Final element failure alarms, are they an essential feature of managing functional safety for your SIFs?

Ian Kemble, Senior Safety Consultant, ABB Consulting, Billingham, Teesside, TS23 4EB, UK

Abstract

The decision as to whether or not to implement a safety function trip failure alarm(s) frequently prompts lively debate and is attracting increasing attention from both industry and regulators alike. Such debate is typically driven by the various different interpretations and implementation of applicable alarm management and functional safety standards. On face value, implementing such alarms might seem an obvious “improvement”, but the challenge is to determine whether the net result will actually deliver a true and measurable safety improvement.

Safety Instrumented Functions (SIFs), or Plant Trips are typically highly reliable automated systems that on detection of the initiation of a potential hazardous event, automatically activate/deactivate one or more final element devices to put the process into a safe state. SIF failure alarms therefore utilise the available feedback signals from the various final element devices and raise an alarm when a SIF is triggered, and one or more of the final elements fails to reach its safe state. The final decision on whether or not to implement a SIF Failure Alarm will depend on a number of factors that need due consideration such as:

- Firstly, how is the alarm to be achieved?
- Where do the feedback signals come from?
- How might the implementation and associated modifications impact existing compliance with the Functional Safety standards (IEC61508 [1] / IEC61511 [2])?
- What are the Alarm Management considerations?

The Alarm Management standard IEC 62682 [3] requires that any alarm should have a defined operator response that can be completed in a timely manner and if anything, encourages a reduction in the total alarm load for operators. The addition of any proposed safe failure alarms is therefore somewhat counter intuitive to this ideal? With little clear guidance on this subject from the safety system vendors or standards committees, the end user must assess the pros and cons on a case-by-case basis and in particular how this might fit within an ALARP demonstration.

This discussion paper is not intended to give a definitive answer to this issue, or even necessarily the author’s opinion, but merely to raise and explore the pertinent arguments in such a way as to help others arrive at a suitable answer and to help judge for themselves.

Keywords: Alarm Management, Functional Safety, Safety Instrumented Functions

Background

In delivering numerous Functional Safety, Alarm Management and Alarm Rationalisation consultancy assignments, across all process industry sectors, with varying degrees of DCS technology implemented and diverse operational hazards & risk, operating companies are finding the question regarding the implementation of safety function (Trip or SIF) Failure Alarms as becoming an increasingly common subject. As with many aspects of Functional Safety, it can be argued that different parties can adopt, quite different perspectives, which invariably prompts lively debate.

Since that debate tends to be driven by different interpretations of the applicable Alarm Management and Functional Safety standards, it is not the intention of the author to give a definitive answer to this question, or even necessarily a defined opinion, but merely to raise the pertinent arguments in such a way as to help the reader arrive at a suitable answer and to judge for themselves.

Necessity or Nice to Have?

A Trip or Safety Instrumented Function (SIF) is of course, typically an electrical, electronic or programmable electronic system that on detection of certain process conditions that indicate the potential initiation of a hazardous event, automatically activates/deactivates one or more final element devices to put the process into a safe state.

The design, implementation and overall management of these SIFs for process industries is described in the standards IEC 61508 [1] and IEC 61511 [2]. These standards define the lifecycle approach necessary to identify and quantify the requirements for a SIF, the methodology for its design and implementation and the steps needed to validate that design and its performance and safety integrity level (SIL) throughout its operational life.

Such specifications and design documents may also include the definition of associated alarms in accordance with the Alarm Management standard IEC 62682 [3]. Depending on the rationale set out in the end user’s alarm management philosophy, this might include for the identification of alarms associated with the performance of the SIF, in other words “SIF Failure Alarms”.

For the purposes of this discussion, alarms associated with SIF sensor self-checking and logic solver diagnostics etc. have been excluded since, in the majority of cases, detection of such faults would automatically initiate the executive action of the SIF and this is normally defined in the Safety Requirements Specification (SRS).

