NORSOK STANDARD

Z-008

Edition 3, June 2011

Risk based maintenance and consequence classification

Standards Norway
Strandveien 18, P.O. Box 242
N-1326 Lysaker
NORWAY

Telephone: + 47 67 83 86 00
Fax: + 47 67 83 86 01
Email: petroleum@standard.no
Website: www.standard.no/petroleum

Foreword

The NORSOK standards are developed by the Norwegian petroleum industry to ensure adequate safety, value adding and cost effectiveness for petroleum industry developments and operations. Furthermore, NORSOK standards are, as far as possible, intended to replace oil company specifications and serve as references in the authorities' regulations.

The NORSOK standards are normally based on recognised international standards, adding the provisions deemed necessary to fill the broad needs of the Norwegian petroleum industry. Where relevant, NORSOK standards will be used to provide the Norwegian industry input to the international standardisation process. Subject to development and publication of international standards, the relevant NORSOK standard will be withdrawn.

The NORSOK standards are developed according to the consensus principle generally applicable for most standards work and according to established procedures defined in NORSOK A-001.

The NORSOK standards are prepared and published with support by The Norwegian Oil Industry Association (OLF), The Federation of Norwegian Industry, Norwegian Shipowners' Association and The Petroleum Safety Authority Norway (PSA).

NORSOK standards are administered and published by Standards Norway.

Introduction

The purpose of this NORSOK standard is to provide requirements and guidelines for

- establishment of technical hierarchy,
- consequence classification of equipment,
- how to use consequence classification in maintenance management,
- how to use risk analysis to establish and update PM programmes,
- how to aid decisions related to maintenance using the underlying risk analysis,
- spare part evaluations.

This NORSOK standard is applicable for different purposes and phases such as:

- **design phase**: establish initial maintenance programme as an input to manning requirements and system configuration. Selection of capital spare parts;
- **preparation for operation**: development of initial maintenance programmes for implementation into maintenance management systems and selection of spare parts;
- **operational phase**: updating and optimisation of existing maintenance programmes. Guidance for prioritising work orders. Lifetime extension.

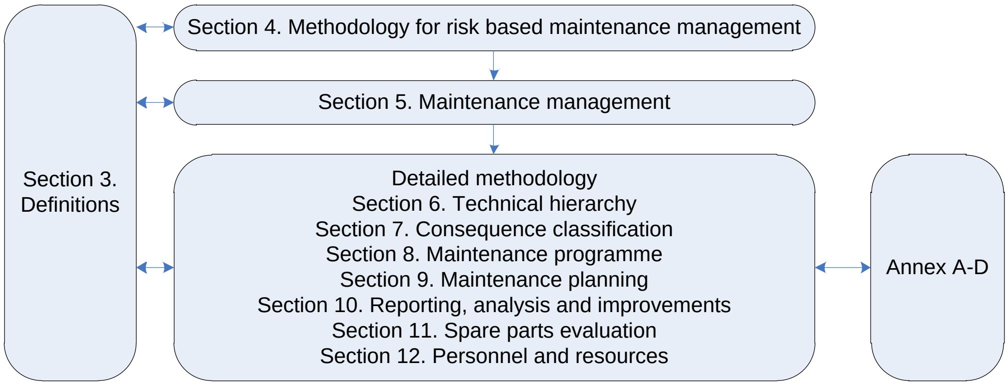
As a basis for preparation and optimisation of maintenance programmes for new and in service facilities all risk elements shall be taken into account, i.e. risks related to

- personnel,
- environment,
- production loss,
- direct and indirect cost including reputation.

The term "criticality analysis" is removed from Edition 2 of this NORSOK standard and replaced with consequence classification. This is due to a conflicting use of criticality analysis in the industry; some use it to describe a consequence analysis and some to describe a risk (probability and consequence) analysis.

This NORSOK standard is meant to define level of how this shall be done and deviations shall only provide better solutions with regards to maintenance management. This NORSOK standard should also be seen in conjunction with ISO 20815.

The standard describes the key work processes with explanation and requirements to each of them, and is organized in the following way:



1 Scope

This NORSOK standard is applicable for preparation and optimisation of maintenance activities for plant systems and equipment including

- offshore topside systems,
- sub-sea production systems,
- oil and gas terminals.

