Report

Guidelines for standardised classification and failure reporting for safety equipment in the petroleum industry

An APOS project report

Author(s):

Stein Hauge (SINTEF), Solfrid Håbrekke (SINTEF), Mary Ann Lundteigen (NTNU), Shenae Lee (SINTEF) and Maria Vatshaug Ottermo (SINTEF)

Report No:

2023:00108

Client(s):

Multiclient

SINTEF Digital
Postal address:
Postboks 4760 Torgarden
7465 Trondheim, Norway

Switchboard: +47 40005100

info@sintef.no

Enterprise /VAT No:
NO 919 303 808 MVA

Report

Guidelines for standardised classification and failure reporting for safety equipment in the petroleum industry

KEYWORDS

SIS
Equipment grouping
Failure taxonomies
Standardisation
List of Properties (LoP)
Information model

VERSION 01 (open version)	**DATE** 2023-03-10

AUTHOR(S)

Stein Hauge (SINTEF), Solfrid Håbrekke (SINTEF), Mary Ann Lundteigen (NTNU), Shenae Lee (SINTEF) and Maria Vatshaug Ottermo (SINTEF)

CLIENT(S) Multiclient	**CLIENT'S REFERENCE** Erik Korssjøen
PROJECT NO. 102020273	**NO. OF PAGES** 142

SUMMARY

This document provides guidance on how to report and classify failure and maintenance data for safety equipment, as a basis for improved follow-up and future automation. Standardised equipment grouping, equipment properties and simplified failure taxonomies are suggested. Focus is on safety instrumented systems (SIS) but selected non-instrumented safety critical equipment types are also covered.

As part of future digitalisation, establishing a standardised information model for functional safety and safety instrumented function (SIF) follow-up will be an important prerequisite. A main objective with this guideline is to contribute towards such a model, by identifying standardised equipment properties and associated property values. The suggested taxonomies and properties have therefore been compared and mapped against recognised standards and relevant electronic equipment libraries.

PREPARED BY Stein Hauge	SIGNATURE Stein Hauge
CHECKED BY Lars Bodsberg	SIGNATURE Lars Bodsberg
APPROVED BY Anita Øren	SIGNATURE Anita Øren

REPORT NO.	ISBN	CLASSIFICATION	CLASSIFICATION THIS PAGE
2023:00108	978-82-14-07940-1	Unrestricted	Unrestricted

Document history

VERSION	DATE	VERSION DESCRIPTION
01 internal	Date	Preliminary draft of chapters 1–4 for APOS member comments
02 internal	2019-08-30	Draft guideline (excl. appendices) for APOS member comments
03 internal	2019-11-30	Updated guideline (excl. appendices) for all PDS member comments
04 draft	2022-12-12	Updated guideline (incl. appendices) for all PDS member comments
01 open	2023-03-10	Final version (rev. 01)

Table of contents

Preface

The current work has been carried out as part of the APOS research project "Automated process for follow-up of safety instrumented systems (SIS)" (*Norw: Automatisert prosess for oppfølging av instrumenterte sikkerhetssystemer*). The project is supported by the Research Council of Norway and the APOS and PDS forum[1] members. The project duration has been 2019-2022. We would like to thank everyone who has given input and comments to the report, and who has participated in numerous meetings, seminars, and workshops.

PDS forum members
APOS project members
KONGSBERG
equinor
AkerBP
ConocoPhillips
safetec
AkerSolutions
SIEMENS energy
altera
REPSOL
Vysus Group
SINTEF
NTNU – Trondheim Norwegian University of Science and Technology
ABB
aibel
NEPTUNE ENERGY
OKEA
OPTRONICS
origo
ORS
proactima
Honeywell
ROSENBERG
DNV
EMERSON
TechnipFMC
TroCo
eni vår energi
PETROLEUM SAFETY AUTHORITY NORWAY
Sjøfartsdirektoratet Norwegian Maritime Authority
RÅDGIVNING
GASSCO

The main purpose of the APOS research project has been to simplify and standardize reporting and classification of SIS failures, including the classification of safety equipment, and to provide a basis for increased automation and standardisation of SIS follow-up, including a specification for an information model for functional safety. The APOS project comprises seven related activities:

1. **H1: Guidelines for standardised equipment classification and failure reporting (this report)**
2. H2: Potential for automated follow-up of safety equipment /21/
3. H3: Guideline for follow-up of Safety Instrumented Systems (SIS) in the operating phase /8/
4. H4: Standardised/electronic SRS format /24/
5. H5: Information model for functional safety /20/
6. H6: Project summary and presentation
7. H7: PDS Data handbook, 2021 Edition /2/

This report documents project activity one (H1).

Trondheim March 2023

[1] PDS is a Norwegian acronym for reliability of safety instrumented systems. For more information about PDS forum and the APOS project, reference is made to www.pds-forum.com

1 Introduction

1.1 Background and objective

This guideline documents activity one (H1) in the APOS research project "Automated process for follow-up of safety instrumented systems (SIS)" (*Norw: Automatisert prosess for oppfølging av instrumenterte sikkerhetssystemer*). A main purpose of this project is to simplify and standardise reporting and classification of SIS failures, including the classification of safety equipment, and to provide a basis for increased automation and standardisation of SIS follow-up.

Standardised equipment grouping and the APOS project

To enable consistent failure registration and classification, it is important to have a common structure for classification of safety critical equipment. This guideline therefore suggests taxonomies and ontologies[2] for grouping and classification of SIS equipment. For each type of equipment, the associated *properties* (and possible property values) that are assumed to affect reliability the most are also specified.

It should be stressed that the properties in this APOS guideline focus on *reliability performance and functional safety*. When digging into different equipment libraries as discussed later in this guideline, more extensive lists of properties (LoP) are found since for other use cases, such as production performance, additional and/or other properties will apply. Hence, the selection of which properties to include will heavily depend on the specific need of the user/discipline under consideration. In this report we focus on functional safety related properties.

The equipment grouping in this guideline serves as a basis for other APOS activities such as the updated PDS data handbook (H7), the standardised APOS information model (H5), the specification for a standardised electronic SRS format (H4) and the potential for automated follow-up of safety equipment (H2). Figure 1-1 gives an overview of the APOS activities. For further information about the APOS project and the other activities, reference is made to the APOS and PDS forum web page: https://pds-forum.com.

[2] A *taxonomy* describes a way of classification focusing on the hierarchical relationships between entities. *Ontologies* are more sophisticated in the sense that they provide richer information, also about the relationships among entities.

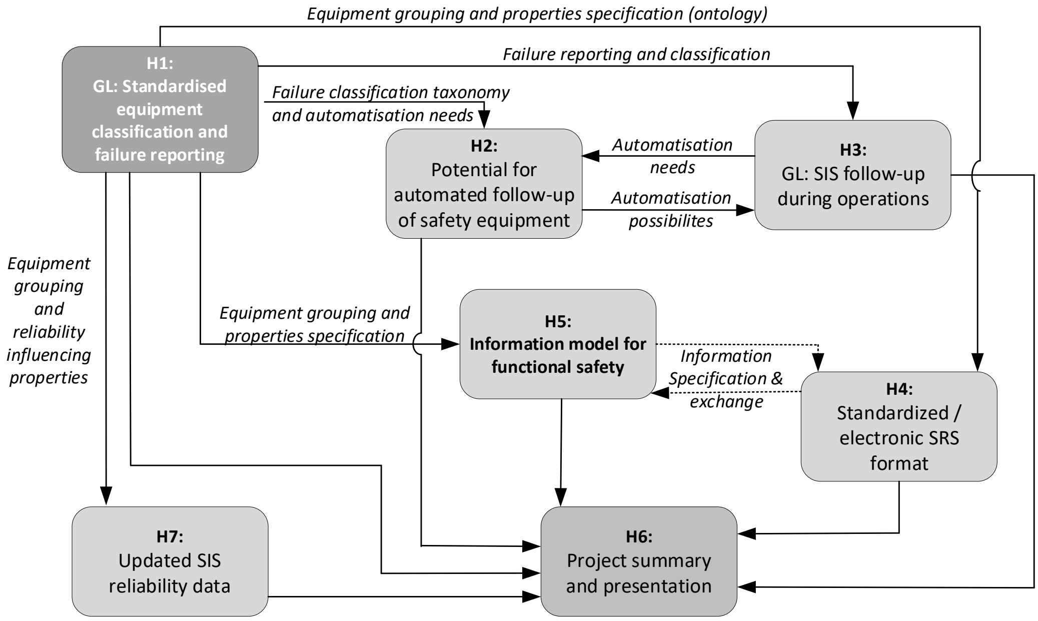

Equipment grouping and properties specification (ontology)
Failure reporting and classification
H1:
GL: Standardised equipment classification and failure reporting
Failure classification taxonomy and automatisation needs
H2:
Potential for automated follow-up of safety equipment
Automatisation needs
Automatisation possibilites
H3:
GL: SIS follow-up during operations
Equipment grouping and reliability influencing properties
Equipment grouping and properties specification
H5:
Information model for functional safety
Information Specification & exchange
H4:
Standardized / electronic SRS format
H7:
Updated SIS reliability data
H6:
Project summary and presentation

Figure 1-1: Illustration of APOS project activities and relationships

Standardised failure registration

The collection and application of relevant failure and maintenance data are essential parts of the follow-up of safety equipment. The data is used to estimate failure rates for quantification of reliability performance, including the optimisation of regular test intervals (see APOS activity H3). The most suited measures to correct failures can also be identified based on information from the failure data collection and classification.

Based on the equipment group classification, this guideline suggests simplified taxonomies for selected failure reporting parameters. This includes detection method, failure mode, failure cause and standardised definitions of safety critical failures and fail/pass criteria. The main purpose of these taxonomies is to highlight the most important parameter options and thereby simplify the process of failure registration and classification. One example is the limitation of failure modes based on the equipment under consideration, e.g., if a valve is selected, only failure modes relevant for valves are included.

The collection of failure and maintenance data is often subject to concerns about the adequacy, quality, and uncertainty of the data. An important starting point for addressing these concerns is to ensure that failures are registered in a *consistent* way, with a high level of precision about failure mode, detection method, and failure cause. As per today, the failure reporting and classification require considerable manual resources. It is therefore useful to make a division between parameters that *must* be reported (mandatory) and parameters that *should* be reported (recommended). Reporting of failure cause is e.g., highly recommended whenever some information is available, but cannot be considered mandatory, due to frequent lack of information.

Equipment included in this report

The prime focus of this guideline is SIS equipment, including relevant subsea components, but some non-SIS equipment (e.g., PSVs, and deluge nozzles) is also covered. Drilling and well intervention equipment is not included in this version of the guideline.

Potential for simplified and automated failure registration

The provision of automatic user guidance can be important to aid the users of e.g., the computerised maintenance management system (CMMS) choosing the correct parameters, e.g., by using text pop-ups, mouse-over and pre-filled choices. Such help texts could for example appear in the maintenance system (or the app) where the failure notification is reported, or secondary in the operational procedures accompanying failure reporting and classification. The help texts (or even pre-filling of fields in the notification) could also draw on information from automated systems such as the safety and automation system (SAS), the information management system (IMS) and condition monitoring systems (CMS) which can provide input about e.g., detection method and failure mode. This, however, requires automatic data exchange (interoperability) between the CMMS and the mentioned systems.

For a discussion of the potential for more automated failure classification, reference is made to the report documenting APOS activity H2, /21/.

Semantic interoperability and information modelling

As the APOS project has progressed, the importance of *semantic interoperability*[3] as an essential prerequisite for future digitalisation of the process industry, has become increasingly clear. *Interoperability* is a characteristic that denotes the capability to exchange and/or share information and *semantic* relates to the fact that - to obtain interoperability – the industry must use *common* terminology and naming (hereunder ontologies and taxonomies) to specify equipment, functions, processes, properties, etc. in a standardised manner. Therefore, this H1 report discusses and references relevant international standards and contains equipment libraries that provides important input to standardised information models for functional safety (see also activity H5 report, /20/).

1.2 Motivation and ambitions

According to the Petroleum Safety Authority (PSA) Norway's Management regulations §19 /10/, the operator shall ensure that HSE data are collected, processed, and used for e.g., carrying out and following up analyses, building generic databases, and implementing measures. This guideline shall contribute towards:

- More efficient and improved reporting of SIS failure data by providing simplified and more intuitive taxonomies.
- More automated failure registration, classification, and analysis. In this respect, common taxonomies and reporting formats are essential.
- Facilitating semantic interoperability and further digitalisation of SIS and safety integrity level (SIL) follow-up by providing standardised classification schemes, reliability influencing properties (including possible property values) and associated unique identification codes/references.
- Facilitating improved data sharing and comparison:
    - between facilities,
    - between operators,
    - between operators and vendors
    - as input to the PSA (e.g., RNNP).

[3] Semantic interoperability is the ability of computer systems to exchange data with unambiguous, shared meaning. Semantic interoperability is a requirement to enable machine computable logic, inferencing, knowledge discovery, and data federation between information systems. https://en.wikipedia.org/wiki/Semantic_interoperability

The guideline is relevant for several categories of personnel working with safety related equipment. Target groups include:

- personnel involved in digitalisation initiatives related to SIS equipment and functional safety
- personnel responsible for developing and configuring information, maintenance, and reporting systems (both operators and vendors)
- personnel performing maintenance and writing notifications related to SIS
- personnel that collect, classify and/or quality assure failure and maintenance data
- personnel performing data analysis and further follow-up of SIS performance

1.3 Relationship to ISO 14224:2016 and other relevant standards

ISO 14224:2016 /4/ provides a comprehensive basis for the collection of reliability and maintenance data and offers standardised taxonomies for many of the equipment types and parameters included in this guideline. It contains general equipment data common to all equipment classes, as well as equipment class specific data, including classification schemes (taxonomies) for e.g., detection method, failure mode, failure cause. In addition, common definitions of safety critical failures are given. ISO 14224 covers both safety and production related equipment, whereas the APOS project is limited to safety critical equipment.

This guideline is aligned with the ISO 14224:2016 standard but aims to further operationalise and clarify the different taxonomies by providing examples, descriptions and illustrations related to parameter choices, e.g., what are the criteria for choosing delayed operation for a typical process shutdown (PSD) valve, what is a casual observation versus a real process demand, what are the suggested failure modes for fire doors, how shall the different failure modes be interpreted operational wise, etc.?

Bridging of different industry practices is also highlighted. Whereas some operators apply the standard ISO 14224 codes (with some modifications), other operators have simplified their reporting system by e.g., just applying two different detection methods (e.g., "hidden" versus "revealed") and two different failure modes (e.g., "impaired safety function" versus "other maintenance related failures"). This guideline suggests simplified taxonomies and classification schemes, and at the same time compares these suggested schemes against relevant standards such as ISO 14224.

For future digitalisation and standardisation, the current guideline also provides a selection of information elements, including *properties* that are expected to especially affect the reliability performance of the equipment. There are three main initiatives for developing equipment property libraries, including the IEC common data dictionary (CDD)[4], the CFIHOS/RDL[5] dictionaries (having their end points at ISO 15926) and ECLASS[6]. For a more thorough discussion of these issues see section 2.4, and Appendix B.

[4] The IEC common data dictionary is continuously under development and will for e.g. process automation equipment be available online at: https://cdd.iec.ch/cdd/iec61987/iec61987.nsf/TreeFrameset?OpenFrameSet&ongletactif=1

[5] CFIHOS (Capital Facilities Information HandOver Specification) and RDL (Reference Data Library) are digitalised equipment information libraries that can be found at http://data.15926.org/cfihos/ and http://data.15926.org/rdl, respectively

[6] ECLASS is a "global reference data standard for the classification and unambiguous description of products and services". It is a preferred dictionary for standardised semantic by Industry 4.0 but has not been further explored in this guideline where focus is on the process industry. Further information can be found at https://eclass.eu/en/eclass-standard

1.4 Content of guideline

Table 1-1 summarises the content of this guideline and provides references to applicable chapters and sections. As seen from Table 1-1 the guideline has two main parts: "Equipment grouping and properties" and "Failure reporting and classification".

Table 1-1: Content of this guideline

Content	Topics discussed	Ref. in guideline
Introduction	Background and motivation for the APOS project and this guideline. Overview of other APOS activities. Relationship to ISO 14224 and other relevant standards.	Ch. 1
Part 1: Equipment grouping and properties	Classification scheme for equipment grouping with links to associated reliability influencing property tables.	Ch. 2
	Detailed datasheet with reliability influencing properties and associated property values.	App. B
	Description of additional properties and data elements for functional safety information modelling.	Ch. 2.5 and App. C
Part 2: Failure reporting and classification	Discussion of parameters in failure registration.	App. D
	Detection method classification.	Ch. 3
	Failure classes and equipment specific failure modes.	Ch. 4.2 and App. E
	Fail/pass criteria, and associated failure modes.	Ch. 4.3 and App. F
	Failure cause classification.	Ch. 5 and App. G
References	References to relevant reports, standards, guidelines, etc.	Ch. 6
APOS terms and definitions	A collection of definitions and explanations of selected terminology used in the APOS project reports.	App. A

Part 1 - Equipment grouping and properties

2 Equipment grouping and functional safety properties

2.1 Motivation

A grouping of safety critical equipment with comparable and standardised properties is necessary for several purposes:

- Ensuring that the same equipment taxonomies and standardised property definitions are applied throughout the lifecycle of the equipment, from project design to operation.
- To serve as input to a standardised information model that shall exist and be enriched across the lifecycle phases.
- Enabling standardised (and equipment specific) taxonomies and automatised registration and classification of failures of equipment within a group.
- For maintenance management: the specified equipment groups are subject to targeted test and maintenance programs.
- Structuring of failure data: the equipment groups (and number of items) define how failures can be aggregated and merged for the purpose of estimating equipment failure rates. The associated properties specify which additional data elements that should be included as part of the failure reporting.
- Comparing, merging, and analysing data from different facilities and/or operators.
- Enabling effective and standardised operational follow-up on a facility (and on a suitable level).

As already discussed in section 1.3, ISO 14224:2016 is a main standard for grouping of equipment in the oil and gas industry, and therefore provides important input to this chapter.

Furthermore, to ensure standardised grouping and naming of equipment properties and other information elements, other standards and equipment libraries such as IEC 61987 /5/ /6/ (and online CDDs), ISO 15926 /22/ and ISO/IEC 81346 /7/, etc. have been consulted. In addition, input from equipment experts have been received through participation in dedicated workshops and written comments.

2.2 How to group equipment?

Two main criteria typically apply when grouping equipment:

- *Function of the equipment*, i.e., what the main function of this type of equipment is, e.g. to detect fire or gas, blow down a vessel, shut down the well-stream, measure the level in a tank or cut the power to normally energised equipment.
- *Design of the equipment*, i.e., specific design or principle of the type of equipment under consideration, such as actuation principle for a valve (e.g. hydraulic versus pneumatic), valve design (e.g. ball versus gate valve), measuring principle for a gas detector (e.g. catalytic versus IR), etc.

The application of the above criteria has, as far as possible, been aligned with already established industry practices, implying that hierarchically most equipment is initially organised by function, and then (at some underlying level) by design. An example for input devices is:

Process transmitters → pressure transmitters → differential pressure transmitter

Here the two first levels are functional, while the third level represents a specific equipment design, in this case measuring principle. There are some exceptions to this classification, and the division between function and design can sometimes be unclear, as will be seen when the equipment grouping is performed and described in Table 2-3 (for topside equipment) and Table 2-4 (for subsea equipment).

ISO/IEC 81346 /7/ is an international standard describing structuring principles and referencing ("tagging") of industrial equipment. This standard promotes the usage of three main aspects: (1) function (what the object does or is intended to do), (2) location (where the object can be found) and (3) product (how the object is constructed). Aspect (1) and (3) correspond with the two main criteria discussed above (function and design). The location aspect can be captured by defining *physical location* as a general property but is also partly defined by the tag number (or "functional location") of the equipment itself.

2.3 Equipment grouping and associated reliability influencing properties

In this report, a *three-level hierarchy* for equipment grouping has been suggested. This structure has been derived from analyses of current industry practices, international standards, discussion with equipment experts and the identified needs and requirements to the subsequent use of data, e.g., as input to a standardised information model, cf. activity H5 in APOS, /20/.

Note that industry practices for grouping of equipment are comparable but not completely similar. Hence, the suggested APOS grouping will not be one-to-one with all company pracitices, but will hopefully include the most relevant items, although sometimes at another hierarchical level.

2.3.1 Level 1 (L1): Main equipment groups - equipment class

L1 represents the grouping of equipment typically sharing a common main functionality and corresponds roughly to *equipment class* as defined in ISO 14224. Examples of main functionality are e.g. to detect a process upset, detect hydrocarbons or a fire, stop the process flow or facilitate evacuation.

Typical application for L1: Failure and maintenance data collected for equipment at L1 may be applied when a coarse analysis is needed, but current industry practice does not usually rely on L1 data when evaluating whether the reliability performance and associated functional test intervals are adequate. Instead, L2 or L3 data is normally applied to capture the variations in reliability performance that are due to e.g., different design principles, measuring principles and other properties.

2.3.2 Level 2 (L2): Safety critical elements - equipment type

L2 represents the *most important* characteristics of the L1 equipment groups. For example, the most important characteristic for gas detectors is *what type of gas can be detected,* and for a process transmitter it is what process variable is being measured (level or pressure or flow, etc.). As compared to the L1 group, these safety critical elements will therefore often have a further specified (sub)functionality, e.g., to detect H_2S gas, to measure high level, or (for a valve) to shut in and isolate the riser.

Note that the safety critical elements presented in this report in many cases correspond to *equipment type* as defined in ISO 14224. *Barrier element* is another term often used with the same meaning as safety critical element.

With respect to tag number format, each equipment type (or safety critical element) will normally have the same function and type code (see Annex B in NORSOK Z-DP-002) /23/, and for safety systems (i.e., NORSOK system 70-79) also the same system code (see Annex A in NORSOK Z-DP-002).

Typical applications for L2: Failure rates for equipment within an L2 group will normally be comparable and can therefore be appropriate for determining test intervals and performing SIS follow-up. This level of refinement often corresponds to the defined barrier elements in the RNNP[7] statistics (with some exceptions, such as e.g. for fire and gas detectors – which corresponds to L1). Maintenance and test programs will also often be targeted at this level, although sometimes at level 3 (see below).

2.3.3 Level 3 (L3): Equipment reliability influencing properties

For *additional detailing* of the safety critical elements, L3 is represented by a common set of *reliability influencing properties* (RIPs), i.e. properties with a potential to impact the reliability performance of the equipment within an L2 group. For example, among topside emergency shutdown valves (ESV/XVs), there can be ball valves, globe valves, and gate valves handling fluids of different types, and a process sensor can be mounted directly in the fluid or via a side chamber (bridle).

When collecting reliability data for a group of equipment, an adequate number of equipment units (tags) is preferrable, since the ability to base decisions on quantitative analysis relies on statistical confidence in the data. Therefore, to obtain samples of adequate size, it is important to *limit* the number of properties, and in Table 2.2 only the most important reliability influencing properties are included. For each identified property, a list of suggested or allowed property values are also given. These, together with relevant references, are specified in the referred equipment library datasheets in Appendix B. For a more detailed discussion of sample sizes and operational follow-up, see the APOS H3 guideline /8/. See also ISO 20815, Annex E.2 /25/ for some general guidance concerning qualification and application of reliability data.

The defined L3 properties also provide input to future data collection and to the standardised information model described in APOS activity H5 /20/. As per today, it is often difficult to document differences in reliability for specific properties. For example, for shutdown valves, reliability performance differs between valves in dirty service and clean service, but insufficient data is often available to quantify such differences. By having designated and predefined properties for each equipment type, such reliability differences will be easier to document by filtering out all valves in dirty service (without having to know each specific tag number).

Typical applications for L3: L3 enables analysis of potential reliability differences due to the specified properties and thereby facilitates further differentiation of failure rates and optimisation of test intervals (given enough operational experience, i.e., adequate size of the L3 group). The specific properties can be applied as "identifiers" for limited populations of equipment that requires special follow-up. One example related to the *process medium* property may be to pay more attention to the need for heat tracing for flow transmitters located in pipelines with three phase flow than for transmitters located in pipelines with dry gas.

2.4 Equipment grouping tables and classification of properties

2.4.1 DLOPs and OLOPs

The IEC 61987 series of standards /5/ have defined List of Properties (LOPs) for *process automation equipment* and make a split between device list of properties (DLOP) and operating list of properties (OLOP). Such a split is also suggested in this guideline.

[7] RNNP: Risikonivå på Norsk sokkel (English: Trends in risk level in the petroleum activity)

The device list of properties (DLOP) is, according to IEC 61987, the essential part of a complete list of properties for a device type and include aspects used to describe "the mechanical construction, the electrical construction and performance of a device". Each DLOP thus describes a particular device type.

The operating list of properties (OLOP) contains aspects related to the operational environment of the device, device design requirements as well as applicable boundary conditions. Note the operating properties can be dynamic and change throughout operation, e.g., the fluid handled can be different from one production phase to another. Hence, these properties need to have some kind of time stamp or history/version to track changes to the property.

Table 2-1 gives an overview of the reliability influencing properties that have been considered as being of particular interest for the equipment groups included in this report. Note that Appendix C describes *additional* general properties and data elements that will also be required as part of a more complete information model for SIF/SIS follow up.

Table 2-1: Classification and description of reliability influencing properties (RIPs)

Type of property	Property	Property description
DLOP	Sensing/measuring principle	How the physical entity in some form (e.g., gas, flame, force, mass, volume, etc.) is measured. IEC 61987-1/2006[8] has the following general definition of measuring principle "Phenomenon serving as the basis of a measurement".
	Mounting principle	Mounting and/or process connection characteristics related to the equipment, e.g., thermowell or clamp-on for a temperature transmitter or intrusive (internal) versus non-intrusive (external) sand detectors.
	Design principle	Design principle/type related to the equipment, e.g. whether it is a ball or gate valve, a tubing retrievable or wireline retrievable downhole safety valve, etc.
	Device type	Here used to specify type of component (when other specified properties are not directly applicable) such as digital or analogue I/O card, etc.
	Actuation principle	Type and/or design of actuator, e.g., hydraulic, pneumatic, or electric. (Single acting or double acting, etc.).
	Internal diagnostic / self-test feature	Here used to specify the type of internal diagnostic capabilities implemented within the component itself, e.g., line monitoring and range checking.
	External diagnostics / comparison	Here used to specify the type of diagnostic capabilities implemented externally to the component itself, such as discrepancy alarm with reference transmitter.
	Dimension	For some equipment types, such as valves, pumps and fire dampers, the dimension may impact the performance, e.g., large bore valves versus small bore valves.
	Configuration	Here used to specify e.g., the configuration of the UPS battery package and the configuration of the firewater pump drive system.

[8] IEC 61987-1/2006 Industrial-process measurement and control – Data structures and elements in process equipment catalogues – Part 1: Measuring equipment with analogue and digital output, section 3.27

Type of property	Property	Property description
OLOP	Fluid handled / severity	Characteristics/properties related to the medium that the equipment handles. Three classes of medium properties are defined: • clean/benign service • medium/moderate service • dirty/severe service *See Appendix A.2 for further definition*
	Phase properties	A description of the properties characterising the phase(s) of a substance for which a measurement is performed, here defined as: • liquid level (liquid-gas) • liquid interphase level (liquid-liquid) • solids level *Note: Here applies specifically for level measurement*
	External exposure	Describes the severity of external exposure (severe, moderate, or low) such as a weather exposed versus a shielded area, indoor versus outdoor, etc.
	Function	Main function of equipment under consideration, such as process isolation, fire extinguishant release, and H_2S detection.
	Application	The application in which the equipment is used: ESD, PSD, process control, blowdown, HIPPS, HVAC, unit control/protection, and combinations of these.

2.4.2 Equipment libraries

As per today there is no single equipment library or standard that contains all relevant equipment. Some equipment is not yet defined (see Appendix B for details) and there is overlap between standards. In this guideline the following equipment libraries have been referred to (with active links):

- For process automation equipment, IEC 61987 is referred to when applicable (with its unique International Registration Data Identifier (IRDI)-codes),
- For selected low voltage (LV) switchgear, IEC 62683 is referred to,
- For other equipment (and when overlapping with IEC CDDs) CFIHOS (Capital Facilities Information Handover Specification) and RDL (Reference Data Library) have been referred to.

The CFIHOS Reference Data Library has been set up to have its endpoint at: http://data.15926.org/cfihos. It is set up as an extension of http://data.15926.org/rdl/, meaning that each CFIHOS item is directly or indirectly a specialisation of a class in the ISO 15926 RDL and hence of an entity type in ISO 15926-2. The CFIHOS library and properties are still under development, implying that equipment found in RDL does not always have its counterpart (or specialisation) in CFIHOS.

For most of the equipment types covered in this guideline, *equipment property tables* have been developed where active links to the applicable libraries discussed above are included. This is exemplified for flow transmitters in Table 2-2, where the property "sensing/measuring principle" have been detailed out in terms of property values. Note that there is also an additional table (B.1) with properties that are common for all process transmitters (such as diagnostics, fluid severity, application, and function).

For a more detailed explanation of the content of the equipment property tables, see Appendix B.

Table 2-2: Equipment property table – exemplified for flow transmitters (ref. Table B.5)

Equipment description			**IRDI code** **(IEC 61987 CDD)** 0112/2///61987#....... **CFIHOS**	**ISO 14224 reference/ other specified reference/ comment**
L1 (Equipment class): Input devices – process transmitters			ABA751	ISO 14224: Section A.2.5.2
L2 (Equipment type): Flow transmitters			ABA761	ISO 14224: Table A.71
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**	DLOP: ABA005 OLOP: ABA003	ISO 14224: A.73 General OLOP for flow measuring equipment
DLOP	Sensing/measuring principle	- Coriolis mass flow	ABA763	ISO 14224: Table A.73
		- Thermal	ABA764	
		- Sonic nozzle	ABC566	
		- DP Pitot tube	ABA768	
		- DP V-cone	ABA770	
		- Variable area (rotameter)	ABA771 (ABA772)	
		- DP Venturi tube	ABA773	
		- DP Orifice plate	ABE425	
		- Positive displacement	ABA783	
		- Electromagnetic	ABA792	
		- Turbine	ABA799	
		- Ultrasonic	ABA801	
		- Vortex	ABA802	

2.4.3 Equipment tables for topside and subsea equipment

Table 2-3 (topside) and Table 2-4 (subsea) present the suggested breakdown for grouping of equipment and identify the most important properties that can affect the reliability of safety equipment for topside and subsea equipment, respectively. Links to the equipment property tables in Appendix B are given in the rightmost column.

To follow up functional safety, several additional properties and parameters are required both on equipment and SIF level. Examples are model/manufacturer, safety properties including SIL and PFD requirements, additional safety requirement specification (SRS) requirements such as response times and test and maintenance intervals, operational history information, failure records, etc. These properties and parameters are further discussed in section 2.5 and in Appendix C.

It should also be stressed that the ticked-off reliability influencing properties (RIPs) in Table 2-3 and Table 2-4 represent the properties considered *to influence equipment reliability the most*. Other properties, such as e.g. pressure-class or material selection for valves, may also affect equipment reliability, but to make data collection more manageable, only the most important RIPs are included in the functional safety model. These other properties will, however, be available in the overall information model for the equipment, but typically covered by other disciplines such as mechanical, process, etc. See section 2.5 for further discussion. Also note that there is a separate report from APOS activity H5, "Information model for functional safety", /20/ that goes into more detail on information modelling.

Finally note that the general, greyed out, properties apply for *all equipment types* listed under the relevant equipment class. E.g., for process transmitters, the general property "Internal diagnostics" and its associated property value picklist (see Table B.1) will apply for all types of all process transmitters. Or said in other words: all the general properties on for the L1 level *are inherited* for all underlying L2 equipment.

