Safety and automation system (SAS)
Contents

FOREWORD 2
INTRODUCTION 2

1 Scope 3

2 Normative references 3

3 Definitions and abbreviations 3
  3.1 Function definitions 3
  3.2 Abbreviations 5

4 Functional requirements 5
  4.1 Control levels, distribution 5
  4.2 SAS functions 6
  4.3 Package integration and categorisation 9
  4.4 Human machine interface 10
  4.5 Application program development and configuration 14

5 System requirements 15
  5.1 Change management and access rights 15
  5.2 Hardware 15
  5.3 Software 16
  5.4 Requirements to spare capacity 16

Annex A (normative) Testing of SAS 17
Annex B (normative) Time response 18
Annex C (informative) Conceptual SAS topology 19
Foreword

The NORSOK standards are developed by the Norwegian petroleum industry as a result of the NORSOK initiative, agreed in 1993, to establish standards that ensure adequate safety, value adding and cost effectiveness for all parties involved and thus are used in existing and future petroleum industry developments.

These standards are developed according to the consensus principle generally applicable for most standards work and according to established procedures.

The preparation and publication of the NORSOK standards is supported by OLF (The Norwegian Oil Industry Association) and TBL (Federation of Norwegian Manufacturing Industries), even after the termination for the NORSOK initiative in 2000. NORSOK standards are administered and issued by NTS (Norwegian Technology Centre).

The NORSOK standards are prepared in lack of availability of adequate international standards and will be used to provide the Norwegian industry input to the international standardisation process. Subject to development and publication of international standards, the relevant NORSOK standard will be withdrawn.

Annex A is for information only
Annex B forms a normative part of this NORSOK standard.

Introduction

This standard replaces and supersedes previous NORSOK standard I-CR-002, Safety and Automation Systems (SAS), rev. 1, December 1994. This standard has been given revision 2 as being a continuation from I-CR-002 rev. 1.
1 Scope
This standard covers functional and technical requirements and establishes a basis for engineering related to Safety and Automation System Design. This standard shall be used together with I-001 “Field Instrumentation”, I-005 “System Control Diagrams”, Z-010 “Electrical, Instrumentation & telecommunication Installation” and S-001 “Technical Safety”.

The SAS Life Cycle Cost should be used as a criterion for the evaluation of the system. This includes engineering, commissioning, documentation, spare parts, and production loss during system repair and modifications/maintenance in the operational phase.

2 Normative references
The following standards include provisions which, through reference in this text, constitute provisions of this NORSOK standard. Latest issue of the references shall be used unless otherwise agreed. Other recognized standards may be used provided it can be shown that they meet or exceed the requirements of the standards referenced below.

- 89/336/EEC EMC Directive
- ISO 10418 Recommended practice for Analysis, Design, Installation and Testing of Basic surface Safety Systems for Offshore Production Platforms