The systems involving the following types of equipment:

- mechanical equipment:
  - static and rotating equipment;
  - piping.
- instrumentation;
- electrical equipment.

Excluded from the scope of this NORSOK standard are

- load bearing structures,
- floating structures,
- risers and pipelines.

In principle, all types of failure modes and failure mechanisms are covered by this NORSOK standard.

This NORSOK standard covers

- definition of relevant nomenclature,
- brief description of main work flow related to maintenance and which elements this typically involves,
- definition of risk model and failure consequence classes,
- guidelines for consequence classification, including
  - functional breakdown of plants and plant systems in MFs and sub functions,
  - identification of MF and sub function redundancy,
  - assessment of the consequences of loss of MFs and sub functions,
  - assignment of equipment to sub functions and associated consequence classes.
- description of how to establish an initial maintenance programme, and how to update an existing programme,
- description on how to use the classification in combination with probability for decision making related to prioritising work orders and handling spare parts.

2 Normative and informative references

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

2.1 Normative references

API RP 580,	Risk-Based Inspection
DNV RP-F-206,	Riser Integrity Management
DNV RP-F-116,	Integrity Management of Submarine Pipeline System
DNV RP-G-101,	Risk Based Inspection of Topside Static Mechanical Equipment
IEC 60300-3-11,	Dependability Management Part 3-11: Application guide – Reliability centred maintenance
IEC 61508,	Functional safety for electrical/electronic/programmable electronic safety-related systems
IEC 61511,	Functional Safety – Safety instrumented systems for the process industry sector
ISO 17776,	Petroleum and natural gas industries – Offshore production installations – Guidelines on tools and techniques for hazard identification and risk assessment

ISO 20815[1],	Petroleum, petrochemical and natural gas industries – Production assurance and reliability management
ISO 13702,	Petroleum and natural gas industries – Control and mitigation of fires and explosions on offshore production installations – Requirements and guidelines
ISO 14224,	Petroleum, petrochemical and natural gas industries – Collection and exchange of reliability and maintenance data for equipment
NORSOK S-001,	Technical safety
NORSOK Z-013,	Risk and emergency preparedness analysis
OLF 070,	Guidelines for the Application of IEC 61508 and IEC 61511 in the petroleum activities on the continental shelf
OLF 122,	Life extension guideline

2.2 Informative references

BS 3811,	Glossary of terms used in terotechnology
EN ISO 12100,	Safety of machinery – General principles for design – Risk assessment and risk reduction
EN 13306,	Maintenance – Maintenance terminology
EN 15341,	Maintenance – Maintenance Key Indicators
NORSOK Z-DP-002,	Coding system

3 Terms, definitions and abbreviations

For the purposes of this NORSOK standard, the following terms, definitions and abbreviations apply.

3.1 Terms and definitions

3.1.1
availability
ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided (see EN 13306)

3.1.2
can
verbal form used for statements of possibility and capability, whether material, physical or casual

3.1.3
condition monitoring
continuous or periodic measurement and interpretation of data to indicate the degraded condition (potential failure) of an item and the need for maintenance (see BS 3811)

NOTE Condition monitoring is normally carried out with the item in operation, in an operating state or removed, but not subject to dismantling.

3.1.4
consequence
outcome from an event

NOTE There may be one or more consequences from an event. Consequences may range from positive to negative. However, consequences are always negative for safety aspects. Consequences may be expressed qualitatively or quantitatively (see API RP 580).

3.1.5
consequence classification
quantitative analysis of events and failures and assignment of the consequences of these.

NOTE See definitions in 3.1.6, 3.1.7 and 3.1.8.

[1] NORSOK Z-016 was replaced by ISO 20815 in 2008.

3.1.6
consequence HSE
health, safety and/or environmental consequence of an event

3.1.7
consequence production
effect with regard to production of a functional failure where effects of mitigation (e.g. spares, manning, tools) and compensation measures are not considered (= unmitigated consequence)

3.1.8
consequence other
other consequences as a result of a functional failure other than HSE or production consequence

NOTE May also include monetary losses and loss of reputation.

3.1.9
corrective maintenance
maintenance carried out after fault recognition and intended to put an item into a state in which it can perform a required function (see EN 13306)

3.1.10
equipment class
class of similar type of equipment units (see ISO 14224)

NOTE E.g. all pumps.