Table 2-3: Suggested equipment group hierarchy - topside

Equipment class (L1)	Equipment type – L2	DLOP									OLOP					Reference/link to RIP datasheet
		Sensing / measuring principle	Mounting principle	Design principle	Device type	Actuation principle	Internal diagnostics / self-test	External diagnostics / comparison	Dimension	Configuration	Fluid handled / severity	Phase properties	External exposure	Function	Application	
Input devices - Process transmitters	General – all process transmitters						x	x			x			x	x	Equipment property library B.1
	Level transmitters	x	x									x				Equipment property library B.2
	Pressure transmitters	x	x													Equipment property library B.3
	Temperature transmitters	x														Equipment property library B.4
	Flow transmitters	x														Equipment property library B.5
	Vibration transmitters	x														Equipment property library B.6
Input devices - Process switches	General – all process switches						x				x			x	x	Equipment property library B.7
	Level switches	x										x				Equipment property library B.8
	Pressure switches	x														Equipment property library B.9
	Temperature switches	x														Equipment property library B.10
	Flow switches	x														Equipment property library B.11
	Position switches	x	x													Equipment property library B.12

Equipment class (L1)	Equipment type – L2	DLOP									OLOP					Reference/link to RIP datasheet
		Sensing / measuring principle	Mounting principle	Design principle	Device type	Actuation principle	Internal diagnostics / self-test	External diagnostics / comparison	Dimension	Configuration	Fluid handled / severity	Phase properties	External exposure	Function	Application	
Input devices - Auxiliary switches and transmitters	HVAC (air flow) transmitters	x												x		Ref. to flow transmitters and Equipment property library B.5
	Flow transmitter for aspirating gas or smoke detector[1)]	x												x		Ref. to flow transmitters and Equipment property library B.5
	Flow switch for aspirating gas or smoke detector[1)]	x												x		Reference is made to flow switches and Equipment property library B.11
	Universal gas transmitter/sensor[2)]															**Not yet included**
Input devices - Push buttons	Manual push buttons / call points						x						x	x		Equipment property library B.13
	CAP switches[3)]						x						x	x		Equipment property library B.13
Fire and gas detectors	General – all fire and gas detectors						x						x			Equipment property library B.14
	HC gas detectors	x		x												Equipment property library B.15
	Toxic gas detectors	x												x		Equipment property library B.16
	Other gas detectors	x												x		Equipment property library B.17
	Smoke detectors	x		x												Equipment property library B.18
	Heat detectors	x														Equipment property library B.19
	Flame detectors	x														Equipment property library B.20

Equipment class (L1)	Equipment type – L2	DLOP									OLOP					Reference/link to RIP datasheet
		Sensing / measuring principle	Mounting principle	Design principle	Device type	Actuation principle	Internal diagnostics / self-test	External diagnostics / comparison	Dimension	Configuration	Fluid handled / severity	Phase properties	External exposure	Function	Application	
Logic solvers and interface elements (control logic units)	Logic solvers				x		x						x		x	Equipment property library B.21
	I/O modules				x		x								x	Equipment property library B.22
	Communication/ network modules				x										x	Equipment property library B.23
	Power supply				x										x	Equipment property library B.24
Valves	General – all topside valves			x	x	x			x		x				x	Equipment property library B.25
	Topside shutdown and isolation valves															Equipment property library B.25
	Blowdown and fast opening valves															Equipment property library B.25
	Solenoid/pilot valves															Equipment property library B.25
	Pressure relief valves															Equipment property library B.25
	Deluge valves															Equipment property library B.25
	Other fire-fighting valves															Equipment property library B.25
	Ballast water valves															Equipment property library B.25
	Miscellaneous valves and arrangements															Equipment property library B.25

Equipment class (L1)	Equipment type – L2	DLOP									OLOP					Reference/link to RIP datasheet
		Sensing / measuring principle	Mounting principle	Design principle	Device type	Actuation principle	Internal diagnostics / self-test	External diagnostics / comparison	Dimension	Configuration	Fluid handled / severity	Phase properties	External exposure	Function	Application	
Nozzles	Nozzles (firefighting)			x	x						x					Equipment property library B.26
Fire-fighting equipment	Fire water monitors			x		x					x					Equipment property library B.27
	Foam mixture			x												Equipment property library B.28
	Fire water pump drive system		x							x						Equipment property library B.29
Pumps	Miscellaneous pumps		x	x							x			x		Equipment property library B.30
HVAC dampers	Fire and gas (shut off) dampers				x	x			x				x		x	Equipment property library B.31
Electric generators	Emergency generators			x						x						Equipment property library B.32
Combustion engines	Lifeboat and MOB boat engines			x	x											Equipment property library B.33
Uninterruptible power supply	UPSs & battery packages			x												Equipment property library B.34
Switchgear	Circuit breakers, contactors, and relays			x	x					x						Equipment property library B.35
Escape, rescue, and evacuation	Fire doors			x	x	x				x						Equipment property library B.36
	Watertight doors			x	x	x				x						Equipment property library B.37
	Emergency lights				x								x			Equipment property library B.38
	MOB-boat															**Not yet included**
	Escape chute															**Not yet included**
	Escape chute release systems															**Not yet included**

Equipment class (L1)	Equipment type – L2	DLOP									OLOP					Reference/link to RIP datasheet
		Sensing / measuring principle	Mounting principle	Design principle	Device type	Actuation principle	Internal diagnostics / self-test	External diagnostics / comparison	Dimension	Configuration	Fluid handled / severity	Phase properties	External exposure	Function	Application	
Emergency communication equipment	Loudspeakers and flashing beacons				x								x			Equipment property library B.39
	Telemetry systems			(x)										x		Equipment property library B.40
	Radios and telephones				x											Equipment property library B.41
Lifeboats	Lifeboats			x												Equipment property library B.42
	Lifeboat launch/ release systems			x												Equipment property library B.43

Notes:

[1] These items often have a dedicated tag and failures should therefore be registered against this tag-number (and not against the associated detector). Leakages in associated flow piping is a well-known reliability problem.

[2] These sensors can interface several gas detector types, incl. toxic, oxygen and combustible gases. Sometimes tagged with main detector and sometimes with dedicated/separate tag. Last option preferable for improved failure registration.

[3] Assumed located indoor

Table 2-4: Suggested equipment grouping - subsea

Equipment class (L1)	Equipment type – L2	DLOP									OLOP					Reference/link to RIP datasheet
		Sensing / measuring principle	Mounting principle	Design principle	Device type	Actuation principle	Internal diagnostics / self-test	External diagnostics / comparison	Dimension	Configuration	Fluid handled / severity	Phase properties	External exposure	Function	Application	
Subsea input devices	Subsea process sensors	(x)			x						x				x	Equipment property library B.44
	Subsea leak detectors	x													x	Equipment property library B.45
	Subsea sand detectors	x	x													Equipment property library B.46
Subsea production control	Master control station (located topside)															**Not yet included**
	Umbilical hydraulic/ chemical line															**Not yet included**
	Umbilical power/ signal line															**Not yet included**
	SEM – subsea electronic module															**Not yet included**
Subsea valves	General – all subsea valves			x		x			x		x				x	Equipment property library B.47
	Xmas tree isolation valves				x					x						Equipment property library B.48
	Manifold and flowline valves				x											Equipment property library B.49
	Pipeline and riser valves				x											Equipment property library B.50
	Subsea solenoid control valves				x											Equipment property library B.51

Equipment class (L1)	Equipment type – L2	DLOP									OLOP					Reference/link to RIP datasheet
		Sensing / measuring principle	Mounting principle	Design principle	Device type	Actuation principle	Internal diagnostics / self-test	External diagnostics / comparison	Dimension	Configuration	Fluid handled / severity	Phase properties	External exposure	Function	Application	
Downhole Well Completion Valves	General – all well completion valves			x	x	x					x					Equipment property library B.52
	Downhole safety valve (DHSV)															Equipment property library B.52
	Annulus subsurface safety valve (ASV)															Equipment property library B.52
	Downhole chemical injection valve (CIV)															Equipment property library B.52
	Downhole gas lift valve (GLV)															Equipment property library B.52

2.5 Additional general properties and data elements

In the following, an overview of additional properties and data elements required to establish an overall information model for follow-up of safety equipment and their associated SIFs is given. This overview is probably not complete but should describe most of the required information.

The different properties and requirements have been grouped according to some further defined commonalities (top level). For this purpose, two levels are discussed, the SIS equipment level and the (composite) SIF level.

2.5.1 Safety Instrumented System (SIS) Equipment Level

Below, the suggested grouping of SIS equipment level properties are further discussed and explained:

A. *Equipment ID & references:* i.e., general attributes, "labels" and references that are required to sufficiently identify the equipment under consideration. This will include information about the associated installation, functional location / tag nr. / NORSOK system number, class, and type of equipment (ref. previous section), specific physical location, equipment boundaries, equipment manufacturer, model specification, and a reference to the SIF(s) that the equipment belongs to.

B. *Reliability Influencing properties (RIPs):* i.e., properties with a potential to impact the reliability performance, here specifically the failure rate, of the equipment under consideration. These RIPs have been further split into, see section 2.3.4:

    i. *Device list of properties (DLOPs),* i.e., aspects used to describe the construction and design of the device, such as dimensions of a valve, measuring/sensing principle of a transmitter, type of internal diagnostics for a gas detector, etc.
    ii. *Operating list of properties (OLOPs),* i.e., aspects related to the operational environment in which the device is used, e.g., type of service/medium, degree of weather exposure, functional application (e.g., ESD and/or PSD) etc.

C. *Safety list of properties (SLOP):* here defined as functional safety and reliability related "*properties characterising the ability of an item to perform a required function under given conditions for a given period of time*"[9]. These properties shall be defined within the context of the functional safety standards to which the SIS equipment shall adhere, i.e., particularly IEC 61511 /13/ (and IEC 61508 /12/). This implies that the SLOPs are largely (but not completely) defined by the SRS. Note that whereas the RIPs (DLOPs and OLOPs) mainly affect the *inherent failure rate* of the equipment itself, the SLOPs represent properties with a further impact on the probability of failure on demand (PFD). E.g. MTTR (mean time to restoration), test interval, and hardware fault tolerance (HFT) are all examples of such properties. The SLOPs can (based on where they mainly apply) be further divided into two classes, design related properties, and operation and maintenance related properties[10]:

[9] See IEC 61987 CDD: https://cdd.iec.ch/cdd/iec61987/iec61987.nsf/TreeFrameset?OpenFrameSet&ongletactif=1

[10] Note that several of the SLOPs defined in design are to be considered as requirements and assumptions for operation, and as such have their equivalent during operation, e.g., assumed test interval from design versus implemented test interval during operation and assumed failure rate from design versus calculated operational failure rate, etc.

   i. *Design related,* i.e., safety properties and parameters mainly applicable to the equipment design, e.g. the assumed failure rate from design, fail safe design, stated diagnostic coverage (DC), etc.
   ii. *Operational and maintenance (O&M) related,* i.e., safety properties and parameters mainly applicable to the operation and maintenance of the equipment, such as test interval, test method and coverage.

D. *O&M inventory properties:* i.e., properties related to the operational and maintenance history of the equipment under consideration, normally found in the CMMS, such as:

   i. *Operational inventory properties,* e.g., service start and end date, time in operation, demand rate, etc.
   ii. *Maintenance inventory properties,* e.g., number and dates of functional tests, test results, findings from other maintenance activities, etc.

E. *Failure history properties:* i.e., properties related to the failure history of the equipment under consideration, such as date of failure, reference to failure notification and/or work order, how the failure was detected, failure mode, etc.

The suggested grouping of and associated functional safety properties are illustrated in Figure 2-1. Note that there may be several approaches for grouping of properties, also depending on use case. Other disciplines will have other submodels as indicated in the rightmost part of Figure 2-1. As such, other properties, that in some cases can be relevant for functional safety (such as mentioned pressure class for valves) will be available, but via other (discipline) submodels.

Values for DLOPs and OLOPs (RIPs) are specified in the equipment property libraries in Appendix B. The possible values for the additional data elements are further detailed in Appendix C.

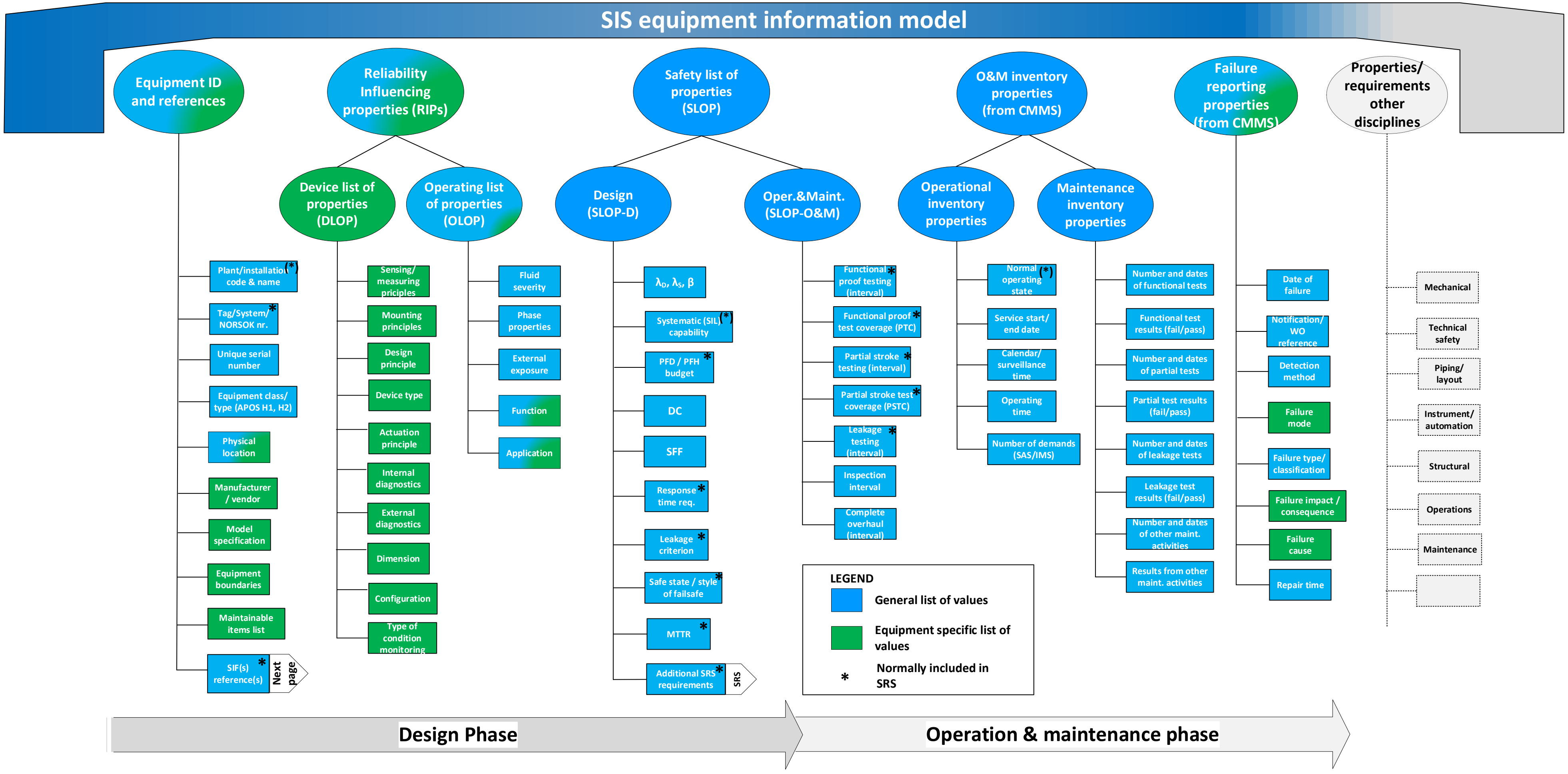

SIS equipment information model
Equipment ID and references
Plant/installation code & name (*)
Tag/System/ NORSOK nr. *
Unique serial number
Equipment class/ type (APOS H1, H2)
Physical location
Manufacturer / vendor
Model specification
Equipment boundaries
Maintainable items list
SIF(s) reference(s) *
Next page
Reliability Influencing properties (RIPs)
Device list of properties (DLOP)
Sensing/ measuring priciples
Mounting principles
Design principle
Device type
Actuation principle
Internal diagnostics
External diagnostics
Dimension
Configuration
Type of condition monitoring
Operating list of properties (OLOP)
Fluid severity
Phase properties
External exposure
Function
Application
Safety list of properties (SLOP)
Design (SLOP-D)
λ_D, λ_S, β
Systematic (SIL) capability (*)
PFD / PFH budget *
DC
SFF
Response time req. *
Leakage criterion *
Safe state / style of failsafe *
MTTR *
Additional SRS requirements *
SRS
Oper.&Maint. (SLOP-O&M)
Functional proof testing (interval) *
Functional proof test coverage (PTC) *
Partial stroke testing (interval) *
Partial stroke test coverage (PSTC) *
Leakage testing (interval) *
Inspection interval
Complete overhaul (interval)
O&M inventory properties (from CMMS)
Operational inventory properties
Normal operating state (*)
Service start/ end date
Calendar/ surveillance time
Operating time
Number of demands (SAS/IMS)
Maintenance inventory properties
Number and dates of functional tests
Functional test results (fail/pass)
Number and dates of partial tests
Partial test results (fail/pass)
Number and dates of leakage tests
Leakage test results (fail/pass)
Number and dates of other maint. activities
Results from other maint. activities
Failure reporting properties (from CMMS)
Date of failure
Notification/ WO reference
Detection method
Failure mode
Failure type/ classification
Failure impact / consequence
Failure cause
Repair time
Properties/ requirements other disciplines
Mechanical
Technical safety
Piping/ layout
Instrument/ automation
Structural
Operations
Maintenance
LEGEND
🟦 General list of values
🟩 Equipment specific list of values
* Normally included in SRS
Design Phase
Operation & maintenance phase

Figure 2-1: Typical content of functional safety information model – SIS equipment level

2.5.2 Safety Instrumented Function (SIF) Level

A SIF can be considered as a *composite asset* comprising sensor(s), logic solver(s), and final element(s). Hence there is a SIF level and an underlying SIS equipment (or component) level (previous section). Therefore, to have a complete information model for SIS follow-up, relevant information at the SIF level must also be included. This includes SIF Id information, properties describing the SIF configuration, requirements from the SRS at the SIF level, as well as SIF operational history information. This is illustrated in Figure 2-2.

The possible values for these additional data elements are further detailed in Appendix C.

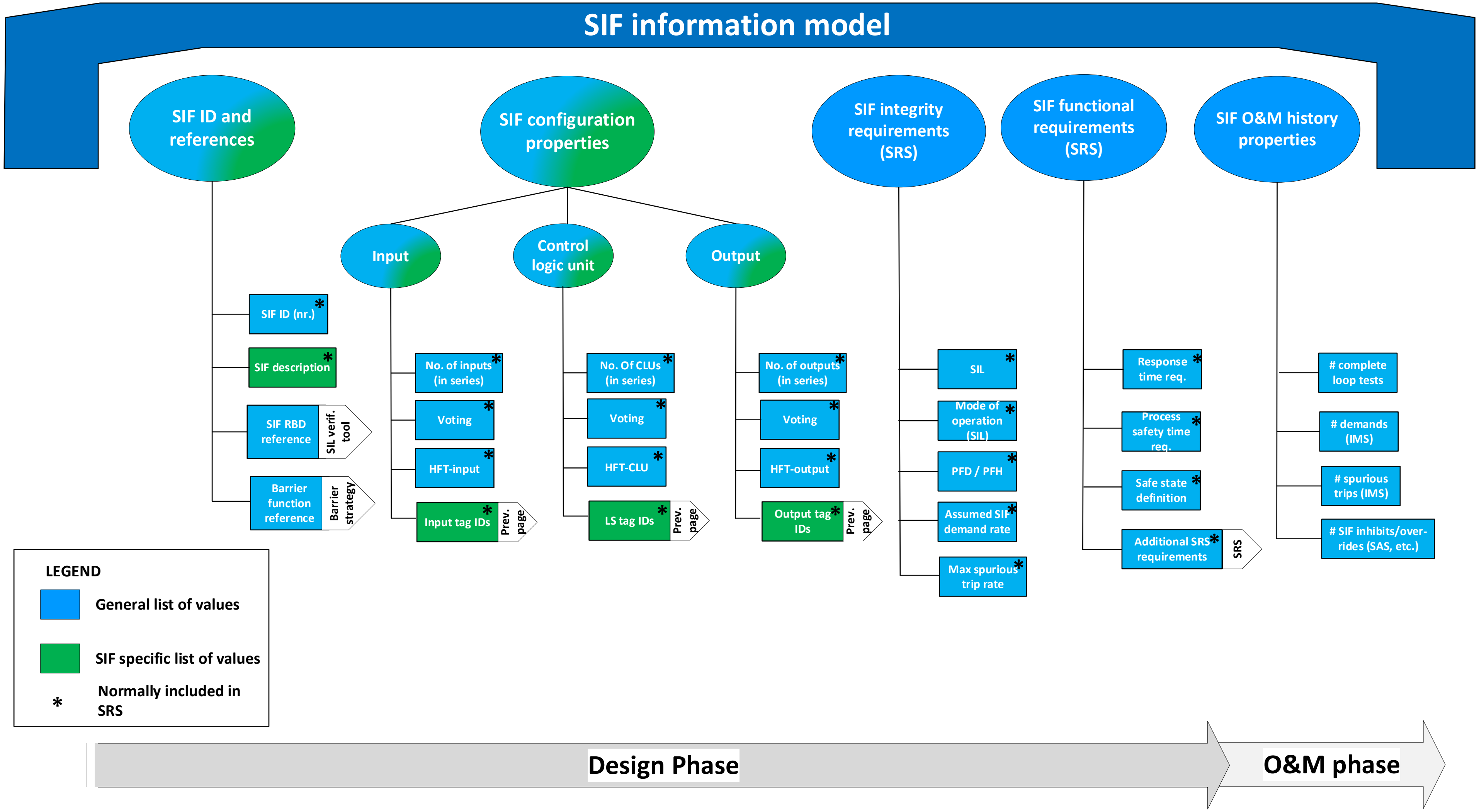


Figure 2-2: Content of functional safety information model – SIF level

Part 2 - Failure reporting and classification

3 Detection methods

3.1 Introduction

Detection method characterises how the failure was discovered. The classification of detection method serves two main purposes:

i. To distinguish between a detected failure and an undetected failure which is used for SIL-analysis and follow-up[11]. A detected failure is a failure that is revealed *upon occurrence*, typically by online diagnostics or condition monitoring, whereas an undetected failure is a *hidden or latent* failure that has occurred sometimes in the past and is revealed either by a scheduled activity (e.g., upon testing), or during an unscheduled activity (such as a shutdown or a casual observation).

ii. For considering the effectiveness of different monitoring regimes, e.g., to assess the proportion of failures detected upon testing, the proportion of failures detected by self-diagnostics or to estimate how many failures are detected upon demand.

Note that the first purpose strictly speaking only requires two categories (detected and undetected), whereas the second purpose requires a further division of detection method categories.

ISO 14224 has identified ten categories for detection method and as per today most companies apply these categories (or variants of them) for classifying detection method. This approach suits both purposes listed above, but it has been pointed out that determining the correct detection method category can be difficult. As a result, some companies have implemented simplified schemes, e.g., to classify failures as either "hidden" or "revealed" (corresponding to undetected or detected failures). Note that this simplified scheme mainly suits the purpose of splitting between detected and undetected failures, rather than identifying the specific detection method.

3.2 Detection method taxonomy

In this guideline we suggest a flexible taxonomy that can serve both purposes mentioned, different company practices and at the same time be compatible with ISO 14224. Based on company needs and preferences, it is possible to either implement several levels, e.g., level D1 and D2 as suggested in this guideline, only level D0 (as some companies have already implemented), or only the ISO 14224 taxonomy.

Figure 3-1 illustrates the suggested detection method taxonomy and the relationships between the different categories. Note that the greyed-out level D1 and D2 is the preferred solution in this guideline, but the suggested taxonomy includes a mapping towards the hidden/revealed categorisation and the ISO 14224 categories.

[11] In addition, it is necessary to decide whether the failure is dangerous (DU/DD) or safe or non-critical. This cannot be decided by detection method alone since additional information about failure mode will be required.

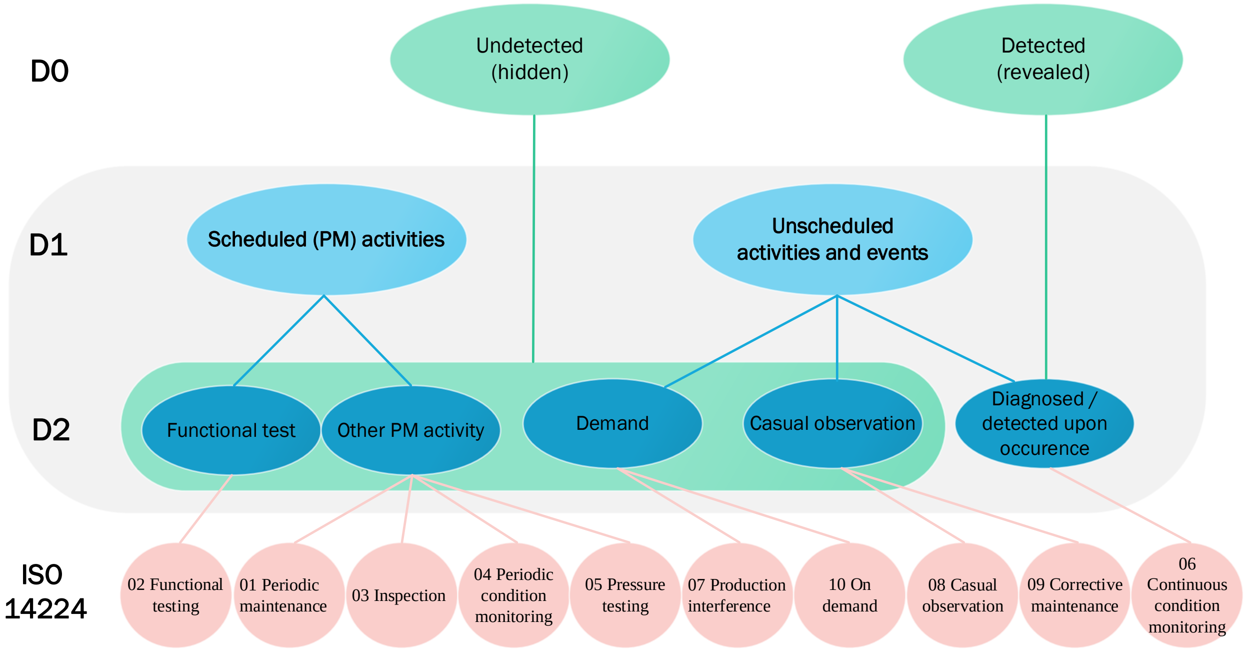


Figure 3-1: Suggested (greyed-out) detection method hierarchy and mapping towards ISO 14224 alternatives [12]

It should be noted that in maintenance notifications the ISO category "01 Periodic maintenance" is often selected even though a functional test has been performed. Ideally, "02 Functional testing" should be used consistently for functional test activities.

Level 0 (D0)

This level focuses on the division between undetected and detected failures. For companies that are mainly interested in this split, this two-tier categorisation can be enough, but it provides limited information about the detection method (or associated activity) itself.

Level 1 (D1)

As mentioned, ISO 14224 has identified ten categories of detection methods. These are sorted into three main activities: scheduled activities, continuous monitoring, and casual occurrences. This guideline suggests a comparable level 1 (D1) taxonomy, however with slightly different categories to avoid possible confusion that is sometimes experienced with the ISO categories (e.g., how to interpret "continuous monitoring", "are all demands casual?", "What is production interference?" etc).

Level 2 (D2)

In many cases, there may be a need for more detailed knowledge about the detection method, e.g., whether the failure was detected during testing or another planned activity, whether it was detected casually or upon a demand, or whether the failure was detected by self-diagnostic upon occurrence. This

[12] Concerning the mapping it is here assumed that the ISO 14224 category "02 functional testing", in addition to closure test, covers testing of internal leakage requirements for a valve (by pressurising segment upstream of the valve), whereas "05 pressure testing" here relates to the activity of testing whether a valve or a blind flange is completely tight when isolating a segment for maintenance (as such "05 pressure testing" could also have been classified under "casual observation").

guideline therefore suggests one additional refinement level for the classification of detection method: Level 2 (D2). Note that *five* D2 categories are suggested as compared to *eleven* (including "other") in ISO 14224.

As seen from Figure 3-1, the D2 taxonomy for unscheduled activities and events suggests a differentiation between actual demands and casual observations. Even though both detection methods are used to define failures as *undetected*, it is still of interest to understand the distribution of the two. In general, it is important to know how well the regular or planned activities can reveal failures, and failures found during demands or by casual observations should ideally be as low as possible. The reliance on casual observations is of specific importance if considering operational changes, such as e.g., reduced manning on a facility.

In general, the four D2 detection methods "Functional testing", "Other PM activity", "Demands" and "Casual Unscheduled activity" will be relevant for all types of equipment, whereas "Diagnosed/immediately detected event" mainly applies to equipment with built in self-diagnostic and/or condition monitoring functionality.

Table 3-1 identifies several examples for each D2 taxonomy field which may be useful for selecting the most appropriate option.

Table 3-1: Suggested detection method hierarchy

D0	Detection method (D1)	Detection method (D2)	Examples	Corr. ISO 14224 categories (cf. ISO Table B.4)
Hidden / Undetected	1. Scheduled activities	1.1 Functional test	• Proof test / PM test / SIL test • Leakage test of shutdown valve • Partial stroke test of shutdown valve • Proof test of gas detector	02 Functional testing
		1.2 Other PM activity	• Periodic overhauling / service • Planned periodic inspections and walkarounds • Planned activations between testing (e.g., planned periodic activation of fire dampers during night shift) • Periodic condition monitoring (thermography, off-line vibration measuring, oil analyses, etc.) • Preventive maintenance preparations	01 Periodic maintenance 03 Inspection 04 Periodic condition monitoring
	2. Unscheduled activities and events	2.1 Demand	• ESD / PSD trip (review of automatic shutdown reports, event logs, physical checks in field) • Other demands / activations (e.g., operation of valve, start of pump, start of emergency generator, closure of fire door, resets after shutdown, minor hydrocarbon leak activating nearby gas detector) • During production upsets and instabilities (and associated lack of demand response from equipment, e.g., no level transmitter response on high level)	07 Production interference 10 On demand

D0	Detection method (D1)	Detection method (D2)	Examples	Corr. ISO 14224 categories (cf. ISO Table B.4)
		2.2 Casual observation	• Failure revealed casually when working on / maintaining or preparing maintenance on *other / nearby* equipment • *New/additional* failure on same item revealed when performing repair/CM • Casual observation during production (e.g., attempt to close valve during re-routing of production) • Unplanned walkaround checks • Casual observation on screen (without diagnostic alarm), e.g., manual comparison of process transmitters from central control room (CCR) • Casual observation from monitoring logs / event logs	05 Pressure testing [1] 08 Casual observation 09 Corrective maintenance
Revealed / detected	**3. Alarmed upon occurrence** [2]	**3.1 Diagnosed / immediately detected event**	• Self-test/diagnostic alarm (e.g., line gas detectors give alarm if beam is blocked) • Online and immediately alarmed comparison of instruments • Immediate detection by continuous condition monitoring (HART alarms, etc.) • Immediate detection of physical damage (e.g., detector out of location during material handling)	06 Continuous condition monitoring

Notes:

[1] Pressure testing classified as casual observation, see footnote 10

[2] If failure revealed within a further defined time-period (e.g., 24 hours) select "diagnosed / immediately detected event". If not, unscheduled activity / casual observation should be chosen as detection method.

4 Failure modes and fail/pass criteria

4.1 Introduction

In IEC 61511 /13/, failure mode is defined as the "manner in which failure occurs". A SIS equipment can have several failure modes, either resulting in loss of the safety function of the equipment (fail to start of a fire pump), a spurious trip (spurious operation of a gas detector), a degradation of the equipment function (a minor internal leakage of an ESD valve) where the safety function is still intact, or a failure mode with no (immediate) effect on the equipment function (noise when closing a valve). In this guideline, special attention is given to the failure modes that imply a loss of the defined safety function, but the other failure modes mentioned are also discussed. Failure mode taxonomy is further discussed in section 4.2 and Appendix E.

For completeness, failure modes related to loss of containment and loss of explosion (EX)-protection have also been included. It is standard practice in companies to consider such failures as critical, although not critical for the safety function of the equipment as such. An example is a moderate external leakage from a PSD valve. The valve may perform its safety function and close upon a demand, but due to the external leakage, the valve will need immediate repair.

Based on the safety critical failure modes (the dangerous failures) which cause loss of the equipment's safety function, it is possible to define standardised fail/pass criteria to apply upon functional testing of the equipment. This is further described in section 4.3 and Appendix F.

