WHITE PAPER

The role of Alarm Annunciators in managing plant safety

AUTHOR:

T. Dzwig
R&D Manager
Omniflex

Table of Contents

Abstract

Alarm Annunciators are a vital tool in safety management. The need for Functional Safety assessment continuously pushes the technical performance of alarm annunciators upwards.

Operator involvement puts a limit on reliability of safety functions but may be beneficial in managing complex demands.

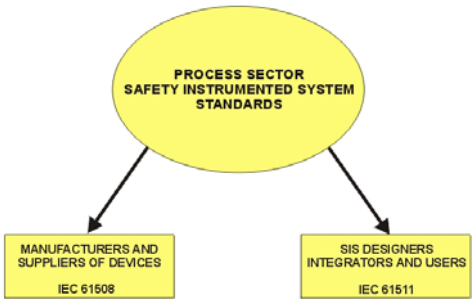
This paper explores the realistic boundaries of performance of alarm annunciators and operators in safety critical applications.

Introduction

Within industrial applications an alarm can be defined as "indication requiring an immediate response by the operator" [1]. Such indication normally reflects abnormal condition within the plant process. Alarm annunciators are devices which accept inputs from field sensors (typically via relay contacts e.g. from trip transmitters) and provide visual indication, such that the illuminated light or screen can be immediately and uniquely associated with a specific input. Alarm annunciators have a long history in most sectors of industry.

With the number and meaning of various alarms on the plants growing, the need for a systematic approach to alarm handling became evident. The earliest version of ISA18.1 standard [2] of 1977-79 already set the framework and concepts of processing of alarms and describes systematically the sequence of events that should be followed in the annunciator and performed by the operator, from alarm occurrence to eliminating the abnormal condition and resetting the alarm.

In the last two decades the issues of functional safety have also steadily gained importance. The IEC61508 standard [3] introduced a very broad but systematic framework which allows plant engineers to apply the functional safety concepts systematically to all modern control equipment. Following that generic standard, the process industry sector standard IEC61511 [4] was introduced. Both these standards enjoy wide international acceptance. Because of reliability requirements defined for safety-related alarms, standalone annunciators lend themselves to a rigorous assessment. This paper therefore focuses on the role of standalone annunciators in functional safety.



The role of the operator is sometimes seen as a drawback, because of basic unreliability of human actions. However, the operator plays an important role, as his actions may have broader impact such as getting to the root causes of problems and dealing with unexpected events and thus making the plant safer.

Basic concepts of alarm annunciators

An alarm is generally defined as an indication of an abnormal process condition. An alarm annunciator is therefore a device which signals the presence of abnormal process conditions using a visual display usually supplemented with an audible warning (buzzer, siren).

Once the annunciator device receives the alarm input, a sequence of actions is necessary in order to return the process to normal condition. The annunciator itself has therefore a sequence of states that has to be followed in order to return to indicating the conditions as normal. These typically include at least the following:

- **acknowledge** – activating a pushbutton to stop indicating the alarm as a new alarm (also referred to as **accept**)
- **reset** – activating a pushbutton in order to return the annunciator device to a normal state. This should only be possible after the abnormal condition has actually been removed or returned to normal, which results in that particular alarm not indicating any more.

Further development of these concepts eventually leads us to a distinct implementation in a device that is specifically designed to handle alarm inputs – i.e. an alarm annunciator.

It has to be noted here that by definition an alarm requires operator's response. If a response cannot be defined for an indicated condition then it shouldn't be displayed as an alarm.

In modern technology, these requirements, can be implemented in either a dedicated device i.e. alarm annunciator or in SCADA/DCS (PC) software and displayed on

computer screens. However, there are reasons why standalone alarm annunciators enjoy continued widespread acceptance. These include:

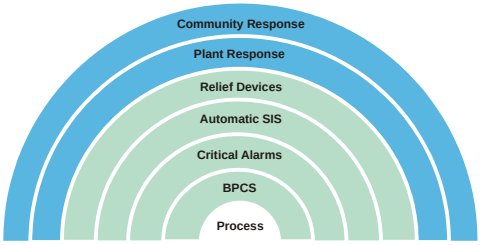
- High brightness and permanent visibility of lamp indicators, whether implemented using semiconductor technology or incandescent light. Often it is possible to use the displays in outdoor conditions, where CRT or LCD displays are not effective.
- Simultaneous visibility. Alarm annunciators can be physically grouped and organised into display panels that can display hundreds of alarms, all visible simultaneously. This is generally not possible with screens.
- Constant positioning of each alarm allows for instant pattern recognition by operator.
- The direct link between abnormal condition and an indicated alarm is maintained. This is crucial when monitoring a safety-related alarm [3]. The boundaries of the safety function that the annunciator fulfills are easily determined and allow for detailed reliability assessment as described later in this paper.

