WHITE PAPER

Legacy Safety Instrumented Systems (SIS)
When to maintain or evolve?
Today, the use of programmable control systems to implement safety functions is now a common practice within the Process Industries and Functional Safety Management (FSM) achieved by established IEC 61508 and IEC 61511 standards.

However, for over 30 years, protection and mitigation systems have been installed on high hazard facilities comprising and including emergency shutdown systems, fire & gas systems, boiler management systems, etc. These legacy systems provide an essential layer of protection when the plant and equipment experience operational disturbances which can potentially go out of control leading to an incident.

Unfortunately incidents continue to occur on a regular basis in such process industry installations where Safety Instrumented Systems (SIS) have been installed and are assumed to meet the current operational risk reduction requirements. It therefore follows that managing, operating and maintaining your SIS against current industry good practice requirements should go some way to preventing these incidents occurring in the first instance.

For those legacy systems that have been well managed and maintained (or conversely those that have not) and thus performed as expected, with either good or poor reliability and availability over many years, there comes a time when a number of contributing factors drive the impetus for change. These include:

- Maintaining performance whilst spares and OEM support become less available
- Avoiding spurious trips and production outages due to system degradation

Given the above issues, the end user will therefore be required to establish a strategy towards evolution of the safety controller, operating at the heart of the SIS, in order to maintain functional safety performance associated with the continued life of the asset it is protecting.
The drivers for technology change?

Such legacy systems will have been introduced as first and second generation fail-safe solid state electronic and programmable electronic safety platforms with redundancy in the form of TMR technology, or 1oo2 technology, with a high level of diagnostic capability. This redundancy premise, with a focus on meeting reliability and availability, was at the forefront of safety requirement specification during this period i.e. the key market drivers for a ‘best in class’ solution as prevalent at the time. However, it must be recognized that some safety solutions may have been engineered using a platform that has not been specifically designed / certified to any historic industry standards.

Whilst such systems may have provided reliable solutions over many years, it is inevitable that product obsolescence and potential hardware failures will increase rapidly towards end of serviceable life. A further driver may come from regulatory authorities to replace platforms where the safety credibility cannot be established.

From experience, the key driver for change in many circumstances is that the technology will not be supported by the original OEM provider. This scenario may be due to several combining aspects such as technology advances, product lifecycle obsolescence, component availability or OEM acquisition / merger / closure as the supply chain continues to re-structure to meet market drivers.

For present day requirements, the challenge for the asset operator is to maintain protective measures in line with current operating hazards that exist on site. When considering legacy SIS, the modern terminology and expectations for demonstrable risk reduction management that we work to today, will not have been the key features for the development of the original protection system in the past.

During the lifetime of the legacy SIS, it would be typical that the main drivers for the end user with regard to safety related systems will have been to focus on:

- Maintainability, a recognition of reliable SIS that ideally can be continued for service, but is limited to end-of-life issues as a feature of obsolescence statements from the original OEM provider
- Alignment to operating plant life expectancy i.e. shutdown / decommissioning
- Maintaining knowledge and experience to support the equipment as part of the corporate memory and within the OEM service organisation
- A recognition of management KPIs highlighting the increased servicing and call-out costs, increased spares usage and increasing production downtime
- Ensuring safety measures are maintained during the final stages of technology OEM support i.e. service, spares, maintenance, etc.
- Management of change implications on the technology as safety functions are either added or removed to match operational risk reduction requirements (impact assessment)
- Consideration of any changes in asset information management requirements for asset improvement
- Consideration of any impact from the local regulatory authorities and industry good practice expectations for operating, maintaining and modifying the SIS
Applicable safety standards back in the day?

