

Safety and automation system (SAS)

This NORSOK standard is developed by NTS with broad industry participation. Please note that whilst every effort has been made to ensure the accuracy of this standard, neither OLF nor TBL or any of their members will assume liability for any use thereof. NTS is responsible for the administration and publication of this standard.

Norwegian Technology Centre
Oscarsgt. 20, Postbox 7072 Majorstua
N-0306 Oslo
NORWAY

Telephone: + 47 22 59 01 00
Fax: + 47 22 59 01 29
Email: norsok@nts.no
Website: www.nts.no/norsok



Documents
Document Sharing Hub

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	15
5 System requirements	16
5.1 Change management and access rights	16
5.2 Hardware	16
5.3 Software	17
5.4 Requirements to spare capacity	17
Annex A (normative) Testing of SAS	18
Annex B (normative) Time response	19
Annex C (informative) Conceptual SAS topology	20

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 Subject to development and publication of international standards, the relevant NORSOK standard will be withdrawn.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 C is for information only

Annex A and 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

Definition	Explanation
Alarm	Discrete change of data resulting in an audio/visual annunciation in the control room, requiring operator acknowledgement as well as input to alarm list.
Alarm categories	The following categories are defined, not reflecting priority or criticality of the alarm: Action alarm: Alarm feature including blocking facilities intended for automatic safeguarding actions in order to protect equipment, environment or human beings. Warning alarm: Alarm without blocking facilities intended for abnormal conditions enabling operator intervention in order to prevent further escalation. Fault alarm: Alarm associated to fault or failure in the instrument and/or control device.
Blocking	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.
Conflict	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).

Definition	Explanation
Display	Display: The display is the visualisation of computer output. Display screen: The display screen is the surface that is used for the visualisation of operator information, graphics, display areas and displayed data. Display area: The display area is a window of a display screen that is used to present information from one or more applications. Display element: 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. Display properties: The display properties defines the background colour, display element update rate, linked displays, dynamic function keys, etc.
Dynamic information	Information displayed on the display screen reflecting the state of the process or system. The following dynamic information elements are defined : - Alarm - Event - Binary status - Analogue value
Event	Discrete change of state resulting in a displayed status in the control room as well as input to the event list.
Fieldbus	Fieldbus is an all-digital two-way communication system, which interconnects "field" equipment such as sensors, actuators and controllers.
Override	Override function intended to set the output signal to predefined state, independent of changes in logic states.
PDS	PDS is a reliability/availability calculation procedure available from SINTEF
SAS	SAS is defined as the overall Safety and Automation System. SAS performs monitoring, logic control and safeguarding of a 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.
SAS unit	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.
Shutdown level	Signal latch included in the common signal path between a group of initiators and a group of actuating devices.
Suppression	Disable alarm annunciation as well as any associated automatic actions.

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 direct 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.