The basic concepts described here lead logically to further possible options which result in the definition of specific alarm sequences, i.e. series of internal states in the annunciator which are preferable, when the nature of the particular abnormal process condition is considered. In alarm annunciators, the correct sequence can be selected by the plant designer and it may be possible to select different sequences for different types of alarm.

The definitions and requirements for alarm annunciator sequences, options and other functionality are defined in [2].

Layers of Protection

The functional safety standards define the method of ensuring plant safety as a structure of successive “Layers of Protection” (see [4]).



Protection layer is only effective if it is independent of lower protection layers. Risk reduction methods must be applied to eliminate all unnecessary inherent risk, before further protection methods are applied.

The defined layers are as follows:

BPCS – Basic Process Control System. The plant control system clearly is the foundation of safe operation. It’s correct design and function is necessary, as the plant should be safe when in “normal” mode.

Critical Alarms – these alarms are of highest priority and some of them can be classified as being safety-related and involved in a safety function. These alarms provide early warning of an impending unsafe condition that requires immediate action to mitigate.

Automatic SIS (Safety-Instrumented Systems) – automatic protection systems that have to be used where the operators cannot be relied upon any more (e.g. because of the level of risk or required fast reaction time).

Relief devices – such as pressure valves or flares. Most often physical means used to prevent damage to equipment or danger to life.

Plant response – this is a “mitigation layer” and not a “prevention layer”. This involves a plan of action (e.g. containment) where the disaster has happened already.

Community response – this layer plays a role when plant response methods have been exhausted (fire brigade, evacuation).

The role of electronic and programmable electronic devices is in alarm annunciators to handle critical alarms and automatic SIS layers to perform automatic shutdown.

Alarm annunciators in SIL-rated safety systems

The IEC61508 standard [3] deals with electronic and programmable-electronic devices which need to have proven design for high-reliability in order to ensure "functional safety".

The standard defines four Safety Integrity Levels (SIL) which are be categorised according to Probability of Failure on Demand (PFD) or probability of failure per hour.

SIL	PFD	Failures/hr
SIL1	< 0.1	$< 10^{-5}$
SIL2	< 0.01	$< 10^{-6}$
SIL3	< 0.001	$< 10^{-7}$
SIL4	< 0.0001	$< 10^{-8}$

The use of alarm annunciators as part of safety-related systems is restricted by the reliability of human operators, which is generally considered insufficient to meet high reliability requirements. The IEC61508 standard does not exclude the possibility of a person being part of a safety-related system but human factor requirements are not considered in detail in the standard (Part 1, par. 1.2 Note 2). The reliability associated with the human operator is most often considered to have an associated PFD (Probability of Failure on Demand) of 1E-01 [5] (90% probability that the operator will successfully respond to the alarm). This would make even a SIL1 system impossible to design where a human operator is involved (1E-01 to 1E-02 is required for a SIL1 safety-related system). However, with a high level of training and clear procedures in place, it can be accepted that the operator PFD defined as "response to an alarm" can be as good as 1E-02 [5], in which case using an alarm annunciator in a SIL1 system is possible. When applying IEC61508 to assess safety-related alarms it therefore becomes clear that annunciators which involve the human operator can only be targeted at SIL1 level at best.

Most modern alarm annunciators have reliability figures at least ten times that of the operator and are therefore not a significant factor in assessing the reliability of the entire alarm function.

The next step in maintaining the safety of the process monitored by the alarm annunciator is to provide clear operator procedures. All standards require the system designers to guard against "operator overload". NAMUR document NA102 [1] specifically states that in the "rare instances" where a person is part of the safety function, there are special demands on the alarm system, namely:

- safety-oriented engineering
- total absence of ambiguity
- clear instructions for action (procedures)

Typically, as a guideline, the operator is required to respond within 1 to 30 minutes. The alarms requiring less than 5 minute responses will be very high priority, while the ones requiring 20 minutes or more will be lower priority. This will be possible if the operator responds to one alarm or an easily recognisable combination of several alarms. However, the combination of indicated alarms can in theory be an indeterminate number, which will make it impossible for the human operator to respond reliably. A human operator could possibly identify clearly a combination of several events, provided it's less than 10 and even then great effort must be invested in system design and alarm prioritisation to ensure that a realistic number of unambiguous procedures is available.

