Principles for alarm system design

February 2001
YA-711

Table of contents

1 INTRODUCTION

1.1 Background and objective

The Norwegian Petroleum Directorate (NPD) has through supervisory activities revealed unsatisfactory conditions related to alarm systems on petroleum production installations on the Norwegian Continental Shelf. Experience has shown that alarm systems could have been given more attention during design and procurement of new systems as well as during modification and operation of existing systems. Since alarm systems are essential in safe operation of petroleum installations, it is of vital importance that these systems are designed according to recognised principles for human-machine interface design and available human factors knowledge.

This document describes a set of established principles for well-functioning alarm systems.
The purpose of this document is to help those involved in the design, procurement, maintenance and operation of alarm systems. It is intended to help both in improving existing systems as well as during development of new systems and modifications. The objective is to ensure selection of systems complying with applicable Norwegian offshore regulations as well as safety, efficiency and high production availability.

This document gives guidance on alarm generation, structuring, prioritisation, presentation and alarm handling. The requirements are based on the latest international recognised requirements on alarm systems available at the time of writing, with focus on realistic solutions based on research and best practice from different process industries. Each of the requirements describes functionality that should be considered essential or very valuable in a high quality alarm system.

This document has been produced by Institutt for energiteknikk (IFE) in Halden under a contract with the Norwegian Petroleum Directorate. The following IFE personnel have participated in preparing the guideline: Øystein Veland, Magnhild Kaarstad, Lars Åge Seim and Nils Førdestrømmen.

1.2 Structure of the document

The presentation of overall requirements to the alarm system is followed by more detailed requirements concerning each of these topics: Alarm generation, structuring, prioritisation, presentation and handling.

Each requirement is presented as follows:

Requirement

Objective: Explains the rationale behind the requirement.

Comments: Complementing comments to the requirement with examples showing how the requirement could be met etc.

Numbers in superscript ([1, 2]) are document references.

1.3 Definitions

This section defines important terms used in this document. Some of these may not be familiar to readers in the industry, and some terms currently used in the industry have been redefined. These terms have been introduced to make some essential clarifications that are needed for precise definitions of the functionality required of a high quality alarm system. The terms are all widely recognised internationally and are used in authoritative reference literature [3].

Alarm types

Basic alarms are generated by detecting deviations on single process measurements or single pieces of equipment.

Aggregated alarms are generated by combining the state of a number of basic alarms that together describe the state of a process system or sub-system more precisely than a single alarm.

Model-based alarms are alarms generated based on online simulations by mathematical models of parts of the process.

Key alarms are a selection of important alarms presented in a way that makes them available and usable even during alarm overloads. All important safety-related alarms must be defined as key alarms, but also other alarms could be included if appropriate.

Alarm processing and handling

Signal filtering is the processing of the raw input signals to the alarm system in order to remove signal noise and other information that is unimportant for the purpose of an alarm system, such as small, rapid oscillations.

Signal validation is to verify that information from a signal is trustworthy, and is available from smart transmitters or signal monitoring software.

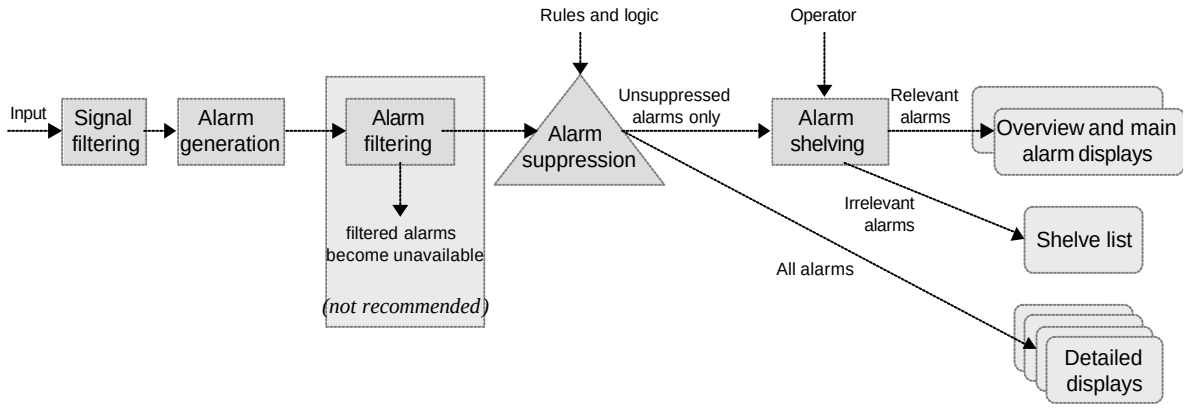
Alarm filtering means preventing an alarm signal so that it is not available for the operator in any part of the system.

Alarm suppression means preventing an alarm from being presented in main alarm displays, e.g. overview displays, but the alarm is still available in the system at a more detailed level.

