Drivers for a Safety System Upgrade

Adam Howard, Business Manager, Oil & Gas Solutions, EMEA and
Tom Shannon, Head of EPC, Oil & Gas Solutions, EMEA

The decision to upgrade a safety system in a process plant is never one that is taken lightly. The drivers behind this decision are often complex and influenced by many factors and stakeholders. Asset owners commonly find themselves faced with a primary and secondary set of reasons for a safety system upgrade.

The primary reasons cannot be ignored. While asset owners may face a different range of primary drivers, from plant to plant, they most often include safety system equipment obsolescence. Obsolescence occurs when an asset's life has been extended beyond its original design. Similarly, if a significant portion of a plant or asset is being upgraded, many asset owners will take this opportunity to upgrade the safety system as well. The poor maintenance and management of the current system is another primary driver.

Secondary reasons are the additional benefits gained as a result of having to implement a safety system upgrade. These benefits contribute in terms of asset productivity, optimized manning, preventative maintenance and optimized asset performance. Examples include improved functionality and compliance with current codes and standards.

Providing a solution to address the primary and secondary drivers come in both project costs (Capex) and, potentially, lost production while the system is being replaced (Opex). An asset owner needs to understand and consider the true overall cost implications at the same time as the requirement to upgrade.

The Role of a Safety System

Many process plants separate their control systems from their safety systems. For these plants, the distributed control system (DCS) manages the normal operation of the plant. The safety instrumented systems (SIS) is dedicated to helping preserve life, the environment and the equipment being monitored. Some of the most common applications include fire and gas (F&G), process shutdown (PSD) 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. In addition, the system observes 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 help minimize the impact to personnel, the environment and the assets being protected.

The core objective of the PSD and ESD is to help protect people, the environment and production assets against misuse, equipment failure and against catastrophic failure in the plant. The PSD normally acts on a subsystem basis whereas the ESD system acts on an 'area' or plant-wide basis. Once activated, it may require an orderly shutdown of the production process to help 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.

Primary reasons to consider an upgrade to your safety system

Drivers behind safety system upgrades can vary, but primary objectives to consider an upgrade usually fall under two categories: safety system obsolescence and poorly maintained/upgraded safety systems. Both of these reasons justify the need for a safety system equipment upgrade.

1) 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:

- **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 in oil and gas production– is often difficult to accommodate due to physical space and system interface constraints.
- **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.

Obsolescence driven upgrades

Because upgrades driven by obsolescence are so common, we'll explore this topic further through the lens of the oil and gas industry. Two of the major reasons an asset owner in the oil and gas industry would decide to upgrade based on obsolescence 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.
- **Asset expansion or modification.** Oil and gas platforms may require large modifications as their original design capacities are changed to incorporate new CAPEX projects, such as new oil well tie backs, or compression trains to increase ailing production. Projects of this scale require large modifications to the safety systems to incorporate the changes required. This may be considered the best time to upgrade the system if expandability is an issue or if adding additional "dated" technology makes no sense — especially if the capital project budget may cover the upgrade costs.

Lifecycle management

As the safety systems components last for varied durations, it is important to keep a record of all the sub systems and modules, not just one component. For example, to keep a record of just the processor version or software revision would not be enough.

Figure 1 shows the average system component lifecycle and highlights the key components, such as I/O cards and controllers, which reach the end of their design life at 15 to 20 years respectively. A server's average life is much shorter due to a manufacturer's Operating System upgrades, health care requirements and/or security protocols required to remain current.

