Alarm Management Meets SIS

Table of Contents

Abstract 3

Keywords 3

Definitions 3

SIS Basics 4

Alarm Management Basics 4

Alarm Requirements 5

Prevent a Potential SIF Trip – Pre-alarm 5

When a Trip Occurs – First Out Alarm 6

Bypass Alarms 6

Failure Mode Alarms 7

Unnecessary Alarms 7

Summary 8

Abstract

Detrimental impacts of alarm floods on plant operations are well known, yet very little progress has been made in industry to eliminate them. One of the worst contributing offenders to this problem is the proliferation of alarms that are typically configured in a SIS.

This paper discusses a unified approach to producing SIS alarms based on sound alarm management principles and consistent with requirements with industry alarm management and SIS standards. The paper discusses:

- Alarm requirements as they are dictated by the **SIS Standard** (ANSI/ISA-61511)
- Requirements from the **Alarm Management** standard (ANSI/ISA 18.2)
- Any potential conflicts between the two
- How to conform to the standards and still have an alarming scheme(s) make sense
- Pitfalls and misconceptions that can hinder a successful alarm management implementation when SIS is involved

Keywords

- Alarms
- Alarm management
- SIS
- Process safety
- ISA
- IEC

Definitions

This paper makes use of the following technical terms and acronyms:

- **ISA** – International Society of Automation. ISA publishes multiple standards covering process automation in common industry use. Among these are two standards referenced in this paper:
  - ANSI/ISA 18.2-2016, Management of Alarm Systems for the Process Industries, aka the AM standard or ISA 18.2
  - ANSI/ISA-61511-1-2018, Functional Safety – Safety Instrumented Systems for the Process Industry Sector, aka the SIS standard or ISA-61511
- **Alarm** – Audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a timely response (ISA18.2)
- **Alarm System** – collection of hardware and software that detects an alarm state, communicates the indication of that state to the operator, and records changes in the alarm state (ISA18.2)
- **AM** – Alarm Management. Collection of processes and practices for determining, documenting, designing, operating, monitoring, and maintaining alarm systems (ISA18.2)
- **Safety Function** – Function to be implemented by one or more protection layers, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event (ISA-61511)
- **SIF** – Safety Instrumented Function. Safety function to be implemented by a safety instrumented system (SIS) (ISA-61511)

- **SIS** – Safety Instrumented System. Instrumented system used to implement one or more safety instrumented functions (ISA-61511)
- **BPCS** – Basic Process Control System. System which responds to input signals from the process, its associated equipment, other programmable systems and/or operators and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any SIF (ISA-61511)
- **IPL** – Independent Protection Layer. A device, system, or action that is capable of preventing a scenario from proceeding to the undesired consequence without being adversely affected by the initiating event or the action of any other protection layer associated with the scenario (American Institute of Chemical Engineers)

SIS Basics

This section discusses only those aspects of SIS that impact proper alarming and is by no means a complete summary of SIS principles, design or implementation. Such a discussion is well beyond the scope of this paper.

A SIS, composed of one or more SIFs, is designed to take automated action (usually shutdown) to prevent an unwanted safety consequence. It will bring a plant to a safe state in the event of a detected process excursion or manual activation. Each SIF is required to be independent of the BPCS and of any other IPL. Because a SIF needs to provide a minimum level of risk reduction (how much risk reduction is needed is determined during design), it might use redundant sensors and final elements, but this is not a requirement.

No operator intervention is usually required for proper functioning of a SIF. That said, many SIFs do involve operator intervention. These are generally manual activation switches for emergency isolation, depressurization, shutdown, etc. Also, fire and gas detection systems (FGS) may be considered as SIFs. Many FGSs don’t include automated protective action (rely on manual intervention to mitigate the release or fire). This paper will concentrate on the majority of SIFs, those that are completely automated and require no operator intervention.

Even though no operator intervention is required for automated SIF functioning, operator actions may be advisable to:

- Prevent a SIF trip before the fact
- Troubleshoot – why did the SIF trip?
- Secure the remainder of the plant
- Restart
- Troubleshoot problems with SIS components

The SIS standard, ANSI/ISA-61511, and its Technical Reports, discuss design, give recommendations and set requirements associated with all aspects of safety instrumented systems.

Alarm Management Basics

This section discusses only those aspects of AM that impact proper alarming of a SIS and is by no means a complete summary of AM principles, design or implementation. Such a discussion is well beyond the scope of this paper.