Alarm shelving is a facility for manually removing an alarm from the main list and placing it on a shelve list, temporarily preventing the alarm from re-occurring on the main list until it is removed form the shelf. Shelving will normally be controlled by the operator, and is intended as a "last resort" for handling irrelevant nuisance alarms that have not been caught by signal filtering or alarm suppression mechanisms. [3]

The two synonymous terms *inhibit* and *blocking* are applicable to action alarms only, and refer to the prevention of a shutdown action by disabling the input signal from the alarm to the shutdown logics, while still presenting the alarm to the operator. [4]

Override is the disabling of a signal from shutdown logics to an individual shutdown action. While not directly related to alarms, action overrides is a potentially dangerous disabling of a part of the safety system, and thus constitute an important abnormality to be considered in the design of key information displays. [4]



The illustration above shows the relationship between different alarm processing and handling concepts referred to in this document.

Other definitions

Alarm prioritisation is a categorisation of alarms based on the importance of each alarm for the operator tasks.

Overview displays are designed to help operators get an overview of the state of the process. Overview displays include: Main alarm lists, tiles or annunciator alarm displays, as well as large screen displays showing key information.

Selective lists show only a selection of the available alarm information, based on selection and sorting criteria specified by operators.

Conceptual unit: A bulk of information (e.g. process, task, or system related) used by operators in their mental processing, such as a comparison of a temperature measure against an alarm limit.

Aggregated conceptual unit: Contains the information structure and content of several conceptual units, but is in itself a separate conceptual unit, such as a compressor trip.

Perception: The registration of sensory inputs. For alarm information to be easily perceived, it is important that it is clearly visible among other types of information, and it must be easy to interpret the essential elements in the information (what is wrong, where is it, how serious is it - these are the elements that are essential in the further cognitive rocessing)

Cognitive processing is the processing of new information in the human brain based on previously acquired knowledge. The effectiveness of the processing depends on how the new information is perceived, as well as in what form the knowledge used in the processing is stored and how it can be accessed (i.e. by simple recognition or demanding recall).

Cognitive response: A type of response in which the operator does not perform any physical actions, but requires him to do some internal processing of information.

2 FUNCTIONAL REQUIREMENTS

2.1 Alarm system purpose

An alarm system is a basic operator support system for managing abnormal situations and it has the following two functions:

The primary function of the alarm system is to warn the operator about a situation that is not normal [3]

The warning function helps the operator control the future behaviour of a complex plant by attracting attention to undesired process conditions.

The system should inform the operator about plant conditions that require timely assessment and possibly corrective action in order to maintain plant goals in terms of safety, productivity, environment and efficiency.

Each alarm should alert, inform and guide the operator. [1,3]

Alarms should:

- Be relevant to the operator's role at the time
- Indicate what response is required
- Be presented at a rate that the operator can deal with
- Be easy to understand

The secondary function of the alarm system is to serve as an alarm and event log [3]

The log function supports the operator's need to analyse the events that have lead to the current or previous process conditions.

The alarm log should be used for:

- Analysis of incidents
- Optimising plant operation

The alarm log should be flexible and contain also events, suppressed alarms and other pieces of information that were not presented in main alarm list, but which could be useful for offline investigation of incidents.

Alarm log information should also be used for monitoring and improving the alarm system performance.

The alarm system must provide *useful* information and functionality to support the operator's tasks. Information must be presented and handled in a way that is compatible with human capabilities and limitations, so that the system remains *usable* for the operator in all situations.

In addition to the alarm system, a number of other information sources may be important in the management of abnormal situations, such as trend systems, video surveillance, overview displays for quick situation assessment, process simulations, and advanced operator support systems for condition monitoring, diagnosis, or computerised procedures.

2.2 General requirements

1) The alarm system shall be explicitly designed to take account of human factors and limitations [3]

The design should ensure that the alarm system remains usable in all process conditions, by ensuring that unacceptable demands are not placed on operators by exceeding their perceptual and cognitive capabilities.

Alarms shall always be presented of a rate that allows the operator to have time to recognize and understand them, and adequate time should be allowed for the operator to carry out his response.

Perceptual factors:

There are limitations on the ability of the human brain to take in information. The perception of information requires a certain amount of time, and we can only hold about 7±2 units of information at the same time. Because of this it is important that, for all credible accident scenarios, the designer should demonstrate that the total number of safety related alarms and their maximum rate of presentation does not overload the operator.

Cognitive factors:

When several units of information can be combined into one single meaningful representation (i.e. an aggregated alarm), the brain capacity required for handling this particular information will be reduced, and the brain will be able to handle more information effectively. The brain also has other facilities that helps increase the capacity of perception, which can be supported by information that is intuitively understood and pattern recognition in the information presented.

The information presented by the system should be effective and valuable:

- Use as many aggregated conceptual units as possible
- Use aggregated conceptual units for suppression of alarms with less information content
- The content of the alarm message should minimize the need for information recall from long-term memory. For instance, an operator cannot be expected to recall or recognise the meaning of 5000 different tag numbers. Because of this the alarm message should be designed to include more descriptive information.

Actions:

Any claims made for operator action in response to alarms must be based upon sound human performance data and principles.

The alarm system should be adapted to the operator's defined tasks, identified and described through systematic task analysis.

2) The alarm system should be context sensitive [1,2,3]

Alarms should be designed so that they are worthy of operator attention in all the plant states and operating conditions in which they are displayed.