3.1.11
failure
termination of the ability of an item to perform a required function (see EN 13306)

NOTE 1 After failure the item has a fault which may be complete or partial.
NOTE 2 “Failure” is an event, as distinguished from a “fault”, which is a state.

3.1.12
failure cause
circumstances during design, manufacture or use which have led to a failure (see ISO 14224)

3.1.13
failure impact
impact of a failure on an equipment's function(s) or on the plant (see ISO 14224)

NOTE On equipment level, failure impact can be classified in three classes: critical, degraded, and incipient.

3.1.14
failure mechanism
physical, chemical or other processes which lead or have led to failure (see EN 13306)

3.1.15
failure mode
effect by which a failure is observed on the failed item (see ISO 14224)

3.1.16
failure rate
number of failures of an item in a given time interval divided by the time interval (see EN 13306)

NOTE 1 This value is an approximation.
NOTE 2 In some cases time can be replaced by units of use.
NOTE 3 In most cases 1/MTTF (where MTTF is mean time to failure) can be used as the predictor for the failure rate, i.e. the average number of failures per unit time in the long run if the units are replaced by an identical unit at failure. Failure rate can be based on operational or calendar time.

3.1.17
fault
state of an item characterized by inability to perform required function, excluding such inability during PM or other planned actions, or due to lack of external resources (see ISO 14224)

3.1.18
generic maintenance concept
GMC
set of maintenance actions, strategies and maintenance details, which demonstrates a cost efficient maintenance method for a defined generic group of equipment functioning under similar frame and operating conditions

3.1.19
hazard
potential source of harm (see ISO 17776)

NOTE In the context of this NORSOK standard, the potential harm may relate to human injury, damage to the environment, damage to property, or a combination of these.

3.1.20
hidden failure
failure that is not immediately evident to operations and maintenance personnel (see ISO 14224)

NOTE Equipment that fails to perform an “on demand” function falls into this category. It is necessary that such failures be detected to be revealed.

3.1.21
inspection
activity carried out periodically and used to assess the progress of damage in a component

NOTE 1 Inspection can be by means of technical instruments (e.g. NDT) or as visual examination.
NOTE 2 EN 13306 has been deviated from in order to apply to the most common use of the term “inspection” in the oil and gas industry, which relates inspection and inspection management to the activity of checking the conformity of the equipment by NDT instruments or visual examination at regular intervals.

3.1.22
item
any part, component, device, subsystem, functional unit, equipment or system that can be individually considered (see EN 13306)

NOTE 1 Item is also known as tag or functional location.

3.1.23
maintainable item
item that constitutes a part, or an assembly of parts, that is normally the lowest level in the hierarchy during maintenance (see ISO 14224)

3.1.24
maintenance
combination of all technical, administrative and managerial actions during the life cycle of an item intended to retain it in, or restore it to, a state in which it can perform the required function (see EN 13306)

3.1.25
maintenance effectiveness
ratio between the maintenance performance target and the actual result (see EN 13306)

3.1.26
maintenance management
all activities of the management that determine the maintenance objectives, strategies, and the responsibilities and implement them by means such as maintenance planning, maintenance control and supervision, improvements of methods in the organisation including economical aspects (see EN 13306)

3.1.27
maintenance strategy
management method used in order to achieve the maintenance objectives (see EN 13306)

3.1.28
may
verbal form used to indicate a course of action permissible within the limits of this NORSOK standard

3.1.29
modification
combination of all technical, administrative and managerial actions intended to change the function of an item (see EN 13306)

3.1.30
performance standard
PS
the performance standard describes the role of the barrier as a risk reducing measure and its relations to other safety systems managing a potential hazard. The performance standard outlines the requirements of the specific system in terms of its functionality (i.e. the essential duties that the system is expected to perform), integrity (i.e. reliability and availability parameters of the particular barrier) and survivability (i.e. the functionality of the barrier under the conditions of a major accident when the system is required to operate)

3.1.31
preventive maintenance
PM
maintenance carried out at predetermined intervals or according to prescribed criteria and intended to reduce the probability of failure or the degradation of the function of an item (see EN 13306)

3.1.32
production assurance
activities implemented to achieve and maintain a performance that is at its optimum in terms of the overall economy and at the same time consistent with applicable framework conditions (see ISO 20815)

3.1.33
redundancy
existence of more than one means at a given instant of time for performing a required function in an item (see EN 13306)

NOTE 1 Active redundancy; redundancy wherein all means for performing a required function are intended to operate simultaneously.