Prior to 2000, legacy SIS solutions will have been aligned with standards such as DIN 19250 and VDE 0801 & ISA 84 and supporting application management via documents such as the UK HSE PES guides. At this period of time, the concept of safety integrity levels (SIL’s) was not a normal feature of specification and design. Many organizations utilised prescriptive standard ‘off the shelf’ solutions for a range of process measurement parameters. Standard OEM suppliers may have also augmented their solutions with a range of differing third party equipment, again with a wide range of supporting data sets, i.e. from comprehensive to non-existing supporting technical information.

Such standard solutions will have been based on prescriptive designs, previous operating history and standard proof test frequencies to match across all trip and alarm loops regardless of protection severity. In some high hazard manufacturing organisations some further delineation of importance may have required additional redundancy and increased proof test frequencies to be implemented to certain trip function requirements based on the hazardous events defined during the project hazard studies, i.e. identification of a ‘Grade’ or ‘Class’ of trip and alarm functionality e.g. ‘Class A - high level of importance for safety’, ‘Class B - medium level of importance for safety’ and ‘Class C - operational asset loss importance’.

More and more PES systems have been introduced (and by association a whole raft of differing software covering firmware, embedded and application) into the process industries to provide a level of SIS protection. Accordingly, several new supporting standards have been developed and issued to provide guidelines for engineering and operation of safety-related systems. These include IEC 61508 and IEC 61511.

Today IEC 61508 and IEC 61511 are becoming the end user and supply chain default lifecycle management standards for the approach to developing protection and mitigation systems to meet industry good practice requirements.

Although not a mandated standard(s) to meet legal requirements, in many countries these standards are a demonstration of good practice requirements when things unfortunately go wrong, which in essence transports such industry leading standards to become a legal benchmark by association; and hence the inescapable linkage for adoption by both the end user and supply chain alike.

Fundamentally these standards provide industry good practice guidance for demonstrating a cohesive link between the quantitative and qualitative techniques and approaches necessary for hazard and risk management requirements. This determines how the safety function and safety integrity is migrated via the Safety Requirements Specification (SRS) into the functional design of the SIS. It is no longer the norm to provide just a prescriptive design functional description and supporting cause and effects to design and engineer the necessary solution.
Legacy technology may have had (but not necessarily) some form of formal certification via an accredited body such as DIN. The certification processes involved will usually have focused on random hardware failures against component failure data and supporting quality management systems. Software techniques and measures will have had some form of V-model development lifecycle approach applied as required of earlier coding standards such VDE 080, however systematic capability assessment would have been non-existent and thus software development and testing would have been subject to the discretion of the individual coding engineers and their particular ‘style’ of coding and verification.

In many cases there was no formal certification of legacy technology used in protective systems i.e. PLC’s, solid state relays, etc. Redundancy was usually the solution deployed as a requirement to meet availability, rather than to meet reliability.

In a number of circumstances, legacy safety related systems were designed as bespoke company specific solutions, or the EPC re-use of a previous solution approach. It was also not uncommon for low level safety functions to be routed through the normal control system causing confusion as to what was a dedicated safety function as opposed to a process interlock.

It could be observed that industry as a whole had differing perceptions as to what constituted control, process interlock or dedicated safety and the resultant mixture of safety and non-safety functions across a range of systems, devices and communications. To this day, adding alarm functionality in all types of control systems and covering all eventualities is easy to configure, but historically this further adds confusion as to which critical alarm events are truly aligned for safety.

The introduction of IEC 61508 initially added further confusion where suppliers and end users were claiming SIL capability without understanding the detailed requirements of the standard. The original compliance with IEC 61508 would remain strongly biased to random hardware failures and PFD and the take up of the new concepts of Hardware Fault Tolerance (HFT) combined with Safe Failure Fraction (SFF) and Systematic Capability (SC), were difficult to grasp. To some extent experience suggests this is still true today, however the advent of Ed 2 of the IEC 61508 standard has gone some way to reinforce the importance of the architectural and systematic capability requirements necessary to achieve safety functionality and integrity.