The alarm system should be designed to support the different operator tasks throughout a disturbance. It should adapt to varying information needs and be usable in a wide range of process states, such as:

- Start up
- Normal operation
- Small disturbance
- Severe disturbance
- Process shutdown in progress
- Process shutdown completed
- Fire/gas warning
- Emergency shutdown in progress
- Blow-down in progress

Example: When an emergency shutdown is released, the goal state of the process and the operator's tasks change significantly. The alarm system should adapt to this change and present only information relevant in the current situation, such as valves failing to close etc. The large number of expected alarms coming in from pumps being stopped, low pressures etc., are irrelevant as warnings in this situation and should be suppressed from the main alarm displays.

When the shutdown has completed, special alarms could be enabled whose purpose is to detect unexpected behaviour in isolated process segments.

Context sensitivity can be achieved by making the alarm system adapt to changes in the plant state using extensive automatic alarm suppression and/or dynamic alarm limits.

3) Operators shall receive instruction and systematic training in all realistic operational usage of the alarm system [1,3]

The objective of such training is to ensure that the usage and functionality of the alarm system are familiar and well understood by operators.

Basic alarm system training should cover:

- Prioritisation rules
- Suppression mechanisms
- The alarm system user interface
- Alarm acceptance practice

Using the alarm system during large process disturbances will typically be very different from using it during normal operation. Regular and realistic training, such as simulator training, in handling all kinds of disturbances should therefore be provided to ensure that operators will be able to use the alarm system in the critical situations when it is needed the most.

For alarm suppression to be effective, operators must be allowed to gain practical experience and develop confidence in the suppression strategies being used in the system.

4) The alarm system design shall be based on an alarm philosophy [3]

The alarm philosophy constitutes the basic rationale for the alarm system.

The alarm philosophy should discuss:

- The main functions of the alarm system: Warning and logging.
- The role of the operator, how this changes according to operating state, and what support the operator needs in the different states
- How the design should take account of human limitations
- Use of alarm priorities: The purpose of using priorities, how priorities are defined in the system, and the rationale behind the definitions
- The use of alarm acceptance, describing its purpose and how operators should be trained to practice it
- Standards
- Alarm generation principles
- Alarm structuring principles
- Presentation media

Important principles in the philosophy should include:

- Every alarm should require an operator response.
- Adequate time should be allowed for the operator to carry out his response

5) The alarm system shall be properly documented, and clear roles and responsibilities shall be established for maintaining and improving the system [3]

Documentation should ensure that good practice is established and sustained throughout modifications of the system, and that the designers and users of the system have a common understanding of the functionality of the system. It should also ensure that each alarm

defined in the system is documented with a description of the purpose of the alarm and a criticality assessment. Defining clear roles and responsibilities should ensure that ownership is established to all problems and tasks related to the alarm system throughout its lifetime.

In addition to the *alarm philosophy* described above, the following should be documented:

Alarm design strategy: Based on the alarm philosophy, this should be a structured methodology for alarm system development that ensures that every alarm is justified, properly engineered and documented. Important issues are: User involvement, identification of user needs, performance targets, guidance to sub-contractors on the design of alarms, dictionary of terms and abbreviations to be used in alarm messages.

Site alarm management strategy: Describes the allocation of roles and responsibilities for maintaining and managing the alarm system, as well as procedures for review, maintenance, system performance monitoring, testing, modification and documentation.

Individual alarms: The system should be self-documenting and provide detailed information about each alarm (purpose of the alarm, as well as configuration information about suppression criteria etc.)

6) It should be easy for process experts to build into and maintain knowledge and intelligence in the alarm system over time [1]

A good alarm system requires that a lot of process knowledge will be built into the system to optimise the alarm generation, suppression and presentation based on process expertise and operational experience.

Alarm system configuration tools should be provided that makes it easy for process engineers to improve the systems over time by building into the system the knowledge required to achieve effective alarm suppression, and to optimise signal filtering settings, alarm limits and priorities.

7) Performance requirements to the alarm system should be defined [3]

Performance requirements are important to ensure that the alarm system is useful to the operators in all relevant operational situations. To meet the requirements performance monitoring should serve as input to the process of improving the alarm system.

A performance monitoring system should be provided that implements tools and methods for measuring various performance indicators in the alarm system. The monitoring system should be used for regular performance analysis to identify problems or weaknesses in the alarm system, both during normal operation and in process disturbances.

This information should be used for continuous improvement of the system. If a process simulator is available, the monitoring system should be used in conjunction with the simulator for tuning the performance of the alarm system with regard to alarm limits, signal filtering, alarm suppression, etc., in a wide range of process conditions.