NOTE 2 Standby redundancy; redundancy wherein a part of the means for performing a required function is intended to operate, while the remaining part(s) of the means are inoperative until needed.

3.1.34
reliability centred maintenance
RCM
method to identify and select failure management policies to efficiently and effectively achieve the required safety, availability and economy of operation (see IEC 60300-3-11)

3.1.35
repair time
part of active corrective maintenance item during which repair is carried out on an item (see EN 13306)

3.1.36
risk
combination of the probability of an event and the consequences of the event (see ISO 17776)

3.1.37
risk based inspection
RBI
risk assessment and management process that is focused on loss of containment of pressurized equipment in processing facilities, due to material deterioration

NOTE These risks are managed primarily through equipment inspection (see API RP 580).

3.1.38
safety function
physical measures which reduce the probability of a situation of hazard and accident occurring, or which limit the consequences of an accident (see NORSOK S-001)

3.1.39
safety system
system which realises one or more active safety functions.

3.1.40
shall
verbal form used to indicate requirements strictly to be followed in order to conform to this NORSOK standard and from which no deviation is permitted, unless accepted by all involved parties

3.1.41
should
verbal form used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required

3.1.42
unsafe failure modes
failure modes dangerous to personnel but which do not threaten the MF of the equipment

3.2 Abbreviations

API	American Petroleum Institute
BoM	bill of material
BS	British Standard
CMMS	computerized maintenance management system
DNV	Det Norske Veritas
EN	European Standard
FMECA	failure mode, effect and criticality analysis
GMC	generic maintenance concept
HSE	health, safety and environment
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
KPI	key performance indicator
MF	main function
NDT	non destructive testing
OLF	Oljeindustriens Landsforening
OREDA®	offshore and onshore reliability data
P&ID	process and instrumentation diagram
PM	preventive maintenance
PS	performance standard
PSA	Petroleum Safety Authority
PU	parallel unit
QRA	quantitative risk analysis
RBI	risk based inspection
RCM	reliability centred maintenance
SAR	safe analysis report
SIL	safety integrity level

4 Methodology for risk based maintenance management

4.1 General

Risk assessment shall be used as the guiding principle for maintenance decisions. This NORSOK standard describes how to apply this in an efficient manner. The key elements of this methodology are as follows:

a) consequence classification of functional failure;
b) use of GMCs in combination with classical RCM methods. The GMCs are developed by RCM analysis including plant experience. The GMCs will implicit express the probability of failure via the maintenance tasks and the maintenance interval assigned. It is recommended that the GMCs are adjusted to the local conditions via a cost-benefit assessment and including other local conditions;
c) in case no GMCs are applicable or the purpose of the study requires more in-depth evaluations, an FMECA/RCM/RBI analysis should be carried out. Identification of relevant failure modes and estimation of failure probability should primarily be based on operational experience of the actual equipment. Alternatively generic failure data from similar operations may be used with sufficient reliability data qualification in accordance with ISO 20815, Annex E.2;
d) the application of the consequence classification and additional risk factors for decision making related to corrective maintenance and handling of spare parts.

As important as the risk assessment, is having well defined work processes and company/management commitment. This NORSOK standard describes the main work flow and sets minimum requirements to each of the steps in this process. Further the process points out the importance of continuous improvement based on reporting and analysis of the plant condition.

4.2 Safety functions

Establishment of function requirements for the safety functions should be based on risk evaluations of accidental events, which will determine the safety systems and their performance. The overall performance shall be documented in the form of PSs or equivalent. The PS will set requirements with respect to availability, capacity and performance of safety functions. Reference is made to NORSOK S-001, ISO 13702, IEC 61508, IEC 61511, OLF 070 and ISO 20815. ISO 14224, F.3, lists the most common safety systems/components for an oil and gas installation with definition of critical/dangerous failure modes.

One of the most important tasks for the maintenance organisation is to maintain this performance during the lifecycle of the plant. Availability requirements should be used to determine the programme for PM activities and the required contingency plans in the event of failure.