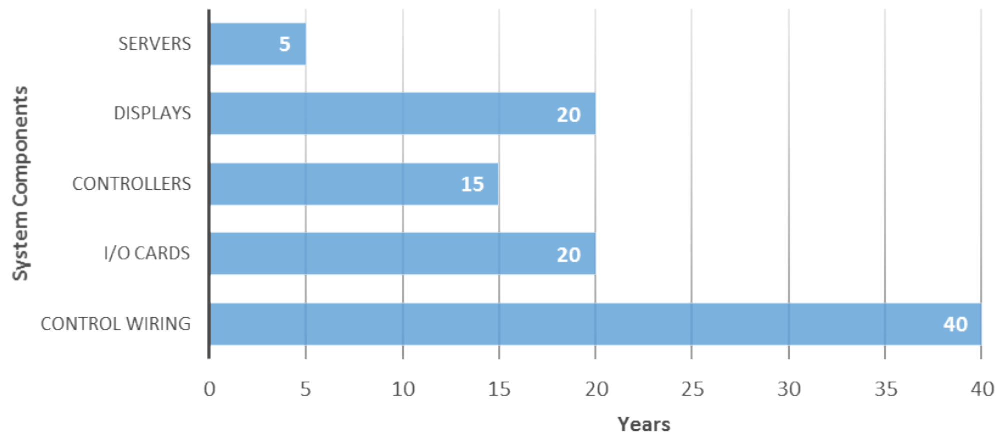

Figure 1. Average System Component Life

As shown, the control wiring of the system is robust and can be maintained for up to 40 years in service. Since the control wiring life is much longer than other components, it allows for re-use when considering the safety system upgrade. The benefits of reusing wiring during an upgrade include:

- System changeover time is kept to minimum.
- Modifications and disruption of the existing system are kept to a minimum.
- Potential for online 'live' migrations is maximized.

Due to the varied lifespans of system components, lifecycle management is an important process to maintain. Managing a complete record of the sub systems and modules is vital to accomplishing a successful and efficient safety system upgrade.

Obsolescence review

A good way of recording the status of the system components is to conduct regular obsolescence reviews. These reviews detail and record the individual subsystems and modules of a system (i.e, make, model, serial number where possible). All of the parts, to module level, should be assessed using the manufacturer's information, which allows the assessor to determine the current status of the part. Is it still in production? Is it supportable? When is the last buy date? An obsolescence review will allow the owner of the system to build the lifecycle status of the system.

A traffic light reporting structure (Figure 2) can help to visually identify issues and determine the urgency of an upgrade. The asset owner can then use this information to support an informed and balanced decision on whether a full or partial safety system replacement or upgrade is required and compare this to the other major factors that affect the decision, such as field life.

In the simplified example below, it shows that the ESD systems are the least supportable element of the overall safety system. In this case, if the remaining asset life is three years, then a mitigation strategy would be developed to sustain the existing system for the remainder of the asset life. If the projected life is, for example, 6 years, then the ESD systems would need to be migrated together with the PSD 4 system. The remaining systems could be maintained. If the asset life is a projected 10+ years then the most cost-effective option would likely be a full safety systems upgrade.

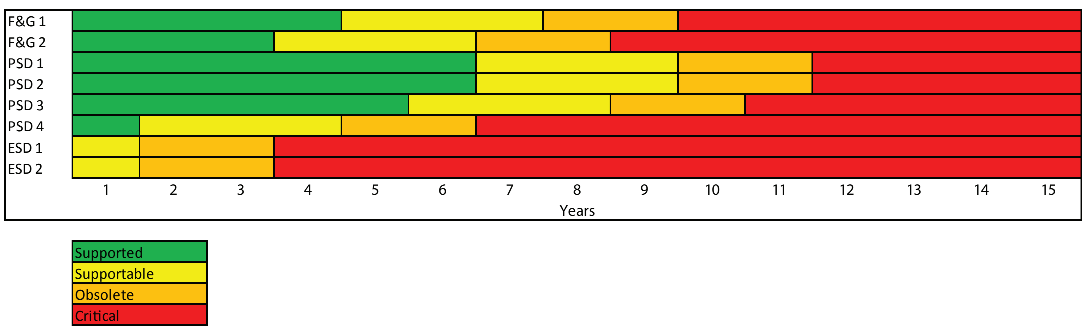

Figure 2. Example safety systems obsolescence overview

2) Poorly maintained and upgraded safety systems

Most process industries can be proud of an excellent safety record. However, there are instances where the high standards demanded are not always met.

It is necessary for a safety system to be properly maintained and upgraded during its life. If system modifications have been poorly implemented and design documents, drawings and panels have not been kept up to date, it can lead to very low confidence in the ability of the safety system to do its job when called upon.

Personnel working in a live plant need to know that they are protected at all times. No one wants to have a poorly maintained system involved in their protection. Unfortunately, some appalling examples of 'problem systems' exist in every process industry, and they are a scourge on the day-to-day reliability of the processes and the safety of personnel and the environment.

Below are some examples of poorly maintained/upgraded systems. Most professionals would want to replace these systems with tidy, well-maintained, documented and regularly-tested systems.