In contrast, today’s technology strongly follows the certification requirements associated with compliance to IEC 61508 and IEC 61511. In determining suitability for use in a Safety Instrumented Function (SIF), then requirements for random hardware failures, used in parallel with architectural constraints and systematic capability (which are as equally important), are utilised as the key design data metrics for achieving a suitable SIF solution.

As such, compliance for legacy systems would not generally meet the design criteria as specified in today’s safety related standards.
When the pressure is on?

So as an operating asset owner are you reaching the stage in the lifecycle of your existing legacy SIS where you are now seeing an increasing uptake in your spares utilisation? In conjunction with this effect are what spares you have available now somewhat limited in number? In some cases are only well-known internet-based selling domains really your last resort for additional spares?

In addition, have you received notification from your OEM supplier that due to obsolescence the systems are no-longer supported? Are you at the point where corporate memory retention is at an all time low, i.e. anyone who knew anything about the SIS and how to keep it operational has either left or retired? Is it the situation that anyone in the team who is left to face the music is managing a wider range of issues on a wider set of technical fronts with limited or no time to think on the next steps for maintainability or replacement?

If this sounds familiar to your organisation, then you are not alone as many end user operators are facing a similar dilemma given the simultaneous timing of the drivers for changes happening now and in the next 3-5 year period based on the life expectancy of the current SIS installed base.

Also, it must not be forgotten that modern company operational requirements now mandate that asset management KPI’s will be a stakeholder requirement going forward. Also note that the SIS is to provide increasing assurance for safety whilst increasing availability because most operating companies cannot afford spurious trips in the light of tight profit margins and the demanding markets they operate in.

So how big is the challenge? When operating with a legacy system installed, the end user will be undertaking to manage three key requirements:

- Modifying the system to change, add or remove safety functionality dependant on operating requirements for existing plant, new plant, decommissioning, etc.
- Maintaining the system to the ‘as new condition’ including performing proof tests, recommended maintenance and repairs
- Applying items 1&2 above to plant operating life expectancy

According to the safety standards, any change to the SIS generated from either of the above key requirements to operate and maintain a legacy SIS will be undertaken by management of change procedures and will feature as a minimum impact assessment. The impact assessment will determine the scope, size, complexity and functional safety implications of the proposed change and depending on plant operating life expectancy what constitutes the short to longer-term solution.

Any change associated with legacy systems and documentation can become a minefield as the end user has to be able to justify that the legacy system’s original design intent has not been compromised and meets, in all respects, the level of risk reduction required for the operating plant today.

Difficulties may be experienced in obtaining sufficient and appropriate documentation that supports the basis of change and the current operating logic / cause and effects. As such, these may have changed out of all recognition from when the plant was first commissioned some 20-30 years ago.

Assuming that the basis of safety has been maintained throughout the plant operating life, and there is robust supporting evidence to support this claim, then a simple or complex modification of the legacy system may be appropriate.
To progress with a simple modification, supporting evidence would include basis of design documentation that has been appropriately maintained over the years, PID’s / cause & effects that are up to date, alarm and trip testing schedules are correct and that evidence of management reviews for safety performance exist etc. Also, where appropriate to the generation of legacy systems, re-hazop / risk reviews are valid in support of the operating basis of safety.

Even if this is the case, then it may still be appropriate to review the performance KPI’s as discussed earlier in this paper, which may justify the decision of a replacement legacy system as identified in the plant life expectancy discussion found later in this paper.

For more complex modifications, this may have an effect on the original basis of design to such an extent that the system is required to be managed from first principles, i.e. full lifecycle management will need to be applied. This would also be the case if the basis of the design documentation is inadequate or there are discrepancies between existing logic and documented safety function requirements.
Impact of operating plant life expectancy?

Regardless of requirements, the impact assessment needs to consider plant life expectancy. If the plant is scheduled to be decommissioned in a few years time then this will have a different focus to that if it is decided the operating philosophy is to be extended for another 15 years or so.