4.2 Failure mode taxonomy

This guideline suggests a taxonomy with a limited number of failure modes for each equipment group, i.e., the taxonomy is *equipment specific*. The idea is that the use of some carefully selected failure modes, considered as being the most relevant for an equipment group, will simplify reporting and thereby improve both the amount and quality of failure mode reporting in notifications. *Premisses* for the suggested taxonomy include:

i. As for detection method, the suggested failure modes have been arranged at two levels, F1 and F2. Selected failure mode in combination with detection method is enough to determine whether it is a dangerous undetected (DU) failure or not.
ii. To facilitate and simplify selection of failure mode at level 1, user guidance should be provided. Since the key issue is to separate safety critical failures from (all) other failures, a short and precise definition of the equipment's safety function is provided at this level (cf. illustration in Figure 4-4).
iii. When a failure mode at level 1 (F1) is selected, this will limit the number of relevant failure modes at level 2 (F2).
iv. The level 2 (F2) list of failure modes shall be *complete* in the sense that the failure modes "Other" or "Unknown" are avoided. If the correct failure mode is not found, only the F1 failure mode is reported.
v. A mapping towards ISO 14224 has been included (i.e., which ISO failure modes are included/excluded and new failure modes suggested).

4.2.1 Suggested failure mode hierarchy

Three basic failure modes are suggested at the F1 level:

- **Dangerous failures (D):** covers all failure modes that prevent the *equipment unit* from performing its defined safety function. D does not give any detailed information about *how* the failure occurred, and thus level 2 (F2) failure modes are necessary to specify in more detail.
- **Safe/spurious failures (S):** covers the failure modes that either cause a spurious operation of the equipment and/or maintain the equipment in a safe state. Note that these failures are not dangerous with respect to the safety function of the equipment but may often be critical for production. To enable more detailing of *how* these failures appeared, it is necessary to further specify level 2 failure modes.
- **Non-critical failures:** Non-critical (NONC) failures shall cover all failure modes that are not safety critical (dangerous), not safe/spurious (production critical) or do not imply loss of containment or impaired EX protection. They include:
  - **Degraded failures (DEG):** i.e., failures where the ability of the equipment to carry out the required safety function (or maintain production) has not ceased but is *reduced*, and which over time may develop into dangerous or safe (S) failure modes. Further specification of this degradation is given as an F2 failure mode.
  - **No effect failure (N-E):** i.e., failures that have no direct effect on the equipment function. Further specification is given as an F2 failure mode.

In addition, two non-functional-safety related level 1 (F1) failure modes have been included:

- **Loss of containment (LOC):** LOC covers failure modes that are not directly critical for the defined safety function but is considered critical since loss of containment represents a hazard in itself. LOC does not give any detailed information about the leakage as such, and therefore F2 failure modes can provide additional information.
- **Loss of EX protection (LEX):** LEX similarly covers failure modes that are not directly critical for the defined safety function but are still critical due to increased ignition hazard.

A general illustration of the suggested taxonomy (greyed-out) is shown in Figure 4-1. Note that an additional F0 level has been added to illustrate the main division between dangerous failures that imply loss of the equipment's main safety function and all other failures. This division also reflects the reporting practice in some companies where focus is mainly on reporting at this level.

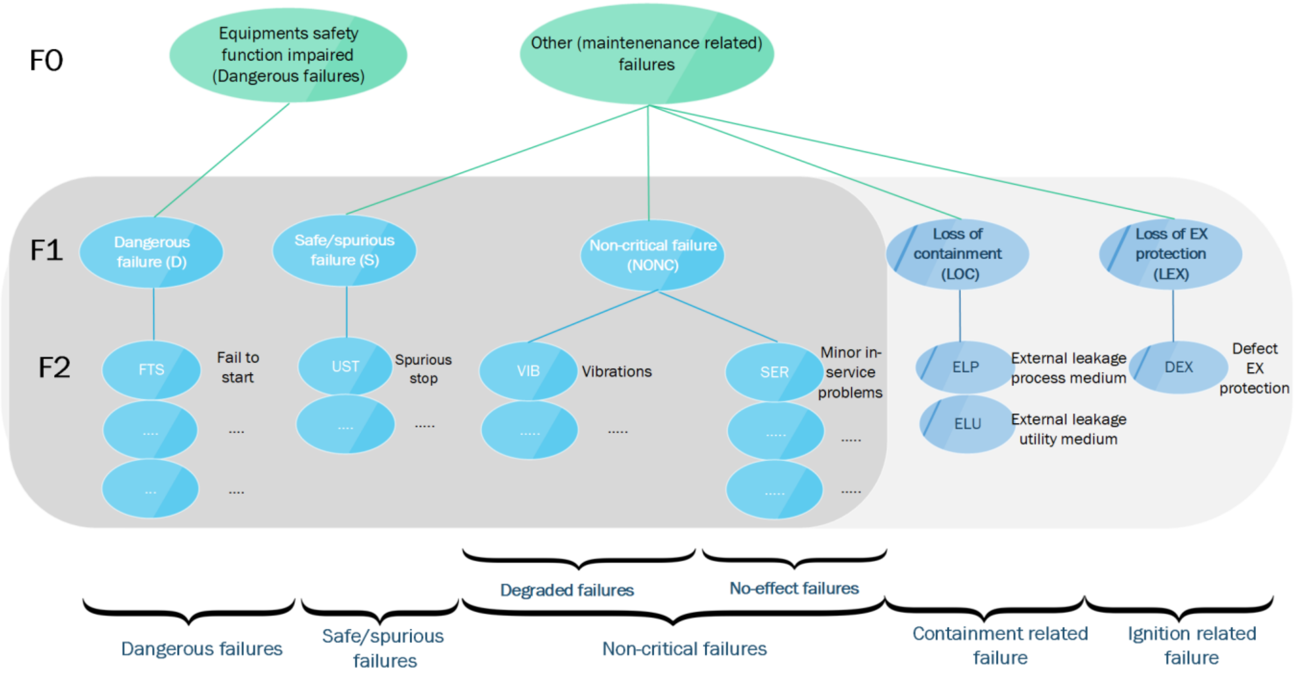

F0
Equipments safety function impaired (Dangerous failures)
Other (maintenenance related) failures
F1
Dangerous failure (D)
Safe/spurious failure (S)
Non-critical failure (NONC)
Loss of containment (LOC)
Loss of EX protection (LEX)
F2
FTS
Fail to start
UST
Spurious stop
VIB
Vibrations
SER
Minor in-service problems
ELP
External leakage process medium
ELU
External leakage utility medium
DEX
Defect EX protection
Degraded failures
No-effect failures
Dangerous failures
Safe/spurious failures
Non-critical failures
Containment related failure
Ignition related failure

Figure 4-1: Suggested (greyed-out) failure mode hierarchy – general illustration

Note that the suggested F2 level in the failure mode hierarchy is comparable to the ISO 14224 approach, however with the exception that the number of level 2 choices have been slightly reduced for each equipment group (see sections 4.2.3 and 4.2.4).

The suggested failure mode hierarchy is further illustrated in Figure 4-2 and Figure 4-3, here exemplified for shutdown valves and IR gas detectors respectively.

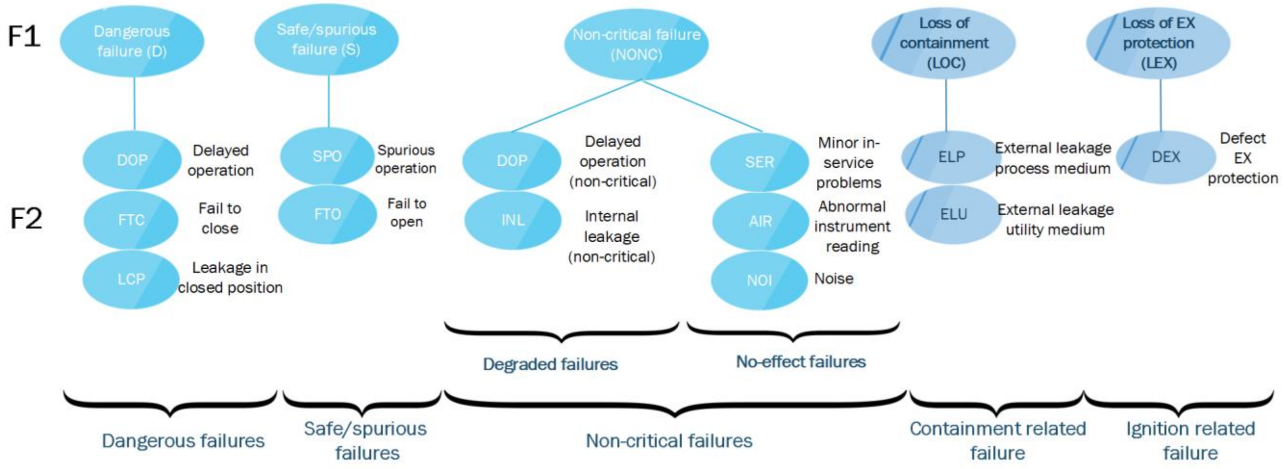

F1
Dangerous failure (D)
Safe/spurious failure (S)
Non-critical failure (NONC)
Loss of containment (LOC)
Loss of EX protection (LEX)
F2
DOP
Delayed operation
FTC
Fail to close
LCP
Leakage in closed position
SPO
Spurious operation
FTO
Fail to open
DOP
Delayed operation (non-critical)
INL
Internal leakage (non-critical)
SER
Minor in-service problems
AIR
Abnormal instrument reading
NOI
Noise
ELP
External leakage process medium
ELU
External leakage utility medium
DEX
Defect EX protection
Degraded failures
No-effect failures
Dangerous failures
Safe/spurious failures
Non-critical failures
Containment related failure
Ignition related failure

Figure 4-2: Failure mode hierarchy – shutdown valve example

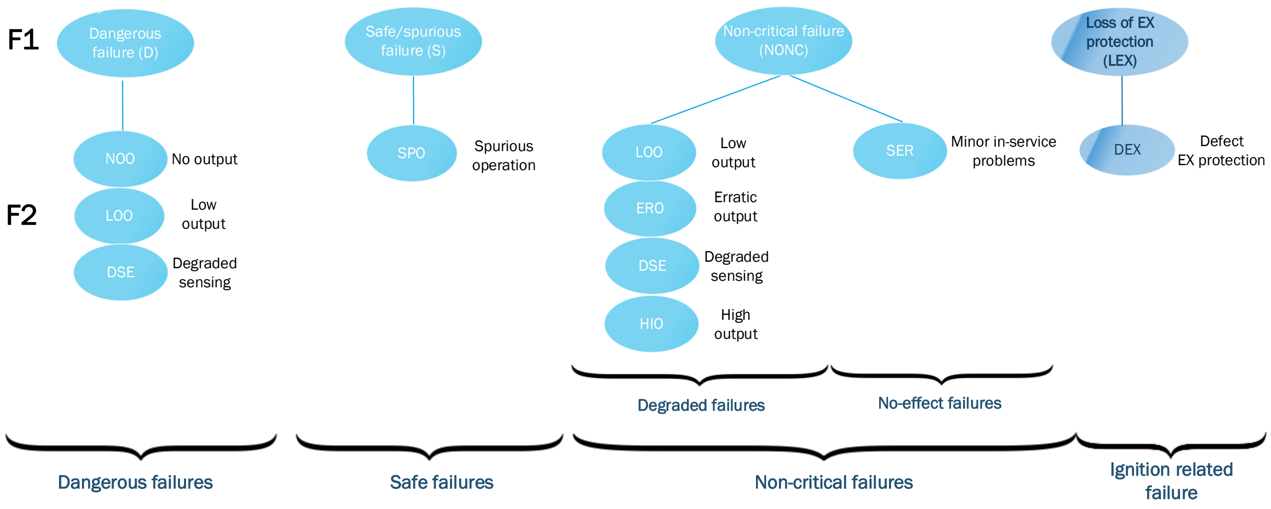
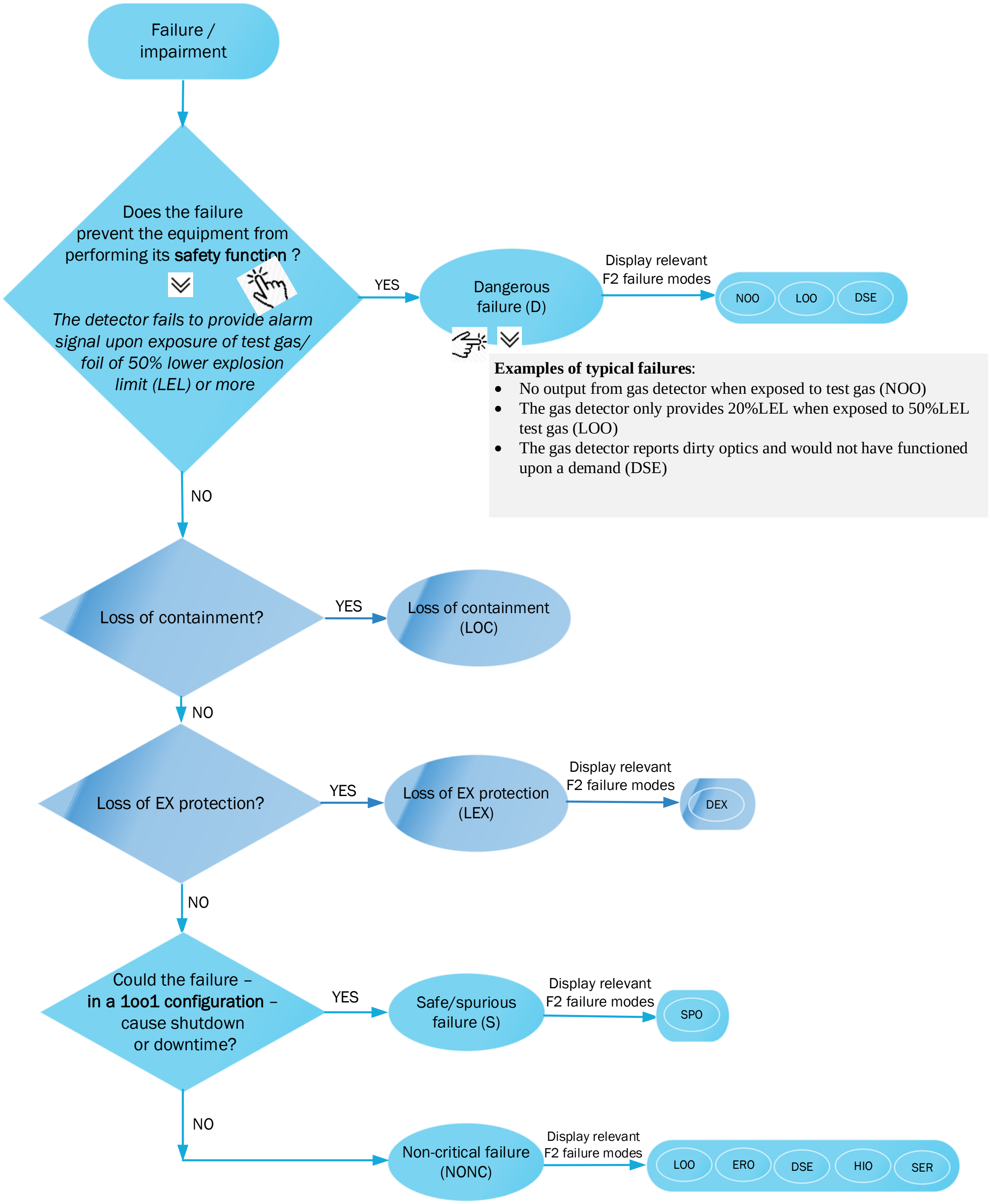


Figure 4-3: Failure mode hierarchy – IR gas detector example

4.2.2 Selection of failure mode at level 1 – user aid

As seen from Figure 4-1 to Figure 4-3, the selection of correct failure mode at level 1 (F1) is essential to identify the dangerous failures. To simplify user selection of correct failure mode at this level, a flow diagram / decision tree has been suggested. This is illustrated in Figure 4-4.


Failure / impairment
Does the failure prevent the equipment from performing its **safety function** ?
The detector fails to provide alarm signal upon exposure of test gas/ foil of 50% lower explosion limit (LEL) or more
YES
Dangerous failure (D)
Display relevant F2 failure modes
NOO
LOO
DSE
NO
Loss of containment?
YES
Loss of containment (LOC)
NO
Loss of EX protection?
YES
Loss of EX protection (LEX)
Display relevant F2 failure modes
DEX
NO
Could the failure – **in a 1oo1 configuration** – cause shutdown or downtime?
YES
Safe/spurious failure (S)
Display relevant F2 failure modes
SPO
NO
Non-critical failure (NONC)
Display relevant F2 failure modes
LOO
ERO
DSE
HIO
SER

Examples of typical failures:

- No output from gas detector when exposed to test gas (NOO)
- The gas detector only provides 20%LEL when exposed to 50%LEL test gas (LOO)
- The gas detector reports dirty optics and would not have functioned upon a demand (DSE)

Figure 4-4: Flow diagram for determination of failure mode at level 1 (IR gas detector example)

Here, the definition of a dangerous failure for the given equipment can be obtained (e.g., by using mouseover) and it is possible to get examples of relevant failures on level 2 (F2) for the specific equipment (here exemplified by typical dangerous failures for an IR gas detector).

A similar flowchart could for example be implemented as an automatic pop-up in the maintenance system when a failure mode shall be registered. Alternatively (and easier to implement), the flowchart could be included as part of a written failure registration procedure. For equipment types where e.g., the LOC, the LEX or the safe failure modes are not relevant, the flowchart can be further simplified. Note that when using such a flowchart, the number of failure modes that the user must choose between will be narrowed down significantly (in this gas detector example maximum five).

There is also a separate report from APOS activity H2, "Potential for automated follow-up of safety equipment", /21/, that discusses the potential for user aided failure parameter determination in more detail.

4.2.3 List of suggested level 2 (F2) failure modes

Table 4-1 lists the level 2 (F2) failure modes suggested in this guideline together with some relevant *examples and comments*. The table also describes which type of equipment each failure mode applies to. The suggested failure modes correspond to the failure modes from ISO 14224 together with a few specifically defined failure modes (cf. notes to the table below). A comparison/mapping with ISO is also found in the detailed tables in Appendix E.

Table 4-1: F2 failure modes suggested in this guideline

Code	F2 Failure mode	Relevant equipment / *examples*
AIR	Abnormal instrument reading	Applies to limit switches, valves, pumps, and engines/generators: • *Incorrect position feedback from valve limit switches* • *Faulty pump instrument indication* • *Faulty engine fuel level reading*
DEX[1)]	Defect EX protection	EX barrier not functional, equipment is an ignition source/ potential ignition source. Applies to SIS equipment that are designed to be placed in Ex zones. Some examples: • *Installed equipment not certified for the respective Ex zone* • *Ex d flame path with severe damage* • *Considerable water/liquid ingress in Ex e equipment with a possibility for creeping/leakage current* • *Considerable damaged Ex e equipment which renders the Ex-protection defect* • *Loss of overpressure with no electrical disconnection in Ex p* • *An intrinsically safe loop calculation on an already installed and operative circuit gives a result which results in non-approval of the circuit (Example: Equipment have been replaced without a proper MoC)*
DOP	Delayed operation	Applies to valves, dampers, and doors where travel time requirements are relevant: • *Closing time of ESD valve is exceeding the requirement* • *Opening time of blowdown valve is too long* • *Excessive closure time of fire damper*
DSE[2)]	Degraded sensing	Applies to detectors: • *Dirty optics on optical F&G detectors* • *Snow on the detector lens*
ELP	External leakage – process medium (oil, gas, condensate, water)	Applies to all valves, pumps, and *transmitters/process sensors*: • *Water leakage from fire water pump* • *HC leakage from ESD valve* • *External leakage from pressure transmitter tubing*
ELU	External leakage – utility medium (hydraulic oil, etc.)	Applies to valves, dampers, pumps, and engines: • *Hydraulic leakage from valve actuator* • *Leakage of instrument air from fire damper actuator* • *External leakage of lubricant or cooling medium from pump* • *External leakage of lubricating oil from diesel engine*
ERO	Erratic output	Applies to input elements, logic, pumps, engines/generators and UPS/battery package: • *Sensor output is oscillating or unstable* • *Pump output is unstable* • *Incorrect output from logic solver*
FTC	Fail to close	Applies to valves, dampers, and doors: • *ESD valve does not close on command* • *Fire damper does not close on signal* • *Fire door does not close and latch*

Code	F2 Failure mode	Relevant equipment / *examples*
FTF	Fail to function on demand	Applies to process switches, pushbuttons, solenoids, logic solvers, deluge nozzles/skid, emergency lights, speakers, radios, and release systems • *Pushbutton fail to provide safety trip / alarm when activated* • *Process switch fails to provide safety trip / alarm signal upon further specified input.* • *The solenoid valve does not change position upon signal* • *The emergency light does not light up upon signal* • *The lifeboat release mechanism does not function upon demand* Note that FTF is a rather *unspecific* failure mode but is applicable for relatively simple equipment that can fail critically in mainly one way.
FTO	Fail to open	Applies to valves, dampers, doors, and circuit breakers/relays: • *Blowdown valve does not open on command* • *PSV does not open within required pressure* • *Fire damper does not re-open after closure* • *Circuit breaker does not open upon signal*
FTS	Fail to start on demand	Applies to pumps and engines: • *Ballast water pump does not start on signal* • *Diesel engine fails to start during testing*
HIO	High output	Applies to input elements and *pumps and engines*: • *Sensor output is above required output* • *Ballast pump delivers more water than specified*
INL	Internal leakage	Applies to non-critical internal leakages through e.g., engines and subsea valves: • *Internal leakage of fuel in diesel engine* • *Internal leakage of utility medium in subsea valve*
IOF[3)]	I/O card failure	Applies to I/O card failures: • *I/O card fails to transfer specified signal*
LCP	Leakage in closed position	Applies to valves, dampers, and watertight doors where requirement to tight shut-off may be relevant: • *Leakage rate through closed valve is above requirement* • *Internal leakage to flare through closed blowdown valve* • *Internal leakage through fire damper* • *The (watertight) door integrity (gasket) is not intact*
LOO	Low output	Applies to input elements and fire water valves/monitors, pumps, engines/generators and UPS: • *Sensor output is below required value* • *Firefighting agent pressure/level is below specified minimum* • *The fire water monitor/pump does not deliver water/foam within expected amount* • *The UPS provides inadequate power supply*
NOO	No output	Applies to input elements *and fire water monitors*: • *No output from sensor* • *Sensor does not react to specified stimuli (pressure, gas, smoke, etc.)* • *The fire water monitor does not operate / oscillate*

Code	**F2 Failure mode**	**Relevant equipment / *examples***
NOI	Noise	Applies to valves, dampers, pumps, and engines: • *Noise from valve when closing* • *Noise from fire damper when closing* • *Valve from pump while running*
OHE	Overheating	Applies to pumps engines/generators and UPS: • *Overheating of lifeboat engine* • *Overheating of UPS*
SER	Minor in-service problems	Applies to most equipment types as a collective term for no-effect failures that do not affect the equipment function: • *Loose items, dirt, corrosion* • *Lacking tag-plate* • *Needs re-painting* • *Small leakage of utility medium from valve not affecting the main function of the valve* • *Passive fire protection removed from valve*
SPO	Spurious operation	Applies to most equipment types as a collective term for failures that cause a spurious operation/trip of the equipment • *False gas alarm from gas detector* • *Shutdown valve closes without closing signal* • *PLC sends a shutdown signal without an acknowledged input*
STD	Structural deficiency	Applies to pumps, engines/generators, and *valves/dampers*: • *Minor cracks in firewater pump housing* • *Cracks in diesel engine block* • *Erosion/wear of valve sealing surfaces*
STP	Fail to stop on demand	Applies to pumps and engines/generators: • *Ballast water pump does not stop on signal* • *Diesel engine does not stop on signal*
UST	Spurious stop	Applies to pumps, engines, and generators • *Spurious stop of pump while running* • *Unexpected stop of engine while running*
VIB	Vibration	Applies to pumps and engines and generators: • *Abnormal vibration of pump*

Notes:

[1] DEX (defect EX protection) is not an ISO 14224 failure mode but is suggested in this guideline since operators apply this failure mode as a means of reporting and managing ignition control failures.

[2] DSE (degraded sensing) is not an ISO 14224 failure mode but is suggested in this guideline due to frequently alarmed events for optical F&G detectors such as dirty/contaminated optics, fog/dew, snow, ice, obstacles, where measures (cleaning, clearance of scaffolding canvas, etc.) are required and a notification is registered. Dirty optics is generally compensated by the detector itself by increasing the intensity of the beam. Dirty optics alarm is considered as a degraded failure – not a critical failure, since it is assumed that a pre-warning/alarm is always given.

[3] IOF (I/O card failure) is not an ISO 14224 failure mode but is suggested in this guideline to cover safety critical failures to I/O cards since today such failures are often registered on other related equipment tags and/or other failure modes.

4.2.4 Equipment specific failure modes

A complete table with equipment specific failure modes is given in Appendix E.

4.3 Standardised fail/pass-criteria

The industry has pointed out the need for standardisation of fail/pass criteria since slightly different criteria are used by the operators today. Since the equipment installed on the various facilities and their functionalities are (more or less) the same, it should be possible to also have common test procedures and fail/pass criteria for the equipment.

The main objective of standardisation of fail/pass criteria is to obtain a more common classification practice between facilities and operators, which will again contribute to more comparable failure rates (and RNNP reporting). To standardise failure reporting it is necessary to standardise and further specify the definitions and criteria of a dangerous failure. To be able to identify what is a dangerous failure and not – precise fail criteria need to be established. In practice this implies to define which failure modes are dangerous for a specific equipment, and – *if necessary* - further specify at which "point" the failure mode becomes critical. E.g., for an internal leakage (LCP) through a safety valve, the exact leakage rate at which the failure is defined as safety critical must also be specified.

Several industry workshops have been conducted in the APOS project, where standardised definitions of dangerous failures and fail/pass criteria have been discussed. Together with the operators own test procedures, PSA 2018 /11/, ISO 14224 /4/, NORSOK S-001/19/ , and relevant API standards /16/, /17/, /18/, this has resulted in suggested standardised fail/pass criteria for many of the equipment classes and types listed in Table 2-3 (only topside equipment has been covered so far). These criteria are further described and defined in Appendix F.

5 Failure causes

The failure cause is the circumstances associated with design, manufacture, installation or use that have resulted in a failure. A closely related parameter is *failure mechanism* which is the *apparent, observable process* that leads to an equipment failure. In practice, it is often difficult to distinguish failure mechanism from failure cause, and in fact they may be overlapping when the description of the failure cause is sufficiently detailed. Also, information about failure cause(s) is often scarce. The failure cause normally relates to a single equipment failure but may also be common for several equipment units (cf. common cause failure).

The identification of failure cause(s) is important for several reasons:

- Understanding the *initiating event, sequence and other circumstances* that led to the failure, to avoid repeating failures:
    - of the same component
    - of other similar components exposed to the same cause
- Identifying *measures* to either
    - identify/detect the failure cause(s) early (prior to failure)
    - remove the failure cause(s)
    - reduce the frequency of the failure cause(s) and subsequent failures
    - reduce the consequences of the potential failures
- Evaluating if it is a systematic or random hardware failure, or whether it is a common cause failure, which is relevant for further analysis and identification of risk reducing measures.

From observable cause to root cause

There are often several layers of the failure cause; from the direct/observable cause to the underlying (and often unobservable) root cause, see Figure 5-1. In failure analysis (and in ISO 14224), "failure cause" is often thought of as the underlying root cause. During failure registration and classification, the root cause is rarely known, but some information about the failure circumstances, e.g., the direct cause or observable *failure mechanisms*, may be available, and will be relevant for equipment repair and further failure analysis / root cause analysis.

In some cases, the root cause may be identified immediately, e.g., when an operator inadvertently hits a line gas detector out of position or when checking of a transmitter reveals that it has been incorrectly calibrated. However, in most cases the root cause is unknown when initially filling out the notification, but can be identified through:

- Maintenance activities in field:
    - repair of the component
    - overhaul/repair or technical analysis of the equipment in the workshop
- Analysis of data or equipment:
    - studying condition monitoring data or other relevant process data
    - vendor analysis of the (sometimes replaced) unit after failure
- Study of information:
    - studying technical information about the equipment (P&IDs, user and installation manuals, maintenance manuals, etc.) and holding this up against any observed failure circumstances
- Other types of root cause analysis (e.g., 5-why analysis)

It should also be noted that in some cases there may be more than one root cause, as well as additional contributing causes that can impact the failure sequence. A **contributing cause** will impact the failure sequence but will not alone cause the failure. An example is *corrosive environment and vibration* (contributing causes) that causes more rapid degradation of a component originally subject to *incorrect choice of material* (root cause).

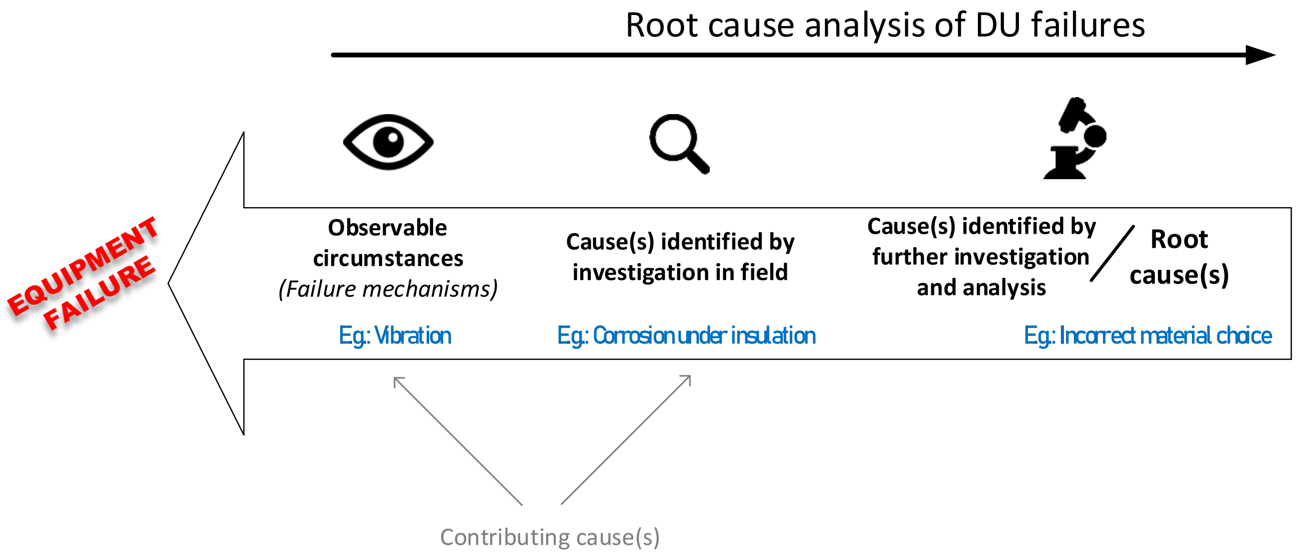

Root cause analysis of DU failures
EQUIPMENT FAILURE
Observable circumstances
(Failure mechanisms)
Eg: Vibration
Cause(s) identified by investigation in field
Eg: Corrosion under insulation
Cause(s) identified by further investigation and analysis
Root cause(s)
Eg: Incorrect material choice
Contributing cause(s)

Figure 5-1: Failure cause development and analysis

In Appendix G, failure cause is further discussed, and a slightly adjusted failure cause taxonomy, as compared to ISO 14224, is suggested.

6 References

/1/ Hauge, S., Kråkenes, T., Hokstad, P., Håbrekke, S., and Juin, H., (2013). Reliability Prediction Method for Safety Instrumented Systems, PDS Method Handbook. SINTEF Report A24442

/2/ Ottermo, M., Hauge S., and Håbrekke S., (2021). Reliability Data for Safety Equipment, PDS Data Handbook. SINTEF Report 2021:00370, ISBN 978-82-14-06468-1

/3/ ISA-TR84.00.03 (2019), Automation Asset Integrity of Safety Instrumented Systems (SIS).

/4/ ISO 14224 (2016), Petroleum, petrochemical and natural gas industries — Collection and exchange of reliability and maintenance data for equipment.

/5/ IEC 61987-1 (2006). Industrial-process measurement and control - Data structures and elements in process equipment catalogues

/6/ IEC 61987-11 (2016). Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 11: List of properties (LOPs) of measuring equipment for electronic data exchange - Generic structures

/7/ IEC 81346-1 (2022). Industrial systems, installations and equipment and industrial products - Structuring principles and reference designations. Part 1: Basic rules

/8/ Håbrekke, S., Hauge, S., and Lundteigen, M.A., (2023). Guideline for follow-up of Safety Instrumented Systems (SIS) in the operating phase, Ed. 3 (APOS H3). SINTEF Report no. 2023:00107

/9/ Hauge, S., Hoem, Å. S., Hokstad, P., Håbrekke, S., and Lundteigen, M.A., (2015). Common Cause Failures in Safety Instrumented Systems, SINTEF Report no. A26922

/10/ Petroleum Safety Authority (PSA) Norway (2021), All regulations, https://www.ptil.no/en/regulations/all-acts/. Accessed 2021-04-05

/11/ Petroleum Safety Authority (PSA) Norway (2018). Risikonivå i norsk petroleumsvirksomhet. Krav til selskapenes rapportering av ytelse av barrierer. Rev. 15. 11.01.2018.