This discussion will concentrate on alarms associated specifically with the action of the SIF final elements as indicated in figure 1 below. Here, the concept of a SIF failure alarm is therefore to utilise feedback signals from the various final element devices and raise an alarm when a SIF is triggered, and one or more of the final elements fails to reach its safe state (e.g. a shutoff valve fails to close) within a predetermined time period.

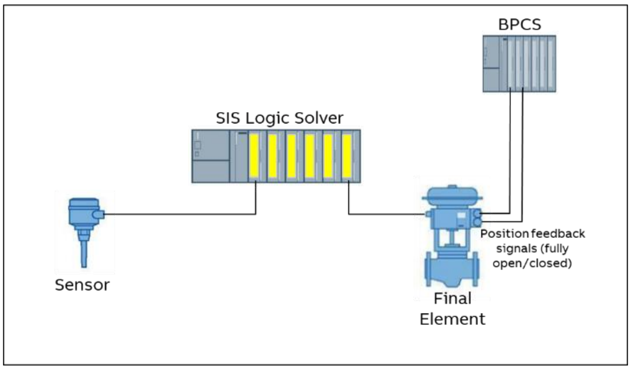

Figure 1 – Typical Arrangement for a SIF with Final Element Feedback

This type of potential performance issue is also an interesting dimension for the designers of such safety functions when there are process safety considerations associated with declared Process Safety Times (PST) that are a requirement of the safety function's SRS.

In this context, a somewhat simplistic view to the implementation of SIF Failure alarms is the argument that "if the feedback signals are there, why wouldn't you use them?". Intuitively, it seems reasonable to assume that any additional monitoring/verification of safety function operation will improve process safety and indeed, current experience suggests that some End User organisations are reporting that visiting regulatory authorities are already making that very observation.

However, as with many things, "the devil is in the detail". So, when deliberating the aspect of SIF Failure Alarms from a Functional Safety perspective, those responsible may wish to consider the following:

- How will these signals be specified and by whom in the context of the safety requirements specification?

  Additionally, how will forward and backward traceability to such requirements be established across the entire safety lifecycle phases?

- Where do these final element feedback signals come from, via what system (BPCS or SIS)? and do these feedback devices need to be SIL capable and/or form part of the SIF proof testing and maintenance regimes?

- If the field feedback devices are deemed to be part of the SIF functionality, what impact does that have on the complexity of the SIF design and the associated achieved SIL calculation?

  In other words, can you still meet your target SIL when you add in the failure rates of the feedback devices? Also, what bearing (if any) would this monitoring and the associated alarms have on claims for diagnostic coverage for the SIFs?

- Most operational alarms are presented to the control room operators by non-SIL certified systems, such as the DCS HMI. If SIF Failure Alarms are considered to form an integral part of the operation of the SIF, does that imply that they must be routed through and presented by SIL capable equipment?

- Is feedback from the final element device enough to validate correct SIF action anyway? It might tell you the limit switch on your shutoff valve actuator has been made, but you are really interested in knowing that your dangerously rising level has now stopped rising – what if the actuator is faulty, or if the valve is passing?

- Is it sufficient to only monitor and alarm the primary final elements of the SIF? What about secondary actions or "Trip Tidy-up" functions? Many SRS documents include secondary SIF actions that are not directly associated with the primary hazard scenario, but are intended to minimise the risk of consequential hazards and/or equipment damage created by the SIF action (e.g. stopping an upstream pump from pumping against a closed ESD shutoff valve), or to simply bring the plant into a more stable state that will be easier to recover and restart from. In such cases, there is a question as to whether any of these secondary action final elements warrant their own failure alarms.

- It is not uncommon for the action of a SIF to be triggered by more than one initiating cause and may act upon multiple final elements. In such circumstances, is the failure alarm and the associated operator response the same for all SIF failure modes? If not, do you need to consider multiple failure alarms for the same SIF?

Alarm Management Considerations

The international standard for Alarm Management IEC 62682 [3] 3.1.7 defines an alarm as “an audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a timely response.” Therefore, for an alarm to be valid, it must have a defined operator response that can be completed in the available time to complete that action, and for that action to take effect.

