safety risks when compared to more contemporary systems, but can also cause lost production time due to unnecessary trips or shutdowns.

Contrary to popular belief, installing an upgraded safety system does not necessarily require a lengthy shutdown of the facility. With careful planning and detailed, thorough engineering, a safety system can be upgraded with minimal disruption to facility operations.

The Role of a Safety System

In oil and gas production operations, the distributed control system (DCS) manages the normal operation of the plant. The function of the safety instrumented systems (SIS) is to preserve life, the environment and the equipment being monitored.

The most common types of safety systems in oil and gas production are the fire and gas (F&G) and emergency shutdown (ESD) systems. The primary objective of the F&G system is to monitor for the presence of fire through smoke, heat and flame detection, as well as for potentially dangerous levels of hydrocarbons by “line of sight”, “point” and acoustic gas detection methods. If any of these conditions are detected, the system implements appropriate alarming, firefighting and suppression measures in order to minimize the impact to personnel, environment and assets being protected.

The core objective of the ESD system is to protect people, the environment and production assets against misuse, equipment failure and against catastrophic failure in the plant. When the ESD system is activated, it may require an orderly shutdown of the production process to protect personnel and the integrity of the plant. Typically, the F&G and ESD systems are physically independent of each other and separate from the DCS.
Drivers for a Safety System Upgrade

Facility owners normally upgrade their safety systems for a variety of reasons, ranging from equipment obsolescence to the need to take advantage of the benefits of extended or more advanced functionality. Some of the major drivers include:

- **Prolonging field life.** Many oil and gas reservoirs continue to generate viable quantities of product well beyond the intended life of the original field design. Consequently, the platform has to be upgraded – often on a rolling refurbishment basis – to accommodate these extended operations. These upgrades also can help reduce annual maintenance costs while simultaneously reducing unplanned downtime and unexpected repair costs.

- **Meeting current codes and standards.** Currently installed safety systems were designed and built in accordance with the codes and standards in force at the time. Since then, the industry has moved forward and legacy systems have not been upgraded to current standards and technologies. For example, while IEC-61508 was introduced in 1999, many legacy systems have not yet been reassessed to determine if they comply with this standard.

- **Improving functionality.** Operational requirements have changed in the last 20 years as technology has advanced to include capabilities such as remote operations, improved diagnostics and simplified interfacing between systems. For example, advanced asset management tools are available that can help gather and analyze vital data from across production facilities. While this may not be a prime driver for system upgrades, it is often a key factor in the cost-benefit analysis.

Safety System Obsolescence

Every piece of equipment or system will eventually come to the end of its useful lifecycle. Based on our experience, safety systems need to be upgraded some 15 to 20 years after initial installation. For safety systems, this can become apparent in a number of ways:

- **Equipment obsolescence.** Equipment often becomes obsolete when the underlying components are no longer manufactured. While “last-buy” options from manufacturers can temporarily address this, the ongoing maintenance and support of these systems will no longer be viable once the supplier support infrastructure can no longer service the equipment.

- **Erroneous operation.** As safety system components age and fall “out of tolerance,” no longer performing within their designed parameters, part of the system could begin to operate erroneously. Since safety systems are designed to fail to a safe state, this can often result in unnecessary and costly shutdowns.

- **Inability to expand or enhance the system.** Legacy systems, particularly hardwired systems, are difficult to expand, beyond small changes. Therefore, expansion to accommodate new features – such as additional subsea tie-backs, artificial lifts or compression facilities – is often difficult to accommodate due to physical space and system interface constraints. In addition, older systems may not meet current industry standards.
Safety System Upgrade Strategies

Implementing a safety system upgrade requires an in-depth analysis and risk assessment of the existing technology, so you have a solid understanding of the requirements needed for a new system. A safety system upgrade should follow a systematic and well-documented process. We recommend the following approach:

• Establish a baseline
• Evaluate the current system architecture
• Build and thoroughly test the new system in the factory
• Meticulously plan and manage the system migration

Establish a Baseline

The first step in a safety system upgrade is to establish a clear understanding of the existing design, including the specific nature of the system’s core architecture and the functional operation. The “as-built” documentation status of many mature systems is poor, conflicting or non-existent. As a result, engineers often need to “reverse engineer” the installed system to either confirm that the existing documentation is correct or mark it up to determine how to proceed.