/12/ IEC 61508 (2010). Functional safety of electrical/electronic/ programmable electronic (E/E/PE) safety related systems. Part 1-7, Ed. 2.0.

/13/ IEC 61511 (2016). Functional safety - safety instrumented systems for the process industry sector. Part 1 – 3, Edition 2

/14/ ISO/TR 12489 (2013). Petroleum, petrochemical and natural gas industries - Reliability modelling and calculation of safety systems

/15/ Rausand, M (2014). Reliability of Safety-Critical Systems. Theory and Applications. John Wiley & Sons. ISBN 978-1-118-11272-4

/16/ API RP 14B (2015), Design, Installation, Operation, Test and Redness of Subsurface Safety Valve Systems. American Petroleum Institute. 2015.

/17/ API RP 14 C (2018), Analysis, Design, Installation, and Testing of Safety Systems for Offshore Production Facilities, Eighth Edition, Includes Errata 1.

/18/ API RP 17V (2015), Recommended Practice for Analysis, Design, Installation, and Testing of Safety Systems for Subsea Applications. American Petroleum Institute. Errata 1, July 2015.

/19/ NORSOK S-001 (2018). Technical safety.

/20/ Hauge, S., Lundteigen, M. A., Ottermo, M.V., Lee, S., and Petersen, S., (2023), Information model for functional safety (APOS H5), SINTEF Report no. 2023:00109

/21/ Lee, S., Ottermo, M. V., Hauge, S., Håbrekke, S., an Lundteigen, M.A., (2023), Potential for automated follow-up of safety equipment (APOS H2), SINTEF Report no. 2023:00110

/22/ ISO 15926, Integration of life-cycle data for process plants including oil and gas production facilities. Various parts and dates. Digitalized equipment information libraries can be found at http://data.15926.org/cfihos/ and http://data.15926.org/rdl

/23/ NORSOK Z-DP-002 (1996). Coding systems.

/24/ Hauge, S., Kvam, E. (Safetec) and APOS H4 working group, Specification for standardised electronic SRS (APOS H4 project memo), March 2023.

/25/ ISO 20815 (2018), petroleum, petrochemical and natural gas industries — Production assurance and reliability management.

A Abbreviations and definitions

This appendix contains abbreviations, definitions, and explanations of some of the terminology used in this report.

A.1 Abbreviations

Below is a list of abbreviations used in this report.

API	American petroleum institute
APOS	*Norwegian acronym for* Automated process for follow-up of safety instrumented systems
ASR	Automatic shutdown report
ASV	Annulus subsurface safety valve
CAP	Critical action panel
CCF	Common cause failure
CCR	Central control room
CDD	Common data dictionary
CFIHOS	Capital facilities information handover specification
CIV	Chemical injection valve
CLU	Control logic unit
CM	Corrective maintenance
CMMS	Computerized maintenance management system
CMS	Condition monitoring system
DC	Diagnostic coverage
DD	Dangerous detected
DEG	Degraded
DLOP	Device list of properties
DHSV	Downhole safety valve
DU	Dangerous undetected
ESD	Emergency shutdown
ESV	Emergency shutdown valve
EX	Explosion protection
F&G	Fire and gas
FMECA	Failure mode, effect, and criticality analysis
GLV	Gas lift valve
HH	High high
HART	Highway addressable remote transducer (communication Protocol)
HC	Hydrocarbon
HFT	Hardware fault tolerance
HH	High high
HIPPS	High integrity pressure protection system
HMI	Human machine interface
HSE	Health, safety, and environment
HVAC	Heating, ventilation, and air conditioning
ID	Identification
IDTA	International digital twin association

IEC	International electrotechnical commission
IMS	Information management system
IR	Infrared
IRDI	International registration data identifier
ISA	International society of automation
ISO	International organization for standardization
LEL	Lower explosive limit
LL	Low low
LoP	List of properties
MOB	Man overboard boat
MoC	Management of change
MTTR	Mean time to repair
NA	Not applicable
N-E	No effect (failure)
NONC	Non-critical
NORSOK	Norsk sokkels konkuranseposisjon
O&M	Operation and maintenance
OLOP	Operating list of properties
OT	Operational technology
PFD	Probability of failure on demand
PLC	Programmable logic controller
PM	Preventive maintenance
PSA	Petroleum safety authority (Norway)
PSD	Process shutdown
PSV	Pressure safety valve
RDL	Reference data library
RIP	Reliability influencing property
RNNP	Trends in risk level in the petroleum activity in Norway
SAR	Safety analysis report
SAS	Safety and automation system
SIL	Safety integrity level
SIF	Safety instrumented function
SIS	Safety instrumented system
SLOP	Safety list of properties
SPO	Spurious operation
SRS	Safety requirement specification
SSIV	Subsea isolation valve
TR	Technical report
QA	Quality assurance
UPS	Uninterruptible power supply
VSD	Variable speed drive
XMT	Xmas tree
XO	Crossover

A.2 Definitions and explanations

Table A-1: Terms and definitions

Automatic Shutdown Report (ASR)	The ASR application analyses the sequence of alarms and events that originates when a shutdown occurs and then creates detailed reports indicating the initial cause that has tripped the shutdown and provide status information for final elements (e.g., valves and breakers) that are expected to go to safe position.
Common cause failures (CCF)	Failures of multiple items, which would otherwise be considered independent of one another, resulting from a single cause (ISO 14224:2016, /4/).
Corrective maintenance	Maintenance carried out after fault detection to effect restoration (ISO 14224:2016, /4/).
Critical failure	Failure of an equipment unit that causes an immediate cessation of the ability to perform a required function (ISO 14224:2016, /4/).
Dangerous failure	A failure that impedes or disables a given safety action (IEC 61511:2016, /13/). *APOS comment: A fraction of these failures will be revealed by automatic diagnostic tests and are denoted dangerous detected failures. The residual dangerous failures, not detected by self-tests, are denoted dangerous undetected failures.*
Degraded failure	Failures where the ability of the equipment to carry out the required safety function (or maintain production) has not ceased but is reduced, and which over time may develop into a critical failure (PDS data handbook, 2021, /2/).
Detection method	Method or activity by which a failure is discovered (ISO 14224:2016, /4/).
Diagnostics coverage	Fraction of dangerous failures rates detected by diagnostics. Diagnostics coverage does not include any faults detected by proof tests (IEC 61511:2016, /13/).
Down time	Time interval during which an item is in a down state. Note 1 to entry: The down time includes all the delays between the item failure and the restoration of its service. Down time can be either planned or unplanned. (ISO 14224:2016, /4/)
Failure	<of an item> loss of ability to perform as required (ISO 14224:2016, /4/).
Failure cause (root cause)	Set of circumstances that leads to failure. Note 1 to entry: A failure cause can originate during specification, design, manufacture, installation, operation, or maintenance of an item. (ISO 14224:2016, /4/)
Failure mechanism	Process that leads to failure. Note 1 to entry: The process can be physical, chemical, logical, or a combination thereof. (ISO 14224:2016, /4/)
Failure mode	Manner in which a failure occurs (ISO 14224:2016, /4/).
Failure rate	Conditional probability per unit of time that the item fails between *t* and *t+dt*, provided that it has been working over [0,*t*] (ISO 14224:2016, /4/).

Fluid severity	The fluid handled is categorised into three severity classes: *Clean/benign service* Dry gas and homogenous light and low viscous, low friction liquids such as pure condensate, fresh water, scrubbers downstream dehydration, etc. *Medium/moderate service* Wet gas and processed (separated) homogenous liquids, e.g. 1st stage scrubber, sea water lines downstream separators, drain tanks, etc. *Dirty/severe service* The fluid shall be defined as dirty if it is anticipated that the fluid contains particles, e.g., well stream processing or fluids containing asphaltenes, sand, corrosion products, coke or catalyst. The fluid shall not be regarded as clean upstream of, and including, the unit separating particles from the fluid, e.g., an inlet separator on a production facility shall be regarded as dirty service. The same applies for a 2nd stage separator since there is no effective oil/particle separation in a separator. However, a downstream gas scrubber may be regarded as clean. (APSO categorisation based on Equinor SR-36056)
Periodic test (proof test)	Planned operation performed at constant time intervals in order to detect the potential hidden failures which can have occurred in the meantime. Note 1 to entry: The unsafe hidden failures of a safety system which are not detected by the diagnostic tests can be detected by periodic tests. Such tests are named "proof tests" in the standards dealing with functional safety. ISO 14224:2016, /4/)
Proof test	Periodic test performed to detect dangerous hidden failures in a SIS so that, if necessary, a repair can restore the system to an ‘as new’ condition or as close as practical to this condition (IEC 61511:2016). *APOS comment: If the proof test can detect all dangerous hidden failures, the proof test coverage is 100%. If the proof test is not able to detect all dangerous hidden failures, the proof test coverage is less than 100%.*
Random hardware failure	Failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware (IEC 61511:2016)
Redundancy	Existence of more than one means for performing a required function of an item (ISO 14224:2016, /4/).
Reliability	Ability of an item to perform a required function under given conditions for a given time interval (ISO 14224:2016, /4/).
Safe failure	Failure which favours a given safety action Note 1 to entry: A failure is "safe" only with regard to a given safety function. (IEC 61511:2016, /13/)
Spurious trip	Unexpected shutdown resulting from failure(s) in the control/monitoring system or error(s) imposed on the control/monitoring system originating from the environment or people (ISO 14224:2016, /4/).
Systematic failure	Failure related to a pre-existing fault, which consistently occurs under particular conditions, and which can only be eliminated by removing the fault by a modification of

	the design, manufacturing process, operating procedures, documentation or other relevant factors (IEC 61511:2016, /13/).

B Equipment property tables

This appendix includes tables with equipment properties for selected equipment as specified in Table 2-3 (topside equipment) and Table 2-4 (subsea equipment). Each table includes:

- A description of equipment class (L1) and equipment type (L2) under consideration
- A list of reliability influencing properties (RIPs) of particular interest for SIL follow-up and failure rate differentiation (RIPs classified as either DLOP or OLOP)
- For each RIP the allowed property values are specified
- Reference/link to IEC 61987 common data directory (CDD) unique IRDI code (where applicable)
- Reference/link to IEC 62683 common data directory (CDD) unique IRDI code (where applicable)
- Reference/link to ISO 15926 reference Data Library (RDL) and/or CFIHOS code (where applicable)
- Reference to appropriate ISO 14224 section or table (where applicable)

Additional comments to the equipment property tables:

- The writing style <*name*> quotes the name of the equipment or property as specified in the referenced CDD and/or data library,
- When no link is given to CDD and/or data library, this implies that no relevant item has been found (indicated by a blank field or "not found" or "NA")

To ease electronic data transfer it may, in a future version of this document, be considered to develop Excel sheets/tables (or other relevant formats) with the same information.

B.1 Input devices

This section contains *equipment property tables* for four categories of input devices:

- Process transmitters
- Process switches
- Auxiliary switches and transmitters
- Push buttons

B.1.1 Process transmitters

Equipment property library B.1 lists properties that are common to all process transmitters, whereas B.2 – B.6 list properties and associated property values that are specific for level, pressure, temperature, flow, and vibration transmitters respectively.

Equipment property library B.1: Input devices – process transmitters – common properties

Equipment description			IRDI code (IEC 61987 CDD) 0112/2///61987#....... CFIHOS	ISO 14224 reference/ other specified reference/ comment
L1 (Equipment class): Input devices – process transmitters			ABA751	ISO 14224: Section A.2.5.2
L2 (Equipment type): NA (generic for process transmitters)				
Property Category	**Type of reliability influencing properties (L3)**	**Possible property values**	DLOP: ABV504 OLOP: ABV503	ISO 14224: Table A.73 General DLOP and OLOP codes, see specific transmitter types
DLOP	Internal diagnostic / self-test feature		ABN781	ISO 14224: Table A.73 and APOS specific
		- No self-test		
		- Automatic loop test		
		- Range checking [1]		
		- Input filtering [2]		
		- Combined		
	External diagnostics / comparison	- No external diagnostic / comparison		APOS specific
		- Measuring values checked against reference transmitter		
		- Measuring values checked against algorithm [3]		
OLOP	Fluid handled/ severity [4]		CFIHOS-50000051	ISO 14224: Table A.73 and APOS specific definitions CFIHOS id. relates to fluid (not severity in particular)
		- Clean/benign service		
		- Medium/moderate service		
		- Dirty/severe service		
	Application	- ESD (emergency shutdown)	CFIHOS-60001771	ISO 14224: Table A.73 It has been commented by APOS project members that these properties do not significantly impact reliability as such but nevertheless may be important classification properties. Note that the CHIFOS id. relates to *loop application* and is therefore listed under application (no parallel found in IEC 61987)
		- PSD (process shutdown)	CFIHOS-60001772	
		- EDP (Emergency depressurisation - blowdown)	CFIHOS-60001775	
		- PCS (process control)	CFIHOS-60001770	
		- HIPPS	Not found	
		- Equipment monitoring/protection	CFIHOS-60001776	
		- Combined (several)	CFIHOS-60001777	
	Function	- Process safety		
		- Process control		
		- Aspirating gas detection		
		- Aspirating smoke detection		
		- HVAC (air flow)		
		- Combined		

[1] Input / process value is within acceptable/specified limits

[2] E.g. low-pass filter to prevent high-frequency noise from disturbing the sensor element. There are also (SIL certified) PT transmitters that automatically verifies whether the process pressure varies (to detect e.g. blockages in impulse tubing).

[3] Algorithm based on different process inputs and/or machine learning algorithm

[4] See table of definitions in Appendix A.2 for a description of the severity classes

Equipment property library B.2: Input devices – process transmitters – level transmitters

Equipment description			IRDI code (IEC 61987 CDD) 0112/2///61987#....... CFIHOS	ISO 14224 reference/ other specified reference/ comment
L1 (Equipment class): Input devices – process transmitters			ABA751	ISO 14224: Section A.2.5.2
L2 (Equipment type): Level transmitters			ABA803	ISO 14224: Table A.71
Property Category	Type of reliability influencing properties (L3)	Possible property values	DLOP: ABE735 OLOP: ABE727	ISO 14224: Table A.73 General OLOP for level measuring equipment
DLOP	Sensing/measuring principle	- Displacement	ABA804	
		- Capacitance	ABA806	
		- Floating element	ABA809	
		- Differential pressure	ABA813	
		- Nucleonic	ABA819	
		- Radar	ABA824	
		- Guided wave radar	ABA827	
		- Laser	ABA828	
		- Ultrasonic	ABA829	
		- Gravimetric	ABD390	
		- Level glass	ABA693	
	Mounting principle		ABH128 CFIHOS-50000127	Not covered in ISO 14224: Table A.73 (APOS specific) ABH128 relates to "process equipment connection" CFIHOS-50000127 relates to "connection type" This property is closely related to measuring principle (and therefore simplified to two choices.
		- Direct mounted [1]		
		- Bridle (chamber) [2]		
OLOP	Phase properties		ABG457 CFIHOS-50000052	Covered implicitly in ISO 14224 Table A.73
		- Liquid level (liquid-gas)		
		- Liquid interphase level (liquid-liquid)		
		- Solids level	CFIHOS-60001223	
		-		

[1] Measuring directly in the fluid

[2] Measuring indirectly in a side chamber

Equipment property library B.3: Input devices – process transmitters – pressure transmitters

Equipment description			IRDI code (IEC 61987 CDD) 0112/2///61987#....... CFIHOS	ISO 14224 reference/ other specified reference/ comment
L1 (Equipment class): Input devices – process transmitters			ABA751	ISO 14224: Section A.2.5.2
L2 (Equipment type): Pressure transmitters			ABA831	ISO 14224: Table A.71
Property category	Type of reliability influencing properties (L3)	Possible property values	DLOP: ABA029 / ABA031 OLOP: ABA026	ISO 14224: A.73 General OLOP for pressure measuring equipment
DLOP	Sensing/measuring principle	- Absolute pressure transmitter	ABA832	ISO 14224: Table A.73
		- Differential pressure transmitter	ABA833	
		- Gauge pressure transmitter	ABA834	
	Mounting principle [1]		ABH128 CFIHOS-50000127	Not included in ISO 14224 Table A.73.
		- Tube connection		
		- Remote seal		

[1] It has been commented by APOS project members that type of process connection may affect transmitter reliability in dirty services.

Equipment property library B.4: Input devices – process transmitters – temperature transmitters

Equipment description			IRDI code (IEC 61987 CDD) 0112/2///61987#.......	ISO 14224 reference/ other specified reference/ comment
L1 (Equipment class): Input devices – process transmitters			ABA751	Section A.2.5.2
L2 (Equipment type): Temperature transmitters			ABA835	Table A.71
Property category	Type of reliability influencing properties (L3)	Possible property values	DLOP: ABE767 OLOP: ABF867	ISO 14224: A.73 General OLOP for temperature measuring equipment
DLOP	Sensing/measuring principle	- Thermocouple (element)	CFIHOS-30000478 ABA879	ISO 14224: Table A.73
		- resistance	ABA 876	
		- expansion	Not found	
		- Bimetal	ABL981	
		- Radiation temperature transmitter (infrared)	ABA836	

Equipment property library B.5: Input devices – process transmitters – flow transmitters

Equipment description			IRDI code (IEC 61987 CDD) 0112/2///61987#....... CFIHOS	ISO 14224 reference/ other specified reference/ comment
L1 (Equipment class): Input devices – process transmitters			ABA751	ISO 14224: Section A.2.5.2
L2 (Equipment type): Flow transmitters			ABA761	ISO 14224: Table A.71
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**	DLOP: ABA005 OLOP: ABA003	ISO 14224: A.73 General OLOP for flow measuring equipment
DLOP	Sensing/measuring principle	- Coriolis mass flow	ABA763	ISO 14224: Table A.73
		- Thermal	ABA764	
		- Sonic nozzle	ABC566	
		- DP Pitot tube	ABA768	
		- DP V-cone	ABA770	
		- Variable area (rotameter)	ABA771 (ABA772)	
		- DP Venturi tube	ABA773	
		- DP Orifice plate	ABE425	
		- Positive displacement	ABA783	
		- Electromagnetic	ABA792	
		- Turbine	ABA799	
		- Ultrasonic	ABA801	
		- Vortex	ABA802	

Equipment property library B.6: Input devices – process transmitters – vibration transmitters

Equipment description			IRDI code (IEC 61987 CDD) 0112/2///61987#....... CFIHOS	ISO 14224 reference/ other specified reference/ comment
L1 (Equipment class): Input devices – process transmitters			ABA751	ISO 14224: Section A.2.5.2
L2 (Equipment type): Vibration transmitters			Not found in IEC-CDD CFIHOS-30000378	ISO 14224: Table A.71 include code for vibration. Note that CFIHOS link is not (yet) working.
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**	Not found	ISO 14224: A.73 (vibration transmitters not explicitly discussed)
DLOP	Sensing/measuring principle	- Acceleration	Not found	
		- Velocity	Not found	
		- Orientation (gyroscope). Laser displacement	Not found	
		- Capacitive displacement/Eddy current	Not found	
		- Pressure/microphone (frequency)	Not found	

B.1.2 Process switches

Equipment property library B.7 lists properties that are common to all process transmitters whereas B.8 – B.12 list properties and associated property values that are specific for level, pressure, temperature, flow and limit switches respectively.

Equipment property library B.7: Input devices – process switches – common properties

Equipment description			**IRDI code** **(IEC 61987 CDD)** 0112/2///61987#....... **CFIHOS**	**ISO 14224 reference/ other specified reference/ comment**
L1 (Equipment class): Input devices – process switches			ABA697	ISO 14224: Section A.2.5.2
L2 (Equipment type): NA (generic for all process switches)				
Property Category	**Type of reliability influencing properties (L3)**	**Possible property values**	DLOP: ABV504 OLOP: ABV503	ISO 14224: A.73 General DLOP and OLOP codes, see specific switch types
DLOP	Internal diagnostic / self-test feature		ABN781	ISO 14224: Table A.73 and APOS specific
		- No self-test		
		- Automatic loop test		
		- Range checking [1]		
		- Combined		
OLOP	Fluid handled/ severity	-	CFIHOS-50000051	ISO 14224: Table A.73 and APOS specific definitions CFIHOS id. relates to fluid (not severity in particular)
		- Clean/benign service		
		- medium/moderate service		
		- dirty/severe service		
	Application	- ESD (emergency shutdown)	CFIHOS-60001771	Table A.73 It has been commented by APOS project members that these properties do not significantly impact reliability as such but nevertheless may be important classification properties The CHIFOS id. relates to *loop application* and is therefore listed under application (no parallel found in IEC 61987)
		- PSD (process shutdown)	CFIHOS-60001772	
		- EDP (Emergency depressurisation - blowdown)	CFIHOS-60001775	
		- PCS (process control)	CFIHOS-60001770	
		- HIPPS	Not found	
		- Equipment monitoring/protection	CFIHOS-60001776	
		- Combined (several)	CFIHOS-60001777	
	Function	- Process safety		
		- Process control		
		- Aspirating gas detection [2]		
		- Aspirating smoke detection [2]		
		-		

[1] E.g. low-pass filter to prevent high-frequency noise from disturbing the sensor element. There are also (SIL certified) PT transmitters that automatically verifies whether the process pressure varies (to detect e.g. blockages in impulse tubing).

[2] Relevant for flow switches

Equipment property library B.8: Input devices – process switches – level switches

Equipment description			**IRDI code** **(IEC 61987 CDD)** 0112/2///61987#....... **CFIHOS**	**ISO 14224 reference/ other specified reference/ comment**
L1 (Equipment class): Input devices – process switches			ABA697	ISO 14224: Section A.2.5.2
L2 (Equipment type): Level switch			ABA703	ISO 14224: Table A.71
Property Category	**Type of reliability influencing properties (L3)**	**Possible property values**	DLOP: ABE755 OLOP: ABE727	ISO 14224: Table A.73 General OLOP for level measuring equipment
DLOP	Sensing/measuring principle	- Displacement level switch	ABA704	ISO 14224: Table A.73
		- Electrical based (capacitance, conductance)	ABA705	
		- Float level switch (magnetic, tilt)	ABA708	
		- Hydraulic pressure level switch	ABA711	
		- Mechanical level switch (rotary paddle)	ABA712	
		- Nuclear level switch	ABA714	
		- Resistance tape switch	ABA715	
		- Thermal level switch	ABA716	
		- Vibrating level switch (fork, rod)	ABA717	
		- Wave level switch (free space radar, guided wave radar, optical, microwave, ultrasonic)	ABA720	
OLOP	Phase properties		ABG457 CFIHOS-50000052	Covered implicitly in Table A.73
		- Liquid level (liquid-gas)		
		- Liquid interphase level (liquid-liquid)		
		- Solids level	CFIHOS-60001223	

Equipment property library B.9: Input devices – process switches – pressure switches

Equipment description			**IRDI code** **(IEC 61987 CDD)** 0112/2///61987#....... **CFIHOS**	**ISO 14224 reference/ other specified reference/ comment**
L1 (Equipment class): Input devices – process switches			ABA697	ISO 14224: Section A.2.5.2
L2 (Equipment type): Pressure switch			ABA732	ISO 14224: Table A.71
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**	DLOP: Not found OLOP: ABA026	ISO 14224: Table A.73 OLOP general for pressure measuring equipment
DLOP	Sensing/measuring principle	- Gauge pressure switch	ABA733	ISO 14224: Table A.73
		- Absolute pressure switch	ABA734	
		- Differential pressure switch	ABA735	

Equipment property library B.10: Input devices – process switches – temperature switches

Equipment description			**IRDI code** **(IEC 61987 CDD)** 0112/2///61987#....... **CFIHOS**	**ISO 14224 reference/ other specified reference/ comment**
L1 (Equipment class): Input devices – process switches			ABA697	ISO 14224: Section A.2.5.2
L2 (Equipment type): Temperature switch			ABA737	ISO 14224: Table A.71
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**	DLOP: Not found OLOP: ABF867	ISO 14224: Table A.73 OLOP general for temp. measuring equipment
DLOP	Sensing/measuring principle	- Bimetallic temperature switch	ABA738	ISO 14224: Table A.73
		- Filled-system temperature switch	ABA739	
		- Resistance thermal device (RTD) switch	ABA740	
		- Thermocouple temperature switch	ABA741	
		- Differential temperature switch (Bimetallic, filled-system, RTD, TC)	ABA742	
		- Radiation temperature switch	ABE332	

Equipment property library B.11: Input devices – process switches – flow switches

Equipment description			**IRDI code** **(IEC 61987 CDD)** 0112/2///61987#....... **CFIHOS**	**ISO 14224 reference/ other specified reference/ comment**
L1 (Equipment class): Input devices – process switches			ABA697	ISO 14224: Section A.2.5.2
L2 (Equipment type): Flow switch			ABA698	ISO 14224: Table A.71
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**	DLOP: Not found OLOP: ABA003	ISO 14224: Table A.73 OLOP general for flow measuring equipment.
DLOP	Sensing/measuring principle	- Mechanical flow switch (paddle, rotating vane)	ABA699	ISO 14224: Table A.73
		- Thermal flow switch	ABA701	
		- Variable area flow switch	ABA702	

Equipment property library B.12: Input devices – process switches – position switches

Equipment description			**IRDI code** **(IEC 61987 CDD)** 0112/2///61987#....... **CFIHOS**	**ISO 14224 reference/** **other specified reference/** **comment**
L1 (Equipment class): Input devices – process switches			ABA697	ISO 14224: Section A.2.5.2
L2 (Equipment type): Position switch			ABA728	ISO 14224: Table A.71
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**	DLOP: ABV520 OLOP: Not found	ISO 14224: Table A.73 DLOP for position transmitter!
DLOP	Sensing/measuring principle	- Electromechanical switch	ABA729	ISO 14224: Table A.73
		- Photoelectric switch	ABA730	
		- Proximity switch	ABA731	
	Mounting principle		ABH128 CFIHOS-50000127	Not explicitly covered in ISO 14224 Table A.73 (APOS specific) ABH128 relates to "process equipment connection" CFIHOS-50000127 relates to "connection type". This property is closely related to measuring principle.
		- Mechanical link		
		- Contactless		

B.1.3 Auxiliary switches and transmitters

No specific data sheets have (yet) been developed for this category.

B.1.4 Push buttons

The IEC 61987 CDD focus on process equipment under the measurements and control segment and does not (per February 2022) contain dictionaries for push buttons and call points (pushbutton switch briefly mentioned as type of switch; 0112/2///61987#ABN275).

Push buttons is listed as a component in the *IEC 62683 CDD* (for Low voltage switchgear and control gear). It should however be noted that therein push buttons apply for *local emergency shut down for a specific electrical equipment* (such as a motor) and is therefore less relevant for most of our functions (see Table B.13). Therefore, in Table B.13 CFIHOS and/or ISO RDL are mostly referred (and IEC references put in brackets).

Equipment property library B.13: Input devices – push buttons

Equipment description			IRDI code (IEC 62683 CDD) 0112/2///62683#....... CFIHOS	ISO 14224 reference / other specified reference / comment
L1 (Equipment class): Input devices – push buttons			CFIHOS-30000459 (ACC517)	ISO 14224: Section A.2.5.2 "Control switch" being superclass for push buttons in both IEC 62683 and CFIHOS
L2 (Equipment type): Manual push button & call points incl. CAP switch			CFIHOS-30000459 CFIHOS-30000127 (ACC517)	<Push button> <manual call point>
Property category	Type of reliability influencing properties (L3)	Possible property values	DLOP: Not found OLOP: Not found	ISO 14224: Input device properties covered in Table A.73 IEC 62683 do not distinguish between DLOPs and OLOPs
DLOP	Internal diagnostic / self-test feature [1]		(ACC013)	ISO 14224: Table A.73 and APOS specific
		- No self-test		
		- Loop monitoring [2]		
		- Combined		
OLOP	External exposure	- High/Severe [3]		External exposure not covered explicitly in ISO 14224 Table A.73.
		- Medium/Moderate [4]		
		- Low/shielded [5]		
	Function	- Emergency Shutdown (ESD) initiation	rdl/RDS7057791	The CFIHOS data-model does not yet differentiate between different types of pushbuttons, so references to ISO RDL is therefore given. It has been commented by APOS project members that this property does not impact reliability as such but is nevertheless an important classification property
		- Fire water deluge release	rdl/RDS7057836	
		- Inergen release	rdl/RDS305054	
		- Water mist release	rdl/RDS315089	
		- F&G manual initiation	Not found	
		- Electrical isolation	Not found	
		- CAP initiation	Not found	
		- Local equipment emergency stop button	ACC022	

[1] Some push buttons may be connected directly to F&G-node, whilst others are connected via a fire central. Although the equipment is similar, the difference in diagnostics coverage may lead to different dangerous undetected (DU) failure rates - λ_{DU}

[2] The implementation of termination resistors is a prerequisite for automatic loop monitoring

[3] E.g. equipment in classified areas, outdoor and naturally ventilated rooms

[4] E.g. equipment in high exposure areas but with weather protection, inside containers or instrument rooms

[5] E.g. equipment in unclassified mechanically ventilated rooms

B.2 Fire and gas detectors

The IEC 61987 CDD has not (per December 2022) developed data directories specifically for fire and gas detectors. Neither has such detectors been found in the other domains of the IEC CDD.

The ISO 15926 online browser (http://data.15926.org/rdl/) include fire and gas detectors and CFIHOS has further developed these equipment types and is therefore referred *when relevant* in the below tables.

Property libraries are included for the following types of fire and gas detectors:

- HC gas detectors (Equipment property library B.15)
- Toxic gas detectors (Equipment property library B.16)
- Other gas detectors (Equipment property library B.17)
- Smoke detectors (Equipment property library B.18)
- Heat detectors (Equipment property library B.19)
- Flame detectors (Equipment property library B.20)

As well as common properties listed in Equipment property library B.14 below.