An important part of a good AM program is alarm justification. Justification compares a proposed alarm against AM principles, rules, criteria and requirements. Typical justification criteria can be summarized in a series of keywords that should be applied to each and every alarm:

- **Abnormal** – every alarm should indicate and abnormal condition (i.e., something that is unplanned or unexpected). This is explicitly stated in the alarm definition.
- **Action** – also explicitly stated in the definition, every alarm requires timely operator action. If no action is needed, an alarm isn’t needed either.

- **Consequences** – there is an unwanted event that is likely to occur if the alarm is ignored (no action is taken) or if the action is insufficient or incorrect. This is implied by the alarm definition – if there's no potential consequence, then no action would be necessary. If no action is expected or needed, then no alarm is needed either.
- **Unique** – when an abnormal event occurs, and that event requires operator action to avoid a consequence, only one alarm is necessary. Additional alarms that alert the operator to the same malfunction only serve to distract rather than to aid the operator to take appropriate response.

The AM standard, ISA-18.2, and its Technical Reports, set requirements and include recommendations concerning design, implementation and operation of alarms and alarm systems.

Alarm Requirements

This may surprise a reader, but neither of the two ISA standards referenced requires that any particular alarm be configured or annunciated.

Furthermore, the basics mentioned above would teach that no alarm is needed for a well-designed and working fully automated SIF to perform its function. This conclusion is easily drawn from: no operator intervention (action) is required for such a SIF to perform, and an alarm is not needed (or desired) if no operator action is required.

So, with no alarms actually mandated, what alarms are appropriate relating to a SIS? The following sections will discuss a unified approach to alarming SIS. This approach recommends alarms for preventing a potential SIS trip, responding to a trip when it occurs, and troubleshooting in the event of SIS malfunction.

Prevent a Potential SIF Trip – Pre-alarm

Prevention of a potential SIF trip is an important function of the alarm system and the operator. A pre-alarm is often configured to alert the console operator that a SIF trip may occur in the near future. A process value is moving away from typical operation, and is approaching a SIF trip setting.

Preventing the potential trip is important for two reasons:

- If the trip is prevented, this effectively reduces the demand rate on the SIF, and ultimately reduces the probability of the potential safety event that the SIF is designed to prevent.
- A SIF trip usually results in reduced or completely lost production, potentially off-spec production or at very least inefficient operation. The SIF trip is costly to most operations.

Applying AM basic principles to design of the pre-alarm leads to these considerations:

- Only one pre-alarm is necessary for each potential cause of a trip. For example, if there are 3 redundant transmitters in a 2 out of 3 voting arrangement, then a good pre-alarm to configure is on the median of the 3 transmitters. There is no need to alarm all 3 transmitters, since this would result in 3 alarms rather than 1 when a process deviation occurs.
- If there is a control (BPCS) transmitter separate from the SIS transmitters, then the pre-alarm could be placed on the controller. This provides an alarm that is independent from the SIS.
- Decision of pre-alarm placement is up to the facility and its alarm rationalization team.

However, if operator response to an alarm is identified (usually in a Process Hazards Analysis or Layers of Protection Analysis) as an IPL, this can dictate the placement of the pre-alarm. A pre-alarm that also serves as an IPL introduces additional considerations, primarily to ensure the integrity of the IPL. The IPL has an assigned risk reduction – its integrity is important in maintaining that risk reduction. Considerations in maintaining IPL integrity:

- The alarm should be easily recognizable as an IPL, with an indication either on the process display or the alarm summary.

- If the IPL alarm is annunciated in the middle of an alarm flood, its effectiveness will be greatly diminished. Therefore, state-based alarming or similar designed suppression should be in place for flood prevention.
- Typical limit is one alarm as IPL per SIF.
- A defined response procedure should be in place.
- Operators should be trained on recognition of the alarm as an IPL and on expected response.
- The IPL alarm should be tested.

When a Trip Occurs – First Out Alarm

There are some AM practitioners who advocate that no alarm is needed when a SIF trips because there is no operator action required. While it is true that no operator action is needed for the SIF to function, follow-up actions are expected and needed, as listed above in SIS Basics. So, a trip alarm is indeed appropriate – it is a unique announcement of an abnormal condition that requires action to prevent a consequence. Operator actions in response to a trip are to secure the rest of the plant, determine/correct the cause of the trip and restart when able. If no operator response is taken, consequences for the plant will be upset or inefficient operation and production loss.

The best way to provide a unique trip alarm is via the first out from the SIS logic solver. The first out will identify that a trip occurred and which of several potential causes initiated the trip. The first out also prevents other trip alarms from annunciating, so the operator receives only one alarm.