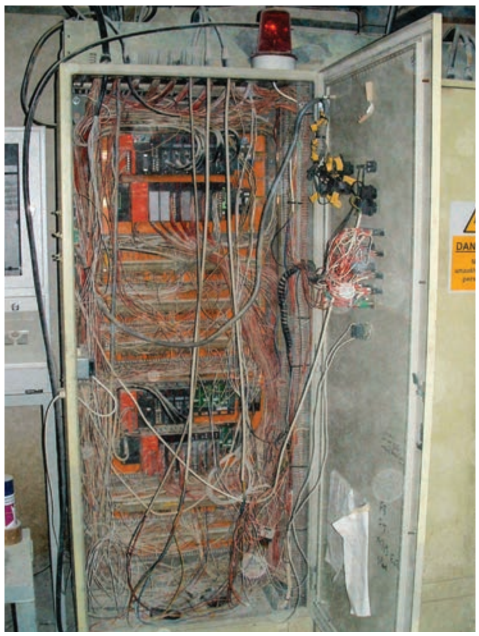

Figure 3. This picture speaks for itself.

Figure 4. Shocking example of a very poorly maintained system.

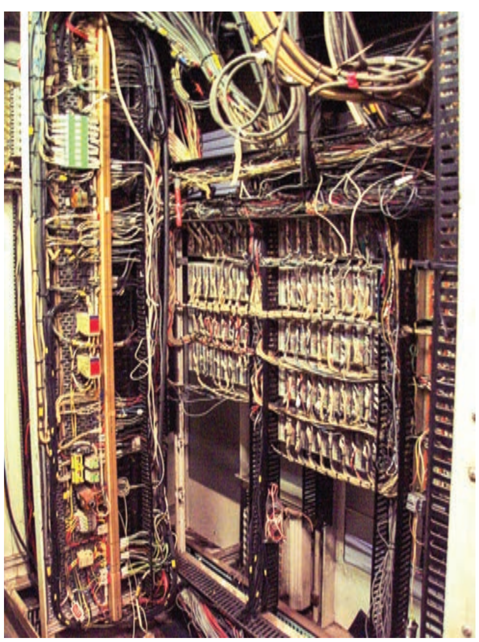

Figure 5. This panel infrastructure has been used to expand and add system functionality and clearly utilizes "dated" technology. An upgrade is required.

Figure 6. Using "gaffer" tape to patch a control panel is NOT indicative of a well maintained system.

Secondary reasons to consider an upgrade to your safety system

A safety system upgrade will bring advantages to the asset owner and other stakeholders. Those advantages that extend beyond the primary reasons of obsolescence or a poorly maintained system are considered secondary reasons. These additional advantages can benefit the asset owners and other stakeholders when making the decision to upgrade. Two of the most beneficial secondary reasons include:

- **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 of installation. 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 1998, followed by IEC-61511 for the process industries, many legacy systems have not yet been reassessed to determine if they comply with these standards. Compliance with current codes and standards will not only help to improve the functional safety management of the plant, but also help to minimize the risk of exposure to litigation. If a safety system caused an issue and was not compliant with current codes and standards, the asset owner could be faced with legal action.
- **Improving functionality and efficiency.** 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. For example, the benefits in terms of asset productivity, maintenance, manning and optimized asset performance will lead to a fiscal return on investment that will assist the commercial case for an upgrade.

Conclusion

Whether an asset owner's primary driver is removing obsolescence or improving poorly maintained/upgraded systems, a safety system upgrade can resolve many of these concerns. However, these drivers should not be considered exclusively in terms of primary drivers. The benefits that secondary drivers bring can play a significant role in the decision to upgrade a safety system. Two of the most impactful secondary drivers include improving functionality and efficiency and meeting current codes and standards. The secondary drivers will lead to long term benefits to the plant related to productivity, efficiency, operability, and most critically operator safety and the environment.

While this whitepaper discusses why a safety system should be upgraded, the process for implementing a new safety system is extremely important — especially if minimum downtime is a key factor in the decision process. Rockwell Automation can help you define a cost effective upgrade to maximize return on investment. The Company has a proven track record in undertaking safety system upgrades and migrations on 'live' assets (i.e. while the facility is active and not in a shutdown or turnaround). To learn more about our proven methods for implementing 'live' safety system upgrades, please read ***A Practical 'Live' Migration Strategy for Upgrading Safety Systems.***

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication PROCES-WP009B-EN-P – July 2019
Supersedes PROCES-WP009A-EN-P – September 2015