

The role of Canopus Alarm Annunciators in managing plant safety

Abstract

Alarm Annunciators are a crucial tool in safety. This article explores the realistic boundaries of management. The need for Functional Safety performance of alarm annunciators and assessment continuously pushes the technical operators in safety critical applications. performance of alarm annunciators upwards. Operator involvement puts a limit on reliability of safety functions but may be useful in managing complex demands.

Introduction

Within industrial applications an alarm annunciators can be defined as “indication requiring an immediate response by the operator” . 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 & audio 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 ISA standard 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 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 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 article 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 **Canopus** 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.

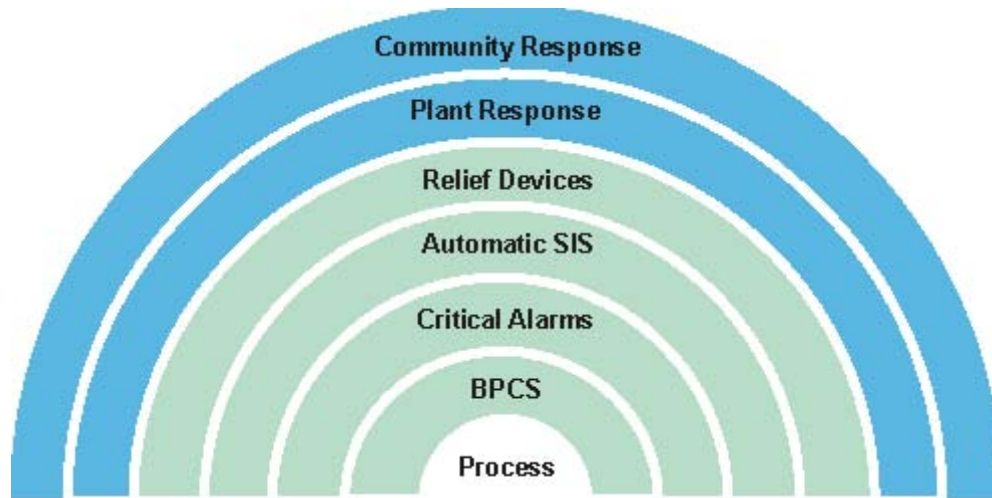
In modern technology, these requirements, can be implemented in either a dedicated device i.e. alarm annunciator or in SCADA/DCS (PC) software and displayed on computer screens. However, there are reasons why **Canopus** standalone alarm annunciators enjoy continued widespread acceptance. These include:

- 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 . The boundaries of the safety function that the annunciator fulfills are easily determined and allow for detailed reliability assessment

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.

Layers of Protection

The functional safety standards define the method of ensuring plant safety as a structure of successive “Layers of Protection”



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 rated safety systems

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. However, with a high level of training and clear procedures in place, it can be accepted that the operator “response to an alarm” can be as good as IEC standard , in which case using an alarm annunciator in a system is possible.

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”. 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, 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 16point 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.

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
- d) alarms requiring fast response should be automated
- e) 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 . 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.

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 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 as per designed 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

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 safety-systems and their compliance with IEC61508 is becoming a requirement.

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

- While preparing this article we have taken help of some articles from web.