If a first out is not available from the SIS, a facility should strive to provide an alarm to announce the trip; this would often be based on the trip initiated indication from the SIS. However, it is important that only one alarm be configured for any given SIF trip activation.

If the SIF preforms per design, then the pre-alarm and the first out (or trip) are the only two alarms that are needed. Any additional alarms that sound will be considered unnecessary or a nuisance.

Bypass Alarms

Many SISs allow for bypass of its SIFs or of individual transmitters. Some of the bypasses are initiated at the control console by the console operator; others have field bypasses for the outside operator or maintenance technician. SIF bypasses are useful for testing, calibrating or repairing components.

If a bypass is active, this means that all or part of the SIF involved will not function if a demand occurs. This can lead to a hazardous situation; therefore, a facility should have strong procedures in place for managing bypasses. The procedures will outline approval, monitoring and communication requirements, along with releasing the bypass when no longer needed.

Although it is common practice, providing an alarm on a bypass that is initiated by the console operator is not recommended. Such an alarm merely informs the operator that he/she pressed a button and adds little or nothing to the integrity of the system.

However, a field-initiated bypass may be an appropriate alarm, particularly if the technician forgets to inform the console operator in advance.

Bypass re-alarms may be useful also, especially if the bypass is still active at shift change. This will inform the new console operator that enhanced monitoring is needed. The shift changeover procedure would usually cover bypass communication; the alarm is provided in case there is a breakdown in that changeover.

Failure Mode Alarms

A typical SIS will provide a number of potential component and system failure alarms. Most of these are needed to ensure that the console operator is aware of problems with the system and can perform such actions as making alternative monitoring or control moves, writing maintenance request tickets for repair and informing others of the problems. Common and recommended failure alarms are:

- **Fail to trip** – one or more final element did not change as expected (usually valve failed to close, or pump failed to stop). This alarm should have the highest priority available in the alarm system because a potentially serious hazard may exist.
- **Fail to reset** – one or more final element did not move to operating position as expected. This is much less serious than the fail to trip, but an alarm; it should probably be the lowest priority. The consequence of this failure is that the system will not be able to restart normally.
- **Transmitter deviations** – one or more transmitters in a voting scheme is not agreeing with the others. The concern here is that the SIF may be degraded – it may not trip if a process deviation occurs or may trip prematurely. Best practice is to include the BPCS transmitter in the deviation calculation also, so that a potential control problem can be detected.
- **Transmitter failure** – one or more transmitters in a SIF voting scheme has failed. This can be caused by no or bad reading, reading outside of extended range, or other transmitter issues. This also indicates a potential SIF degradation.
- **Various SIS system issues** – internal system faults, component failures, power supply issues, etc. One caution here is that these can be a source of multiple nuisance alarms. Each potential alarm should be justified before an alarm is configured. If a mechanism exists to route these alarms directly to a maintenance technician or other party responsible for the repair, this should be considered.

Unnecessary Alarms

There are a number of other alarms that are often configured in conjunction with SIS but are not needed. Any alarm in a SIS that is not discussed above would usually be considered superfluous. These unnecessary alarms do not adhere to one or more of the justification keywords. Here is a partial list of common alarms that are configured, but not needed:

- Alarm on each individual transmitter in a voting arrangement – only one pre-alarm is needed, and this should be configured on a minimum, maximum or median value calculation. Alarming all transmitters separately generates two, three or more alarms where only one is necessary. One justification often proposed for alarming all SIF transmitters is to indicate when one of them is drifting; but, the transmitter deviation alarm will advise the operator of a drifting transmitter.
- Alarm on the trip transmitter(s) at the trip point. This alarm is not needed because the first out or trip alarm announces that the SIF has taken its action. There is no need to sound additional alarms from the trip transmitter(s).
- Final element moving to the trip position (typically, valve closing or motor stopping). The final element moving to the trip position when commanded is a normal event, because that is exactly what is expected. Alarming the trip position is problematic also because it may prompt the operator to waste time attempting to reopen the valve to clear the alarm. A better alarm on the final element is the failure alarm discussed above.
- Bypass alarm – discussed above.

Summary

A well-designed alarming scheme for a SIS will provide the console operator with alarms that are justified and necessary, but without flooding the operator with multiple nuisance alarms. Alarms that should be considered are:

- Pre-alarm
- First out or trip alarm
- Transmitter deviation and failure
- Fail to trip
- Fail to reset
- Other system failures

When determining SIS alarms, a designer or rationalization team should strive to provide only one alarm for each problem detected, and to follow sound AM principles.