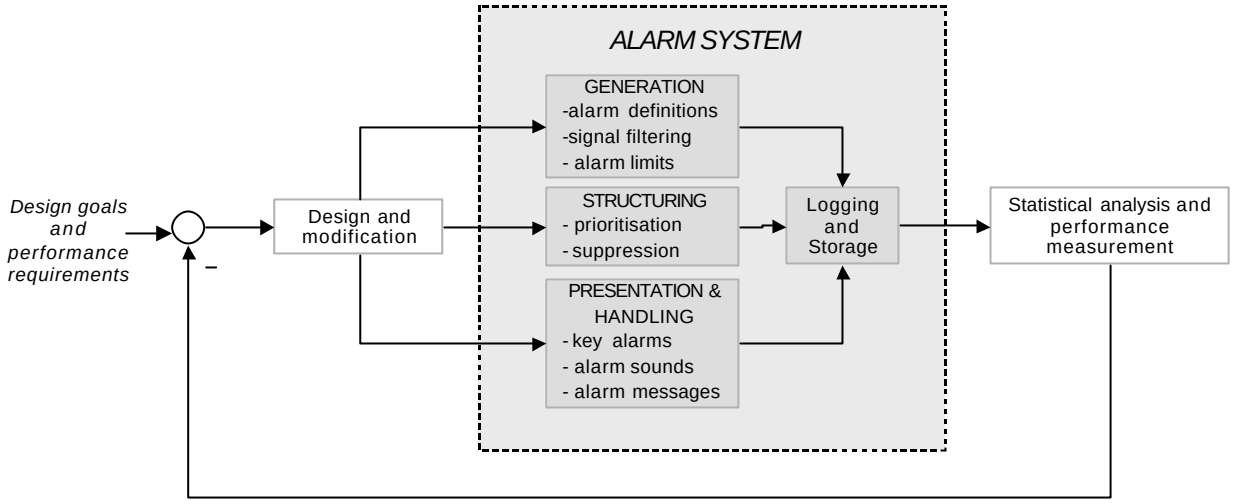


Figure: Alarm system improvement illustrated as a feedback loop. Various online and offline measures are used to verify how well the system performs, and deviations from design goals and requirements serve as input to system modifications and improvements.

The performance of the alarm system should be assessed during design and commissioning to ensure that it is usable and effective under all operation conditions. Regular auditing should be continued throughout plant life to confirm that good performance is maintained.[3]

Performance measures include:

- Rate of incoming alarms (with priority distribution)
- Number of alarms in main list (with priority distribution)
- Frequency distribution of alarms: For identifying any "bad actors" that contribute significantly to the overall alarm load
- Operator response times (time before acceptance): Too long or too short response times indicate that the system is not being used as intended

Alarm rates in steady operational conditions:

Alarm rate (average values)	*Consequence*
More than 1 alarm pr. minute	Very likely to be unacceptable
One per 2 minutes	Likely to be over-demanding
One per 5 minutes	Manageable
Less than one per 10 minutes	Very likely to be acceptable

Alarm rates during major plant upsets:

Alarm rate (average values)	*Consequence*
More than 10 alarms per minute	Definitely excessive and very likely to lead to the operator abandoning the use of the system
2-10 per minute	Hard to cope with
Less than 1 per minute	Should be manageable, but may be difficult if several alarms require a complex operator response

It should be verified that the priority distribution of alarms occurring in a disturbance is actually helpful in focusing on only a few important alarms at any time.

Other operator actions logged could also be analysed statistically to find possible nuisance alarms, by identifying alarms that are frequently shelved or alarm limits that are frequently changed.

8) There should be an administrative system for handling access control and documentation of changes made to the alarm system

The administrative system should prevent unauthorised modifications to the system and ensure that all changes are traceable and properly documented.

The system should administer changes and adjustments to the alarm system, such as setting new alarm limits, shelving and inhibiting. An integrated system for documenting changes and adjustments should require certain information to be entered before changes are effectuated. Such information could include:

- Person responsible for the change
- Reason why the change has been done
- Expected duration, possibly with automatic notification when this time has elapsed. (Apply only to temporary changes).

Access control mechanisms should allow non-critical alarms to be easily modified by operators, while changes to critical alarms require special authorisation.

There should be procedures and systems for reporting incidents, deficiencies, problems, and potential problems related to the alarm system. It should be clearly defined who is responsible for following up these reports.

9) The alarm system shall be fault tolerant

A fault tolerant system ensures that safety critical information is always available to the operators, both in normal operation and in emergency situations.

Factors to be considered include: redundant CPU, I/O and bus systems, UPS as back up to electrical/electronic equipment and displays. The alarm system shall be critically evaluated and assigned a Safety Integrity Level (SIL class) according to IEC 61508.

10) System response time shall not exceed 2 seconds [4]

Short system response times are essential for the system to remain useful in critical situations with high demands on operators.

Alarms should be presented in main alarm displays within 2 sec after occurrence.

For presentation in main alarm lists, a time stamping resolution of 1 s will be sufficient. In the alarm log and for use by the suppression logics, 100 ms time stamping or better is required.

11) Safety critical functions should be identified and documented. Status information and failure alarms from these functions should be clearly presented and continuously visible on dedicated displays

If safety critical functions are degraded or threatened, operators should be immediately alerted due to the possible consequences of such failures.

Examples of such functions can be (but are not limited to):

- Emergency Power system status information and failure alarms
- Fire Pumps failure alarms and status information (e.g. running, stopped, auto/man, standby etc.)
- Fire Protection System status information (e.g. released, available) and failure alarms (e.g. failure to act on demand, low fire water pressure etc.)
- Flare & relief system

The safety critical functions should be shown at a high level of abstraction by combining relevant information into graphical representations that give operators a brief overview of the availability and status of a function.