3 Definitions and abbreviations

3.1 Function definitions

<table>
<thead>
<tr>
<th>Definition</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm</td>
<td>Discrete change of data resulting in an audio/visual annunciation in the control room, requiring operator acknowledgement as well as input to alarm list.</td>
</tr>
<tr>
<td>Alarm categories</td>
<td>The following categories are defined, not reflecting priority or criticality of the alarm:</td>
</tr>
<tr>
<td>Action alarm:</td>
<td>Alarm feature including blocking facilities intended for automatic safeguarding actions in order to protect equipment, environment or human beings.</td>
</tr>
<tr>
<td>Warning alarm:</td>
<td>Alarm without blocking facilities intended for abnormal conditions enabling operator intervention in order to prevent further escalation.</td>
</tr>
<tr>
<td>Fault alarm:</td>
<td>Alarm associated to fault or failure in the instrument and/or control device.</td>
</tr>
<tr>
<td>Blocking</td>
<td>Disabling of a safeguard action, but allowing associated alarm annunciation as well as manual/automatic control. Blocking applies to both individual action alarms and input signals effecting safeguarding and disabling functions.</td>
</tr>
<tr>
<td>Conflict</td>
<td>Process shutdown obstructed by control mode on object (i.e. not all initiated shutdown actions are performed due to equipment failure or blocked mode on shutdown actions).</td>
</tr>
<tr>
<td>Definition</td>
<td>Explanation</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Display</td>
<td><strong>Display:</strong> The display is the visualisation of computer output. <strong>Display screen:</strong> The display screen is the surface that is used for the visualisation of operator information, graphics, display areas and displayed data. <strong>Display area:</strong> The display area is a window of a display screen that is used to present information from one or more applications. <strong>Display element:</strong> Display elements are selectable (from a library) building blocks for display areas representing the graphic presentation and/or, if applicable, the dynamic behaviour of an object including operator interaction. A display element can be as simple as a numerical value or as complex as a complete object display for a process object. <strong>Display properties:</strong> The display properties defines the background colour, display element update rate, linked displays, dynamic function keys, etc.</td>
</tr>
<tr>
<td>Dynamic information</td>
<td>Information displayed on the display screen reflecting the state of the process or system. The following dynamic information elements are defined: <strong>- Alarm</strong> <strong>- Event</strong> <strong>- Binary status</strong> <strong>- Analogue value</strong></td>
</tr>
<tr>
<td>Event</td>
<td>Discrete change of state resulting in a displayed status in the control room as well as input to the event list.</td>
</tr>
<tr>
<td>Fieldbus</td>
<td>Fieldbus is an all-digital two-way communication system, which interconnects “field” equipment such as sensors, actuators and controllers.</td>
</tr>
<tr>
<td>Override</td>
<td>Override function intended to set the output signal to predefined state, independent of changes in logic states.</td>
</tr>
<tr>
<td>PDS</td>
<td>PDS is a reliability/availability calculation procedure available from SINTEF.</td>
</tr>
<tr>
<td>SAS</td>
<td>SAS is defined as the overall Safety and Automation System. SAS performs monitoring, logic control and safeguarding of an installation. SAS comprises all control equipment as a total, integral concept, either from one vendor or acquired from several sources. Subsystems made as stand-alone units communicating through custom made serial links are also considered as part of SAS. System Topology Principles as shown in Annex C are applicable independent of the SAS size and complexity.</td>
</tr>
<tr>
<td>SAS unit</td>
<td>SAS unit consists of CPU with associated equipment such as I/O racks and cards, bus communication, power supplies, signal conditioning units and termination facilities for field cables. Operator stations and gateways are also considered as SAS units.</td>
</tr>
<tr>
<td>Shutdown level</td>
<td>Signal latch included in the common signal path between a group of initiators and a group of actuating devices.</td>
</tr>
<tr>
<td>Suppression</td>
<td>Disable alarm annunciation as well as any associated automatic actions.</td>
</tr>
</tbody>
</table>
3.2 Abbreviations

CCR central control room
CPU central processing unit
ESD emergency shut-down (system)
FB function block
F&G fire and gas
FTC field termination cabinet
FWP fire water pump
HMI human machine interface
HVAC heating ventilation and air conditioning
IMS information management system
ISO international standard organisation
LCC life cycle cost
LQ living quarter
MCC motor control centre
NPD norwegian petroleum directorate
OS operator station
PA public announcement
PCS process control system
PDCS power distribution control system
PDS pålitelighet av datamaskin baserte sikkerhetssystemer (reliability of computer based safety systems)
PSD process shut-down (system)
RIO remote inputs/outputs
RMS rig management system
SAS safety and automation system
SCD system control diagram
SINTEF stiftelsen for industriell og teknisk forskning ved norges tekniske høyskole (the foundation for scientific and industrial research at the norwegian institute of technology)
UPS uninterrupted power supply
VDU visual display unit

4 Functional requirements

4.1 Control levels, distribution

SAS network shall be dual redundant. Each SAS unit directly connected to the SAS network shall be connected to both buses.

4.1.1 Location

1. ESD
   • SAS control units shall be located in room safe by location.
   • Shall be centralised, in vicinity of CCR.

2. F&G
   • SAS control units shall be located in rooms safe by location.
   • SAS control units may be distributed or centralised.

3. PSD
   • SAS control units should be located in rooms safe by location.
   • SAS control units may be distributed or centralised.

4. PCS
   • SAS control units should be located in rooms safe by location.
   • SAS control units may be distributed or centralised.

5. PDCS
   • SAS control units should be located in rooms safe by location.
   • SAS control units may be distributed or centralised.
6. Mechanical package control
   • SAS control units for equipment packages should not be located in hazardous or environmental exposed areas.