Figure 1 provides a pictorial representation of alarms that are recommended in and related to a SIS.

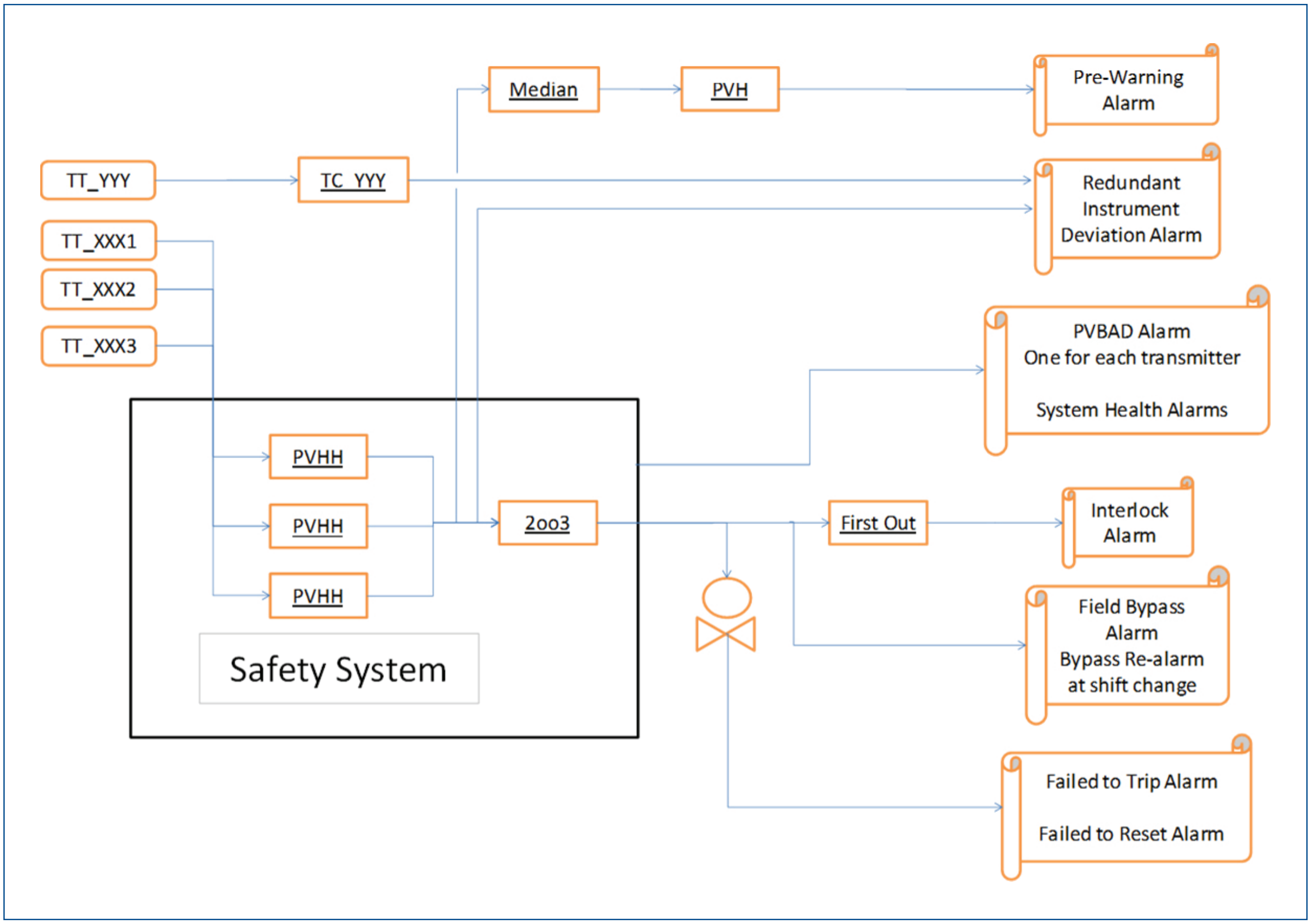

Figure 1 – Recommended unified approach to SIS alarming

Emerson
North America, Latin America:
☎ +1 800 833 8314 or
☎ +1 512 832 3774

Asia Pacific:
☎ +65 6777 8211

Europe, Middle East:
☎ +41 41 768 6111

🌐 **www.emerson.com/alarmmanagement**

The contents of this publication are presented for informational purposes only, and while diligent efforts were made to ensure their accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. All sales are governed by our terms and conditions, which are available on request. We reserve the right to modify or improve the designs or specifications of our products at any time without notice.