12) Status information related to safety system functions, such as blocking/inhibit and override, shall be easily available on dedicated lists and in process displays

It is of great importance that operators can get a quick overview over all inhibitions and overrides set in the safety system, including time of activation, purpose of activation, expected duration of activation, and person/position responsible for activation.

Important actions such as blocking/inhibit and override should be handled by the administrative system to provide access control and documentation of each action.

2.3 Alarm generation

13) Every alarm shall require an operator response [1,3]

This is to ensure that no unnecessary alarms are defined in the system.

A response could be a physical action to manipulate the process state, contact field operator, instrument technicians etc. It may also be a purely cognitive response, where the operator only does some mental processing.

A status change that will never require any operator response should be defined as an event rather than an alarm. Warnings about conditions that cannot be responded to by control room operators directly should instead be directed to the appropriate personnel.

14) The alarm system shall be able to generate basic alarms [1, 3]

Basic alarms provide the functionality needed to detect simple disturbances in the process.

The system must be able to generate the following kinds of alarms:

- Conventional state variable alarms comparing analogue measurements with predefined static or dynamic alarm limits
- Binary alarm switches
- Rate-of-change alarms
- Component fault alarms (e.g. indicating a discrepancy between control and feedback signals, sensor failure etc)
- System alarms indicating a problem in the alarm or process control system itself
- Simple group alarms

15) The alarm system should include generation of aggregated alarms or/and model based alarms [2]

Such alarms should only be used when leading to a significantly reduced number of basic alarms through suppression, or when providing more direct guidance towards the cause of the problem, rather than its symptoms.

Aggregated alarms could include:

- Plant system state alarms (compressor train trip, etc.)
- Missing alarms when expected alarms do not occur
- Functional alarms (e.g. loss-of-cooling)

Model-based alarms could include:

- Fault detection by comparing actual measurements with simulated performance
- Using data from model-based control to detect changes in process dynamics

16) All alarm limit settings should be systematically determined and documented during plant design, commissioning and operation [3]

Proper alarm limits settings are important to ensure that alarms are triggered early enough for effective response to be performed by operators, while on the other hand attempting to minimise the number of false alarms caused by too tight alarm limits.

Alarm limits should be set based on

- Plant dynamics
- Shutdown limits
- The likely rate of change of the signal during an upset
- The time it will take the operator to respond and correct the problem generating the alarm

Original settings as well as later alarm limit changes should be documented with reasons.

For each alarm limit it should be identified what authorisation is required to change the limit.

17) Operators could be permitted to change some alarm limits [3]

This is to obtain a more flexible and usable system, where operators can adapt the alarm system to varying process conditions.

An administrative system should be used to prevent unauthorised changes, and to ensure that each change is documented with reasons and person responsible.

18) Signal filtering should be used [2,3]

Signal filtering is used to prevent measurements that fluctuate around their alarm limits from generating useless, repeated alarms that disturb operators unnecessarily and contribute to the problem of alarm flooding.

Analogue measurements should be low-pass filtered to remove measurement noise in the process control system. The filter frequency should be adjustable.

Dead-bands should be used to avoid alarms going on and off when measurements fluctuate around the alarm limits. The dead-band should be adjustable.

Time-delay and time limit mechanisms should be used to avoid nuisance alarms from digital switches without built-in dead-band. Delays and limits should be adjustable.

19) Signal validation should be used [1]

If available, signal validation should be used to ensure that the input signals to the alarm system are reliable.

Signal validation information could be available from smart transmitters, or from special software for monitoring and validating signals.

The operator should be warned about unreliable signals that might have direct influence on his tasks.

Alarm suppression logic shall be designed so that no alarms will be suppressed by an unreliable signal.

2.4 Alarm structuring

20) It should be possible to select, group and sort alarms

Selection, sorting and grouping facilities should be provided to make the system more flexible and usable by letting operators configure online what information they would like to have presented, adopted to their special needs.

The following are some possible criteria for grouping and sorting alarms:

- Time
- System
- Area
- Operator responsibility
- Priority

It should also be simple to get an overview over alarms that are suppressed, shelved or inhibited.

21) Alarm suppression functions shall be included in the system [1,3]

The objective of alarm suppression is to ensure that the presented alarms at any time are relevant to the operator's work under the current process conditions, and to avoid alarm flooding during process disturbances.

Alarm suppression principles should be easy to understand.

These are some alarm suppression principles that could be used:

- Suppress alarms resulting from testing.
- Alarms that are a direct consequence of other alarms in a disturbance shall be suppressed unless they are key alarms to the operator.
- Suppress redundant alarms, where several alarms alarm the same deviation.
- Suppress alarms from e.g. components out of order, from components being unavailable due to maintenance, testing etc.
- Use suppression based on the operating state of particular plant items or shutdown logics.
- Use first-out processing of shutdown alarms: Present the alarm that triggers a shutdown, while suppressing all other alarms that are merely consequences of the shutdown actions.
- If alarm suppression hinges on a signal that is not trustworthy, the alarm shall not be suppressed.