During this phase of the project, the safety integrity level requirements may need to be established or re-affirmed. In some instances, this may necessitate revisiting the original system design approach. Carrying out this assessment not only means the design of the upgraded system can be compared to current SIS standards, but also may significantly reduce the complexity of the system needed.

Once this baseline is firmly defined, you can determine which system upgrades, enhancements and improvements may be needed. While this preparatory work can take a considerable amount of effort, it is absolutely essential in helping ensure the functionality is correct and the design is traceable.
Evaluate the System Architecture

In order to execute a “live” migration from the legacy system to the new system, designers need to exploit the inherent redundancy built into the legacy safety system. Given that most legacy systems have an “A” and “B” side (see Figure 1), each executing the same logic, one “side” can be switched off and removed without shutting down the system. It should be noted that while the system is in this degraded state, it is fully operational and, if designed that way, fail-safe. However, by switching off one “side,” the system redundancy and fault-tolerant capabilities will no longer be available, the implications of which need to be understood through an appropriate risk review.

This configuration will allow the new system to be installed and run in parallel to the legacy system, allowing a safer, quick and effective migration between the systems during live plant operations.

Figure 1: Safety Systems Upgrade - Live Migration
Build, Test and Document

Once the new system is built, it is essential that it is fully tested against the defined and agreed-upon baseline before it is installed in the field. By testing the system before the live changeout in the field occurs, you can be confident that the functionality will meet the operational requirements. Any functional enhancements can only be implemented and tested after these tests are completed.

During this phase, it also is critical to get the buy-in from all interested parties, particularly the oil and gas company’s operators and the relevant certifying authority. Oil and gas producers will focus on safety concerns, the functionality of the new system, how it will be migrated and any operational constraints that will need to be addressed. The certifying authority will need to be assured that you have clear and demonstrable processes in place to show that the system build, test and – later on – commissioning and operation is safe and complies with legislative requirements, as well as local and international standards.

In addition to the build and test records that the system manufacturer produces, the engineering team should produce comprehensive and detailed work packs that include method statements, implementation details, reversionary plans and check sheets to verify the installation, commissioning and handover of the system. This is essential in recording – to the satisfaction of the certifying authority – the work undertaken in implementing the upgraded system.

Installing and Migrating to the New System

Once the new system has been tested and shipped, it can be installed and commissioned. The following is an overview of the steps needed to migrate from the legacy system to the new system during live operations. It is at this phase of the project that the detailed planning and preparation already undertaken will prove critical to the successful migration of your safety system.

• Fully verify the functionality of the existing legacy system, including any standing inhibits or overrides retained from that system.

• Install the new system in its final location. Once installed, carry out basic functional tests – often called “travel-well” tests – to help ensure that the system is fully operational ahead of the system migration.

• Remove one “side” of the legacy system (in this case, side “B” – see Figure 2). This is one of the risk areas due to the possibility of inadvertent operation of the system, such as loose wiring disturbance. The system is now in the degraded state.
• Hook up the field inputs, such as fire and gas detectors, to the new system, while retaining the inputs to the legacy system. The new system can now “see” the same inputs as the existing system but, because the outputs are not hooked up, the new system is not carrying out any executive actions (see Figure 3 below).