Equipment property library B.14: Fire and gas detectors – common properties

Equipment description			**IRDI code** **CFIHOS**	**ISO 14224 reference/ other specified reference/ comment**
L1 (Equipment class): Fire and gas detectors			CFIHOS-30000640	ISO 14224: Section A.2.5.1 <Detector> general with subclasses e.g., gas detector and smoke detector.
L2 (Equipment type): NA (generic for all F&G detectors)				
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**		ISO 14224: Table A.70
DLOP	Internal diagnostic / self-test feature	- Automatic loop test (line monitoring)		ISO 14224: Table A.70
		- Self-verify in active use		
		- Combined		
OLOP	External exposure	- High/Severe [1)]		ISO 14224: Table A.70 and APOS specific
		- Medium/Moderate [2)]		
		- Low/shielded [3)]		

[1)] E.g. equipment in classified areas, outdoor, air intakes

[2)] E.g. equipment in high exposure areas but with weather protection, inside containers or instrument rooms

[3)] E.g. equipment in unclassified mechanically ventilated rooms

Equipment property library B.15: Fire and gas detectors – HC gas detectors

Equipment description			**IRDI code** **CFIHOS**	**ISO 14224 reference/ other specified reference/ comment**
L1 (Equipment class): Fire and gas detectors			CFIHOS-30000640 <Detector general>	ISO 14224: Section A.2.5.1
L2 (Equipment type): HC gas detectors			CFIHOS-30000432 <Gas detector>	ISO 14224: Table A.68 CFIHOS does not distinguish between HC gas detectors and toxic gas detectors.
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**	NA	ISO 14224: Table A.70
DLOP	Sensing/measuring principle		CFIHOS-40000341	ISO 14224: Table A.70
		- Catalytic	CFIHOS-60000273	
		- IR	CFIHOS-60000644	
		- Open path	CFIHOS-60000896	
		- Ultrasonic (acoustic)	CFIHOS-60001310	
	Design principle	- Point		ISO 14224: Table A.70 Design principle to some degree covered by sensing principle.
		- Line (open path)		
		- Aspirating		

Equipment property library B.16: Fire and gas detectors – Toxic gas detectors

Equipment description			**IRDI code** **CFIHOS**	**ISO 14224 reference/ other specified reference/ comment**
L1 (Equipment class): Fire and gas detectors			CFIHOS-30000640 (Detector general)	ISO 14224: Section A.2.5.1
L2 (Equipment type): Toxic gas detectors			CFIHOS-30000432 (Gas detector)	ISO 14224: Table A.68 CFIHOS does not distinguish between HC gas detectors and toxic gas detectors.
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**	NA	ISO 14224: Table A.70
DLOP	Sensing/measuring principle		CFIHOS-40000341	ISO 14224: Table A.70
		- Catalytic	CFIHOS-60000273	
		- Electrochemical	CFIHOS-60000439	
		- IR	CFIHOS-60000644	
		- Semiconductor (metal oxide)	CFIHOS-60001191	
OLOP	Function	- H_2S detector	CFIHOS-30000895	<Personal H_2S detector> CFIHOS link not (yet) functional
		- CO detector	Not found	
		- NH_3 detector	Not found	
		- Combined detector	Not found	

Equipment property library B.17: Fire and gas detectors – Other gas detectors

Equipment description			**IRDI code** **CFIHOS**	**ISO 14224 reference (or other specified reference) / comment**
L1 (Equipment class): Fire and gas detectors			CFIHOS-30000640 (Detector general)	ISO 14224: Section A.2.5.1
L2 (Equipment type): Other gas detectors			CFIHOS-30000432 (Gas detector)	ISO 14224: Table A.68 CFIHOS does not distinguish between different type of gas detectors.
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**	NA	ISO 14224: Table A.70
DLOP	Sensing/measuring principle		CFIHOS-40000341	ISO 14224: Table A.70
		- Catalytic	CFIHOS-60000273	
		- Electrochemical	CFIHOS-60000439	
		- IR	CFIHOS-60000644	
		- Conductivity	Not found	
OLOP	Function	- O_2 detector	Not found	
		- O_2 analyser	Not found	
		- H_2 detector	Not found	
		- Oil mist detector	Not found	
		- Combined detector	Not found	

Equipment property library B.18: Fire and gas detectors – smoke detectors

Equipment description			IRDI code CFIHOS	ISO 14224 reference/ other specified reference/ comment
L1 (Equipment class): Fire and gas detectors			CFIHOS-30000640 (Detector general)	ISO 14224: Section A.2.5.1
L2 (Equipment type): Smoke detectors			CFIHOS-30000470	ISO 14224: Table A.68
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**	NA	ISO 14224: Table A.70
DLOP	Sensing/measuring principle		CFIHOS-40000341	ISO 14224: Table A.70
		- Ionization	CFIHOS-60000654	
		- IR	CFIHOS-60000643	
		- Optical	CFIHOS-60000898	
		- Photoelectric	CFIHOS-60000946	
	Design principle	- Standard smoke detector	CFIHOS-30000470	ISO 14224: Table A.70
		- Aspirating smoke detector - conventional w/ air sampling	Not found	
		- Aspirating smoke detector - integrated early warning w/ air sampling	Not found	
		- Multidetector smoke/heat	CFIHOS-30000082	

Equipment property library B.19: Fire and gas detectors – heat detectors

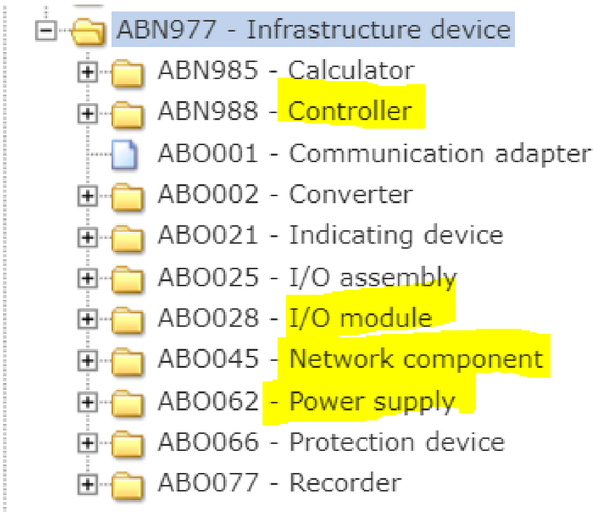
Equipment description			**IRDI code** **CFIHOS**	**ISO 14224 reference/ other specified reference/ comment**
L1 (Equipment class): Fire and gas detectors			CFIHOS-30000640 (Detector general)	ISO 14224: Section A.2.5.1
L2 (Equipment type): Heat detectors			No CFIHOS ref. found RDL/RDS2229121 RDL/RDS477089	ISO 14224: Table A.68
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**	NA	ISO 14224: Table A.70
DLOP	Sensing/measuring principle	- Rate of rise	CFIHOS-60001037	ISO 14224: Table A.70
		- Fixed temperature (rate compensated)	CFIHOS-60001036	
		- Combined (heat and smoke)	CFIHOS-30000082	

Equipment property library B.20: Fire and gas detectors – flame detectors

Equipment description			**IRDI code** **CFIHOS**	**ISO 14224 reference/ other specified reference/ comment**
L1 (Equipment class): Fire and gas detectors			CFIHOS-30000640 (Detector general)	ISO 14224: Section A.2.5.1
L2 (Equipment type): Flame detectors			CFIHOS-30000425	ISO 14224: Table A.68
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**	NA	ISO 14224: Table A.70
DLOP	Sensing/measuring principle		CFIHOS-40000341	ISO 14224: Table A.70
		- Multi-spectrum IR	CFIHOS-60000643 (Infrared – general)	
		- Single frequency IR		
		- Single frequency UV	CFIHOS-60001311 (Ultraviolet- general)	
		- Multi-spectrum UV/IR		
		- Visual flame imaging (camera/video/pixel)	CFIHOS-60000262	

B.3 Logic solvers and interface elements ("Control logic units")

The IEC 61987 CDD has defined an equipment group named "infrastructure device", and hereunder some sub-categories seem of particular relevance. See figure below:



- ABN977 - Infrastructure device
  - ABN985 - Calculator
  - ABN988 - Controller
  - ABO001 - Communication adapter
  - ABO002 - Converter
  - ABO021 - Indicating device
  - ABO025 - I/O assembly
  - ABO028 - I/O module
  - ABO045 - Network component
  - ABO062 - Power supply
  - ABO066 - Protection device
  - ABO077 - Recorder

A supplementary source of data dictionary is the online ISO 15926 (http://data.15926.org/rdl/), in particular filtered with CFIHOS to circle out those developed for the process sector. Entries and codes from this dictionary are only added in case the same equipment or property is not covered by the IEC 61987 CDD.

Section A.2.5.3 in ISO 14224 deals with Control logic units (CLUs), but on a rather overall level and with potential for more detailing.

B.3.1 Logic solvers

Equipment property library B.21 lists properties sufficient to identify different types of controllers, their safety and diagnostic attributes and application. Some additional remarks:

- HFT will be an important configuration property due to a high number of variants and ways of naming *KooN* architectures, also considering incorporation of diagnostics and the realisation of hot and passive redundancy. HFT will however appear under safety list of properties (SLOP), see discussion in section 2.5. At the device level, the configuration is an internal property of a compounded product.
- "Mode of operation" (low demand, continuous demand or high demand) and diagnostic coverage (#ABB170#001) will be other relevant properties that will also appear under SLOPs.

Equipment property library B.21: Logic solvers

Equipment description			**IRDI code** **(IEC 61987 CDD)** 0112/2///61987#....... **CFIHOS**	**ISO 14224 reference/** **other specified reference/** **comment**
L1 (Equipment class): Logic solvers and interface elements			ABN977 <Infrastructure device>	ISO 14224: Section A.2.5.3
L2 (Equipment type): Logic solvers / Controllers			ABN988 < Controller>	ISO 14224: Table A.74, Table A.75
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**		(ISO 14224: Table A.76)
DLOP	Device type	- Non-safety certified		<SIL system/subsystem> Value list Type A, type B, other
		- Safety certified – programmable		
		- Safety certified – hardwired		
		- Fire central		
	Internal diagnostic / self-test feature	- Temperature monitoring		Between controllers Relevant for hardwired signal
		- Internal self-test		
		- Watchdog		
		- Line monitoring	ABC321	
		- Combined [1]		
OLOP	Application	- ESD	CFIHOS-60001771	This property may not impact reliability as such, but is nevertheless an important classification property Note that the CHIFOS id. relates to *loop application* and is therefore listed under application (no parallel found in IEC 61987)
		- PSD	CFIHOS-60001772	
		- F&G		
		- PCS	CFIHOS-60001770	
		- Unit control (Equipment monitoring/protection)	CFIHOS-60001776	
	External exposure	- Indoor cabinet		
		- Outdoor cabinet		

General note: <*Name*> indicates preferred name in IEC 61987 CDD

[1] Select 'combined' if possibility for multichoice not available/possible

B.3.2 I/O modules

Equipment property library B.22 identifies various I/O modules and interfacing devices, but do not distinguish safety from non-safety application. It is suggested to include device properties for safety and non-safety applications at controller level, following the practise of CDD.

As for controllers, important properties such as HFT, mode of operation and DC are included under SLOPs, see section 2.5.

Equipment property library B.22: I/O modules

Equipment description			**IRDI code (IEC 61987 CDD)** 0112/2///61987#....... **CFIHOS**	**ISO 14224 reference/ other specified reference/ comment**
L1 (Equipment class): Logic solvers and interface elements			ABN977 <Infrastructure device>	ISO 14224: Section A.2.5.3
L2 (Equipment type): I/O module			ABO028 <I/O module>	ISO 14224: Table A.74, Table A.75
Property category	**Type of reliability influencing properties (L3)**	Table A.76	NA	(ISO 14224: A.76)
DLOP	Device type	- Analogue input	ABO030	<Analog input module>
		- Digital input	ABO031	<Discrete input module>
		- Digital output	ABO037	<Discrete output module>
		- Input/output module	ABO041	<Input/output module>
		- Intrinsic safety isolator (galvanic)	ABO068	<Isolated barrier>
		- Zener barrier	ABO069	<Zener barrier>
		- Trip amplifiers	ABA415	<Switching current difference>
	Internal diagnostic / self-test feature	- Internal self-test	ABC189	<Device diagnostic>
		- Line monitoring	ABP077	<line fault monitoring>
		- Temperature limitations		
		- Combined [1)]		
OLOP	Application	- ESD	CFIHOS-60001771	Note that this property may not impact reliability as such but is nevertheless an important classification property The CHIFOS id. relates to *loop application* and is therefore listed under application (no parallel found in IEC 61987)
		- PSD	CFIHOS-60001772	
		- F&G		
		- PCS	CFIHOS-60001770	
		- Unit control (Equipment monitoring/protection)	CFIHOS-60001776	

General note: <*Name*> indicates preferred name in IEC 61987 CDD

[1)] Select 'combined' if possibility for multichoice not available/possible

B.3.3 Communication/network modules/power supply

Equipment property library B.23 identifies a list of the most important network components. The devices are the same for safety and non-safety applications. As application, it is proposed to identify at which level of the ANSI/ISA-95 levels (Purdue reference architecture) the equipment is applied, however limited to those levels that are within the boundaries of OT-systems.

Equipment property library B.23: communication/network modules

Equipment description			**IRDI code** **(IEC 61987 CDD)** 0112/2///61987#....... **CFIHOS**	**ISO 14224 reference/** **other specified reference/** **comment**
L1 (Equipment class): Logic solvers and interface elements			ABN977 <Infrastructure device>	ISO 14224: Section A.2.5.3
L2 (Equipment type): Communication/network modules			ABO045 <Network component>	(ISO 14224: Table A.75)
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**	NA	
DLOP	Device type	- Gateway	ABO049	
		- Hub	ABO052	
		- Router	ABO055	
		- Switch	ABO056	
		- Wireless access point	ABO060	
OLOP	Application	- Level 0-2		ANSI/ISA-95 levels (Purdue reference architecture)
		- Level 3		
		- Level 3.5 DMZ		

General note: <*Name*> indicates preferred name in IEC 61987 CDD

Equipment property library B.24 identifies a list of the most important power supply types. The devices are the same for safety and non-safety applications.

Equipment property library B.24: Power supply

Equipment description			IRDI code (IEC 61987 CDD) 0112/2///61987#.......	ISO 14224 reference/ other specified reference/ comment
L1 (Equipment class): Logic solvers and interface elements			ABN977 <Infrastructure device>	Section A.2.5.3
L2 (Equipment type): Power supply			ABO062 <Power supply>	Table A.75
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**	NA	
DLOP	Device type	- Fieldbus power supply	ABO063	
		- Transmitter power supply	ABO064	
		- General purpose power supply	ABO065	
OLOP	Application	- ESD	CFIHOS-60001771	Note that this property may not impact reliability as such but is nevertheless an important classification property. The CHIFOS id. relates to *loop application* and is therefore listed under application (no parallel found in IEC 61987)
		- PSD	CFIHOS-60001772	
		- F&G		
		- PCS	CFIHOS-60001770	
		- Unit control (Equipment monitoring/protection)	CFIHOS-60001776	

B.4 Valves

This section covers the following categories of valves:

- Topside process ESVs and XVs
- Riser ESV
- Topside XT valves
- Topside HIPPS valves
- Blowdown valves
- Fast opening valves
- Solenoid valves
- Pressure relief valves (PSV)
- Deluge valves
- Fire water monitor valves
- Water mist valves
- Sprinkler valves
- Foam valves
- Ballast water valves
- Other valves and valve arrangements

For valves, the operators have some differing practices with respect to how they are categorised in the maintenance system. All operators seem to have valves as an equipment class at level 1. However, at level 2 (equipment type), most operators have a functional breakdown comparable to the one shown in the bullet list above, whereas some operators follow ISO 14224 more strictly, and have design principle (see Table A.77 in ISO 14224) with Ball, Gate, Globe, Butterfly etc. at level 2.

To compensate for these varying practices, one *common equipment property library* that shall cover all valve categories are therefore suggested as shown in Equipment property library B.25.

It should be noted that the IEC 61987 CDD for the equipment category "*Control valve or automated on/off-valve*" makes a split between valve body, actuator and valve/actuator accessories. This may be more in line with manufacturer thinking but is not directly compatible with how operational follow-up of valves is done in practice. This explicit equipment split has therefore not been complied with here.

Also note that both IEC 61987 CDD and CFIHOS seem to denote actuated valves as "control valve", with the meaning that the valve can regulate and even close off the fluid flow. Hence, control valve here includes more than a "control system valve" but also emergency shutdown valves, blowdown valves, etc.

Equipment property library B.25: Valves – all valves

Equipment description			**IRDI code** **(IEC 61987 CDD)** 0112/2///61987#.... **CFIHOS ref.**	**ISO 14224 reference/** **other specified reference/ comment**
L1 (Equipment class): Valves			ABD341	ISO 14224: Section A.2.5.4
L2 (Equipment type): NA – All valves			NA	
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**	DLOP: ABV504 OLOP: ABV503 (General DLOP and OLOP codes)	ISO 14224: Table A.79 DLOPs are given for specific valve designs such as globe (ABE311), ball (ABE317), gate (ABE312), butterfly (ABE314), etc. OLOP ABE307 applies for valve body assembly whereas OLOP ABE308 applies for valve/ actuator accessories
DLOP	Design principle	- Globe	ABD344 CFIHOS-30000839	ISO 14224: Table A.77
		- Gate	ABD345 CFIHOS-30000837	
		- Diaphragm/pinch	ABD346 CFIHOS-30000817	
		- Eccentric plug	ABD348 CFIHOS-30000824	
		- Ball	ABD349 CFIHOS-30000806	
		- Plug	ABD351 CFIHOS-30000859	
		- Butterfly	ABD352 CFIHOS-30000809	
		- Multiple orifice (blowdown)	CFIHOS-30000635	
		- Needle	CFIHOS-30000851	
		- Check	CFIHOS-30000636	
		- Relief valve (PSV) – spring operated	CFIHOS-30000815	
		- PSV – pilot operated	CFIHOS-30000856	
		- PSV – pressure vacuum	CFIHOS-30000861	
		- PSV – rupture (buckling) pin	RDL/RDS2228921	
		- Solenoid valve	ABD371 SCFIHOS-30000681	
		- Pilot valve	ABN159	
		- Quick exhaust valve	ABD380	
		- Axial flow		
		- Sleeve		
		- Double chamber		
		- Flapper (flap) valve		
	Device type	- Process isolation valve	CFIHOS-30000642	<Emergency shut down valve>

Equipment description			IRDI code (IEC 61987 CDD) 0112/2///61987#.... CFIHOS ref.	ISO 14224 reference/ other specified reference/ comment
L1 (Equipment class): Valves			ABD341	ISO 14224: Section A.2.5.4
L2 (Equipment type): NA – All valves			NA	
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**	DLOP: ABV504 OLOP: ABV503 (General DLOP and OLOP codes)	ISO 14224: Table A.79 DLOPs are given for specific valve designs such as globe (ABE311), ball (ABE317), gate (ABE312), butterfly (ABE314), etc. OLOP ABE307 applies for valve body assembly whereas OLOP ABE308 applies for valve/ actuator accessories
		- Riser isolation valve	CFIHOS-30000642	<Emergency shut down valve>
		- X-mas tree master valve	RDL/RDS16552776	<production master valve>
		- X-mas tree wing valve	RDL/RDS16552864	<production wing valve>
		- X-mas tree XO-valve	RDL/RDS16553103	<crossover valve>
		- X-mas tree CI-valve	RDL/RDS16551664	<chemical injection valve>
		- Offloading isolation valve		Note that CFIHOS has defined <Christmas tree>, but not separate valves, see CFIHOS-30000494
		- Pipeline isolation valve		
		- Blowdown valve		
		- FOV in closed flare [1)]		
		- Ballast valve		
		- Deluge valve	CFIHOS-30000639	
		- Fire water monitor valve		
		- Water mist valve		
		- Sprinkler valve		
		- Foam valve		
		- Gaseous agent valve		
		- Pressure relief valve	CFIHOS-30000295	
		- HPU Bleed-off valve		
	Actuation principle			ISO 14224: Table A.79
		- Electric	ABD355 / ABD361	Linear / rotary
		- Hydraulic	ABD357 / ABD363	Linear / rotary
		- Pneumatic	ABD356 / ABD365	Linear / rotary
		- Electro-hydraulic	ABD358 / ABD362	Linear / rotary
	Valve dimension	- 0–1"		ISO 14224: Table A.79
		- 1–3"		
		- 3–18"		
		- > 18"		
OLOP	Fluid handled/ severity [2)]		CFIHOS-50000051	ISO 14224: Table A.79 and APOS specific definitions CFIHOS id. relates to fluid (not severity in particular)
		- Clean/benign service		
		- Medium/moderate service		
		- Dirty/severe service		
	Application	- ESD (emergency shutdown)	CFIHOS-60001771	

Equipment description			**IRDI code** **(IEC 61987 CDD)** 0112/2///61987#.... **CFIHOS ref.**	**ISO 14224 reference/** **other specified reference/ comment**
L1 (Equipment class): Valves			ABD341	ISO 14224: Section A.2.5.4
L2 (Equipment type): NA – All valves			NA	
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**	DLOP: ABV504 OLOP: ABV503 (General DLOP and OLOP codes)	ISO 14224: Table A.79 DLOPs are given for specific valve designs such as globe (ABE311), ball (ABE317), gate (ABE312), butterfly (ABE314), etc. OLOP ABE307 applies for valve body assembly whereas OLOP ABE308 applies for valve/ actuator accessories
		- PSD (process shutdown)	CFIHOS-60001772	The CHIFOS id. relates to *loop application* and is therefore listed under application (no parallel found in IEC 61987) Note that blowdown valves are sometimes categorised together with ESD valves, but should be identified separately for the purpose of e.g. data collection.
		- EDP (blowdown)	CFIHOS-60001775	
		- PCS (process control)	CFIHOS-60001770	
		- Combined ESD/PSD [3]		
		- Combined ESD/PSD/PCS [3]		
		- Combined PSD/PCS [3]		
		- HIPPS		
		- PPS [4]		

[1] Fast opening valve (FOV). Large valve (20-24 inch), with very short response times (2-3 seconds) and with high demand.

[2] See definition in Appendix A, Table A-1

[3] Separate ESD/PSD/PCS solenoids

[4] Pipeline protection system, often combined with ESD

B.5 Nozzles

The following relevant nozzle types have been identified:

- Deluge nozzles
- Water mist nozzles
- Sprinkler nozzles
- Gaseous agent nozzles

Properties common for all nozzles have been listed in Equipment property library B.26. At this stage it has been found sufficient to have one common property table.

Nozzles are briefly mentioned in IEC 61987 and somewhat more detailed out in ISO 15926.

Equipment property library B.26: Nozzles – common properties

Equipment description			**IRDI code** **(IEC 61987 CDD)** 0112/2///61987#....... **CFIHOS / RDL**	**ISO 14224 reference/** **other specified reference/** **comment**
L1 (Equipment class): Nozzles [1]			(ABA886) CFIHOS-30000495	ISO 14224 Section A.2.5.5, ISO 14224 Equipment class code: NO It has been commented by APOS project members that ABA866 is mainly used for instrument. For general nozzle ISO 15926 /CFIHOS should be used.
L2 (Equipment type): NA (generic for all nozzles)			NA	
Property category	**Type of reliability influencing properties (L3) [2]**	**Possible property values**		ISO 14224 Table A.82
DLOP	Device type			ISO 14224 Table A.80 http://data.15926.org/rdl/RDS303794
		- Deluge nozzle	rdl/RDS458009	
		- Water mist nozzle		
		- Sprinkler nozzle	rdl/RDS303029	
		- Gaseous agent nozzle (e.g., halon)	rdl/RDS303794	
	Design principle	- High velocity		ISO 14224 Table A.82
		- Medium velocity		
		- High pressure		
		- Low pressure		
OLOP	Fluid handled/ severity	- Clean (potable water, …)		ISO 14224 Table A.82
		- Medium (sea water, …)		

[1] It has been commented by APOS project members that nozzles are normally followed up on system level and not individually. E.g., that fail/pass criterion is related to percentage of dense nozzles.

[2] It has further been commented that the material quality of the nozzle distribution piping is an important reliability influencing property (e.g., a higher nozzle failure frequency where distribution piping is still in carbon steel).

B.6 Fire-fighting equipment

The following equipment is included:

- Fire water monitors
- Foam mixture
- Fire water pump drive system

Note that fire water pumps, including fire water lift pumps and booster pumps, have been included in the next section under pumps.

B.6.1 Fire water monitors

Relevant properties for fire water monitors are given in Equipment property library B.27.

Equipment property library B.27: Fire-fighting equipment – fire water monitors

Equipment description			**IRDI code** **CFIHOS**	**ISO 14224 reference/ other specified reference/ comment**
L1 (Equipment class): Fire-fighting equipment			CFIHOS-30000313	ISO 14224 Equipment class code: FF NB! CFIHOS link refers to <health, safety and environment equipment class> which is superclass for <firewater monitor>
L2 (Equipment type): Fire water monitors			CFIHOS-30000054 rdl/RDS301319	<Firewater monitor>
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**		NA
	Design principle	- Fixed		NA
		- Self-oscillating (pre-set)		
		- Oscillating – remotely operated ("joystick")		
	Actuation principle	- Electrical		NA
		- Hydraulic		
		- Manual		
OLOP	Fluid handled/ severity	- Fresh water		NA
		- Sea water		
		- Foam/water mixture		

B.6.2 Foam mixture

Relevant properties for foam mixtures are given in Equipment property library B.28.

Equipment property library B.28: Fire-fighting equipment – foam mixture

Equipment description			**IRDI code** **CFIHOS**	**ISO 14224 reference/ other specified reference/ comment**
L1 (Equipment class): Fire-fighting equipment				ISO 14224 Equipment class code: FF
L2 (Equipment type): Foam mixture				NA
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**		NA
DLOP	Design principle	- Turbine		NA
		- Venture		
		- Balanced foam proportioner		
		- Constant flow valves		

B.6.3 Fire water pump drive systems

The following categories of fire water pump drive systems are included:

- Diesel electric
- Diesel hydraulic
- Diesel mechanical

Relevant properties for these drive systems are given in Equipment property library B.29.

Equipment property library B.29: Fire-fighting equipment – fire water pump drive system

Equipment description			**IRDI code** **CFIHOS/RDL**	**ISO 14224 reference/ other specified reference/ comment**
L1 (Equipment class): Fire-fighting equipment				ISO 14224 Equipment class code: FF
L2 (Equipment type): Fire water pump drive system				NA
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**		NA
DLOP	Mounting principle	- Dry mounted		NA
		- Submerged engine		
	Configuration	- Diesel electric [1)]		NA
		- Diesel hydraulic [2)]		
		- Diesel mechanical [3)]		

[1)] Comprising diesel engine, electric generator, and electric motor (and fire water pump).

[2)] Comprising diesel engine, hydraulic pump, and hydraulic motor (in addition to fire water lift pump and fire water booster pump).

[3)] Comprising diesel engine (in addition to fire water pump).

B.7 Pumps

The following relevant types of pumps have been identified:

- Fire water pump
- Fire water lift pump
- Fire water booster pump
- Water mist pump
- Foam pump
- Ballast water pumps
- Offloading pumps
- Bilge pumps
- Low voltage miscellaneous pumps

Properties common for all these pumps have been listed in Equipment property library B.30.

Equipment property library B.30: Pumps – miscellaneous pumps (common properties)

Equipment description			IRDI code CFIHOS/RDL	ISO 14224 reference/ other reference/ comment
L1 (Equipment class): Pumps			CFIHOS-30000550 rdl/RDS327239	ISO 14224 section A.2.2.6 ISO 14224 Equipment class code: PU
L2 (Equipment type): Miscellaneous pumps				NA
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**		ISO 14224 Table A.22
DLOP	Mounting principle	- Dry mounted		CFIHOS-40000561 describes *orientation* (including submerged)
		- Submerged pump	rdl/RDS312299	
	Design principle	- Centrifugal	CFIHOS-30000521	ISO 14224 Table A.20
		- Reciprocating	CFIHOS-30000862	
		- Rotary	CFIHOS-30000864	
OLOP	Fluid handled/ severity [1]		CFIHOS-50000051	ISO 14224: Table A.22 and APOS specific definitions CFIHOS id. relates to fluid (not severity in particular)
		- Clean/benign service		
		- medium/moderate service		
		- dirty/severe service		
	Function [2]	- Fire water main supply	rdl/RDS12958186	<firefighting pump>
		- Fire water lift	rdl/RDS12957646	<seawater lift pump>
		- Fire water booster		
		- Water mist supply		
		- Foam supply		
		- Ballasting [3]		
		- Offloading		
		- Bilge/drainage	rdl/RDS12958141	<drainage pump>

[1] Categories / property values need further specification/definition (includes fresh water, sea water, foam liquid, etc.)

[2] It is considered a matter of preference whether this division should be related to the function-property (as is suggested here), or alternatively as the device-type-property (ref. bullet list in start of this section).

[3] Start and stop functionality. Start of ballast pumps requires UPS power (and main electric supply) and operation of ballast valves. Stop functionality includes circuit breakers to stop pump and operation of ballast valves.

B.8 HVAC dampers

Two main types of dampers have been considered here:

- Fire dampers
- Shut-off dampers

Properties common for the dampers have been listed in Equipment property library B.31. At this stage this has been found to be a sufficient level of detail.

Equipment property library B.31: Fire and gas dampers – common properties

Equipment description			**IRDI code CFIHOS/RDL**	**ISO 14224 reference/ other specified reference/ comment**
L1 (Equipment class): Fire and gas dampers				NA (no separate equipment class or type in ISO 14224)
L2 (Equipment type): NA (generic for all dampers)				
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**		
DLOP	Device type [1]	Fire damper	CFIHOS-30000049 rdl/RDS414314	
		- Gas tight (shut off) damper	CFIHOS-30000232 rdl/RDS414359	
		- Combined fire and gas tight damper		
	Actuation principle	- Pneumatic	rdl/RDS7159829	<pneumatic fire damper> Based on alternatives described in ISO-15138
		- Electric		
		- Manual		
	Dimension	- Length/width of damper (cm/cm)		It has been commented by APOS project members that number of shafts and blades is an important RIP, but this is implicitly covered by length/width.
OLOP	External exposure	- High/severe [2]		
		- Medium/moderate [3]		
		- Low/shielded [4]		
	Application	- F&G		This property will also be given by specified "Device type" since fire dampers will be linked to F&G, Shut-off dampers will be linked to HVAC, etc.
		- HVAC		
		- Combined F&G and HVAC [5]		

[1] In addition, fire class (A0 or A60) and density/tightness class should be specified for fire dampers and gas tight dampers respectively

[2] E.g. equipment in classified areas, outdoor and naturally ventilated rooms

[3] E.g. equipment in high exposure areas but with weather protection, inside containers or instrument rooms

[4] E.g. equipment in unclassified mechanically ventilated rooms

[5] With separate solenoids for F&G and for HVAC

B.9 Electric generators

Only emergency generators are included in this equipment class. Relevant properties are listed in Equipment property library B.32.

Equipment property library B.32: Electric generators – emergency generator

Equipment description			**IRDI code** **(IEC 62683 CDD)** 0112/2///61987#....... **CFIHOS/RDL**	**ISO 14224 reference/** **other specified reference/ comment**
L1 (Equipment class): Electric generators			CFIHOS-30000338 rdl/RDS415709	ISO 14224 A.2.2.3 ISO 14224 Equipment class code: EG
L2 (Equipment type): Emergency generators				NA
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**		ISO 14224 Table A.13
	Design principle	- Low voltage	rdl/RDS431679060	ISO 14224 Table A.13
		- Medium voltage	rdl/RDS408284	
		- High voltage	rdl/RDS408239	
	Configuration	- Internal combustion engine	rdl/RDS433889	ISO 14224 Table A.11
		- External electric drive		

B.10 Combustion engines

Two relevant types of combustion engines have been identified:

- Lifeboat engines
- MOB-boat engines

Relevant properties are listed in Equipment property library B.33.

Equipment property library B.33: Combustion engines – Lifeboat and MOB-boat engines

Equipment description			**IRDI code** **CFIHOS/RDL**	**ISO 14224 reference/** **other specified reference/ comment**
L1 (Equipment class): Combustion engines			rdl/RDS1083734	ISO 14224 A.2.2.1 ISO 14224 Equipment class code: CE
L2 (Equipment type): Lifeboat and MOB-boat engines				NA
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**		ISO 14224 Table A.7
	Device type	- Lifeboat engine		NA [1]
		- MOB-boat engine		
		-		
	Design principle	- Diesel engine	rdl/RDS421154	ISO 14224 Table A.5
		- Gas (Otto) engine	rdl/RDS433934	

[1] Note that in ISO 14224 these engines have been categorised under " Evacuation, escape and rescue".

B.11 Uninterruptible power supply (UPS)

Relevant properties are listed in Equipment property library B.34

Equipment property library B.34: Uninterruptible power supply – UPS and battery packages

Equipment description			**IRDI code** **CFIHOS/RDL**	**ISO 14224 reference/ other specified reference/ comment**
L1 (Equipment class): Uninterruptible power supply			rdl/RDS874754	ISO 14224 A.2.4.1 ISO 14224 Equipment class code: UP
L2 (Equipment type): UPS and battery packages				NA
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**		ISO 14224 Table A.58
DLOP	Design principle	- Low voltage	rdl/RDS431679060	ISO 14224 Table A.58
		- Medium voltage	rdl/RDS408284	
		- High voltage	rdl/RDS408239	
	Configuration	- Dual UPS with standby bypass		ISO 14224 Table A.56
		- Dual UPS without bypass		
		- Single UPS with bypass		
		- Single UPS without bypass		

B.12 Switchgear

The following types of switchgear components are included:

- Circuit breakers
- Contactors
- Relays

Relevant properties are listed in Equipment property library B.35. At this stage one common table is considered a sufficient level of detail.

Equipment property library B.35: Switchgear – common properties

Equipment description			**IRDI code** **(IEC 62683 CDD)** 0112/2///62683#....... **CFIHOS/RDL**	**ISO 14224 reference/** **other specified reference/ comment**
L1 (Equipment class): Switchgear			ACC001 CFIHOS-30000370 rdl/RDS464084	A.2.4.3 ISO 14224 Equipment class code: SG
L2 (Equipment type): Circuit breakers, relays and contactors (common properties)				-
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**		Table A.64
DLOP	Device type	- Circuit breakers	ACC201 CFIHOS-30000323	Table A.63
		- Contactor	CFIHOS-30000326	
		- Relays	CFIHOS-30000364	
	Design principle	- Low voltage	rdl/RDS431679060	Table A.62
		- Medium voltage	rdl/RDS408284	
		- High voltage	rdl/RDS408239	
	Configuration	- External supply of energy to latch		
		- Internally stored energy (spring force) to latch		

B.13 Escape, rescue, and evacuation

Initial property libraries are established for the following equipment:

- Fire doors
- Watertight doors
- Emergency lights

In addition, property libraries are not yet developed for MOB-boats, escape chutes and escape chute release systems.

B.13.1 Fire doors (fire rated door set)

Relevant properties for fire doors are listed in Equipment property library B.36.