22) The system should use alarm suppression, not alarm filtering [1]

Even alarms that are not relevant warnings in the current process conditions may still constitute important status information that should be available in detailed or selective displays. It should therefore be possible to suppress alarms from overview displays without causing the suppressed alarm signals to become unavailable in detailed displays.

Alarm suppression (as opposed to *alarm filtering*) does not remove any information from the system. Suppression merely separates the alarm information into an overview level and one or more detailed levels.

This ensures that the rate and amount of information presented at the overview level can be optimised to meet human limitations, so that relevant new alarms can present themselves in a way that can always be perceived by operators. At the same time, much more information is available at operator request in detailed displays.

23) The alarm suppression in the system should be familiar to the operators, and it should be documented in an easily understandable way [1]

In order to trust the system, operators need to understand why some alarms are suppressed from overview displays while others are not.

To become familiar with a system with a high degree of alarm suppression, the following is required:

- Basic training and documentation describing the general suppression principles used in the system
- Easily available documentation of the suppression criteria related to each alarm
- Systematic training in using the system in all process conditions where suppression mechanisms are activated

2.5 Alarm prioritisation

24) Alarms shall be prioritised [1,3]

The purpose of prioritisation is to help the operator to decide which alarms to deal with when several occur at the same time in a disturbance, and to show especially urgent alarms to the operator during normal operation.

It is not recommended to use more than four alarm priorities in any plant.

A maximum of three priorities should be used within any one type of display for normal display of alarms. An additional priority level for safety-critical alarms could be used.

When there are multiple alarm systems in a plant, a consistent alarm priority definition should be used throughout all systems.

It should not be possible for the operator to change alarm priorities. The alarm configuration system should allow specially authorised personnel such as process engineers to do this.

25) Alarms should be prioritised according to the severity of consequences that could be prevented by taking corrective action [1,3]

Alarm priorities should help the operator focus on the conditions that, if not corrected, will have the biggest impact.

High priority should be used to alarm process conditions with potentially high consequences unless the operator takes corrective action.

The severity of consequences is measured in terms of safety of personnel, protection of equipment, environment, and maintaining and optimising production.

26) Alarms should be prioritised according to the time available for successful corrective action to be performed [1,3]

Alarm priorities should help the operator focus on process conditions that there will be time to handle, and to give primary attention to those conditions that must be handled most urgently.

Higher priorities should alarm process conditions that require attention or action within limited time to avoid consequences.

For high priority alarms, there should be sufficient time available for the operator to act effectively. This is not the case for alarms that trigger shutdown actions.

Lower priorities should be used for process conditions where the need for action is less urgent.

27) There should be an effective priority distribution of process alarms occurring during normal operation and in process disturbances [3]

This is to ensure that the alarm prioritisation will effectively help the operator during plant disturbances. Among the possibly large number of alarms that may occur in these situations, there should be a relatively small and manageable fraction of high priority alarms that direct the operator's attention towards the most important disturbances that he should attend to at any time.

The assignment of alarm priorities should be done based on a target occurrence rate or frequency for each priority. The frequency of occurrence of alarms of different priorities should roughly decrease by a factor of around 5 for each increase in priority: About 80% of alarms occurring should be low priority, 15% should be the second lowest priority, 5% high priority, etc.

28) Every site should have written rules on how priorities should be assigned [3]

This is to ensure that the operators are familiar and comfortable with the prioritisation rules employed by the system designers, so that priority information can be effectively utilised by operators when handling alarms.

The prioritisation rules should be applied consistently to all alarms in all systems used by the operator.

Prioritisation rules with rationale should be part of the alarm philosophy document.

2.6 Alarm presentation

29) A main alarm display shall be provided [1,3]

The main alarm display should support the task of monitoring and controlling the future behaviour of the plant by attracting the operator's attention towards process conditions that require assessment or action. It should show only alarms that are relevant in the current process conditions.

Main alarm displays should present all active alarms that are not automatically suppressed or manually shelved. An important design objective of the alarm system should be to ensure that there are *no alarms presented* at the main alarm display in situations where there are no real problems or abnormalities in the process. ("Dark screen" concept).

The main alarm display should be usable under all process conditions for which it is designed, i.e. by presenting alarm information in a form and at a rate that the operator can cope with. (Ref. requirement 1 and requirement 7 for recommended maximum alarm rate).

For each alarm, operators should be able to rapidly see the priority and alarm state (new, accepted, cleared).

Alarm lists should be:

- Chronologically ordered
- Designed such that repeating alarms do not cause them to become unusable (I.e. same alarm filling up several lines in the list)

Displays with spatially dedicated alarms (tiles/annunciator displays):

- Operators can effectively use pattern recognition that enables them to cope with a large number of alarm
- Does not show the chronological ordering of the active alarms

A main alarm display can be a combination of list and tiles displays as well as separate displays covering different system or areas. The final solution of the main alarm display should be based on the approved operation and alarm philosophy.