4.1.2 Functional distribution
The process systems should be logically distributed into separate SAS units and/or SAS programs in order to optimise mechanical completion, commissioning and maintenance.

4.2 SAS functions

4.2.1 ESD
The ESD system shall have the following features:

1. It shall be possible to test the ESD logic, including I/O cards without unacceptable degradation of the installation safety and reducing the production rate. This shall also include trip signals between SAS units.

2. Safety integrity shall be maintained upon loss of power or any single failure of electronic parts.

3. For all safety-related functions, a maximum reaction time, including field devices, shall be specified.

4. The ESD level shall latch in the tripped state until manually reset in the CCR and in the field. The reset in CCR shall be common to all associated levels.

5. Status of the ESD system, ESD valve status, blocking and override facilities shall be available in the CCR. One single function shall be sufficient to turn off all blockings/overrides.

6. It shall be possible to initiate any ESD level from the CCR.

7. The ESD system shall have high reliability. The reliability shall be verified by the use of PDS or similar calculation methods.

8. The HMI shall be a VDU based solution. Use of large screen should be considered. In addition a functional independent hardwired action panel shall be included.

9. ESD inputs (excl. all inputs from ESD hardwired action panel with exception of ESD release pushbuttons) shall be line monitored, enabling detection of abnormalities. (e.g. earth fault detection, short circuit detection, open circuit detection in the entire circuits, etc.).

10. ESD dedicated fieldbus/RIO’s may be used for ESD inputs/outputs, providing the safety availability is not compromised (i.e. compared to use of HW signalling with compensating measures, ref. item 9 above).

11. Action signals between ESD and F&G shall be hardwired or by means of dedicated safety bus/serial links providing that the safety availability is not compromised (i.e. compared to use of HW signalling with compensating measures, ref. item 9 above). Status signals or repeated information may communicate by use of the main system bus.

4.2.2 F&G
The F&G system shall have the following features:

1. The F&G system may be non-redundant provided successful verification by the use of PDS or similar calculation methods.

2. The F&G system shall be designed so that it can be tested without interrupting other systems on the installation.

3. For all safety-related functions, a maximum reaction time, including field devices, shall be specified.

4. Delay of audible PA alarms to LQ shall be provided in the CCR.
5. Facility for manual start of FWP’s shall be provided in the CCR. This facility shall be independent of any external control system.

6. All loops (excl. F&G mimic loops) for F&G shall be line monitored, enabling detection of abnormalities (e.g. earth fault detection, short circuit detection, open circuit detection in the entire circuits, etc.).

7. Addressable detectors and RIO’s may be used.

8. Reset facilities shall be available grouped per fire area, or a defined group of fire areas.

9. Fire fighting release from the F&G system shall be hardwired.

10. The output signals to the fixed protection systems shall be passive; i.e. energises on fire fighting. Use of passive output signal shall however be taken into consideration during total safety analysis. Possibilities for manually release of fixed protection systems shall be available in CCR.

11. Inter-SAS status signals or repeated information between F&G units may communicate by use of the main system bus.

12. Information about geographical arrangements of detectors and fire areas shall be available in the CCR.

13. It shall be visually distinguished between fire and gas alarms.

14. Status of F&G alarms, blockings, override and release of protection facilities shall be provided in the CCR.

15. The HMI shall be a VDU based solution. Use of large screen should be considered. In addition a functional independent hardwired action panel shall be included.

16. The information on an integrated F&G mimic/matrix shall be kept to a minimum and the F&G mimic/matrix shall typically contain:
   - common gas alarm per safety area
   - common fire alarm per safety area
   - common indication of any blocking per safety area
   - blocking and release facilities of protection skids and electrical isolation
   - selection of pump priorities
   - running status of fire water pumps
   - unavailable status of fire water pumps
   - ring main pressure indication
   - fault indication

17. The HVAC safety related functions shall be integrated in the F&G system.

4.2.3 PSD
1. The PSD functions for hydrocarbon systems according to ISO 10418 shall be implemented in separate SAS unit(s). In systems not covered by ISO 10418 control and shutdown may be handled by the same SAS unit(s).

2. Function testing shall be possible without interrupting the operations of the installation. An overview of the PSD blockings shall be available in CCR.