Equipment property library B.36: Escape, rescue, and evacuation – fire doors

Equipment description			**IRDI code** **CFIHOS/RDL/NOR**	**ISO 14224 reference/** **other specified reference/ comment**
L1 (Equipment class): Escape, rescue, and evacuation				ISO 14224 Equipment class code: ER
L2 (Equipment type): Fire doors			CFIHOS-30000050 rdl/RDS8352120	<fire door> <fire rated door set> Also see NORSOK C-002:2015
Property category	**Type of reliability influencing properties (L3)**	**Possible property values**		
DLOP	Design principle	- Hinged door		
		- Sliding door		
	Device type [1]	- A30	nor/RDS8352210	<FIRE RATED DOOR SET NS 3919:1997 A30>
		- A60	nor/RDS8352255	<FIRE RATED DOOR SET NS 3919:1997 A60>
		- A120	nor/RDS8352165	<FIRE RATED DOOR SET NS 3919:1997 A120>
		- B15	nor/RDS8351940	<FIRE RATED DOOR SET NS 3919:1997 B15>
		- B30	nor/RDS8351580	<FIRE RATED DOOR SET NS 3919:1997 B30>
		- B60	nor/RDS8351625	<FIRE RATED DOOR SET NS 3919:1997 B60>
		- H0		
		- H60		
		- H120		
	Actuation principle	- Manual		
		- Actuated [2]		
	Configuration	- With personnel protection system [3]		
		- Without personnel protection system		

[1] Fire class will influence the weight and thus the closure mechanism.

[2] Actuated doors are normally open and will close upon signal.

[3] Which may prevent the door from going to safe state.

B.13.2 Watertight doors

Relevant properties for watertight doors are listed in Equipment property library B.36.

Equipment property library B.37: Escape, rescue, and evacuation – watertight doors

Equipment description			**IRDI code** **CFIHOS/RDL**	**ISO 14224 reference/** **other specified reference/ comment**
L1 (Equipment class): Escape, rescue, and evacuation				NA ISO 14224 Equipment class code: ER
L2 (Equipment type): Watertight doors				See NORSOK C-002:2015
Property category	**Type of reliability influencing properties (L3)**			
DLOP	Design principle	- Hinged door		
		- Sliding door		
	Device type [1]	- Tightness class (?)		
		[1]		
	Actuation principle	- Manually operated		
		- Actuated [2]		
	Configuration [3]	- With personnel protection system [3]		
		- Without personnel protection system		

[1] Tightness class *may influence the weight* and thus the closure mechanism. Other properties may need to be added.

[2] Actuated doors are normally open and will close upon signal

[3] To prevent accidental crushing of personnel (and which may prevent the door from going to safe state).

B.13.3 Emergency lights

Relevant properties for emergency lights are listed in Equipment property library B.38.

Equipment property library B.38: Escape, rescue, and evacuation – emergency lights

Equipment description			IRDI code CFIHOS/RDL	ISO 14224 reference/ other specified reference/ comment
L1 (Equipment class): Escape, rescue, and evacuation				ISO 14224 Equipment class code: ER
L2 (Equipment type): Emergency lights				
Property category	**Type of reliability influencing properties (L3)**			
DLOP	Device type	- Integrated battery		
		- Central battery bank		
OLOP	External exposure	- High/Severe [1]		
		- Medium/Moderate [2]		
		- Low/shielded [3]		

[1] E.g. emergency lights in outdoor and weather exposed areas

[2] E.g. emergency lights in exposed areas but with weather protection, inside containers or instrument rooms

[3] E.g. emergency lights in unclassified mechanically ventilated rooms

B.14 Emergency communication equipment

The following equipment types are included:

- PA loudspeakers and flashing beacons
- Telemetry systems
- Radios and telephones

B.14.1 PA loudspeakers and flashing beacons

Relevant properties for speakers and beacons are listed in Equipment property library B.39.

Equipment property library B.39: Emergency communication equipment – loudspeakers and beacons

Equipment description			IRDI code CFIHOS/RDL	ISO 14224 reference/ other specified reference/ comment
L1 (Equipment class): Emergency communication equipment				ISO 14224 Equipment class code: EC
L2 (Equipment type): Loudspeakers and beacons				
Property category	**Type of reliability influencing properties (L3)**			
DLOP	Device type	- PA loudspeakers	CFIHOS-30000436 rdl/RDS309464	<Loudspeaker> <Public address loudspeaker>
		- Flashing beacons [1]	rdl/RDS2224513	<Beacon>
OLOP	External exposure	- High/Severe [2]		
		- Medium/Moderate [3]		
		- Low/shielded [4]		

[1] Act as visual alarms in areas with high noise

[2] E.g. speaker located in outdoor and weather exposed areas

[3] E.g. speaker located in exposed areas but with weather protection, inside containers or instrument rooms

[4] E.g. speaker located in unclassified mechanically ventilated rooms

B.14.2 Telemetry systems

Relevant properties for telemetry systems are listed in Equipment property library B.40 (very incomplete).

Equipment property library B.40: Emergency communication equipment – telemetry systems

Equipment description			**IRDI code** **(IEC 61987 CDD)** 0112/2///61987#.......	**ISO 14224 reference/** **other specified reference/ comment**
L1 (Equipment class): Emergency communication systems				ISO 14224 Equipment class code: EC
L2 (Equipment type): Telemetry systems				
Property category	**Type of reliability influencing properties (L3)**			
DLOP	Design principles [1]	-		
		-		
OLOP	Function / application	- Pipeline protection		
		- Offloading		
		- Other		

[1] Relevant properties related to design principles must be defined.

B.14.3 Radios and telephones

Relevant properties for radios and telephones are listed in Equipment property library B.41.

Equipment property library B.41: Emergency communication equipment – radios and telephones

Equipment description			**IRDI code** **CFIHOS/RDL**	**ISO 14224 reference/** **other specified reference/ comment**
L1 (Equipment class): Emergency communication systems				ISO 14224 Equipment class code: EC
L2 (Equipment type): Radios and telephones			rdl/RDS13610435 CFIHOS-30000203 CFIHOS-30000371 rdl/RDS5779644	<radio> <radio transceiver> <telephone> <telephone>
Property category	**Type of reliability influencing properties (L3)**			-
DLOP	Device type	- Lifeboat radio		-
		- MOB-boat radio		
		- Field Ex. telephone		
OLOP		-		
		-		

B.15 Lifeboats

The following equipment is included:

- Lifeboats (free-fall and Davit launched)
- Lifeboat launch/release system

B.15.1 Free fall and Davit launched lifeboats

Relevant properties are listed in Equipment property library B.42.

Equipment property library B.42: Lifeboats – free fall and Davit launched

Equipment description			IRDI code CFIHOS/RDL	ISO 14224 reference/ other specified reference/ comment
L1 (Equipment class): Lifeboats			rdl/RDS11525462	ISO 14224 section A.2.5.6 ISO 14224 Equipment class code: LB
L2 (Equipment type): Free fall and davit launched lifeboats				
Property category	**Type of reliability influencing properties (L3)**			
DLOP	Design principle	- Free fall lifeboat	CFIHOS-60000520	
		- Davit launched lifeboat		
OLOP		-		
		-		

B.15.2 Lifeboat launch/release system

Relevant properties are listed in Equipment property library B.43.

Equipment property library B.43: Lifeboats – launch/release system

Equipment description			IRDI code CFIHOS/RDL	ISO 14224 reference/ other specified reference/ comment
L1 (Equipment class): Lifeboats			rdl/RDS11525462	ISO 14224 section A.2.5.6 ISO 14224 Equipment class code: LB
L2 (Equipment type): Lifeboat launch/release system				
Property category	**Type of reliability influencing properties (L3)**			
DLOP	Design principle	- Free fall lifeboat release system		
		- Davit launched lifeboat lowering system		
OLOP		-		
		-		
		-		

B.16 Subsea input devices

This section describes subsea located sensors and detectors, including:

- Subsea process sensors, including:
  - Pressure sensors
  - Temperature sensors
  - Combined pressure and temperature sensors
  - Flow sensors
- Subsea leak detectors
- Subsea sand detectors

In ISO 14224 subsea input devices are generally classified under "Subsea production control" as a maintainable item under the subunit "Subsea control module (SCM)". It is, however, noted under table A.87 that "*sensors inside the subunit Subsea control module (SCM) should not be mixed with those external at other subsea equipment*".

Note that the *physical location* of the sensor will be an important property which will be specified under additional general properties and "Equipment ID and references", see section 2.5 and Appendix . The following subsea sensor locations are typically relevant:

- Subsea control module (SCM)
- Subsea template/ manifold
- Xmas tree / wellhead
- Subsea processing equipment (pumps, etc.)
- Downhole
- Pipelines
- Riser base

Note that neither IEC 61987 nor other CDDs include references to subsea equipment. Hence the ISO 15926 libraries are referenced.

Also note that the equipment property tables, and property descriptions given for subsea sensors (and other subsea equipment) are incomplete and need further detailing. E.g., it may be considered whether it is necessary to have separate tables for the different subsea process sensor types since e.g., sensing/ measuring principle can differ.

B.16.1 Subsea process sensors

In Equipment property library B.44 some properties for subsea process sensors are listed.

Equipment property library B.44: Subsea input devices – subsea process sensors

Equipment description			IRDI code CFIHOS/RDL	ISO 14224 reference/ other specified reference/ comment
L1 (Equipment class): Subsea input devices				ISO 14224 section A.2.6.1 ISO 14224 Equipment class code: CS
L2 (Equipment type): Subsea process sensors				ISO 14224 Table A.87
Property Category	**Type of reliability influencing properties (L3)**	**Possible property values**		
DLOP	Sensing/measuring principle [1]	- Force-balance (PT)		
		- Thermocouple (TT)		
	Device type [2]	- Pressure sensor		
		- Temperature sensors		
		- Combined pressure and temperature sensor		
		- Flow sensor		
OLOP	Fluid handled/ severity	- Clean/benign service		Must be further defined for subsea applications
		- Medium/moderate service		
		- Dirty/severe service		
	Application	- PSD		It has been commented that this property does not impact reliability as such but is nevertheless an important classification property
		- ESD		
		- HIPPS		
		- PCS		

[1] Other relevant properties for sensing principle may need to be added.

[2] Other device types may need to be added.

B.16.2 Subsea leak detectors

Properties for subsea leak detectors are given in Equipment property library B.45.

Equipment property library B.45: Subsea input devices – subsea leak detectors

Equipment description			**IRDI code** **CFIHOS/RDL**	**ISO 14224 reference/ other specified reference/ comment**
L1 (Equipment class): Subsea input devices				ISO 14224 A.2.5.6 ISO 14224 Equipment class code: CS
L2 (Equipment type): Subsea leak detectors				
Property Category	**Type of reliability influencing properties (L3)**	**Possible property values**		
DLOP	Sensing/measuring principle	- Capacitive detectors (with "collector")		
		- Ultrasonic non-intrusive acoustic leak monitors		
		- Passive acoustic leak detector		
		- Optical methods		
		- Bio sensor methods		
OLOP	Application	- ESD		
		- PSD		
		- Combined ESD/PSD		
		- Monitoring		

B.16.3 Subsea sand detectors

Properties for subsea sand detectors are given in Equipment property library B.46.

Equipment property library B.46: Subsea input devices – subsea sand detectors

Equipment description			**IRDI code** **CFIHOS/RDL**	**ISO 14224 reference/ other specified reference/ comment**
L1 (Equipment class): Subsea input devices				A.2.5.6 ISO 14224 Equipment class code: CS
L2 (Equipment type): Subsea sand detectors			CFIHOS-30000243	<sand detector> (whether topside or subsea unspecified)
Property Category	**Type of reliability influencing properties (L3)**	**Possible property values**		
DLOP	Mounting principle	- Intrusive		
		- Non-intrusive		
	Sensing / measuring principle	- Erosion/electric based		
		- Acoustic based	rdl/RDS16757717	<acoustic sand detector> (whether topside or subsea unspecified)
OLOP		-		
		-		

B.17 Subsea production control (TBD)

This section includes the following equipment:

- Master control station (MCS)
- Umbilical hydraulic / chemical line
- Umbilical power / signal line
- SEM – subsea electronic module

Relevant CFIHOS tag or equipment classes include:
CFIHOS-30000736 <subsea control module>
CFIHOS-30000679 <subsea distribution unit>
CFIHOS-30000713 <subsea distributed temperature sensing fiber optic pod>
CFIHOS-30000725 <subsea umbilical>

And additional relevant RDL refences include:
rdl/RDS16700516 <subsea electronic module> (SEM)
rdl/RDS1299022591 <electrical subsea power unit>

Note that equipment property libraries are not yet developed for these equipment types.

B.18 Subsea valves

This section includes the following subsea located valves:

- Subsea Xmas tree isolation valves
- Subsea manifold and flowline isolation valves
- Subsea pipeline and riser valves
- Solenoid control valves

Common properties for subsea valves are described in Equipment property library B.47. *Note that it may be considered (as for topside valves) to describe all relevant subsea valve properties in one common table.*

Equipment property library B.47: Subsea valves – common properties

Equipment description			**IRDI code** **CFIHOS/RDL**	**ISO 14224 reference/ other specified reference/ comment**
L1 (Equipment class): Subsea valves				ISO 14224 reference: NA [1)]
L2 (Equipment type): NA (general for subsea valves)				
Property Category	**Type of reliability influencing properties (L3)**	**Possible property values**		See Equipment property library B.25 (valves) for references to CDD and CFIHOS for relevant valve properties (not specified whether topside or subsea).
DLOP	Design principle	- Gate valve		
		- Ball valve		
		- Butterfly valve		
		- Flapper valve		
		- Solenoid valve		
		- Check valve		
	Actuation principle	- Hydraulic		
		- Electric		
		- Electro-hydraulic		
		- ROV operated		
	Dimension	- 0–1"		
		- 1–3"		
		- 3–18"		
		- > 18"		
OLOP	Fluid handled / severity	- Clean/benign service		
		- Medium/moderate service		
		- Dirty/severe service		
	Application	- PSD	CFIHOS-60001771	
		- ESD	CFIHOS-60001772	
		- Combined ESD/PSD		
		- HIPPS		

[1)] Subsea valves are listed as maintainable items under different ISO 14224 equipment classes (see tables below).

B.18.1 Subsea Xmas tree isolation valves

Properties for subsea Xmas tree isolation valves are given in Equipment property library B.48 .

Equipment property library B.48: Subsea valves – subsea Xmas tree isolation valves

Equipment description			**IRDI code** **CFIHOS/RDL**	**ISO 14224 reference/** **other specified reference/ comment**
L1 (Equipment class): Subsea valves				ISO 14224 section A.2.6.2 [1] ISO 14224 Equipment class code: XT
L2 (Equipment type): Subsea Xmas tree isolation valves				
Property Category	**Type of reliability influencing properties (L3)**	**Possible property values**		
DLOP	Device type	- Production master valve (PMV)		See Equipment property library B.25 (valves) for RDL references for X-mas tree valves (not specified whether topside or subsea)
		- Production wing valve (PWV)		
		- Crossover valve (XOV)		
		- Annulus master valve (AMV)		
		- Annulus wing valve (AWV)		
		- Chemical injection valve		
		- Methanol injection valve		
	Configuration	- Vertical Xmas tree	rdl/RDS16663478	<subsea vertical christmas tree>
		- Horizontal Xmas tree	rdl/RDS16446837 rdl/RDS16446522	<subsea horizontal christmas tree satellite well assembly> <subsea horizontal christmas tree template well assembly> rdl/RDS7168366 <subsea christmas tree> CFIHOS-30000494 <christmas tree>

[1] Note that subsea Xmas tree isolation valves are listed as maintainable items under the ISO 14224 equipment class "*Subsea wellhead and Xmas tree*".

B.18.2 Subsea manifold and flowline isolation valves

Properties for subsea manifold isolation valves are given in Equipment property library B.49.

Equipment property library B.49: Subsea valves – subsea manifold and flowline valves

Equipment description			IRDI code CFIHOS/RDL	ISO 14224 reference/ other specified reference/ comment
L1 (Equipment class): Subsea valves				ISO 14224 reference: NA [1] ISO 14224 Equipment class codes: - Subsea manifolds: MA - Subsea flowlines: FL
L2 (Equipment type): Subsea manifold and flowline valves				
Property Category	**Type of reliability influencing properties (L3)**	**Possible property values**		
DLOP	Device type	- Manifold isolation valve	rdl/RDS16703028	<subsea manifold valve>
		- Flowline isolation valve		
		- Manifold chemical injection valve		
		-		

[1] Note that subsea manifold and flowline isolation valves will appear as maintainable items under the ISO 14224 equipment classes "*Subsea manifolds*" and "*Subsea flowlines*" respectively.

B.18.3 Subsea pipeline and riser valves

Properties for subsea pipeline and riser isolation and protection valves are given in Equipment property library B.50.

Equipment property library B.50: Subsea valves – pipeline and riser isolation and protection valves

Equipment description			IRDI code CFIHOS/RDL	ISO 14224 reference/ other specified reference/ comment
L1 (Equipment class): Subsea valves				ISO 14224 section A.2.6.3 + A.2.6.7 [1] ISO 14224 Equipment class codes: Risers: PR Subsea pipelines: SL
L2 (Equipment type): Subsea pipeline and riser valves			CFIHOS-90000070 (CFIHOS-30000502)	<subsea pipeline valves> <riser> CFIHOS link to subsea pipeline valves not (yet) functional.
Property Category	**Type of reliability influencing properties (L3)**	**Possible property values**		
DLOP	Device type	- Pipeline isolation valve		rdl/RDS285164 <riser base>
		- Subsea isolation valves (SSIV) at riser base		
		- Subsea HIPPS valve		

[1] Note that subsea pipeline and riser isolation and protection valves appear as a maintainable item under the ISO 14224 equipment class "*Subsea pipelines*" and "*Risers*" respectively.

B.18.4 Solenoid control valves

Properties for subsea solenoid control valves (normally located in SCM) are given in Equipment property library B.51.

Equipment property library B.51: Subsea valves – solenoid control valves

Equipment description			**IRDI code** **CFIHOS/RDL**	**ISO 14224 reference/ other specified reference/ comment**
L1 (Equipment class): Subsea valves				ISO 14224 section A.2.6.1 [1] ISO 14224 Equipment class codes: CS
L2 (Equipment type): Subsea solenoid control valves				
Property Category	**Type of reliability influencing properties (L3)**	**Possible property values**		
DLOP	Device type	- Directional control valve (DCS)	rdl/RDS16744139	<directional control valve> (unspecified whether topside or subsea)
		- Quick dump valve (QDV)	rdl/RDS16760396	<quick dump valve> (unspecified whether topside or subsea)

[1] Note that subsea solenoid control valves appear as maintainable items under the ISO 14224 equipment class "*Subsea production control*".

B.19 Downhole well completion valves

This section includes the following downhole located valves:

- Downhole safety valve (DHSV)
- Tubing retrievable annulus subsurface safety valve (TRSCASSV / ASV)
- Downhole chemical injection valve (CIV)
- Gas lift valve (GLV)

Properties for these subsea valves are described in one common Equipment property library B.52.

Equipment property library B.52: Downhole well completion valves – common properties

Equipment description			IRDI code CFIHOS	ISO 14224 reference/ other specified reference/ comment
L1 (Equipment class): Downhole well completion valves				ISO 14224: Section A.2.7.2 and A.2.7.5 [1)] ISO 14224 Equipment class codes: SS
L2 (Equipment type): NA (general for downhole valves)				
Property Category	**Type of reliability influencing properties (L3)**	**Possible property values**		See Equipment property library B.25 (valves) for references to CDD and CFIHOS for relevant valve properties (not specified whether topside or subsea).
DLOP	Design principle	- Ball		
		- Flapper		
		- Poppet		
		- Check valve		
		- Other?		
	Device type	- Tubing retrievable downhole safety valve (TRSCSSV)	CFIHOS-30000294	<Downhole safety valve>
		- Wireline retrievable downhole safety valve (WRSCSSV)	CFIHOS-30000294	<Downhole safety valve>
		- Annulus subsurface safety valve - Integrated packer and valve unit [2)]		
		- Annulus subsurface safety valve - Dual bore packer w/separate valve [3)]		
		- Tubing retrievable CIV (TRCIV)		
		- Wireline retrievable CIV (WRCIV)		
		- Downhole gas lift valves		
	Actuation principle	- Hydraulic		
		- Electric		
		- Electro-hydraulic		
		- Manually/ROV operated		
		-		
OLOP	Fluid handled / severity	- Clean/benign service		
		- Medium/moderate service		
		- Dirty/severe service		

[1)] Downhole valves, except DHSVs, are listed as maintainable items under downhole well completion in ISO 14224 (section A.2.7.2). DHSVs are described in separate section A.2.7.5

[2)] Both subsea and topside located wells

[3)] Topside located wells only

C Additional properties and data elements for information modelling

This appendix includes tables with additional data elements (properties, requirements, parameters, etc.) that need to be included when establishing a more complete information model for SIF/SIS follow up. The following categorisation of SIS equipment properties was suggested and explained in section 2.5:

A. *Equipment ID & references*

B. *Reliability Influencing properties (RIPs):*
- *Device list of properties (DLOPs),*
- *Operating list of properties (OLOPs).*

C. *Safety list of properties (SLOP):*
- *Design related,*
- *O&M related.*

D. *O&M inventory properties:*
- *Operational inventory properties,*
- *Maintenance inventory properties.*

F. *Failure history properties*

And the following categories were suggested for the SIF level:

A. *SIF ID & references*

B. *SIF configuration properties*
- *Input,*
- *Logic solver,*
- *Output.*

C. *SIF integrity requirements*

D. *SIF functional requirements*

E. *SIF O&M history properties*

C.1 SIS equipment level

SIS equipment properties and associated values are given in table C1. References to the online CFIHOS (or RDL) library and/or IEC 61987 CDD are given when found (and considered relevant).

Table C.1 General SIS equipment properties and possible values

Property category	Property		Property values (picklist)	Incl. in SRS
	Definition	CFIHOS/RDL link IEC 61987 IRDI	Possible values	
Equipment ID and references	Plant code	CFIHOS-10000005 <plant code>	[*Text string*]	
	Plant code or name	CFIHOS-10000006 <plant name>	[Numeric code]	x
	Unique equipment identification (tag, functional location)	CFIHOS-10000166 1) <tag name>	[*Text string*]	(x)
	Unique equipment serial number	CFIHOS-10000163 1) <equipment manufacturer serial number>	[Numeric code]	
	Equipment physical location	CFIHOS-10000002 <area name>	[*Text string*]	(x)
	Equipment class (L1)	CFIHOS-00000033 2) <equipment class>	Ref. Table 2-3 and Table 2-4	
	Equipment type (L2)	NA	Ref. Table 2-3 and Table 2-4	
	Manufacturer / vendor	CFIHOS-10000158 <manufacturer company name>	[*Text string*] CFIHOS link not (yet) functional	(x)
	Model specification (by manufacturer)	CFIHOS-10000159 <model part name>	[*Text string*]	(x)
	Equipment boundaries	Not found	Ref. ISO 14224 + PDS data handbook	
	Maintainable items list	Not found	Ref. CMMS and ISO 14224	
	Unique SIF reference(s)	Not found	[*Text string*]	(x)
RIPs (DLOP + OLOP)			Ref. Table 2-3, Table 2-4 and App. B	
Safety list of properties, SLOP-D	Mean time between failures	ABB016	[years]	
	DU failure rate, λ_{DU}	ABB167	[per hour]	
	DD failure rate, λ_{DD}	ABB168	[per hour]	
	SD failure rate, λ_{SU},	ABB169	[per hour]	
	SU failure rate,	ABB193	[per hour]	
	CCF rate, β		(0, 1)	(x)
	SIL (Systematic capability requirement)	CFIHOS-40000579 <safety integrity level> ABB202	[SIL 1, SIL 2, SIL 3, SIL 4] CFIHOS-50000129 <safety integrity level pick-list> ABJ755 ABK707, ABK708, ABK709, ABK 710	x
	PFD/PFH budget	Not found	[Decimal number]	(x)
	Diagnostic Coverage, DC	ABB170	(0%, 100%)	
	Safe Failure Fraction, SFF	ABB192	(0%, 100%)	
	Response time requirement	ABB593 <control circuit response time>	[Seconds]	x
	Leakage criterion (valves, doors, dampers)	ABD632 <maximum leakage rate>	[kg/s] or [m^3/hour]	
	Safe state / style of failsafe	ABA311	[failsafe, non-failsafe, NA, others] ABL401	x
	Mean Time to Restoration (MTTR)	Not found	[Hours]	(x)

SLOP-O				
	Functional proof test interval	ABB911 <proof test interval>	[Months] or [Year]	x
	Proof test coverage (PTC)	Not found	(0%, 100%)	(x)
	Leakage test interval (valves)		[Months]	x
	Partial stroke test interval (valves)	ABD733 <test interval> property of "partial stroke test": ABD969	[Months] or [Weeks]	x
	Partial stroke test coverage	Not found	(0%, 100%)	(x)
	Inspection interval	ABI510 <inspection cycle> Property of "regular inspection": ABI482	[Months] or [years]	
	Complete overhaul interval	Not found	[Months]	
O&M inventory properties Operation	Normal operating state	rdl/RDS37889 <operating state>	[Norm. running, standby, intermittent]	(x)
	Start date / end date	Not found	[Date: xx.xx.xx] / NA, [Date: xx.xx.xx]	
	Operating time	rdl/RDS14644985 ABN639	[Hours]	
	Calendar / surveillance time	Not found	[Hours]	
	Number of operational demands (SAS/IMS)	Not found	[Integer]	
	Number of functional tests		[Integer]	
	Dates of functional tests [3]		List of [Date: xx.xx.xx]	
	Results of functional tests [3]		List of [fail / pass]	
	Number of partial tests		[Integer]	
	Dates of partial tests [3]		List of [Date: xx.xx.xx]	
Maintenance	Results of partial tests [3]		List of [fail / pass]	
	Number of leakage tests		[Integer]	
	Dates of leakage tests [3]		List of [Date: xx.xx.xx]	
	Results of leakage tests [3]		List of [Fail / pass]	
	Number/dates of other maintenance activities [4]		[Integer] + List of [Date: xx.xx.xx]	
	Result from other maintenance activities [4]		List of [*Text string*]	
Failure reporting properties	Date of failure (s)		List of [Date: xx.xx.xx]	
	Notification / WO reference		List of [*Text string*]	
	Detection method		See Table 3-1 and ISO 14224	
	Failure mode		Ref. Table 4-1, Table E-1 and ISO 14224	
	Failure type / classification		[DU, DD, S, non-critical]	
	Failure cause		See Appendix G and ISO 14224	
	Repair time		List of [*Hours*]	

[1] Note that upon *equipment replacement* the equipment will for practical reasons normally retain the same tag number, but in addition the unique serial number is required e.g., for failure data follow up (the failure data thus "follows" the unique equipment unit)

[2] Note that CFIHOS has defined some 860 equipment classes, whereas ISO 14224 defines 44 topside-related equipment classes and APOS so far has defined 18 topside-related equipment classes (only safety critical equipment)

[3] Note that each test date and test result (fail/pass) must be linked together (matrix of the two lists)

[4] Note that each maintenance activity date and associated results/actions must be linked together (matrix of the two lists)

C.2 SIF level

SIF properties and associated values are given in table C.2. No references to CFIHOS, RDL or IEC 61987 CDD are yet included (and very few relevant ones found).

Table C.2 General SIF level properties and possible values

Property category	**Property definition (L3)**	**Possible property values**	**Incl. in SRS**
SIF ID and references	Unique SIF ID/reference	[*Text string*]	x
	SIF description	[*Text string*]	(x)
	Barrier function reference	[*Text string*]	
SIF configuration properties	Number of inputs (in series)	[Integer]	x
	(For each serial input): Voting	List of [1oo1, 1oo2, 2oo2, 2oo3… koon]	x
	(For each serial input): HFT	List of [Integer]	x
	(For each serial input): Ref. to tags	List of [*Text string*]	x
	Number of logic solvers / CLUs (in series)	[Integer]	x
	(For each logic solver / CLU): Voting	List of [1oo1, 1oo2, 2oo2, 2oo3… koon]	x
	(For each logic solver / CLU): HFT	List of [Integer]	x
	(For each serial logic solver / CLU): Ref. to tags	List of [*Text string*]	x
	Number of outputs (in series)	[Integer]	x
	(For each serial output): Voting	List of [1oo1, 1oo2, 2oo2, 2oo3… koon]	x
	(For each serial output): HFT	List of [Integer]	x
	(For each serial out): Ref. to tags	List of [*Text string*]	x
SIF integrity requirements	SIL requirement	[No SIL, SIL 1, SIL 2, SIL 3, SIL 4]	x
	Mode of operation	[low demand, high demand, continuous]	x
	PFD/PFH requirement	[Decimal number]	x
	Assumed (allowed) SIF demand rate	[Decimal number per year]	x
	Maximum allowable spurious trip rate	[Decimal number per year]	(x)
SIF functional	SIF response time requirement	[Seconds]	x
	Process safety time	[Seconds]	x
	Safe state definition / fail safe state	[*Text string*]	x
	Additional SRS requirements	[*Link to SRS document*]	x
SIF O&M history	Number of complete loop tests	[Integer]	
	Number of SIF demands	[Integer]	
	Number of spurious SIF trips	[Integer]	

C.3 Discussion

C.3.1 Equipment boundaries

An equipment boundary defines the physical elements that are part of an equipment. Having standardised definitions of equipment boundaries is important as an aid for those who register failures into the maintenance system and to ensure that failures are reported against the correct tag number. The standardisation ensures consistency in the failure registration among and across personnel and installations.

For each equipment class (L1) or equipment type (L2), a boundary should be defined indicating which failures to be registered for the given equipment (e.g., since all components or "maintainable items" are not separately tagged).

This guideline does not explicitly define equipment boundaries but mainly refer to ISO 14224 which include many such definitions in Annex A. With a few exceptions the PDS data handbook also adheres to the ISO definitions.

C.3.2 Inventory data

Inventory data is all the information registered into the maintenance system about the equipment unit and its' operational and maintenance history. Inventory data includes equipment ID information such as the location of the equipment, the technical specification of the equipment (manufacturer, model, etc.) as well as the equipment's operational and maintenance history. These data are very important to complement failure data. Some inventory data is mandatory in the sense that equipment cannot be registered unless this data is provided (e.g., tag number) and some data are commonly added (e.g., equipment model, manufacturer, operation start date, no. of tests, no. of demands, etc.). For SIL-follow-up it is important that the inventory data matches the needs for information for the equipment at L1, L2 and (the optional) L3.

Sufficient inventory data is essential for SIL follow up and provides important input to the information model as discussed in APOS activity H5.

C.3.3 Tag. no.

The *tag number* marks the functional identity (also referred to as "functional location") of an equipment and includes information about the equipment type (e.g., pressure transmitter), the location (e.g., separation trains), and (indirectly) the main equipment function (e.g., HH, which indicates process shutdown high setpoint). The number is linked to the equipment inventory datasheet that contains more detailed information about the equipment, such as manufacturer, model, and installation date. A failure is *registered against one unique tag number*, implying that a failure registration inherits the unique links to inventory data as discussed above).

Note that in typical Norwegian projects a tag is not a unique identification of a specific physical item in the way that for example a manufacturer's serial number is. Replacement items inherit the tag of the item they replace. Some projects even use both tag numbering and project specific item IDs, such that the item ID for e.g., a transmitter might change while its tag remains unchanged.

D Parameters in failure registration and classification

Figure D-1 illustrates a typical workflow for failure detection, registration, classification, restoration, and further data analysis. This guideline mainly covers the workflow phases 'Failure detection', 'Initial registration (and classification)' and 'Classification/Reclassification/QA'. Note that activities such as monitoring, data analysis and implementation of measures are covered by the SIS follow-up guideline issued as part of activity H3 in the APOS project, /8/ .

The figure also identifies the most relevant parameters for failure registration (detection method, failure mode, failure mechanism, failure cause), corrective maintenance (failure impact, priority, restoration time) and failure classification (failure cause, failure class, random or systematic, independent or CCF).

These parameters are introduced and briefly discussed in this appendix. A split has been made between mandatory parameters, i.e. parameters required to determine the failure class (DU,DD, S) and parameters that are recommended to report.