Given the various operating philosophies that could be apparent, a number of approaches could be applied to deliver the functional safety performance requirements for the SIS under review. At a high level this could be in the form of the following strategies:

- **Maintain to end-of-life strategy**
  - Good basis of design available
  - Not seeing the KPI’s for failures / increasing costs for the systems as stands
  - Prepared to maintain for life of plant with established resources

- **Modify and evolve to meet new operating requirements strategy**
  - Good basis of design available
  - KPI’s may or may not be providing evidence failures / cost
  - Plan for evolution for life time of plant - change in operating strategy

- **Sticking plaster strategy - option A**
  - No good basis of design available
  - Recognition that the SIS is failing / cost spiraling, KPI’s supporting the issues
  - Not prepared to replace during remaining plant life
  - Will undertake small scale installation of compliant SIS to run in parallel with legacy

- **Sticking plaster strategy - option B**
  - Good or bad basis of design potentially available
  - Recognition that the SIS is failing / cost spiraling, KPI’s supporting the issues
  - Are prepared to replace during remaining plant life
  - Need breathing space to implement new SIS solution - interim strategy plan to be evolved prior to full upgrade
  - Will undertake small scale installation of IEC 615108 compliant SIS to run in parallel with legacy

- **Direct replacement strategy**
  - Good or bad basis of design potentially available
  - Recognition that the SIS is failing / cost spiraling, KPI’s supporting the issues
  - Are prepared to replace during remaining plant life
  - Will schedule evolution in timely manner i.e. plan to evolve next 3-5 year period
Modification to a legacy SIS

When the decision is made to go ahead with modification to a SIS, then functional safety management principles will apply and this will start with the system ‘impact assessment’ i.e. determining the significance of the change affecting functional safety performance and by association what procedures, testing, verification and validation will be applied to meet Functional Safety Management (FSM) requirements (see IEC 61511, clause 17).

Most companies have a management of change system operating at any one time, but experience would suggest the section covering the impact of modification to SIS may not well be detailed sufficiently to allow an analysis of the proposed change and the hazards present which may be affected.

What appears to be a minor modification on paper could have a serious detrimental effect on ability of the SIS to continue to operate correctly when under demand conditions.

With modifications to an existing SIS in the operational environment, the end user should be taking steps to establish the current basis of safety as part of the impact assessment review as detailed earlier in the paper. Responsible operators of SIS will have a modification change process that is aligned to the requirements of good practice such as IEC 61511 and have evidence that audits and assessments of functional safety systems have been occurring on a regular frequency.

Particularly for SIS, key requirements in establishing sustainable safety performance are to demonstrate that existing SIF’s and cause and effects have been proven to be adequate to protect against the known operating hazards to date. Proof test records and proven in use data would be beneficial to support such arguments and to establish any trending issues, but also support confidence in the actual design of any additional SIF’s entering into the SIS via modification.

Once impact assessment has been concluded and plans have been established to implement the proposed changes, then again the process of hazard identification, risk assessment, derivation of target SIL and most importantly the safety requirements specification will be required regardless of the nature of the modification.

What will be important here is that the functional safety management documentation to be applied will be proportionate to the size, complexity, novelty and likely project duration to ensure cost effective project design and implementation relative to the modification scope.
In summary, a ‘maintain’ or ‘evolution’ strategy for your SIS requires a structured review and should form a key part of your overall asset management business philosophy.

Once all implications have been addressed and a strategy agreed, then implementation should be in accordance with IEC 61511 principles. By doing so, your operational strategy is understood and endorsed by all relevant stakeholders and is much more preferable than reactive management i.e. fire-fighting the effects of obsolescence and the potential for failure on demand.

A proactive FSM approach should be in place and be seen as a senior management requirement for development and implementation, regardless of the strategy to be applied.

Conclusion
References

- ABB Safety Lead Competency Center: TuV Accredited Functional Safety Management System