3. Fieldbus and RIO’s may be utilised.

4.2.4 PCS
1. Hardwired process mimic should be avoided.

2. Fieldbus and RIO’s may be utilised.
4.2.5 PDCS
The purpose of the PDCS is to control and monitor the electric power generation and distribution network, ref. NORSOK standard E-001.

4.2.6 Rig management system
The Rig Management System (RMS) is the monitoring and control system of all marine related systems.

Below are listed functions which shall be included in the RMS, as required for the actual installation:

- structural monitoring;
- mooring control;
- ballast/bilge control;
- dynamic position monitoring and control;
- position simulator;
- load and stability calculation.

The following information shall be available if required:

- differential global position reference;
- hydro-acoustic position reference;
- gyrocompass;
- roll, pitch, heave;
- surge, sway and yaw;
- acceleration measurement;
- vertical reference;
- airgap;
- wind speed and direction;
- air temperature and humidity;
- barometric pressure;
- wave height and direction.

4.2.7 Drilling control system
The Drilling Control System includes all drilling related control and safety functions.

Risk analyses shall be carried out in order to disclose the probability and the consequences of single failures or sequential failures that may occur during operation to allow risk reducing measures to be taken. The result of the risk analyses shall be documented.

The safety functions of the Drilling Control System shall have the following features:

1. The safety functions of the Drilling Control System shall be designed in such way that no single defect or failure in the Drilling Control System shall result in loss of the safety function. Safety functions related to ESD and F&G shall not be handled by the Drilling Control System.

2. It shall be possible to test the safety functions of the Drilling Control System, including I/O cards without unacceptable degradation of the safety. This shall also include trip signals between SAS units.

3. For all safety-related functions, a maximum reaction time, including field devices, shall be specified.

4. The safety functions of the Drilling Control System shall have high reliability. The reliability shall be verified by the use of PDS or similar calculation methods.

5. All loops related to the safety functions of the Drilling Control System shall be line monitored, enabling detection of abnormalities. (e.g. earth fault detection, short circuit detection, open circuit detection in the entire circuits, etc.).
4.2.8 Information management system

The Information Management System (IMS) shall be connected to the SAS units in such a way that all data in the SAS units can be selected, processed and presented on IMS terminal and in reporting form.

The IMS shall be configured with hardware and software for connection to the installation office data network.

The IMS shall have programming tools that make it easy to create historical reports for blockings, production data, operational logging, maintenance data, alarm system with searching and sorting facilities etc.

Typical IMS functionality is:
- Long term storage of alarms and events.
- Trend data storage.
- Long term storage of selected measurement values.
- Alarm analysis.
- Administrative tasks

IMS shall typically receive and process data from the following external systems:
- Fiscal metering
- Mooring and positioning system
- Ballast system
- Environmental and platform monitoring system
- Corrosion monitoring system
- Condition monitoring system
- Fuel & flare gas metering
- Oil storage and off-loading system
- Pipeline monitoring

4.3 Package integration and categorisation

This section gives guidelines as to how process and utility equipment packages can be integrated into the SAS, and how operation and control accordingly will be carried out. The individual package unit can have different operation and control philosophy within an installation, depending on operational requirements.

4.3.1 Definition of control classes

Control class 1: All control functions fully integrated utilising project standard software and control unit hardware.

Control class 2: Control units are either directly connected to main SAS network or interfaced to other SAS units utilising project standard hardware or software interface.

Control class 3: Stand alone control units. These control units are not considered as SAS units and no interface to SAS is required.

For all equipment packages categorised as control class 2, a more detail overview should be prepared. This overview should set up project requirements for the various control functions with respect to:
- documentation of application program (i.e. use of System Control Diagram);
- use of project standard function blocks;
- use of project standard control units;
- use of project standard hardware or software interface, including operator interface.
4.4 Human machine interface

4.4.1 Operator interaction and workspace layout

4.4.1.1 Organisation of VDU's and input devices
1. The CCR shall be equipped with a minimum of two independent operator stations.
2. The operator system shall allow at least two operators to operate the installation simultaneously and independently. Additionally F&G and safety system overview shall be displayed permanently or automatically upon safety event.
3. A pointing device and a keyboard including a QWERTY layout shall be used as input device.
4. The keyboard shall be of Norwegian type with Norwegian language drivers.

4.4.1.2 Command input
1. Operator input actions shall be kept simple and uniform.
2. The operator dialogue shall be designed to avoid performing actions unintentionally.
3. It shall be possible to limit the number of opened displayed areas.
4. It shall be easy to navigate between displays. Direct jumping between displays shall be possible.