SIFs are typically designed and implemented as a layer of protection that comes into effect when all attempts by the operator to contain a potentially hazardous situation have failed. In such circumstances, what realistic and meaningful operator response to the SIF Failure alarm then really remains?

In addition, the combination of the designed response time of the SIF and the detection time for any SIF Failure alarm will have eaten into the time interval between detection of the initiating condition and the hazardous event. If the remaining time is insufficient for any realistic SIF Failure operator response to take effect, the alarm serves no useful purpose.

IEC 62682 [3] clause 6.2.9 identifies any alarms critical to process safety for the protection of human life (e.g. safety alarms) as Highly Managed Alarms (HMA) and the standard describes a number of additional alarm management requirements for HMA, which include:

- The Alarm Philosophy shall identify the testing requirements for HMAs prior to putting the alarms in operation. These alarms shall be periodically tested, and the testing shall be documented including
    - The alarm setpoint or logical conditions
    - The alarm priority
    - The audible and visual indications for the alarm
    - Any other functional requirement for the alarm as specified
    - The persons conducting the testing
    - The method of testing and acceptance criteria
    - The results of the testing and resolution of any failures or non-compliance
    - The date of the testing and the date the alarm was put into service
- Formally documented training (both initial plus refresher training) on the response to all new of modified HMAs prior to the Operator’s assuming responsibility.
- An independent HMI may be required for some safety alarms indicating dangerous faults
- Alarm shelving for HMAs shall follow authorisation and reauthorisation requirements as detailed in the Alarm Philosophy and an audit trail shall be maintained.
- Where an HMA is taken out of service for more than one shift, appropriate interim alarms or procedures shall be identified unless the process is in a state where the consequence has been eliminated.
- Additional Management of Change steps may be required depending on the classification of the HMA.

To implement SIF failure alarms across all of the SIFs on a process plant might therefore increase the number of HMA quite significantly, which is counter-intuitive to the recommended alarm management strategy to minimise the number of HMA within an alarm system.

For or Against – Is this a worthwhile proposition?

As with any reasoned debate, in order to make a considered judgement on whether or not to implement SIF Failure Alarms, it is necessary to weigh up the associated pros and cons and whilst what follows is by no means an exhaustive list, it does pick out some of the headline points:

Pros:

- Many of the required feedback signals and diagnostic functions may well be readily available within the existing plant instrumentation, DCS and/or SIS and as such, initial implementation where such equipment is already available should involve minimal physical, or hardware changes.

  In addition, the software reconfiguration necessary would probably involve relatively simple modifications (in some cases as simple as ticking a check box) that can be completed without significant disruption to an operating facility (i.e. low initial implementation cost).

- The introduction of SIF Failure alarms inherently provides additional safety related functionality that might alert operators to otherwise hidden failures.
- Making the operations team aware of a SIF failure provides them with an opportunity to bring the plant into a safe state by other means (e.g. an alternate manually initiated trip), or at the very least, might enable them to initiate the appropriate emergency response and (where relevant) evacuation more quickly.

  This has an impact on both process quality and avoidance of spurious trips impacting on the plant Overall Equipment Effectiveness ratio (OEE) and on the revenues bottom line for the business.
- Since alarms are normally recorded on the system event log and retained historically, the introduction of SIF Failure alarms will provide automatic ongoing monitoring and data records that can be used as part of periodic reviews as required as part of Functional Safety lifecycle compliance.

  In some cases, such data might be used to support field failure rate, or prior use justifications in achieved SIL calculations. Many operating companies utilise the Asset Management Applications provided with modern integrated control and safety systems and data mine this information as part of their "barrier management" programs to automatically detect failures in risk reduction layers.