Alarm points monitored are often in hundreds and not infrequently more than a thousand. The possible scenarios to which the operator may have to respond require serious consideration during safety planning. In a good design, every alarm should have a defined response and adequate time should be allowed for the operator to carry out his defined response. This implies that:

- the alarm should occur early enough to allow the operator to correct the fault;
- the alarm rate should not exceed that which the operator is capable of handling

In several major accidents, such as Three Mile Island in 1979, Milford Haven in 1994 and Eurotunnel fire in 1996, alarm overload was identified in the enquiry as a contributing factor.

For example, Table 1 below summarises the number of theoretically possible combinations for a simple 16-input annunciator. The total is 2^{16}-1 but we get a different number of combinations depending on how many alarms occur simultaneously. In this case "simultaneous" does not have to mean that they are exactly synchronised in time. All it means is that the indicated number of alarms appear on the visual display before the operator has a chance to respond to any one of them (i.e. acknowledge and complete response to any of the alarms).

Number of alarm inputs	Number of simultaneous (un-acknowledged) alarms	Number of possible combinations
16	1	16
16	2	120
16	3	560
16	4	1820
16	5	4368
16	6	8008
16	7	11440
16	8	12870
16	9	11440
16	10	8008
16	11	4368
16	12	1820
16	13	560
16	14	120
16	15	16
16	16	1
Total no of combinations:		**65535**

Table 1. Total number of possible combinations of indicated alarms in a 16-way alarm annunciator.

Obviously in real situations dealing with a 16-point alarm system is quite practical and there are two reasons why, namely:

- with the number of possible combinations increasing – their probability decreases
- the alarms are not random numbers but appear due to process problems. Using the human operator is the most effective method to quickly and logically get to the root cause of the abnormal situation

The typical alarm annunciator has measures to cope with the potential operator overload. Firstly, there is a possibility of grouping the alarms and secondly, there is a possibility of indicating "first out" i.e. identifying which alarm occurred first in a group. Generally, while the "fault-tree" structure could be quite extensive, it is possible for the operator to use his expert knowledge and select the right corrective action very quickly given knowledge of the first alarm in the group to occur.

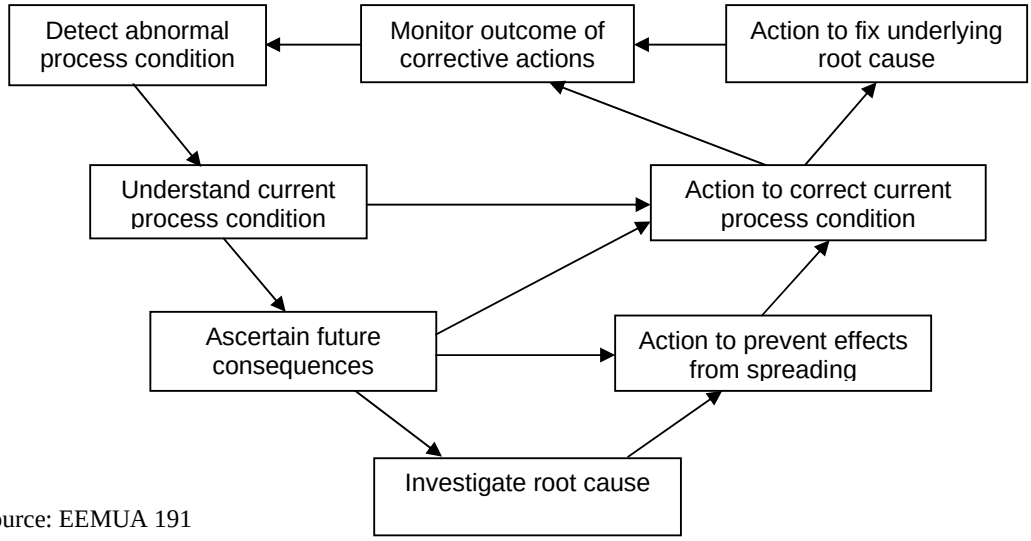
Figure 1 shows an example of a system where over 3000 alarm points were used. The part of the system shown constitutes almost 1500 alarm points.

Figure 1. Alarm Annunciators in the power generation sector (Singapore).