4.4.1.3 Feedback to and validation of operator input
1. The system shall give feedback to the operator that a command has been registered, and that processing has started.
2. Data entries should be validated by the system, e.g. that an entered set point is within the permissible parameter range. When an entry is invalid, an advisory message shall appear indicating the error.

4.4.2 Displayed information

4.4.2.1 General
1. The display screen shall present the information consistent with their function, to achieve secure process control and supervision.
2. Text occurring on the operators VDUs shall be in Norwegian and should be based on “Norsk Term Bank”. Texts for system maintenance functions, not related to normal operations such as system messages and system diagnostic VDU pictures, may be in English.
3. The display screen shall present necessary and sufficient information for task completion. It shall be unnecessary to collect information from several display screens to complete a task.
4. It shall be easy to add and/or modify new display screens.'

4.4.2.2 Display screen layout
1. The display screen shall consist of fixed display areas covering specific purposes. This shall include, but not be limited to: information/status area, application area, dialogue area etc.
2. Other issues to be considered include display title, amount of information on the display screen, background colour, grouping of information, etc.
4.4.2.3 Display area layout
1. The process shall be divided in functional standalone sections on each display area. Natural process splits shall be considered to minimise the number of display interfaces.
2. Layout of the System Control Diagrams should be the basis of the display area layout.
3. Sequence displays should be designed on the sequence chart principle, where every step in the sequence is presented so that information is given about how far the sequence has progressed.

4.4.2.4 Display elements
1. Vendor standard display element library shall be used.
2. The use of display elements shall be consistent throughout the display screens.
3. A text label should accompany display element with dynamic information to identify the physical object.
4. Special attention shall be paid to the readability of text presentation, abbreviations, icons, symbols, numerical data, borders, lines, arrowheads, size and shape, etc.

4.4.2.5 Display properties and data quality
1. The display update rate shall be configured to match the dynamics of the process. However, dynamic alphanumeric values shall not be updated more frequent than once per second.
2. Other issues to consider here would be changing values, data verification for critical variables, etc.

4.4.2.6 Display hierarchy
1. The display system shall allow for a minimum of three levels - overview, system and sub-system displays. Additionally the system shall allow for object displays.
2. Display hierarchy shall be applied on a system basis i.e.
   - shutdown systems (ESD/PSD)
   - fire and gas systems (F&G)
   - process control system

4.4.3 Printing facilities
1. Number of printers shall be kept to a minimum.
2. Failure of one OS or one printer shall not stop printing possibilities.
3. Silent type of alarm/event printers shall be located in CCR or in area adjacent to CCR.
4. The operator shall be able to generate a hardcopy print of any display screen.
5. It shall be possible to generate a printout of following lists; system-generated lists, alarm lists, event lists without using the screen-dump facility.

4.4.4 Coding of information

4.4.4.1 General
1. Coding of information shall be provided when an operator must distinguish between different categories of displayed data.

4.4.4.2 Use of colour
The colour coding as shown in tables below shall be used for process and service lines and equipment.
1. The number of colours used should be kept to a minimum.
2. The colour coding shall be used to distinguish between data categories such as different fluids within the process.

3. Colour coding should not be the only way of distinguishing information, some redundancy at least one other display feature, e.g. tag-number, should be used.

4. Colours used to present static information should not be bright or highlighted.

Table 1 – Colours of process and utility medium

<table>
<thead>
<tr>
<th>Process/utility medium</th>
<th>Colour selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oil</td>
<td>Brown</td>
</tr>
<tr>
<td>Including diesel, crude, lubrication, seal, hydraulic oil and drilling mud.</td>
<td></td>
</tr>
<tr>
<td>Gas</td>
<td>Yellow</td>
</tr>
<tr>
<td>Including fuel, high pressure, low pressure, injection, relief and flare gas.</td>
<td></td>
</tr>
<tr>
<td>Water</td>
<td>Green</td>
</tr>
<tr>
<td>Including potable, ballast, drill, produced, cooling, injection water and steam.</td>
<td></td>
</tr>
<tr>
<td>Air</td>
<td>Blue</td>
</tr>
<tr>
<td>Including instruments and plant air.</td>
<td></td>
</tr>
<tr>
<td>Fire fighting</td>
<td>Orange</td>
</tr>
<tr>
<td>Including firewater and foam.</td>
<td></td>
</tr>
<tr>
<td>Chemicals</td>
<td>Violet</td>
</tr>
<tr>
<td>Including glycol, scavenger, chemicals, cooling and heating medium, drilling and other chemical additives.</td>
<td></td>
</tr>
</tbody>
</table>