Cons:

- In situations where the field signals are not already in place and for new builds/upgrades, there will be a requirement for additional field instrumentation and cabling. For example, this might involve the selection of suitable actuators with limit switches that are SIL capable and the simple addition of extra devices and the associated increased cost for more reliable equipment will have an impact during design and engineering, which may ultimately affect CAPEX approvals.
- In the absence of the application of advanced logical alarm processing, plant trips typically create an associated alarm flood as the process reacts to the effects of the trip. To have any meaningful benefit, all SIF Failure Alarms would need to be engineered in a way to prevent them being lost in any such alarm flood conditions.
- SIF Failure Alarms would increase the number of HMA configured in the system, all of which would require formal management & routine testing, placing an additional burden on resources (i.e. high lifetime maintenance cost) and the potential for creating more opportunities for human error.
- Competency assurance programmes would need to be developed and constantly maintained/refreshed to ensure operators are familiar with the impact of any SIF final elements, their meaning and any logical sequencing/thinking that would need to be applied in such events. All of which would need to be in accordance with defined SOP's. This again would require resources to maintain the validity and revision status of such requirements.
- If the relevant feedback signals and diagnostics are derived through the SIS rather than the DCS, there is potential for increased complexity of existing SIF loops, which could have a knock-on impact on the failure rate of the SIF, thereby negating the perceived safety improvement from adding the alarm in the first place.
- From a Human Factors perspective, there is perhaps some risk of creating a false sense of security during a plant upset, with operators relying on the absence of associated SIF failure alarms rather than actively verifying the safe tripped status of the plant.

Industry Guidance

Current experience identifies that the End Users contemplating the use of such SIF Failure Alarms to date are all still wrestling with the dilemma as to how deal with the issue and sadly, industry guidance in this area is somewhat lacking.

Even the core safety and alarm management standards can be interpreted as pulling in opposite directions. Whilst the Functional Safety standards IEC 61508 [1] & IEC61511 [2] might appear to be in favour of adding SIF Failure Alarms, the Alarm Management standards & guidance (IEC 62682 [3] & EEMUA 191 [4]) are founded on the principle of wherever possible in reducing the number of alarms presented to the operator, which might suggest the opposite view.

The creation of yet another standards committee or focus group to tackle this dilemma might not be desirable, but there is perhaps an opportunity here for at least some form of dialogue between Industry, the relevant stakeholder bodies, including the regulatory authorities in order to give guidance on a consistent approach that would be seen as broadly acceptable.

In the past, there have been some DCS vendor specific white papers published on the subject, but in general these tend to be high level in nature and focus more on the types of diagnostic alarms available within their specific control system platform rather than providing guidance on defining a realistic management strategy, or the necessary details to assess specific operator requirements.

In terms of available implementation guidance, there is often little more in these vendor documents than a summary recommendation that any SIF Failure Alarms implemented should be assigned the highest priority as configured in the system, which effectively, bypasses the alarm prioritisation principles set out in the Alarm Management standards.

The Regulatory Debate

As noted in the introduction of this discussion, many of the End User organisations are reporting that the main driver for consideration of SIF Failure alarms is coming from the questions raised by their regulatory inspectors, and on the face of it, it is difficult to argue against the premise that the addition of such alarms will go towards supporting improvements in overall process and functional safety.

However, for many of the reasons discussed above, it is also equally difficult to define, assess and especially quantify the actual safety improvement that would be delivered. Since the fundamental requirement for operators of high hazard facilities is to demonstrate that risks have been reduced to As Low as Reasonably Practical (ALARP), it could be argued that if an Asset Owner has already demonstrated through their existing Functional Safety Management processes that the risks have been reduced to an appropriate margin below the tolerable limit set for that particular hazard scenario, ALARP has already been achieved. Any decision on the implementation of further measures would be a feature of a cost/benefits analysis as part of ongoing ALARP demonstration.

Asset Owners are duty bound to evaluate investments in safety measures when considering how far to go with the implementation of process safety management requirements as part of their safety lifecycle obligations.

This monetary assessment is normally presented to internal and external stakeholders to support any judgements on whether any further risk reduction measures are deemed to be “reasonably practicable”.

This is usually arranged after inherent safety, good quality design and engineering to codes & standards application and due diligence arrangements have been implemented as part of formal and recognised company PSM/FSM policies, procedures and guidance for what constitutes accepted good practice. This is seen as the minimum baseline for managing hazard and risk in a manufacturing facility.