30) Key alarms shall be shown in overview displays that are permanently on view, with spatially dedicated alarms [1,3]

The purpose of a key alarm display is to improve the management of alarm overloads. Alarm presentation should not rely on alarm lists only to provide the operators with an alarm overview. Alarm lists will always have the potential problem of information flooding during large disturbances, even though alarm suppression should be used to avoid this as far as possible.
Key alarm displays ensure both an information rate and a presentation form that will remain manageable under all process conditions.

Key alarms shall include all alarms that are directly safety related (e.g. fire and gas alarms) and important process alarms related to safety critical systems (e.g. high level alarm in the flare knockout drum).

It could also be beneficial to include other high priority process alarms as key alarms. Key process alarm displays could be useful for avoiding unnecessary shutdowns by providing an overview of the most critical process alarms in large disturbances (typical alarm flooding situations) where important alarms otherwise could be missed in the alarm lists (e.g. high level in separator. Missing this alarm could cause a total production shutdown when reaching high high level)

Suitable key alarm displays could be:

- Tiles, or arrays of alarm annunciators [3]
- Large screen overview displays showing key alarms integrated with other process information [1]

31) An historical log of alarms and events should be available to the operator [1,3]

The log is used for analysing incidents.

Flexible facilities for selection, sorting, grouping and searching in the alarm log should be provided.

32) Alarms should be integrated in process displays [1,3]

Combining relevant process and alarm information in the displays helps reduce the mental workload imposed on operators.

Alarms should be shown in a consistent way across all process displays, using symbols and icons located close to the components or functions to which they are related. It should be easy to see the priority and status of each alarm (active, not active, blocked, shelved, suppressed).

Active main alarms (alarms that are not suppressed or shelved from the main alarm overview displays) should be easily distinguishable, salient features in the process displays.

All active alarms should be shown in the process displays, including those not shown on main list or overview displays due to automatic suppression or operator shelving. This is because they may constitute relevant status information that should be available to the operator at this level. Active alarms that are suppressed or shelved should be less conspicuous than main alarms, and for each alarm it should be indicated whether it is suppressed or shelved.

The process displays should show what alarms are defined and provide access to additional information on each alarm, such as alarm limit and, for trip alarms, shutdown level and actions.

33) Selective list displays should be provided [1]

Selective list displays allow operators to easily configure lists for special purposes.

Selection, grouping and sorting criteria that should be available in selective alarm lists are described in requirement 20). Operators should have full flexibility in setting up selection criteria, but the system should also provide easy access to a number of predefined, commonly used list configurations.

Facilities for showing a list of only high priority alarms could be used to improve the management of alarm overloads.

System alarms on dedicated lists could be useful for maintenance personnel.[1]

34) The priority of alarms should be coded using colours and possibly other means

This is to ensure that different priorities are visually separated in a way that makes it very quick and easy to spot the most important alarms among the less important ones.

The colours used for prioritisation should:

- Be used exclusively for alarms.
- Reflect alarm importance
- Make alarms easily distinguishable from the less important information in the alarm and process control systems.
- Be consistent across different alarm display types.

Redundant visual coding of priority will be useful for increasing clarity, especially for colour-blind users. Symbols, location of information, font type, blink frequency, etc. are among the available means for additional information coding.

35) Audible alarm annunciation should be used when new alarms arrive

Audible annunciation used is to notify the operator about the occurrence and importance of new alarms that require his attention.

Alarm sounds should be selected according to a well-planned overall use of sound in the control room, and alarm sounds that disturb the operators' work and communication should be avoided.

A maximum of 4 different alarm sounds is recommended, and it should be easy to distinguish between the different alarm sounds.

There should be no audible annunciation of alarms that are suppressed or shelved. For low priority alarms it should be considered using one-shot sounds or no sound at all. Voice alarm could be used for announcing extreme safety-related situations.

There should be a central means to silence audible alarms.

A "silent control room" function has been proposed for manually muting or reducing all alarm annunciations for a limited time during severe upsets. This allows operators to abandon the use of the alarm system in situations where it is practically unusable, and does not address the causes of the problems that makes the alarm system unusable.

The recommended approach is to design the alarm system to support operators in all process conditions, instead of using a "silent control room" function that could in practice cover up problems in the system. But if implemented, strict procedures must be used to prevent it from being misused, and it shall be designed to ensure that safety critical alarms are always annunciated.

36) Special visual annunciation should be used for new alarms

Visual annunciation is used to attract operator's attention towards new alarms and distinguish them from alarms that have been accepted.

The use of blinking should be limited. E.g. in alarm messages, only a small symbol should be blinking. Text should never blink.

Instead of blinking, other effects could be used that are less disturbing to the eye (i.e. raised face / 3D-effects that highlight new alarms).

37) Alarm information should be informative and easy to understand

This is to avoid misunderstandings and to minimise the time needed to understand the meaning of each alarm message.

Messages should be consistent and based on standard, agreed-upon terminology and abbreviations actually used by operators.

Alarm messages should include: Priority, alarm state (new, accepted, cleared), visual annunciator (e.g. blinking symbol), alarm identifier, descriptive text, and severity. Optional: Updated measurement value, alarm limit and unit, date and time.

Alarm messages should contain no unnecessary information. The information carriers should be selected in a way that minimise interpretation and memorisation. (E.g. one should not rely on learning of tag names or numbers only)

Different alarm lists content for the main alarm display and log functions of the system may use different alarm message content optimised for each function. This should be done carefully to avoid confusion. An example could be to include date and time only in the alarm log.