The inherent availability of the safety functions should be controlled and documented. The development of failure rate and system unavailability should be used as the basis for changing of test intervals and other mitigating actions to ensure compliance with function requirements.

4.3 Static process equipment

Static process equipment (containment function) has a dual function, i.e. a safety function related to leak failures and a production function related to storing and transporting gas or liquids, see Clause 7.

In order to establish an inspection programme for this equipment, it is necessary to perform detailed evaluations similar to an FMECA, usually named RBI. The process requires knowledge of

- damage mechanism which depends on material properties, internal fluid compositions and the external operational environment – determining the probability of failure,
- consequence of leak failure with respect to personnel, environment damages and financial losses

The combination of the above represents the risk of failure which should be mitigated.

The consequence classification methodology could be applied for screening of static mechanical equipment with the purpose of excluding non-critical equipment for further analysis and prioritise other equipment for in-depth risk evaluations as the basis for preparation of inspection programmes. The result of the RBI process is determination of

- location and extent of inspections and condition monitoring,
- inspection methods,
- inspection intervals.

There exist several standards for performing RBI analysis depending on type of object. Reference is made to DNV RP-G-101 for topside systems, DNV RP-F-206 for risers, and DNV RP-F116 for submarine pipeline systems. For refineries the API RP 580 can be applied.

4.4 Risk decision criteria

Risk based decisions have to be done against defined criteria. The definition of the criteria should be done in accordance with overall company policy for HSE, production and cost. The criteria shall be properly defined and communicated.

This NORSOK standard will not define any generic criteria, but describe an example of such criteria. See also NORSOK Z-013 and ISO 17776. The level of detailing in any risk matrix used is company specific, and can typical vary from a course 3x3 matrix to 5x10.

The following principles should apply:

- the risk matrix should as far as possible be the same for all operation for a company in order to aid common companywide optimisation and devote resources accordingly as well as having a common language for communicating risk;
- further, the same criteria should be used for all equipment and systems (also those excluded from this standard). This is in particular important for topside maintenance and inspection planning which are handling basically the same hardware;
- the consequence of loss of functionality (both loss of MF and sub functions) should take into account the standby redundancy (see 3.1.33) and reduce the impact accordingly.

Annex C gives example of criteria which can be used for classification, development of preventive work tasks and for prioritisation of work orders, as well as for optimisation of spares.

5 Maintenance management – Application of consequence classification

The purpose of this clause is

- to describe the key elements and expectations of the overall maintenance management work process,
- to describe where consequence classification is applicable in the maintenance management work process,
- highlight how risk management aspects are taken into account in the different steps in the process,
- link the main steps to the rest of the document where risk assessment details are described.

This description is not a comprehensive description of maintenance management in its wider sense. However, it gives a short description of what each step typically involves.

Maintenance management is illustrated as a work process where products are produced with low HSE risks and high production performance. The basic model proposed as industry best practice is shown in Figure 1[2].

On an overall level there are resources, management of work processes and results. Each of the elements in the management process may be detailed into a set of sub processes and products. In the following a brief description of the different elements in the maintenance management process is given. Those elements, where risk assessment, use of consequence classification and probability for failure assessment are important, are further described in this document and referenced below.