Table 2 – Colours of electrical systems

<table>
<thead>
<tr>
<th>Electrical systems</th>
<th>Colour selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>11 kV</td>
<td>Blue</td>
</tr>
<tr>
<td>690 V</td>
<td>Orange</td>
</tr>
<tr>
<td>400/230 V</td>
<td>Yellow</td>
</tr>
<tr>
<td>230V UPS</td>
<td>Brown</td>
</tr>
</tbody>
</table>

Table 3 – Colours of alarms and events

<table>
<thead>
<tr>
<th>Alarm/event categories</th>
<th>Colour selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action alarm</td>
<td>Red</td>
</tr>
<tr>
<td>Warning alarm</td>
<td>Yellow</td>
</tr>
<tr>
<td>Fault alarm</td>
<td>Light blue</td>
</tr>
<tr>
<td>Suppressed</td>
<td>Blue</td>
</tr>
<tr>
<td>Blocked</td>
<td>Blue</td>
</tr>
<tr>
<td>Conflict</td>
<td>Red</td>
</tr>
</tbody>
</table>

4.4.4.3 Use of line coding

1. There should be a meaningful difference between various types of lines appearing in the application display areas. Line patterns and widths, together with colours, should be used to distinguish between main fluid streams, by-pass streams, signal lines and lines used to connect labels and symbols in the display.

2. An arrowhead should be used to indicate the flow/signal direction and the relations between various elements, so as to aid the interpretation of information.

3. Further definition may call for lines consisting of dashes of different colours if lines or equipment are designed for multiple fluids.
4.4.4.4 Labelling and abbreviations
1. Labels shall be consistent throughout the display screens.

2. When abbreviations are used, they should be meaningful and commonly recognised such as ‘KOMP’ for the compressor.

4.4.5 Alarm information in application displays
1. Alarms should be presented close to the display element initiating the alarm.

2. The fire and gas displays shall provide a unique reference to the actual physical area effected.

4.4.6 Basic requirements for the alarm and event handling
To ensure that the alarm system will be an effective and useful support to the operator, a critical judgement of what needs to be alarmed should be made as not all measured process parameters need to generate an alarm if they deviate from normal.

The following basic functionality shall be fulfilled by the alarm and event system:

1. The number of alarms during abnormal conditions shall be reduced by alarm processing/suppression techniques in order to have operator attention to the most critical alarms that require operator action.

2. The alarm system should include generation of aggregated alarms.
   Aggregated alarms could include:
   - Process system state alarms (compressor train trip, etc.)
   - Functional alarms (e.g. loss of cooling)

3. The system shall be able to group alarms and events occurring on a sub-system display and present the resulting alarm and event function on the overview display according to the display hierarchy.

4. It shall be easy to distinguish between system alarms, process alarms and events.

5. The system should facilitate a direct jump for any alarm from the alarm list to the applicable process/utility display.

6. The system shall ensure that alarms requiring immediate operator action are presented in a manner that supports rapid detection and understanding by the operator under all alarm loading conditions.

7. No events or alarms shall be lost in the SAS.

8. Alarm information in all the different displays must be consistent, e.g. colour, text, reference, flashing/not flashing etc.

9. The system shall offer means for alarm annunciation as follows:
   - Acoustically and flashing symbol
   - Visually on VDU in process displays, alarm overviews and on alarm lists

10. Through the display system the operator must easily be able to identify alarm state, i.e. new, acknowledged, or cleared.

11. Acknowledging the alarm shall stop the flashing and the audible signal.
    Different audible signals for different priorities should be considered.

12. It shall be possible for operators to silence alarms.

13. All alarms and events shall, independent of SAS unit, by use of attributes have the possibilities to be grouped according to e.g. process section, severity area (alarm section), etc.