38) Alarm information should be easily readable

This is to ensure that the content of each alarm message is presented in a way that is clear, well structured, quick and simple to read.

The following factors should be considered:

- Display layout and information grouping
- Ordering of the different information elements in an alarm message
- Font types and sizes should provide good readability at the intended reading distance
- The use of colour in alarm messages should not cause difficulties reading the message
- Blinking text should never be used

39) Necessary alarm information shall be available from all relevant workplaces

This is to ensure that all relevant personnel have a correct picture of the process conditions within their area of responsibility at any time, and to ensure that alarms are shown near the controls and displays required for corrective or diagnostic action in response to the alarm.

Different personnel may need different info:

- Control room operators
- Technicians
- Additional personnel needed in a disturbance
- System engineers
- Test personnel
- Members of an emergency preparedness team

2.7 Alarm handling

40) Every alarm that is triggered should require acceptance. [1,3]

The operator should be required to accept each alarm to confirm that the alarm message has been read and understood.

An alternative practice is that the operator will accept an alarm only when the associated response has been carried out. The operation and alarm philosophy should describe whether an alarm should be accepted after it has been read or after it has actually been dealt with.

Suppressed alarms (automatic or shelved) should not require acceptance.

It should be possible to accept alarms from the alarm list and from detailed process displays, from all workstations. Updates should be sent to all displays when an alarm is accepted.

It shall be possible to accept each new alarm separately, and a central acceptance of all visible alarms could be provided.

Sound should disappear when all alarms are accepted. In addition, a dedicated button shall be available for silencing an alarm sound without accepting the corresponding alarm.

The acceptance status of an alarm could be useful as a condition for controlling the automatic removal of alarms from the list:

- For some alarms it should be required that the operator has accepted the alarm before it can be automatically removed from the list. This may be the case for high priority alarms, especially for alarms that have triggered actions, because operator response may be required even if the alarmed signal has returned to a normal state.
- Automatic removal of unaccepted alarms could be used to avoid list flooding, especially for low priority pre-warnings that return to normal.

Different principles should be considered for handling the list as alarms are removed:

- List handling will be simplified by automatic compression of the list every time alarms are removed, but this makes it difficult to keep an eye on a particular alarm in the list to verify that corrective actions have been successful.
- Manually controlled list compression using a compress button makes it easier for the operator to see when alarms go off, as he is not disturbed by sudden moves in the alarm list. The drawbacks of using this principle are that an extra operator action is introduced in the handling of alarms, and there is the possibility of filling up the list display with old alarms or blanks.

41) It should be possible to shelve individual alarms [3]

The objective of alarm shelving is to allow operators to remove standing or nuisance alarms that the alarm generation and structuring mechanisms have failed to prevent.

Shelving an alarm means removing it from the main alarm list and placing it on a shelve list. The alarm is then prevented from re-occurring on the main list until it is removed from the shelf. Shelving will normally be controlled by the operator, and is intended as a "last resort" for handling irrelevant nuisance alarms that have not been caught by signal filtering or alarm suppression mechanisms.

The operator shall be able to easily observe what alarms are shelved in the dedicated shelve list, as well as through symbols in the process pictures.

The operator should be required to document the reason for shelving the alarm in an administrative system.

Shelving could be time limited to prevent important alarms to be removed and forgotten. An administrative system should be used to keep track of alarm shelving and provide user authorisation mechanisms that prevent important alarms, such as key alarms, from being too easily shelved by operators.

42) Navigation in alarm displays should be quick and easy [2]

This is to support effective operator response to alarms by allowing quick navigation to additional information.

It shall be possible to navigate from the alarm lists to the process display where the alarm is shown. A minimum number of operator interactions should be required to do this.

It should be possible to click at an alarm in any display to get more information about it, such as alarm response procedures.

The operators should be able to change list mode between

- Operator driven mode, where the operator can scroll freely to any part of the list without being disturbed by new alarms.
- Automatic mode, where the last incoming alarm is always visible at the top or bottom.

Alarm lists should be navigable by scroll bar and page-up/page-down buttons, and should have a flexible text search function.

43) Procedures that specify individual responsibilities for monitoring and controlling large process disturbances and emergency situations shall be available and known by the operators

Such procedures should ensure that work in the control room in critical situations will be effective and well organised.

For emergency situations it should be described how work in the control room should be organised. This includes responsibilities for monitoring and controlling process systems, safety systems, marine systems and communication systems, and also how the different tasks should be prioritised.

Instruction and systematic training in emergency handling is needed for such procedures to be effective.

3 REFERENCES

1. *Alarm-kravspesifikasjon for Amoco Norway Oil Company*, Valhall CCR Upgrade Project, IFE/HR/F-99/1118.
2. *Requirement Specification for the HAMBO Alarm System*, IFE/HR/F-2000/1141
3. *Alarm Systems: A Guide To Design, Management and Procurement*, The Engineering Equipment and Materials Users Association (EEMUA) publication No. 191
4. NORSOK Standard I-002