Figure 2: Safety Systems Upgrade - Live Migration

System ‘B’ removed (System ‘A’ in 1001 Configuration)

Field Transmitter

Analogous Input Module

1oo1 Output Voting Module

System ‘A’

To Current HMI System

Field Output

To New HMI System

Figure 3: Safety Systems Upgrade - Live Migration

New System Installed (System ‘A’ remains in 1001 Configuration)

Field Transmitter

Analogous Input Module

1oo1 Output Voting Module

All inputs individually tested to new logic solver. Test verifies input sub system, C&E logic (via observation or output statue, and HMI.)

To Current HMI System

To New HMI System

Figure 3: Safety Systems Upgrade - Live Migration
• Fully test that both systems see all inputs and that logic solver output actions implemented are identical to the legacy system. In this instance “like for like” functionality (i.e., both the old and new systems respond in exactly the same manner to field input conditions) is critical unless otherwise noted. This can be done by temporarily disabling the appropriate outputs, which can be time-consuming and may not be operationally acceptable, or by observation of the new logic solver against the design documentation.

• Fully verify the human machine interface (HMI) functionality for the new system.

• The outputs of the safety system can now be migrated from the legacy to the new system (see Figure 4). At this stage, the new system will assume control. This also is where the major difference between the migration of an F&G and ESD system occurs. F&G outputs tend to be normally de-energized, or “energize to action,” whereas ESD outputs tend to be normally energized, and therefore “de-energize to action.” This is considered to be a fail-safe design philosophy. Transferring the outputs from one system to another without inadvertently tripping the plant or falsely setting off your fire and gas protection system can be challenging for system migrations of this nature.

Migrating a normally de-energized output is relatively straightforward and is normally done in under a minute per output. During this time, there is no protection for that output.

Migration of normally energized outputs present a different challenge that can be addressed by either electrically “holding up” the output using a temporary supply or locking off the output device. This takes more planning and operational permits and is consequently more time consuming, taking typically one to two hours per output. Figure 5 shows schematically how a critical output circuit may need to be configured during an ESD system output migration.
Once all safety system outputs have been migrated, full control of the safety functions will have passed from the legacy system to the new system.

The new system will now be subjected to full system tests. Since the facility is still live, the tests carried out may be an agreed-upon subset of the full functionality and are often guided by the requirements of the operators and the certifying authority. Any tests that cannot be carried out while the plant is live will need to be delayed until the next facility shutdown when full system tests can be carried out.
Once the upgraded system is fully operational, the legacy system can then be deconstructed. The final system, which has redundancy and fault tolerance built into its design, is shown in Figure 6 below.

![System Migration Complete - Removal of Old System 'A']

**Finding the Best Approach**

Significant cost savings and productivity benefits can be gained from an intelligently designed and properly implemented safety system upgrade strategy. 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 requires careful consideration of the implementation approach and the specific capabilities, limitations and advantages of available technology options.

Live migration of safety systems during plant operations is possible with careful analysis of the system design and operational requirements and a thorough and detailed approach to the engineering and migration strategies. In addition, the need for detailed and comprehensive planning and preparation cannot be overemphasized.

However, the preparatory work can pay off in the long run for the plant operator, and one of the best resources you have available is your system’s vendor. Many safety system providers can provide guidance, design recommendations and on-site assistance to help ease the migration, minimize downtime and optimize your system’s performance.
For example, the strategy outlined in this article is based on an actual safety system upgrade of over 3,000 I/O on an operational production platform project managed by Rockwell Automation. The upgrade caused the end user minimal disruption to their operational requirements while providing the upgraded system needed to meet their functional safety requirements.

**Adam Howard is the EPC Operations Manager for Rockwell Automation. He is based in Aberdeen, Scotland.**

Through its integrated and scalable solutions, team of more than 800 industry specialists, and extensive partner network, Rockwell Automation helps companies in the oil and gas industry improve operational efficiency, throughput and uptime; reduce their total cost of ownership; and boost worker and asset safety across the entire supply chain. For more information on Rockwell Automation services and solutions for the oil and gas industry, please visit [www.rockwellautomation.com/industries/oilgas/](http://www.rockwellautomation.com/industries/oilgas/).