14. The alarms shall, independent of SAS unit, have the possibilities to be grouped according to alarm criticality. The priority of alarms should be coded using colours and possibly other means.
4.4.7 **Time tagging**

1. Events, process and system alarms shall be time tagged in order to identify correct order of sequence of events. This is valid for all SAS units. Time tagging shall be with highest possible resolution, and shall be related to the central Real Time Clock.

4.4.8 **Trend**

1. It shall be possible to trend all the process variables.

2. There should be trend displays showing real-time status and historical trends.

3. The time windows and sampling intervals shall be user-selectable.

4. It shall be possible to show several process variables in the same trend display.

5. The system shall allow for on-line configuration of new objects in trend displays.

4.4.9 **Blocking and suppression**

1. It shall be possible to suppress individual alarms and pre-defined groups of tags (e.g. process system).

2. The system shall provide facilities for reporting any blocking or suppression. The system shall also enable the operator to trace where the blocking/suppression is active.

4.4.10 **Alarm and event lists**

1. Alarm and event text messages shall be presented in lists in a chronological order, based on the time when the alarm or event was activated. The lists shall be dynamically updated. Through selection criteria, the operator shall be able to request different kinds of lists. The following defines the minimum content of the alarm text message; alarm time, alarm title or legend, alarm source (tag), description and priority if used.

2. The alarm text message shall clearly describe the origin and nature of the alarm.

4.5 **Application program development and configuration**

4.5.1 **Programming tools**

A programming tool shall be included in the system and shall as a minimum have the following features:

1. On-line modification of application program without stopping any SAS unit.

2. On-line change of parameters.

3. Load, upload and modifications of application programs via SAS network for any SAS unit directly connected to the SAS network.

4. VDU graphics configuration tool with library of standard symbols.

5. Possibilities of monitoring on-line any dynamic variable in any SAS unit directly connected to the SAS network.

6. Start/stop of application programs.

7. The system shall be self-documenting including both suppliers standard function blocks and project-specified function blocks. The documentation shall be “as programmed” in the executing SAS unit. Verification of application program in programming tool and application program running in executing SAS unit shall be possible on-line.

8. Provisions for application program revision control and traceability.
4.5.2 Function blocks
1. Function block oriented programming with function tag reference should be used.

2. The application programming shall be based upon use of System Control Diagrams as input for the programming.

3. The function block library shall be in compliance with the NORSOK SCD (I-005) standard.

4. It shall be possible to develop high level project specified function blocks (FB) with the same features for programming, testing, maintenance and documentation as supplier standard blocks.

5 System requirements

5.1 Change management and access rights
1. Procedure for change management of the SAS shall be established.

2. The system shall handle different levels of access rights, preventing unauthorised manipulation of specific systems or system attributes (e.g. controller parameters, alarm limits, etc.).

5.2 Hardware
1. Equipment shall fulfil the requirements of the EMC directive 89/336/EEC.

2. A limited number of types of hardware modules shall be used, to ease maintenance and spare part handling.

5.2.1 Remote I/O
1. In order to minimise cabling and hook-up offshore, RIO should be used where applicable.

5.2.2 Input/output cards requirements
1. Field devices should be powered from SAS. In cases where active galvanic isolated barriers are not used, I/O cards shall have galvanic isolation between field and CPU side.

2. No single defect or failure in any I/O card shall affect any other I/O card.

3. Short-circuit in the field shall not damage I/O cards.

4. All I/O cards shall be replaceable under full operating conditions without requiring SAS unit shutdown. Other I/O modules shall not be affected. This applies also to RIO.

5. Installation of additional I/O cards shall be possible without shutdown of SAS unit.

5.2.3 Power supplies, power distribution
1. Each SAS unit shall be powered from two independent 230V AC/50 Hz sources. For operator stations single 230V AC/50 Hz source may be accepted. This is however subject to acceptance by the Client.

2. Internal power supplies for all SAS units including I/O cards shall be dual redundant and replaceable under full operating conditions.

3. CPU and I/O-field instruments shall be powered from different galvanically isolated power supplies.

4. Each power supply shall be designed for 150% of normal consumption or based upon a modular system, which can be expanded without rewiring.

5. Alarm for power supply failures, fuses, earth fault detectors, fans etc. shall be available in the CCR.
5.2.4 SAS termination
1. Any cross wiring shall be included in the SAS unit(s) termination part.
2. It shall be possible to isolate field signals from the SAS unit(s) without disconnecting the cable cores from the terminals.
3. All I/O channels, including spares shall be pre-wired to the system side of the cross wiring terminals.
4. The SAS shall be designed to allow the termination part to be delivered to site at an early stage while testing of application programs continue at SAS supplier workshop. Reconnection facilities shall be pluggable.