The way to deal with this large number of alarms is clearly to:

a) group them into well-defined systematic structure (e.g. each cabinet repeats similar arrangement of alarms)
b) assign more operators
c) operator should be capable of diagnosing the root cause quickly
d) good design must minimise "nuisance alarms"
e) alarms requiring fast response should be automated
f) separate critical alarms onto discrete alarm annunciators that cannot be removed from display and delegate less important alarms to the computer system for off-line analysis

In practice, the role of the operator in dealing with abnormal situation can be very complex [5]. As Figure 2 shows, the response may involve several different types of tasks. Also, the operator response to one abnormal situation may be quite different from that required to an apparently similar situation at another time.



source: EEMUA 191

Figure 2. Operator response to an abnormal situation.

It is therefore clear that safety-related alarms which have to comply with IEC61508 requirement must be clearly identified and distinguished from the multitude of other alarms.

If any alarm is defined as safety-related then:

- it should be designed, operated and maintained in accordance with requirements set out in the standard
- it should be independent and separate from the process control system (unless the process control system has itself been identified as safety-related)
- there should be clear, unambiguous procedure to guide the operator
- claimed PFD figure for operator response must be audited

It should be noted here that even though the operator procedure in response to such an alarm should be always the same, he can still perform actions shown in Figure 2 and thus identify the root cause for the alarm. This will simply lead to safer operation and it is clearly something that automatic system cannot perform.

The typical application of an alarm annunciator is shown in Figure 3. In this example there is a SIL1 SIS consisting of n elements. Their outputs represent n internal states of the process that can be monitored for abnormal conditions. If the alarm annunciator therefore monitors all the internal states, we have good process observability (even though it is a Boolean function only). This is typical of safety functions in low-demand mode. The monitoring of internal states ensures that abnormal trends or conditions can be indicated to the operator, even if the SIS output to the final elements appears normal. This also allows the operator to contribute more towards safety by early detection of impending abnormal condition than performing a simple shutdown function.

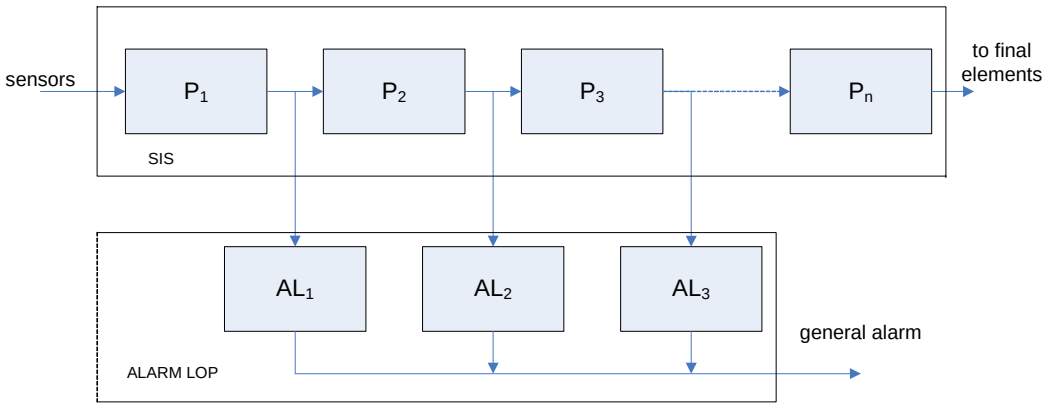


Figure 3. Safety Instrumented System monitored by alarm annunciator.

In the example shown in Figure 3 the annunciator clearly supplements the SIS. Several alarms like this could be classified as SIL1, even including operator PFD.

The role of alarm annunciators in critical alarms requiring SIL classification can be best understood by analysing key concepts of the Risk Graph shown below. This graph is based on IEC61511-3, Figure D.1.

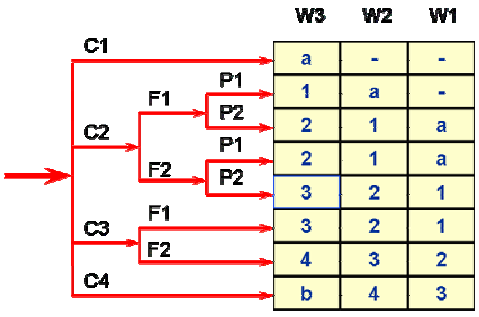


Figure 4. Risk Graph example.

In this graph, the letter symbols denote the following:

W – demand rate (1 - lowest to 3 – highest)
C – consequence (1 to 4)
F – frequency of exposure to hazard (1 to 2)
P – probability of avoiding the hazard (1 to 2)
1,2,3 – SIL Rating
a – no SIL rating necessary
b – single safety function insufficient

When analysing Figure 4 and considering where an alarm annunciator could serve as a suitable layer of protection the following options become clear:

C1 – when consequence is low, high alarm demand rate can be acceptable because of the low risk.