Therefore, an appropriate cost benefit analysis process can be implemented to underpin capital expenditure in both Greenfield projects and Brownfield investment decisions in existing facilities. Here the return on investment is aligned with the risk reduction concepts (reduction in risk to employees and the public) and is required as part of the organisations process safety management regime.

As an example, the UK HSE [5] identifies that something is reasonably practicable unless its costs are grossly disproportionate to the benefits.

In other words, put simply if;

$$\frac{\text{Costs}}{\text{Benefits}} > 1 \text{ x DF}$$

where DF is the 'disproportion factor' then the measure can be considered not worth doing for the risk reduction achieved.

This is one approach that can be used by the Asset Owner in demonstrating that those identified operational risks have been reduced to “as low as is reasonably practicable” (ALARP). This cost benefit analysis should also include for the provision of suitable justifications regarding conservative data/assumptions in the application of any analysis and where appropriate, a detailed demonstration of sensitivity range factors that underpin the conservative approach expected to be applied.

Given the potential for high lifetime management costs associated with the additional SIF Failure Alarms versus what might be in the end a difficult, if not an unquantifiable safety improvement benefit, it is possible that such a cost/benefit analysis could conclude that it falls outside of what could be considered “reasonably practicable”.

However, in order to make such a case would require a detailed and documented justification and the rationale for the underpinning assumptions may not be that readily identifiable.

Whatever the outcome of any individual assessments, what could be argued from a regulatory perspective given the above rationale, is that to do nothing with regards to SIF Failure Alarms will not be acceptable. At the very least, Asset Owners will need to show that the decision-making process on SIF Failure Alarms is an integral part of both their Functional Safety Management and their Alarm Management processes and systems.

In reality, what this means is that traceable documentary evidence that the implementation of SIF Failure Alarms has been given proper consideration and that the final decision can be satisfactorily justified will need to be created and maintained along with all existing functional safety related records. This would therefore be a standard feature of the safety lifecycle phase requirements which may not necessarily be forming part of the PSM/FSM procedural content within operating companies as of today.

Summary

Experience is such that there is already anecdotal evidence when engaging with Asset Owners to suggest that industry regulators are asking challenging questions about the absence of the use of SIF Failure Alarms, requiring those Asset Owners to demonstrate their approach to the implementation and management of such alarms.

However, a SIF Failure Alarm will only occur when the cause of the hazardous event has already been initiated AND the safety function that was specifically designed to protect against that hazard has failed.

An operator is then required to both recognise the SIF Failure Alarm AND take an appropriate action to mitigate that failure within the remaining process safety time. Given all of these considerations, the discussion should centre on what level of risk reduction can be reasonably expected, quantified or justified?

It is often said that "just because you can do something, it isn't always the case that you should", and this certainly applies to the implementation of SIF Failure Alarms.

On face value, implementing such alarms might seem an "obvious improvement", but like many situations it needs to be properly assessed on a case-by-case basis against both the functional safety and alarm management standards to determine whether the net result will actually deliver a true, measurable and worthwhile safety improvement.

Such considerations will also have an impact on the Asset Owners management procedures, competency assurance programmes and the means to ensure that proper verification and validation is applied across the entire safety lifecycle.

After all, if you are challenged by relevant stakeholders, are you confident you have the means in place today to produce suitable evidence to support and document why you did, or didn't do it in your ALARP demonstrations?

REFERENCES

1. IEC 61508: "Functional safety of E/E/PE safety-related systems, Edition 2.0", (2010)
2. IEC 61511: "Functional safety – safety instrumented systems for the process industry sector. Edition 2", (2016)
3. IEC 62682: "Management of alarms systems for the process industries Edition 1", (2014).
4. EEMUA 191: Alarm systems: Guide to design, management and procurement Edition 3 (2015)
5. Health and Safety Executive UK, Guidance "Principles and guidelines to assist HSE in its judgements that duty-holders have reduced risk as low as reasonably practicable."