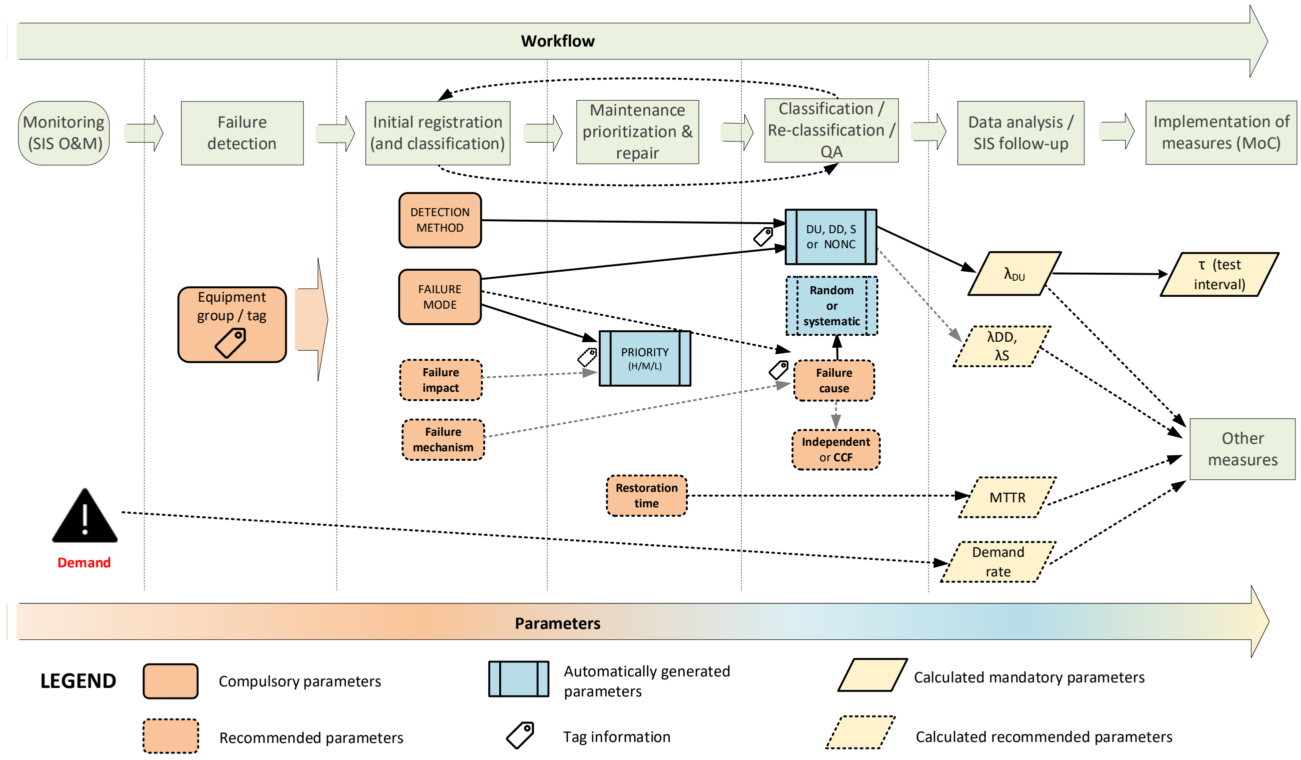


Figure D-1: Failure registration and classification and follow up –workflow and parameters.

Three types of parameters are described based on how registration and classification is suggested performed (see Figure C-1):

1. Manually registered parameters (mandatory and recommended)
2. Automatically generated parameters
3. Calculated parameters

D.1 Manually registered parameters

D.1.1 Detection method (mandatory)

The detection method characterises how the failure has been revealed. Relevant information is whether the failure has been reported automatically (by self-diagnostics) or by personnel, in relation to planned and regular activities (such as preventive maintenance and regular testing), or during irregular activities such as demands, corrective maintenance or random observations.

The proposed standardised taxonomy for detection methods is presented in chapter 3 in the main report.

D.1.2 Failure mode (mandatory)

A failure mode characterises how a failure is brought to our attention, i.e., in what way it is observed that the function has been fully or partially lost. As for detection method, this is considered key information and most maintenance systems provide a pre-defined list of failure modes to select from. A valve, for example, may be required to open on demand, to close on demand, and to keep tight in the closed position. Failure to close or open when demanded, an internal leakage in closed position, and untimely (spurious) activation are all examples of failure modes. Correct reporting of failure modes is essential when determining the severity of the failure. Note that failure mode reporting shall relate to the ***equipment unit (tag) itself,*** and not the voting or the system. For example, a critical failure of a gas detector (e.g., no output) voted 1oo2, shall be classified as dangerous with respect to the lost function of the detector itself, although the associated 1oo2 loop is degraded but will function as intended (if the other detector functions).

The proposed taxonomy for failure modes is presented in chapter 4 in the main report. Associated fail/pass criteria to determine safety critical failure modes are also discussed in chapter 4 (section 4.3).

D.1.3 Failure impact (recommended)

The failure impact characterises the *severity and extensiveness* of the failure mode. The primary use of this parameter today is to determine the priority of notification and work orders. Most maintenance systems have adopted a list that is either identical to the ISO 14224:2016 failure impact classes (which distinguish between *critical, degraded and incipient* failures), or some similar categories such as "dead", "seriously ill" or "unwell". However, for SIL follow-up, it is found that the *failure impact* is a less precise parameter than *failure mode* and is therefore in this guideline only suggested as recommended.

The failure impact can be more precisely identified by combining other mandatory information such as failure mode, tag number, and detection method.

D.1.4 Restoration time (recommended)

The restoration time denotes the time from the failure is detected until the equipment is fully restored. It should be noted that the time at which the failure is detected is not necessarily the same as the time when the failure occurred. For example, a dangerous undetected (DU) failure may occur at any time between two subsequent functional tests, but it is not revealed until the next scheduled preventive maintenance (typical functional test) or at a random opportunity or demand.

Regulations require that compensating measures are implemented to maintain the safety level during the restoration period, and the impact of restoration time in SIL analyses is therefore often considered negligible.

D.1.5 Failure mechanism (recommended)

The *failure mechanism* is related to the *apparent, observable process* that leads to an equipment failure and is in ISO 14224 described as "the physical, chemical or other process or combination of processes that leads to the failure".

Review of maintenance notifications indicates that it is often difficult to separate this parameter from the failure mode and failure cause parameters. A closer look at the ISO 14224 failure mechanism taxonomy, indicates that the failure mechanisms given at level one, are not mutually exclusive. E.g., the suggested category "external influence" may cause other categories of failure such as a mechanical or material failure. Furthermore, the sub-categories specified at level two are in many cases interchangeable with failure modes (which is also pointed out in the standard itself) and for some sub-categories (such as leakage and common cause failure) their suggested associated main category is certainly discussable.

In this guideline, we therefore recommend to report also the failure mechanism parameter, however stressing that more focus should be put on the underlying failure cause.

D.1.6 Failure cause (recommended)

A failure cause characterises the initiating event or condition (i.e., the root cause) in the sequence of events leading to an equipment failure. The failure cause is usually not known when the failure notification is registered. The cause may be revealed later during troubleshooting and repair of the component. A root cause analysis may ensure a structured targeting of the root cause; however, such analyses are only occasionally carried out.

A suggested alternative taxonomy for failure cause is presented in Appendix G. It is also recommended that information about the failure cause is added as free text (as often done today), and that effort is made to ensure that the notifications / work-orders are updated with information about failure cause whenever possible.

The main argument for reporting the failure cause is its importance as an efficient mean to define measures for avoiding repeating failures and associated costly repairs and excessive maintenance. However, since the parameter is not always possible to determine, one choice for the parameter could be "Failure cause unknown". The parameter is therefore not considered "mandatory" but strongly recommended to be registered whenever possible.

D.1.7 Independent failure or CCF (recommended)

An independent failure is a failure that occurs independently of other failures, while a common cause failure (CCF) is an event where more than one failure occurs due to a shared cause. There are also other types of dependent failures, such as cascading failures. However, CCFs are the most common dependent failures considered in reliability analyses.

As for failure cause, this is a type of parameter where the notification / work-order may need to be updated as more information about failure class becomes available. Due to the challenges of identifying a

CCF and/or having enough information to make a proper judgment, the parameter is therefore not considered "mandatory" but is recommended to be registered whenever possible.

D.2 Automatically generated parameters

D.2.1 Failure class - DU, DD, S or NONC

The failure class can be automatically determined if information about the parameters marked as mandatory is properly filled in: i.e., whether the failure is dangerous undetected, dangerous detected, safe (or NONC) can be deduced from a correct registration of *failure mode*, *detection method* and relevant *equipment group / tag information* (see also /21/)

The failure class could be implemented as a separate parameter in the notifications or work orders, automatically filled in, but with the possibility of being manually overwritten.

D.2.2 Priority

This parameter denotes the priority of the restoration action connected to the equipment failure. It is often classified as either high, medium, or low, and results from combining tag properties (assessed equipment criticality and redundancy) with the consequence of the failure (on equipment level). Therefore, by combining the failure mode (or failure impact) with equipment group/tag information, the priority can (ideally) be automatically generated (with the possibility of being manually overruled).

D.2.3 Random or systematic failure

A random failure is a failure occurring at a random point in time, primarily from normal degradation (but according to some taxonomies also from phenomena such as human errors and excessive environmental exposures). Systematic failures are failures that do not occur at a random time, but due to the presence of specific conditions that put the equipment in a fail to function state. Examples include design failures (e.g., not built according to the specification or wrong specification), installation failures, calibration failures, and so on. Systematic failures can, unlike random failures, be prevented “once and for all” if the specific conditions that lead to the failure is removed (e.g., correcting the calibration procedure or improve the training). However, this is not always achieved, sometimes due to lack of proper identification of the root cause, and systematic failures may therefore re-appear as if they were (recurring) random failures. Whether a failure is random or systematic is therefore difficult to determine, at least at the time when the failure notification is registered, but the subsequent failure cause analysis may suggest if the failure was random or systematic. None of the maintenance systems reviewed include a parameter that can identify if the failure is random or systematic. In this guideline it is suggested to link the failure cause directly to random or systematic, i.e., given a selected failure cause, it will be possible to (roughly) determine whether the failure is random or systematic. Determining whether a failure is systematic or not, is helpful for describing appropriate measures for prevention of reoccurring failures as well as for deciding whether more frequent testing is an efficient means for improving the reliability performance.

D.3 Calculated parameters

A calculated parameter is a parameter that is determined based on a formula using values assigned to mandatory parameters and inventory data (such as e.g., time of installation). Calculated parameters such as the rate of dangerous undetected failures (λ_{DU}) and test interval τ were shown in Figure D-1 to indicate workflow and relationships but is mainly the scope of the SIS follow-up guideline, i.e., the main delivery from activity H3 of the APOS project, /8/.

E Equipment specific failure modes

Table E-1 suggests *equipment specific failure modes* for the equipment specified in Table 2-3 (topside) and Table 2-4 (subsea). The failure mode taxonomy includes two levels, i.e., F1 and F2:

- Level 1 (F1) failure modes are D, S, NONC, LOC and LEX (ref. chapter 4), these are the same for all equipment types.
- Relevant level 2 (F2) failure modes are specified for each of the level 1 (F1) modes
- OTH (other) and UNK (unknown) are not included as separate failure modes at level 2. **If relevant F2 failure mode is not found, only F1 failure mode shall be selected.**
- If only level F2 is implemented in the maintenance system (as is usually the case), it may be considered necessary to also implement OTH/UNK.
- For all failure modes, it is recommended that the failure is further described in the free text field due to the variation of failures and to support further failure classification (if necessary).

For some equipment classes (L1 in Table 2-3 and Table 2-4), the relevant failure modes may vary slightly between equipment types (L2 in in Table 2-3 and Table 2-4) within the same equipment class. For such equipment, the failure modes need to be further detailed on L2 or in some cases possibly also on L3. This has, for relevant equipment, been commented in Table E-1.

Additional comments to Table E-1

NONC failure modes

As illustrated in Figure 4-1 to Figure 4-3, the non-critical failures can at level 2 be split into degraded failures and no-effect failures. This is also pursued in Table E-1 in the sense that a split has been made for the NONC failures. The user must however not make this choice explicitly (all these failure modes will be listed under non-critical).

Low complexity equipment – only one level 2 (F2) failure modes

Note that for some equipment groups with relatively low degree of complexity (such as switches, solenoid valves, emergency lights and speakers), FTF (Fail to Function on demand) will often be enough as dangerous failure mode on level 2.

Not applicable (NA) notifications

Often notifications are written for components that are not part of the equipment's main function or incorrectly registered as failure notifications. Examples can be "missing tag plate", "needs re-painting", "missing scaffolding", etc. In such cases, neither of the outlined failure modes at level 1 (or level 2) apply, and the notification should be classified as NA with respect to failure mode. This corresponds to the "No part" failure definition in IEC 61511.

Table E-1: Suggested failure modes for each equipment group

Equipment class / type	Failure mode		Notes	Comparison to ISO 14224
	F1	F2		
Input devices – Process transmitters	D	NOO ERO LOO/HIO[1] FTF	[1] Criticality of failure modes (safety critical or production critical) will depend on whether it is a HH and/or a LL application. Note that some transmitters have both applications (LL and HH).	Additional ISO failure modes (input devices) are ELU, OTH and UNK. ELU is considered causing in-service problems (SER).
	S	SPO HIO/LOO[1]		
	NONC	Degraded HIO/LOO ERO No-effect SER		
	LOC	ELP		
	LEX	DEX		
Input devices – process switches	D	FTF		For a simple device like a process switch, the comprehensive list of ISO failure modes for input devices is considered too excessive – F1 failure modes and some simple F2 failure modes are therefore considered adequate.
	S	SPO		
	NONC	-		
	LOC	ELP		
	LEX	DEX		
Input devices – position switches	D	FTF[1]	[1] Position switches are normally not safety critical but may be so in special interlock applications (e.g., overpressure protection).	Same argument as for process switches.
	S	SPO		
	NONC	AIR[2]		

Equipment class / type	Failure mode		Notes	Comparison to ISO 14224
	F1	F2		
	LEX	DEX	[2] Relates to incorrect position feedback from limit/proximity switches that is normally non-critical but may in some applications be safety critical.	
Input devices – manual pushbuttons and call points	D	FTF		Additional ISO failure modes for input devices are ELP, ELU, HIO, LOO, ERO, OTH and UNK. For a relatively simple device like a pushbutton / call point, the comprehensive list of ISO failure modes for input devices is however considered too excessive – level 1 failure modes and simple level 2 modes are therefore considered adequate.
	S	SPO		
	NONC	–		
	LEX	DEX		
Gas detectors	D	NOO[1] LOO DSE[2), 3)]	[1] For acoustic gas detectors, only NOO is assumed relevant as dangerous failure mode. [2] Degraded sensing (dirty optics) is normally a degraded failure mode, but this depends on type of detector and detector configuration. Some detectors compensate by increased beam/sensitivity upon dirty optics, whereas others not. Also, there can be two levels of dirty optics; (1) a level where the detector must be checked/washed within a certain time (e.g., 7 days) and (2) a level where the detector is not capable of detecting the gas (i.e., a dangerous detected failure where the safety function is impaired). [3] DSE is only relevant for IR/optical gas detectors (not for catalytic gas detectors).	Additional ISO failure modes are OTH and UNK. [4] Note that SER is not an ISO failure mode for gas detection.
	S	SPO		
	NONC	Degraded LOO HIO ERO DSE[2), 3)] No-effect SER[4]		
	LEX	DEX		
Fire detectors	D	FTF NOO ERO LOO[1]	[1] LOO is not relevant for flame detectors.	Additional ISO failure modes (fire detection) are OTH and UNK. SHH and SLL not considered relevant/necessary for fire detectors.

Equipment class / type	Failure mode		Notes	Comparison to ISO 14224
	F1	F2		
	S	SPO HIO		[2] Note that SER is not an ISO failure mode for fire detection.
	NONC	Degraded LOO ERO DSE No-effect SER[2]		
	LEX	DEX		
Logic solvers and interface elements	D	FTF ERO IOF[1]		Additional ISO failure mode (for control logic units) are LOO, HIO and UNK. However, very few failures are generally reported against logic and FTF and ERO are therefore considered to cover most safety critical logic solver failure modes. [1] Note that IOF (I/O card failure) is not an ISO failure mode but introduced to *enable extraction* of I/O card failures.
	S	SPO		
	NONC	SER		
	LEX	DEX		
Valves – shutdown valves (topside)	D	FTC DOP[1] LCP[2]	[1] Only relevant if response time requirement given. [2] Only relevant if internal leakage requirement given. All ESVs and some XVs will normally have an internal leakage requirement. [3] Response time considered too high but within requirement or if no requirement given. [4] Internal leakage below requirement (if given) or internal leakage when no leakage requirement given. [5] Both ELP and ELU may in extreme cases be critical to the main function of the valve and can then cause a dangerous or safe failure (i.e., FTC/FTO, SPO or DOP).	Additional ISO failure modes (valves) are HIO, LOO, PLU (flow restriction), OTH and UNK: • HIO (overspeed) is not considered relevant for valves, and LOO is covered by the DOP failure mode. • PLU is considered covered by the FTC (or FTO) failure mode(s).
	SF	SPO FTO		
	NONC	Degraded DOP[3] INL[4] STD No-effect NOI AIR SER		

Equipment class / type	Failure mode		Notes	Comparison to ISO 14224
	F1	F2		
	LOC	ELP[5] ELU[5]		
Valves – Blowdown and fast opening valves	D	FTO DOP[1]	[1] Only relevant if response time requirement given. [2] Major internal leakage requiring a shutdown/immediate repair. [3] Response time considered too high but within requirement or if no internal leakage requirement given. [4] Both ELP and ELU may in extreme cases be critical to the main function of the valve and can then cause a dangerous or a safe failure (i.e., FTO, FTC, SPO or DOP).	Ref. comments for shutdown valves.
	S	SPO FTC LCP[2]		
	NONC	Degraded DOP[3] ELP INL STD No-effect NOI AIR		
	LOC	ELP[5] ELU[5]		
Valves – Solenoid/pilot valves	D	FTF		For a relatively simple device like a solenoid/pilot valve, the comprehensive list of ISO failure modes for valves is considered too excessive - failure modes at level 1 and simple choices at level 2 are therefore considered adequate.
	S	SPO		
	NONC	–		
	LEX	DEX		
Valves – Ballast water valves	D	FTO/FTC[1] SPO[2]	[1] May be safety/production critical depending on application. [2] SPO (spurious opening or closure) may be safety/production critical depending on application.	
	S	FTC/FTO[1] SPO[2]		

Equipment class / type	Failure mode		Notes	Comparison to ISO 14224
	F1	F2		
	NONC	Degraded INL ELU[3] ELP STD No-effect NOI SER	[3] ELU may sometimes be critical and will in such case cause an FTF or SF (i.e., FTO/FTC or SPO) but will most often be non-critical and thus represent a degraded failure mode.	
Valves – Pressure safety valves (PSVs)	D	FTO[1] DOP[2]	[1] PSV fails to open upon test/demand. [2] PSV opens but at a too high pressure (e.g., not within 120% of set pressure). [3] Major internal leakage requiring a shutdown/immediate repair.	Not all ISO failure modes for valves will be relevant for PSVs.
	S	SPO LCP[3]		
	NONC	Degraded INL STD No-effect AIR SER		
	LOC	ELP		
Valves - active fire protection valves	D	FTO LOO[1]	[1] Fire-fighting agent pressure/level is below specified minimum. [2] External leakage of fire water from the valve.	
	S	SPO FTC		
	NONC	Degraded INL ELP[2] ELU No-effect SER		
Nozzles	D	LOO (FTF)		Additional ISO failure modes for nozzles (separate ISO category) are PLU, FTO, DOP, STD (Structural deficiency),

Equipment class / type	Failure mode		Notes	Comparison to ISO 14224
	F1	F2		
	S	SPO		SPO and OTH. For a relatively simple device like a deluge nozzle, the list of ISO failure modes is considered too excessive and is therefore suggested simplified with only LOO (or alternatively FTF) as dangerous failure. Note that FTF is not an ISO failure mode for nozzles.
	NONC	–		
Firefighting equipment - Deluge skid	D	FTF / LOO		Note that failure of a skid is related to failure(s) of the nozzles on the skid. A certain percentage of failed nozzles will imply either too low output (LOO) or alternatively FTF for the skid.
	S	SPO		
	NONC	–		
Firefighting equipment - Fire water monitors	D	FTF / NOO[1)] LOO[2)]	[1)] The fire water monitor does not operate/oscillate. [2)] The fire water monitor does not deliver water/foam within expected amount.	No specific failure modes for fire water monitors given in ISO. Fail/pass criteria therefore used as a starting point.
	S	SPO		
	NONC	–		
Pumps – Fire water pumps	D	FTS LOO UST[1)] STP[2)]	[1)] UST - unexpected/spurious stop of pump while running. [2)] STP – fail to stop FW pump on demand - may be safety critical for some applications, such as on floating facilities. [3)] External leakage of fire water from the pump. [4)] External leakage of lubricant or cooling medium. [5)] Structural deficiencies / material damage incl. bearing and seal failure (cracks, wear-out, fracture, corrosion, erosion).	ISO 14224 includes several failure modes for pumps. Additional failure modes to those included here are BRD, INL, PDE, PLU, OTH and UNK: • INL – internal leakage – of fire water not considered a relevant failure mode. • PDE – parameter deviation – considered covered by AIR (abnormal instrument reading) and SER (minor in-service problems). • BRD is considered too general failure mode and partly covered by other failure modes instead (e.g., STD). • PLU is considered covered by LOO. Note that STP is not included in ISO 14224 as a failure mode for pumps. Note that Spurious start not considered relevant and spurious stop is covered by the separate failure mode (UST).
	S	STP[2),]		
	NONC	Degraded ELP[3)] HIO ELU[4)] STD[5)] VIB OHE ERO No-effect AIR NOI SER		
	LEX	DEX		

Equipment class / type	Failure mode		Notes	Comparison to ISO 14224
	F1	F2		
Pumps – Ballast water pumps	D	FTS UST	[1] STP – fail to stop ballast pump on demand. The ballast pumps are used to either completely fill or completely empty ballast tanks (a partly filled tank would have a free water surface, which is considered hazardous), such that there is no risk for moving too much water by not being able to stop a pump. Ballast operations (valves and pumps in sequence) are done manually via SAS HMI. If a pump cannot be stopped from SAS, power to it can be turned off manually. [2] External leakage of ballast water from the pump.	See comments to fire water pumps.
	S	–		
	NONC	Degraded STP[1] ELP[2] HIO ELU STD VIB OHE ERO No-effect AIR NOI SER		
	LEX	DEX		
Pumps – Other pumps	D	FTS STP[1] LOO[1] UST[1]	[1] Safety criticality of these failure modes will depend on pump type and application.	Ref. comments to fire water pumps and ballast water pumps.
	S	–		

Equipment class / type	Failure mode		Notes	Comparison to ISO 14224
	F1	F2		
	NONC	Degraded [2] STP[1] ELP[1] HIO ELU STD VIB OHE ERO No-effect[2] AIR NOI SER	[2] Depending on pump type and application it must be considered if these (and/or additional) failure modes are relevant.	
	LEX	DEX		
HVAC – Fire and shut-off dampers	D	FTC DOP[1]	[1] Only relevant if response time requirement. [2] ELU may in some cases be critical (large hydraulic actuator leakage) and can in such case cause a dangerous or safe failure, but will most often be non-critical and thus represent a degraded failure mode. [3] Response time considered too high but within requirement or if no requirement given. [4] Non-critical internal leakage through closed damper.	Not all ISO failure modes for valves will be relevant for fire dampers
	S	SPO FTO		
	NONC	Degraded ELU[2] DOP[3] INL[4] STD No-effect NOI AIR SER		
	LEX	DEX		

Equipment class / type	Failure mode		Notes	Comparison to ISO 14224
	F1	F2		
Engines and generators	D	FTS HIO[1] LOO[1] ERO[1] UST[2]	[1] HIO/LOO/ERO: All the following can be safety critical failures: - Too high/low voltage - Too high/low frequency - Too low power An alternative is therefore to collect them in the common failure mode "erratic output" (ERO). [2] UST - unexpected/spurious stop of engine/generator while running. [3] STP – fail to stop engine/generator on demand – should be considered whether it can also be safety critical for some applications, such as on floating facilities. [4] INL – internal leakage of fuel – only relevant for combustion engines (e.g., diesel engines).	Additional ISO failure modes (for combustion engines, electrical motors and generators) are: BRD, ELF and OHE, PLU (these two only relevant for combustion engines), PDE, OTH and UNK: • BRD is considered too general failure mode and partly covered by other failure modes instead (e.g., STD). • ELF – external leakage of fuel - considered covered by ELU. • OHE – overheating – will eventually cause an unexpected/spurious stop and as such covered by UES. • PLU – plugged – considered by other failure modes (e.g., FTS and LOO). • PDE – parameter deviation – considered covered by AIR (abnormal instrument reading) and SER (minor in-service problems). In addition, the following two ISO failure modes applies for motors only (not generators): ERO, HIO. Note that SPO is not an ISO failure mode for engines or generators. Spurious start not considered relevant and spurious stop covered by this separate failure mode (UST).
	S	STP[3]		
	NONC	Degraded ELU VIB STD OHE INL[4] HIO LOO ERO No-effect NOI AIR SER		
	LEX	DEX		
Uninterruptable power supply – UPSs & battery packages	D	LOO [1] ERO [2]	[1] Low output – the UPS provides inadequate power supply or does not have the required capacity (note that LOO is not an ISO defined failure mode for UPS). [2] ERO: Erratic output may be safety critical depending on degree of voltage failure, see also definition og fail/pass criteria in Table G-1.	Additional ISO failure modes (for UPS - uninterruptible power supply) are: FOF, FOV, OTH, PDE, SPO and UNK: • FOF (faulty output frequency) and FOV (faulty output voltage) considered sufficiently covered by ERO (erratic output). • SPO not considered relevant. • PDE – parameter deviation – considered sufficiently covered by ERO and SER.
	S	-		
	NONC	Degraded ERO [2] OHE No-effect SER		

Equipment class / type	Failure mode		Notes	Comparison to ISO 14224
	F1	F2		
	LEX	DEX		Note that ISO also lists in Table F.1 low capacity (LOC) as a failure mode for UPS, but here it is assumed that low capacity is covered by LOO.
Switchgear – Circuit breakers, Contactors, Relays	D	FTF FTO		ISO 14224 (Table F.1) suggests both FTO and FTF as applicable failure modes for switchgear. For a relatively simple device like a circuit breaker / contactor / relay, failure modes at level 1 could be adequate, however since fail/pass criteria is related to fail to open, this failure mode as well as fail to function and spurious operation are included.
	S	SPO		
	NONC	–		
	LEX	DEX		
Escape, rescue, and evacuation – Fire doors and watertight doors	D	FTC [1] LCP [2] DOP [3]	[1] Door fails to close and latch. [2] Critical leakage through closed door (most relevant for watertight doors) requiring immediate repair. [3] Door closes but travel time exceeds further defined safety critical response time. [4] Door closes but uses excessive travel time (not safety critical).	No specific failure modes for doors given in ISO.
	S	SPO FTO		
	NONC	Degraded INL DOP [4] No-effect SER		
Escape, rescue, and evacuation - Emergency lights	D	FTF	[1] Safe/spurious failure of emergency lights not considered relevant.	No specific failure modes for emergency lights given in ISO.
	S[1]	-		
	NONC	-		
	LEX	DEX		
Emergency communication – PA speakers, telemetry, radios and telephones	D	FTF	[1] Safe/spurious failure of speakers etc. not considered relevant.	No specific failure modes for telecom equipment given in ISO.
	S[1]	-		
	NONC	-		
	LEX	DEX		
Lifeboats – Launch/release systems	D	FTF DOP/QOP [1]	[1] Too long or too fast lowering times only apply for conventional (davit launched) lifeboats (QOP = Quick operation)	ISO failure modes for lifeboats relate both to lifeboat release and operation of the lifeboat itself. In our taxonomy, lifeboat (and MOB boat) engine is located under
	S [2]	-		

Equipment class / type	Failure mode		Notes	Comparison to ISO 14224
	F1	F2		
	NONC	-	[2] Spurious drop of lifeboat or release chute may be considered safety critical.	"Engines and generators", hence here we only consider the launch/release systems.

Equipment class / type	Failure mode		Notes	Comparison to ISO 14224
	F1	F2		
Subsea process sensors	*Ref. process transmitters (topside) – relevance of these failure modes for subsea sensors must be discussed with subsea equipment experts*			
Subsea leak detectors	*Ref. gas detectors (topside) – relevance of these failure modes for subsea detectors must be discussed with equipment experts*			
Subsea valves – Template, wellhead, and Xmas trees isolation valves	D	FTC DOP[1)] LCP[2)]	[1)] Only relevant if response time requirement given (e.g., SSIV). [2)] Only relevant if internal leakage requirement given (e.g., SSIV). [3)] Response time considered too high but within requirement or if no requirement given. [4)] Internal leakage below requirement (if given) or if no requirement given. [5)] Both ELP and ELU primarily represents an environmental risk but may in extreme cases be critical to the main function of the valve and can then cause a dangerous or a safe failure (i.e., FTC/FTO, SPO or DOP).	Additional ISO failure modes (for subsea wellheads and Xmas trees) are ILP, ILU, PLU (flow restriction), OTH and UNK: • ILP (internal leakage process medium) and ILU (internal leakage utility medium) considered sufficiently covered by LCP and INL. • PLU is considered covered by the FTC (or FTO) failure mode(s).
	S	SPO FTO		
	NONC	Degraded DOP[3)] INL[4)] STD No-effect SER		
	LOC	ELP[5)] ELU[5)]		
Downhole well completion valves - DHSV	D	FTC LCP[1)]	[1)] Relevant for DHSVs with internal leakage requirement. [2)] DHSV closing time considered too long. [3)] Internal leakage below requirement (if given) or if no requirement given. [4)] CLW – control-line-to-well communication; Loss of hydraulic control fluids into the well bore. [5)] WCL – well-to-control-line communication; Influx of well fluids into valve control line.	Additional ISO failure modes for DHSV are PCL, OTH and UNK: • PCL (Spurious closure of valve without command) considered covered by the SPO failure mode.
	S	SPO FTO		
	NONC	Degraded DOP[2)] INL[3)] CLW[4)] WCL[5)] No-effect SER		

F Standardised fail/pass criteria

The main objective of this appendix is to contribute towards a "best practice" in the industry with respect to defining common and standardised fail/pass criteria. The standardisation is useful to facilitate selection of the correct failure mode of dangerous failures revealed upon tests or demands. Consequently, the fail/pass criteria focus on failures detected during tests and demands (undetected failures).

Some relevant standards state:

*Clear pass/fail criteria should be established for each of the failure modes, particularly those that are deemed dangerous for the application the device is in. (*ISA-TR84.00.03-2019, sec. 4.3.1)

For items with function tests to detect dangerous undetected failures, the maintenance work order in the maintenance management system shall as a minimum contain:

- *description and requirements of test (e.g. no maintenance before function test);*
- *failure characteristics (e.g. valve does not close within specified time);*
- *acceptance criteria (e.g. closing time 12 seconds);*
- *how the result of a failure shall be reported (e.g. "create notification in CMMS with failure mode Fail to Close").*(NORSOK Z-008, sec. 8.4).

ISO 14224, Table F.1, provides recommended failure definitions (revealed during testing) for much of the equipment listed in Table 2-3 and Table 2-4. The standard also lists applicable failure modes for the equipment types. However, the level of detail is not always sufficient to be directly applied during equipment testing. E.g., for a fire and gas detector the fail-criterion in ISO 14224 is *Fire and gas logic does not receive signal from detector, when detector is tested*. A further definition of how the detector is tested and the detailed criteria for a failed or passed test of the detector is needed. Also, for some of the failure descriptions more than one failure mode are listed. To ensure standardised classification of failure modes, each failure description should be attached to a single failure mode.

For equipment groups defined as barrier elements in RNNP, PSA Norway provides guidance on both failure definition, system boundary and fail criteria in their 2018 version of the memo "Risikonivå norsk petroleumsvirksomhet - Krav til selskapenes rapportering av ytelse av barrierer". See https://www.ptil.no/globalassets/rnnp/datainnsamling/krav-til-rapportering-barrierer-rev15_3.pdf.

Definitions of fail pass criteria are for some specific equipment also found from NORSOK S-001 (2018) and API standards such as API RP 14B (2015), API RP 14C (2017) and API RP 17V (2015).

Table F-1 provides suggested standardised definitions of dangerous failures, fail/pass criteria and associated failure modes for the equipment classes listed in Table 2-3. Note that only topside equipment is covered so far. An explanation of the content of the table is given below:

Dangerous failures

Dangerous failures are often revealed upon functional (proof) tests, in which case they are defined as dangerous undetected (DU) failures. Since fail/pass criteria apply to functional testing dangerous detected (DD) failures, i.e., failure alarmed upon occurrence, are not explicitly considered in this chapter.