5.2.5 Fieldbus
1. The SAS shall support fieldbus technology.

5.3 Software
1. A warm start-up of SAS shall be with predefined output signals. Cold start-up and reboot time for SAS shall take less than 30 minutes, including loading of any system software and application program.
2. The SAS supplier shall provide loading procedures.

5.3.1 Time synchronisation
1. Time synchronisation between SAS units and central real time clock shall not deviate more than ± 50 m/sec. SAS shall receive the time from the central real time clock.

5.4 Requirements to spare capacity
1. Procedure for measuring spare capacity shall be established and verified.

5.4.1 Hardware expandability
1. All control and safety units and FTCs shall have a minimum of 20% installed spare I/O's including trunking for field cables at time of contractual handover to Client. Spare % shall be measured per type of I/O.
   For a well-defined mechanical package, a lower quantity of spare/expandability may be accepted upon Client approval.
   Requirements regarding spare capacity for communication links to be as for hardwired I/O.

5.4.2 CPU performance
1. CPU load of SAS unit(s) at the time of contractual handover to Client shall not exceed 75%. CPU load means percentage of time available for application program (internal CPU handling tasks excluded). The load is measured as an average over a period of twice the slowest scan-rate in use.

5.4.3 Memory
1. It shall be possible to expand control unit memory without any change of application programs and degradation of system performance. There shall be 50% spare capacity at time of contractual handover to Client.

5.4.4 Operator station
1. Requirements regarding spare capacity for operator station with respect to dynamic objects/trend curves/pictures etc. to be as for control unit.

5.4.5 SAS network
1. SAS network traffic shall at the time of contractual handover to Client not in any process-upset condition degrade the performance of the SAS including spare capacity.
Annex A  
(normative)  
Testing of SAS

The SAS vendor(s) shall have available test and/or simulation equipment for the I/O configured.

Facilities for measuring of dynamic loads of SAS unit, communication system and Operator Station shall be made available by the SAS vendor(s).

The tests shall be performed hierarchically, starting first SAS unit tests, then system tests and finally the integration test.

All tests shall be documented. All I/O's shall be tested from the field side of SAS unit(s).

**SAS unit test**

Complete test of hardware and software applications of all SAS units, including applications on Operator Station. The tests shall be performed in accordance with approved test procedures.

**System test**

Several SAS units forming a system shall be tested together. All I/O shall be simulated. System test shall include all inter-unit signals.

**Integration test**

The test shall cover complete SAS including simulation of Control class 2 equipment. In addition to functional test of all systems, dynamic bus and CPU load shall be measured. System fault monitoring shall be tested. The SAS should be alarm and failure free for at least 24 hours.
Annex B  
(normative)  
Time response

The system shall be designed to meet the following performance requirements. All requirements are related to 1 second cycle time.

**Operator command**  
2 sec. for acknowledgement of alarms on the operator station (measured from operator action until acknowledgement is observed on the operator VDU).

**Operator command**  
2 sec. from command to field action (measured from operator action until output card/channel has reached new state).

**Closed loop control**  
Max. 2 sec. from input to output action, i.e. from input signal/ IO module to output signal/ IO module (measured at I/O card terminals). For special control functions shorter cycle time may be necessary in order to fulfil function requirements.

**Alarm display text**  
2 sec. from alarm limit is reached

**Picture update**  
Max. 2 sec. to complete picture on call up for picture containing 100 variables (dynamic objects).

**Picture dynamic update**  
Max. 2 sec. for dynamic objects on picture to show input state/value (measured from input signal I/O card terminals until dynamic point shows same state/value)

**ESD initiation from F&G**  
Max. 4 sec. from confirmed F&G detection to activation of ESD outputs (measured from F&G input signal is in alarm state until ESD outputs are activated).

The time response requirements apply also when the information is transferred via serial communication to/from control systems not fully integrated in SAS.

When utilising link for data transfer, this link shall not degrade the system performance as if utilising hardwired I/O (i.e. I/O transmitted by use of serial communication to be treated as if hardwired I/O were utilised).
Annex C
(informative)
Conceptual SAS topology