C2/F1 – when consequence is higher, an alarm annunciator would only be acceptable when frequency of exposure is low (F1) and it is possible to avoid the hazard (P1). If the probability of avoiding the hazard is low (P2), then an alarm annunciator is not going to offer sufficient protection because of slow human response regardless of calculated SIL rating.

C2/F2 – higher frequency of exposure may be acceptable provided the demand rate is lower (W1 or W2) and probability of avoiding the hazard is good (P1).

C3 and C4 – an alarm annunciator will in all likelihood not offer sufficient protection. (C3/F1/W1 possible only)

Hence, apart from PFD limitations, human response to an alarm also places a limit on SIL rating and places it at either SIL0 (non-critical) or SIL1 (critical, includes the operator). Once the abnormal situation is indicated, the operator needs time to act and follow prescribed procedures in order to restore process conditions back to normal. The time must be sufficient so that operator's actions can be completed before the abnormal situation turns into a hazard.

On the other hand, while operator involvement is limiting the safety-related functions to the SIL1 level, the operator can perform multiple functions as he/she can use his/her expert knowledge and apply more complex responses to abnormal conditions.

Alarm Annunciator as Layer of Protection

Taking the example of Figure 3 as a general illustration of a plant process, it is quite clear that the alarm annunciator naturally fulfils the function of Layer of Protection – above the Basic Process Control System and below the automatic SIS. Its function and assessed PFD allows for significant risk reduction. The alarm annunciator can be an element of the Layer of Protection or even an Independent Level of Protection [4]. This methodology can be applied to all alarms, thus reducing the risk and allowing the number of safety-related alarms to be minimised.

A Layer Of Protection is used to reduce the frequency of the occurrence of the abnormal event. To calculate this frequency reduction, each of the components required for the layer of protection must be analysed to derive a total Probability of Failure on Demand.

Example: Alarm Annunciator as part of a layer of protection.

Let's say we have an Alarm Annunciator with PFD=$2*10^{-3}$. The field alarm sensor would typically have a PFD of not greater than 10^{-4}. The operator, who must react to the alarm, might have an associated and audited PFD of $0.5x10^{-1}$ [5].

Since for one abnormal event the total PFD will be the sum of the component PFD's, it is obvious that the operator contributes the overriding value to the layer of protection.

Total PFD_{avg} = $PFD_{avg\ sensor}$ + $PFD_{avg\ annunciator}$ + $PFD_{avg\ operator}$

Therefore in this example

Total PFD_{avg} = 1E-04+2E-03+0.5E-01=0.0521

(note the limited effect of the equipment PFD in the total calculation)

Where an abnormal event will have a consequence of multiple injuries, the acceptable frequency of occurrence in this example is established to be once in 1000 years.

Let us assume that the estimated unmitigated frequency of occurrence in this example is once in 12 years. The risk reduction factor can then be calculated by the ratio of the estimated frequency and the acceptable frequency, thus 1000 / 12 = 83.3.

If adding the Layer of Protection can reduce the residual Risk Reduction Factor to less than 10, then the required Safety Integrity Level of the safety function is SIL0 (no SIL rating required).

By applying the example layer of protection, the mitigated frequency of occurrence becomes

f = 1/12[years] x 0.0521 = 4.34E-03
(4.34 occurrences in 1000 years)

i.e. an associated risk reduction factor of 4.34. Thus the introduction of the layer of protection has reduced the initial risk reduction factor by an order of magnitude, (or SIL 1 to SIL 0).

Refer to IEC 61511 part 3, Annex F, [4] for further guidelines relating to Layer Of Protection Analysis, (LOPA).

Conclusions

There is no doubt that with the growing emphasis of functional safety and risk reduction, the alarm annunciator is steadily gaining popularity as an important tool in achieving safety objectives.

Annunciators are now an integral part of SIL1 safety-systems and their compliance with IEC61508 is becoming a requirement. Recent reports such as the Buncefield Report are showing that where quantified risk reduction must be demonstrated (including avoidance of environmental catastrophes) this method of risk reduction is highly recommended.

Omniflex is dedicated to provide state-of-the-art products in this field and to promote an understanding of functional-safety issues.

References

1	NAMUR NA102: 2003	Alarm Management
2	ISA-18.1-1979 (R1992)	Annunciator Sequences and specifications
3	IEC 61508: 2000 Parts 1-7	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
4	IEC61511:2004	Functional Safety: Safety Instrumented Systems for the Process Industry Sector
5	EEMUA Publication No.191	Alarm Systems – A Guide to Design, Management and Procurement