Fail criteria

The *fail criteria* provide precise failure definitions and the corresponding failure modes, and thereby define the acceptability of a *functional test*. Each fail criterion corresponds to a certain failure mode. A criterion is often identical to the corresponding dangerous failure definition, or it is split into several criteria and linked towards the relevant failure mode. As for dangerous (safety critical) failures, most fail-criteria apply on *tag level*, whereas some criteria may relate to *groups* of equipment, e.g., that a certain percentage of the tags must fail to define it as safety critical (e.g., emergency lights or deluge nozzles).

Each fail criterion is either *Boolean* or *numeric*: A Boolean criterion is either true or false (pass or fail) with respect to a descriptive criterion, e.g., shutdown valve does not close, pump does not start or sensor does not provide any signal / is frozen. A numerical criterion is a numerical value (requirement) that the corresponding measured value upon the proof test is compared with. The numerical requirement can often be tag specific. Examples of tag specific requirements are travel time requirement for a specific valve (of a certain dimension) and the HH set point(s) of a transmitter. In the tables, Boolean criteria are given in blue cells and numerical criteria are given in green cells:

Fail criteria			Failure modes
Boolean criterion			XXX
Measured value	Compared to	Numerical requirement	XXX

It should be noted that the fail criteria are established for functional (proof) testing but may also be relevant for demand situations, such as during a shut-down situation where valves shall close.

The *pass criterion* (contrary to the fail criterion) is a detailed description of a successful response of the equipment on functional test (or demand) with respect to safety.

Failure modes

The failure modes suggested are the level 2 (F2) failure modes that relate to the level 1 (F1) failure mode D (Dangerous failures which impair the safety function of the equipment) as given in Table E-1.

Notes

Here comments and references to the suggested fail-pass criteria are given. Comparison to ISO 14224, Appendix F, is also commented here.

Table F-1: Definitions of safety critical failures and fail/pass-criteria per equipment group

Equipment class / type	Dangerous failure	Fail criteria			Failure modes	Notes / comments
Input devices - process transmitters	The transmitter does not provide correct signal/alarm when the process parameter falls outside the setpoint limit(s).	The transmitter does not provide any signal.			NOO	• HIO is dangerous if the transmitter shall give L/LL alarm. • LOO is dangerous if the transmitter shall give H/HH alarm. • The 5% deviation criterion is considered as industry practice. • The deviation criterion (5%) may be reassessed for setpoints with high values (e.g. high pressure or temperature) and where the absolute deviation is important. • ISO 14224 (Table F.1) also suggests ERO as applicable failure mode for input devices (pressure, temperature, level, flow, etc.). For HVAC transmitters, ISO 14224 suggests FTF as the only applicable failure mode.
		The transmitter output value is frozen.				
		Transmitter output value	>	105% of LL setpoint.	HIO	
		Transmitter output value	<	95% of HH setpoint.	LOO	
Input devices – process switches	The switch does not provide correct signal/alarm when the process parameter falls outside the setpoint limit(s).	Process condition upon LL/HH alarm	>	105% of LL set point or 95% of HH set point.	FTF	• The 5% deviation criterion is considered as industry practice. • The deviation criterion (5%) may be reassessed for setpoints with high values (e.g. high pressure) and where the absolute deviation is important.
Input devices – position switches (Safety critical limit and proximity switches)	The switch does not confirm the correct position of the associated object (e.g. valve).	The switch does not confirm the correct position of the object (e.g. valve).			FTF	-
Input devices - Manual push buttons and call points	The push button / call point does not provide signal/alarm when activated.	The push button / call point does not provide signal/alarm to the logic when activated.			FTF	• ISO 14224 suggests both NOO, LOO, and FTF as applicable failure modes for manual call points.

Equipment class / type	Dangerous failure	Fail criteria	Failure modes	Notes / comments
Gas detectors	The detector does not provide correct signal/alarm in the presence of gas (in specified concentrations).	The detector does not provide any signal upon exposure of test gas/foil of 50% LEL or more.	NOO	• Test gas of 50% LEL (or more). • A separate assessment is recommended for detectors with low HH level (e.g. detectors in HVAC inlets). • Response times may be relevant to define for detectors in HVAC inlets. • "Blåsokk"/"strømpe" can be used for test of detectors exposed to wind / air flow. • See also NORSOK S-001 sect. 13.4.7 for suggested gas detector response time requirements.
		Detector read value upon exposure of test gas/filter/foil < **Point**: HH level (or 30% LEL in specific cases) **Line**: HH level (or 1.5 LELm in specific cases – equivalent to 30% LEL for point gas detector based on a 5m gas cloud.) **Acoustic**: HH level	LOO	
Fire detectors	**Smoke detector:** The detector does not provide HH alarm upon exposure of smoke. *Fire central not included.*	The detector does not provide HH alarm upon exposure of test smoke.	FTF	• ISO 14224 (Table F.1) suggests NOO, LOO, and FTF as applicable failure modes for fire detectors (smoke, heat, and flame). • See also NORSOK S-001 sect. 14.4.7 for suggested fire detector response time requirements. *The detector is tested by holding a magnet at a dedicated area of the detector such that a spectrum is generated that the detector is tested against.
	Heat detector: The detector does not provide HH alarm upon exposure of heat.	The detector does not provide HH alarm upon heat exposure.	FTF	
	Flame detector: The detector does not provide HH alarm upon exposure of flame.	**Traditional flame detectors:** The detector does not provide HH alarm upon exposure of test lamp. **Modern flame detectors:** The detector does not provide HH alarm upon exposure of magnetic test*.	FTF	
Logic solvers and interface elements	The logic does not initiate specific outputs based on specified inputs in accordance with the C&E.	The logic does not initiate its intended outputs (effects) upon receival of pre-defined inputs (causes).	FTF	• Logic elements are often tested together with input or output elements. However, these failures should be registered on the correct logic element and not on the corresponding input (or output) element.
		The I/O card or isolator/barrier does not provide input/output signal to/from the logic.	IOF	

Equipment class / type	Dangerous failure	Fail criteria			Failure modes	Notes / comments
Valves – Shutdown valves (topside)	The valve does not fully close on signal, exceeds the travel time requirement (if given) or exceeds the leakage requirement (if given).	The valve does not fully close on signal.			FTC	• The valve travel time requirements are based on the PSA/RNNP criteria for safety critical response times and correspond to the severity category *dead* in the CMMS. The companies' trigger point for repair, i.e. severity categories *degraded* or *sick* in the CMMS is however normally half the requirements given in the present table (i.e. 2s/inch). • *Valve travel time* applies from the valve receives the start signal (e.g. from safety node output if measured from SAS time stamps), excluding possible time delay, until valve is fully open/closed (e.g. limit switch). • It is recommended to specify procedures for adjusting the valve travel time with some margin (e.g. to adjust the valve travel time 30% below the given requirement). • Note that for XT valves, the response time requirement is 45s for the *entire* XT (NORSOK S-001). • LCP is critical when leakage rate requirement is given. The leakage requirement corresponds to the point for repair defined as *degraded* or *sick* in the CMMS. • Note that RNNP reporting of shutdown valves include failure reporting of both the valve and the solenoid(s). However, solenoid failures should be reported on the solenoid and not the main valve. [1] According to NORSOK S-001, a facility shall as a minimum be dimensioned to prevent escalation of a gas leak exceeding 0.1 kg/s, implicitly meaning that smaller leaks are not considered critical with respect to escalation. This criterion has been adopted by the industry with respect to acceptable leakage rate through an ESD (segmentation) valve, i.e. maximum leakage rate of 0.1 kg/s. In addition, and as also indicated in NORSOK Z-013), separate risk assessments may be performed that indicate other, possibly stricter, or possibly looser, requirements for individual valves. It has e.g., been commented that an internal leakage through a riser ESV is more critical than for a topside segmentation valve for which the neighboring process segments will be depressurized and
		Valve travel time	>	• Individually established requirement based on risk assessment. • Valves without individually assessed requirement: **Size** **Req.** ≤ 8'' 30s 10''–22'' 4s/inch ≥ 24'' 90s	DOP	
		Internal leakage rate	>	0.1 kg/s or individually assessed criterion [1]	LCP	

Equipment class / type	Dangerous failure	Fail criteria			Failure modes	Notes / comments
						the internal leakage in such case has a limited influence on the initial leakage rate (but will influence the leakage duration).
Valves - Solenoid/pilot valves	The solenoid/pilot does not change position upon signal.	The solenoid/pilot does not change position upon signal.			FTF	-
Valves – Pressure safety (relief) valves	The valve does not start to open / pop when upstream pressure exceeds the specified set point.	Pop (start open) pressure	≤	Minimum of 120% of set point **AND** 50 bar (5 MPa) above setpoint	FTO	• Requirement corresponds to: ○ 120% of set point for PSVs with set point <250 bar ○ 50 bar above set point for PSVs with set point >250 bar. • Premature opening (on too low pressure) can be critical for some PSVs.
		Pop (start open) verified but exceeds the above requirement.			DOP	
Valves- Blowdown (depressurisation) valves and fast opening valves	The valve does not open on signal or exceeds the response time requirement.	The valve does not open on signal.			FTO	• DOP is critical when response time requirement is given. • As for ESVs the valve travel time requirements are based on the PSA/RNNP criteria for safety critical response times and correspond to the severity category *dead* in the CMMS. The companies' trigger point for repair, i.e. severity categories *degraded* or *sick* in the CMMS is however normally half the requirements given in the present table (i.e. 2s/inch). • It is recommended to specify procedures to adjust the actual valve travel time with some 30% margin below the requirement. • Note that RNNP reporting of blowdown valves include failure reporting of both the valve and the solenoid(s). However, solenoid failures should be reported on the solenoid and not the main valve.
		Travel time	>	• Individually established requirement based on risk assessment. • Blowdown valves without individually assessed requirement: **Size** – **Req.** ≤ 8'' – 15s 10''–22'' – 4s/inch ≥ 24'' – 90s	DOP	

Equipment class / type	Dangerous failure	Fail criteria			Failure modes	Notes / comments
Valves – **Ballast valves**	The valve does not open/close on signal within the response time requirement.	The valve does not open on signal			FTO	• DOP is critical when response time requirement is given. *Response time requirements to be specified by operator. • Note that RNNP reporting of ballast water valves include failure reporting of both the valve and the solenoid(s). However, solenoid failures should be reported on the solenoid and not the valve.
		The valve does not close on signal			FTC	
		Response time open	>	Response time requirement open*	DOP	
		Response time close	>	Response time requirement close*		
Valves – **Deluge valves**	**Deluge valve:** The valve does not open on signal.	The valve does not open.			FTO	• ISO 14224 (Table F.1) also suggests DOP as applicable failure mode for the deluge valve. However, in such case an additional response time requirement must be given.
Valves – **Water mist release valve**	The valve does not open on signal, or the system pressure upstream release valve is not within specified value	The valve does not open on signal			FTO	• ISO 14224 (Table F.1) only suggests the FTO failure mode for the release valve, even though the failure definitions include both that the valve may fail to open or the system pressure upstream release valve not being within specified value.
		The system pressure upstream release valve is not within specified value			LOO	
Valves – **Gaseous agent release valve**	The valve does not open on signal, or the agent pressure/level is below some specified minimum.	The valve does not open on signal			FTO	• ISO 14224 (Table F.1) only suggests the FTO failure mode for the release valve.
		The agent pressure/level is below specified minimum			NOO	
Valves – **other fire-fighting valves**	The valve does not open on signal.	The valve does not open on signal.			FTO	• Applies to firewater monitor valves, foam valves and sprinkler valves
Nozzles [1)]	More than 3% of the nozzles on one skid are clogged, or more than one nozzle within each distribution line is clogged.	Number of clogged nozzles	>	3% of nozzles on the corresponding skid (general)	LOO	• ISO 14224 (Table F.1) suggests the PLU failure mode instead of LOO for the nozzles. If the failure is registered per nozzle, PLU is recommended. If the failure is registered per skid or distribution line (which most often is the case), LOO is recommended. [1)] Note that no explicit split has been made between deluge nozzles, water mist nozzles, sprinkler nozzles and gaseous agent nozzles
		Number of clogged nozzles on one distribution line	>	1		

Equipment class / type	Dangerous failure	Fail criteria			Failure modes	Notes / comments
Fire-fighting equipment – **Deluge activation (general requirement)**	Water or foam is not delivered within the response time requirement. (Deluge activation includes start of pump to the most distant nozzle).	Water or foam is not delivered within the response time requirement.			FTF	• ISO 14224 (Table F.1) also suggests the FTO failure mode for the active fire-fighting equipment to reach fire area with water/foam. [1] The PSA requirement is 15s. However, previous requirement of 20s is still yielding for many of the existing facilities.
		Response time (deluge activation)	>	30s (general) 15s [1] (helideck monitors)	DOP	
Fire-fighting equipment – **Fire water monitors**	The monitor does not operate/oscillate, and/or does not deliver water/foam to defined target area.	The monitor does not operate/oscillate or does not deliver water/ foam to defined target area.			FTF	-
Fire-fighting equipment – **Foam mixture**	The foam does not continuously mix into the water with required concentration.	The mixer gives intermittent flow			ERO	
		Foam concentration	< >	0.9% – 1.3%	LOO/ HIO	
Pumps – **Fire water pump**	The pump does not start upon signal, stops while running or delivers less than specified capacity. [1]	The pump does not start upon signal.			FTS	• The failure modes *FTS* and *UST* will also apply for foam pumps and water mist pumps. [1] Note that this failure definition will also apply to the complete firewater pump drive system, i.e. also including the engine and the generator. [2] May be a safety critical failure mode if flooding is a hazard (does not included as a failure mode for fire water pumps in ISO 14224, Table F.1).
		The pump stops unexpected/spurious while running.			UST	
		The pump does not stop upon signal.			STP [2]	
		Capacity at required pressure	<	90% compared to pump design curve	LOO	
Pumps – **Ballast pumps**	The pump does not start upon signal, stop upon signal, or stops while running.	The pump does not start upon signal			FTS	• ISO 14224 (Table F.1) suggests FTS as the only applicable failure mode for ballast pumps. However, the failure definition in the standard includes both fail to start and fail to stop.
		The pump stops unexpected/spurious while running.			UST	

Equipment class / type	Dangerous failure	Fail criteria			Failure modes	Notes / comments
HVAC – **Fire and shut-off dampers**	Damper does not fully close on demand (signal or safety fuse) or exceeds the response time requirement (if given).	The damper does not fully close on demand.			FTC	• To verify that the damper has closed (completely) on demand, a physical check is required to ensure gaskets and safety fuse are intact and that all blades have closed. • For fire dampers, ISO 14224 (Table F.1) in addition suggests FTO and FTS (probably related to associated HVAC fans) as applicable failure modes. [1] DOP is critical for shut-off dampers where response time requirement is given.
		The damper does not fully close within the required response time.			DOP [1]	
Electric generators - **Emergency generators**	Generator does not start on signal, stops while running (before 30 minutes) or delivers too low or too high voltage or frequency	The emergency generator does not start.			FTS	• ISO 14224 (Table F.1) suggests FTS and LOO (wrong voltage upon start) as applicable failure modes for emergency generator. [1] Example requirements from one operator.
		The emergency generator stops unexpected/spurious while running.			UST	
		Voltage delivered by generator	<	+/-2.5% of sufficient voltage [1]	ERO	
		Frequency delivered by generator	<	+/-5% of sufficient frequency [1]		
Combustion engines - **Diesel engines**	The engine does not start on signal.	The engine does not start.			FTS	
		The engine stops unexpected/spurious while running.			UST	
Uninterruptible power supply – **UPSs and battery packages**	The UPS and battery packages do not provide adequate uninterruptible power upon loss of main electrical supply or do not have the required capacity.	The UPS and battery packages do not provide uninterruptible power for minimum 30 minutes.			LOO	• ISO 14224 (Table F.1) suggests low capacity (LOC) as applicable failure mode. Note that ISO 14224 makes a split between central UPS for SIS and UPS for emergency lighting, whereas only the latter has a 30 min duration requirement. [1] The *nominal voltage* is the system *voltage* for which equipment is supposed to be operate.
		Voltage provided by the UPS and battery packages	< >	+6% - -10% of nominal voltage [1]	ERO	
Switchgear - **Circuit breakers, contactors and relays**	The breaker/contactor/relay does not open upon	The breaker/contactor/relay does not open upon demand.			FTF	• ISO 14224 (Table F.1) suggests both FTO and FTF as applicable failure modes for switchgear.

Equipment class / type	Dangerous failure	Fail criteria			Failure modes	Notes / comments
	overcurrent within specified time.					
Escape, rescue, and evacuation - Doors	**Fire doors:** The door does not close (and seal). **Water-tight doors:** The door does not close (and seal) within the time requirement.	The door does not close.			FTC	• ISO 14224 (Table F.19 suggests FTF as the only applicable failure mode for watertight doors (closure mechanism). [1] Note that rresponse time requirements apply for water-tight doors. The suggested response times must be further verified. Max 40s applies for mechanical/hydraulic remote closing system, whereas max 90s applies for manual closure of sliding doors using handpump (with facility in upright position), see also: https://lovdata.no/dokument/SF/forskrift/1991-12-20-878#KAPITTEL_11 [2] QOP = Quick operation
		Response time [1]	>	40s / 90s	DOP	
			<	10s	QOP [2]	
		The door does not seal / is leaking.			LCP	
Escape, rescue, and evacuation - Emergency lights	One or more emergency light (armature) in an area do not activate or remain lit for 30 minutes.	The emergency light does not activate or does not remain lit for 30 min			FTF	Not relevant for facilities with emergency light battery package (tested together with the rest of the UPSs)
Emergency communication - Radios	It is not possible to communicate (two-way) with the radio when operated.	It is not possible to communicate (two-way) with the radio.			FTF	
Emergency communication – PA loudspeakers	The loudspeaker announcement or sirens do not sound, or signal light is not activated in prescribed area upon signal.	The loudspeaker announcement or sirens do not sound, or signal light is not activated in prescribed area.			FTF	-
Lifeboats – Launch / release systems	Launch/release/lowering function does not work when operated.	The Launch/release/lowering function does not work.			FTF	[1] Lowering times only apply for conventional (davit launched) lifeboats (QOP = Quick operation)
		Lifeboat lowering time	>	40m/min	QOP [1]	
			<	18m/min	DOP [1]	

G Failure causes

This appendix presents an alternative failure cause taxonomy with focus on underlying causes. Note that the suggested taxonomy for failure cause *does not* exclude the use of failure mechanism according to ISO 14224 (cf. ISO Table B.2).

G.1 Failure cause taxonomies

Table G-1 summarises two relevant failure cause taxonomies used as input to the suggested APOS taxonomy. These are the taxonomies described in ISO 14224 and the current PDS classification.

Table G-1: Comparison of two failure cause taxonomies

OREDA/ISO 14224[1)]	**Current comparable PDS classification (ref. PDS data handbook, 2021 version)**
1. Design-related causes	Component hardware inadequacies
1.1 Improper capacity	
1.2 Improper material	
2. Fabrication/installation-related causes	
2.1 Fabrication error	Hardware related failure
2.2 Installation error	Installation/commissioning failure
3. Failures related to operation and maintenance	
3.1 Off-design service	Excessive stress failure
3.2 Operating error	Operation & maintenance
3.3 Maintenance error	Operation & maintenance
3.4 Expected wear and tear	Normal aging and degradation
4. Failure related to management	
4.1 Documentation error	Documentation
4.2 Management error	Management
NA	Software related failures

[1)] The ISO categories are based on two category levels. Four ISO categories at level 1 and ten categories at level 2 (when omitting general). In addition, ISO 14224 has defined a fifth level 1 category "Miscellaneous" that includes "no cause found", "common cause", "combined cause", "cascading failure" and "other".

A typical challenge with failure cause classification schemes is the difficulty of finding a suitable (level 1) category based on normal observations related to a failure. E.g., it will often be difficult to know whether a failure originates from design or fabrication. On the other hand, it may be known that some degradation or stress has been involved or that a user related / human error has occurred (e.g., a calibration error).

In the suggested APOS classification we have (as for detection method and failure mode) suggested to define two levels of failure causes; level 1 (recommended) that is a rough categorisation of the failure cause, and level 2 (optional) which in more detail relates to the failure type in terms of the phase and/or activity from where the failure origins.

The suggested level 1 failure cause classes are:

i. Degradation / stress related failures causes (random hardware failures plus excessive stress)

ii. Component (hardware and software) inadequacies (non-degradation related)
iii. Operator and user related failure causes (human interaction failure)
iv. Documentation and management related failure causes
v. Failure cause unknown

The suggested failure cause hierarchy is further illustrated and exemplified in Figure G-1 (note that the "unknown" failure class category is not shown in the figure).

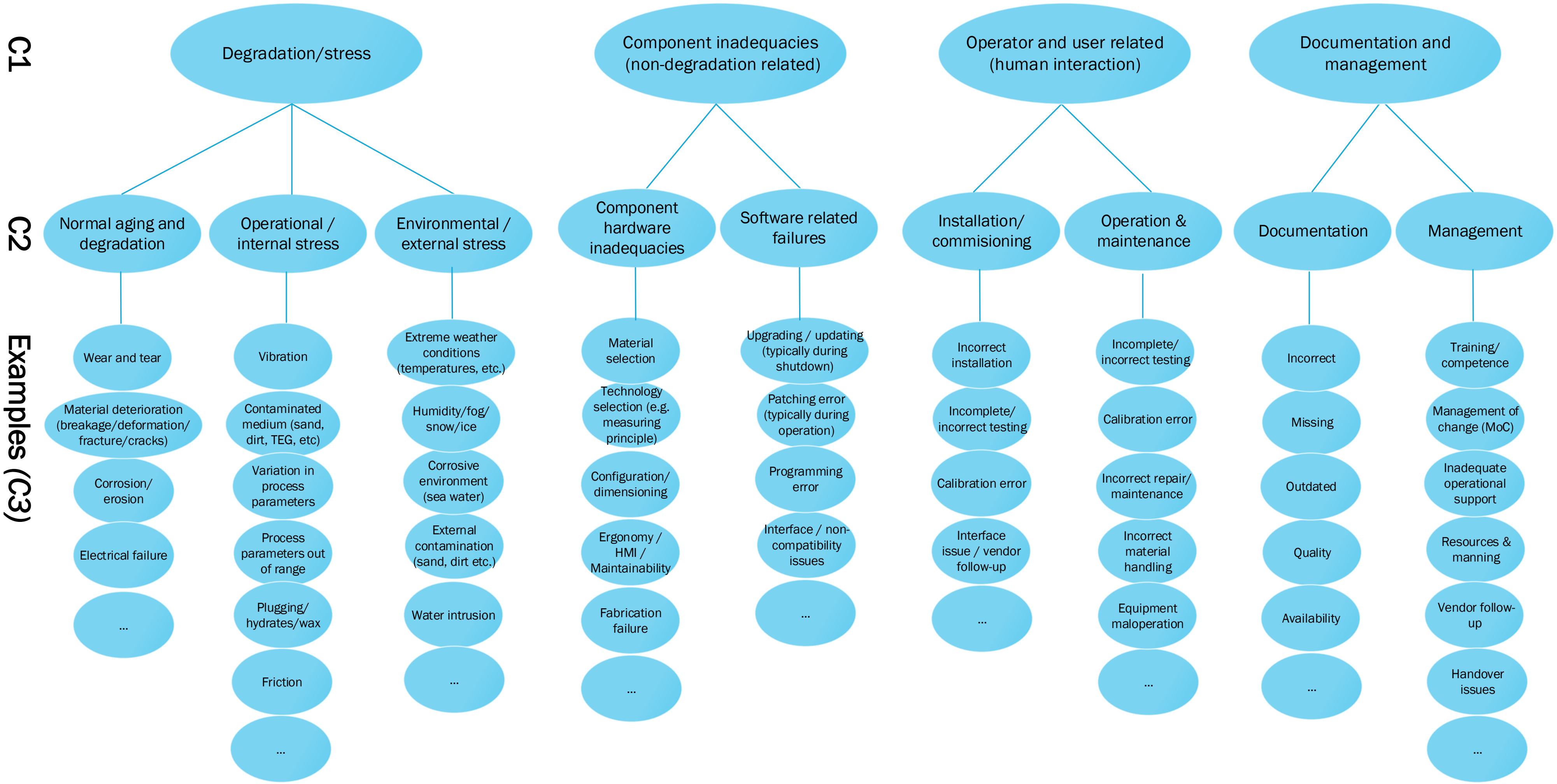

C1
C2
Examples (C3)
Degradation/stress
Component inadequacies (non-degradation related)
Operator and user related (human interaction)
Documentation and management
Normal aging and degradation
Operational / internal stress
Environmental / external stress
Component hardware inadequacies
Software related failures
Installation/ commisioning
Operation & maintenance
Documentation
Management
Wear and tear
Material deterioration (breakage/deformation/ fracture/cracks)
Corrosion/ erosion
Electrical failure
...
Vibration
Contaminated medium (sand, dirt, TEG, etc)
Variation in process parameters
Process parameters out of range
Plugging/ hydrates/wax
Friction
...
Extreme weather conditions (temperatures, etc.)
Humidity/fog/ snow/ice
Corrosive environment (sea water)
External contamination (sand, dirt etc.)
Water intrusion
...
Material selection
Technology selection (e.g. measuring principle)
Configuration/ dimensioning
Ergonomy / HMI / Maintainability
Fabrication failure
...
Upgrading / updating (typically during shutdown)
Patching error (typically during operation)
Programming error
Interface / non-compatibility issues
...
Incorrect installation
Incomplete/ incorrect testing
Calibration error
Interface issue / vendor follow-up
...
Incomplete/ incorrect testing
Calibration error
Incorrect repair/ maintenance
Incorrect material handling
Equipment maloperation
...
Incorrect
Missing
Outdated
Quality
Availability
...
Training/ competence
Management of change (MoC)
Inadequate operational support
Resources & manning
Vendor follow-up
Handover issues
...

Figure G-1: Suggested failure cause hierarchy

For level 2 it is suggested to classify the underlying failure causes according to the following nine (9) underlying categories:

Degradation / stress:

1) **Normal ageing and degradation:** i.e., normal wear and tear, vibration, corrosion/erosion, fatigue / material deterioration, cracking/bursting, electrical failure, etc. Failure causes within this category relates to operation conditions within the design envelope of the component.
2) **Operational / internal stress:** Process related off-design service such as excessive pressures or temperatures, excessive vibration, unforeseen sand production, unforeseen hydrate formation, etc.
3) **Environmental / external stress:** External impacts related to environmental conditions such as contamination, weather impacts (ice, moist, temperatures, etc.), corrosive environment, nearby sandblasting, etc.

Component (hardware and software) inadequacies (non-degradation related)

4) **Component hardware inadequacies:** Failure causes originating mainly from shortcomings during design or fabrication such as inadequate material selection, improper technology such as measuring principle, poor ergonomic / HMI, inadequate dimensioning, etc.
5) **Software related failures:** Software / programming errors, software upgrading/update errors, patching errors, non-compatibility issues, etc.

Operator and user related (human interaction failures)

6) **Installation/Commissioning:** Failure causes related to human errors (human interaction failures) during installation and commissioning (incl. check-out/testing) such as calibration error, incomplete/incorrect testing, incorrect installation, etc. Major modifications are considered as part of this category.
7) **Operation and maintenance:** Operator failures / human errors during operation and maintenance such as testing and calibration errors, repair failures, equipment maloperation etc. Note that in cases where the equipment has been subject to erroneous operation and overloads resulting in *immediate failure* of the equipment, this should preferably be classified under operation and maintenance (cf. examples "equipment maloperation" and "incorrect material handling in Figure 7-2). Minor modifications and component replacements are also included in this category.

Documentation and management

8) **Documentation:** Shortcomings related to technical and operational documentation / drawings / procedures, such as incorrect descriptions, documentation outdated or not available, poor quality, etc.
9) **Management:** Shortcomings and inadequacies related to operational management issues such as lack of training, poor management of change (MoC), inadequate operational support, handover deficiencies, etc.

It is assumed that most failure causes can be placed in one of the suggested level 2 categories (ref. Figure G-1). If not, only failure cause at level 1 can be selected (incl. "failure cause unknown"). Note that the failure cause may often be a compound of several causes and categories. Thus, it should be possible in the notification / work order to *select more than one failure cause* both at level 2, but also at level 1 since e.g., management/documentation will normally only be a contributing cause. Also note, that it will be possible to define an additional level 3 if considered desirable to enable even further specification of the failure cause.

G.2 Uncertainties and the need for failure cause analysis

Determination of failure cause – and root cause in particular – is often challenging and will therefore be associated with much uncertainty. This uncertainty *could be* expressed and assessed in the failure notification / work order by implementing *optional* tick offs, in the form of quality attributes, such as:

- The *assessed uncertainty* related to the selected failure cause(s) can be indicated by three choices:
  - Certain (no need for further investigation / root cause analysis)
  - Uncertain (need for further investigation / root cause analysis)
  - Not relevant (no need for further investigation / root cause analysis)

- *Additional information* about the assumed failure cause(s) and circumstances and any analysis performed/suggested, e.g., included as part of the free text field.

Note that such quality attributes, in theory also could have been implemented for determination of failure mode and detection method.

Failure cause analysis is often a question about time and resources. From a cost/benefit perspective such analysis will be particularly relevant for dangerous undetected (DU) failures, for frequently observed degraded failures with a potential to develop into dangerous failures, as well as for safe failures with a potential to cause loss of production (and obviously also for LOC and LEX failures). Analysis may often be of less relevance for simple/inexpensive components that are easily replaced. A simple flow diagram to evaluate the need for failure cause analysis is suggested in Figure G-2.

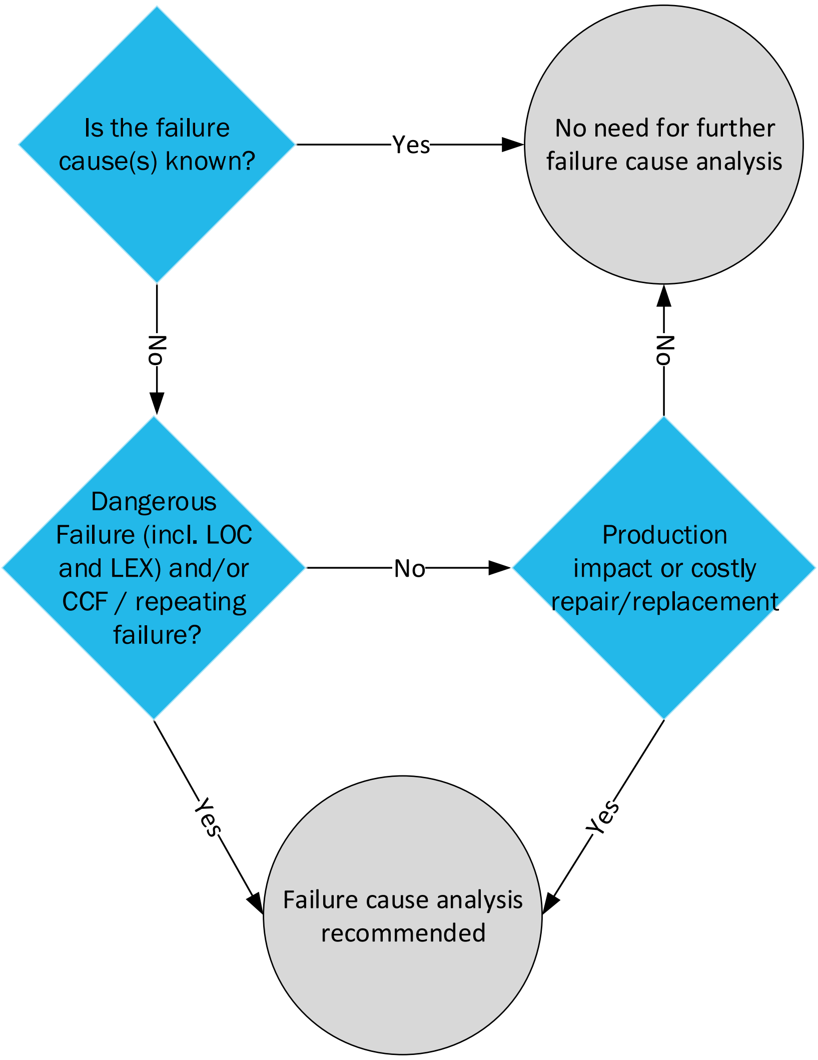

Is the failure cause(s) known?
Yes
No need for further failure cause analysis
No
Dangerous Failure (incl. LOC and LEX) and/or CCF / repeating failure?
No
Production impact or costly repair/replacement
No
Yes
Yes
Failure cause analysis recommended

Figure G-2: Suggested flow diagram for deciding whether failure cause analysis should be performed

Technology for a better society

www.sintef.no