[2] The model is based on PSA “Basisstudie” from 1998

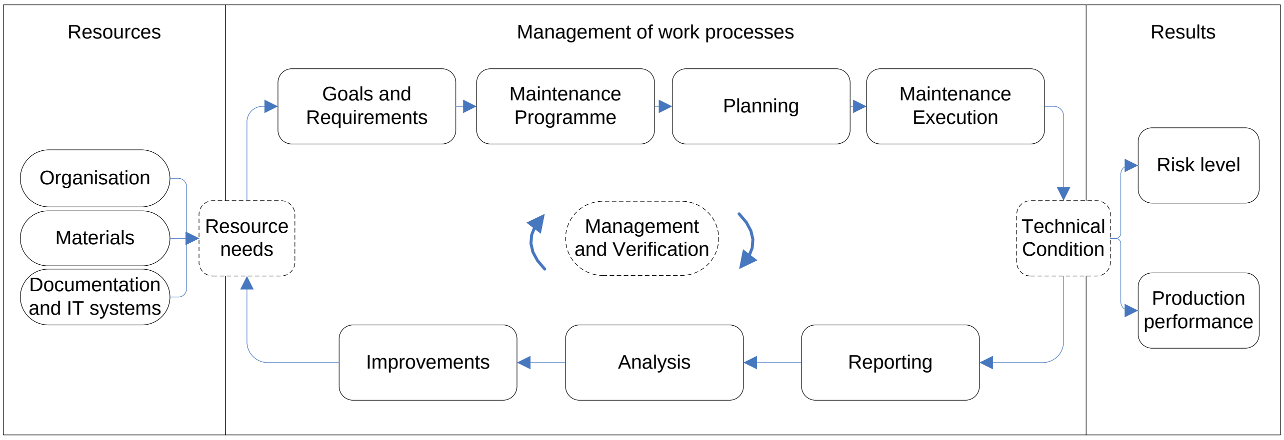


Figure 1 – Maintenance management process

Goals and requirements:

Goals should be established that commit the organisation to a realisable level of performance. The goals should focus on ambition level for

- risk, production and cost,
- regulatory requirements,
- technical condition of the facility in particular the performance of safety systems and critical processes,
- improvement of overall maintenance process.

Maintenance strategies should be defined for the asset.

Maintenance programme:

Failure modes, failure mechanisms and failure causes that can have a significant effect on safety and production shall be identified and the risk determined in order to establish a maintenance programme. The maintenance programme includes maintenance interval and written procedures for maintaining, testing, and preparing the various components within the plant.

This activity will typically involve the following:

- performing consequence classification for functions. The consequence class is inherited by the equipment relevant for the function;
- for equipment representing high consequence in case of failure, the failure mode, failure cause and the connected maintenance programme should be developed, documented and made traceable;
- safety barriers and/or safety functions should be identified, reliability requirements defined for the functions, and a testing programme to maintain the functionality should be developed;
- criteria for when the maintenance programme are to be updated based on time, experienced failures or similar should be defined. In particular failures of safety critical systems shall be analysed and the programme updated on a regular basis.

See Clause 7 and Clause 8.

Planning:

A maintenance plan is a structured set of tasks that include the activities, procedures, resources and the time required to carry out maintenance. Planning consists of budgeting, long term planning, day to day planning and prioritising.

This will typically involve the following:

- have a defined method and criteria for planning and prioritising of both preventive and corrective work based on its impact on HSE and production;
- the plans are regularly monitored and reviewed to access achievement, backlog, and efficiency.

See Clause 9.

Execution:

Execution includes preparations, work permits, carrying out work and reporting mandatory information on the work order. Maintenance and inspection work shall be executed in a safe and a cost-effective manner. System and equipment conditions shall be reported before/after repair for continuous improvement. Risk assessment shall be the basis for operational priorities.

This will typically involve the following:

- work execution shall be performed by competent personnel according to plans, procedures and work descriptions relevant for the actual case;
- the complexity of the work (both for individual jobs and for a set of jobs) should be taken into account;
- a plan for verifying the quality of work executed should be in place;
- the condition of the equipment should be reported after completion of work. For barriers with defined reliability targets, the failure data should be reported to aid analysis and comparison vs. PSs.

See Clause 10.

Reporting:

Reporting involves collection and quality assurance of maintenance data, and presenting these to maintenance departments and management in the form of defined indicators. In particular technical integrity data for safety functions shall be known and reported at appropriate levels to aid decision making.

This will typically involve the following:

- a set of KPIs should be defined for monitoring and follow up of performance;
- key performance indicator performance outside set goals should be reported and acted upon;
- reports of safety performance, production and cost versus goals/budget should be available and communicated in the organization;
- a set of performance data should be reported and compared to established PSs.

See Clause 10.

Analysis and Improvements:

This activity involves carry out analysis of historical maintenance data, and unwanted incidents related to maintenance, e.g. trend analysis, root cause failure analysis. Further the information should be evaluated and implement actions suggested based on the conducted analysis.

This will typically involve the following:

- a defined analysis process shall be in place addressing trigger values, analysis technique and responsibilities. The work shall be documented and monitored;
- the analysis process should include evaluation of maintenance effectiveness, i.e. to what extend the maintenance programme are handling the risks and performance requirements for individual systems or key components;
- the identified improvements, actions should be implemented and the effect should be monitored.

See Clause 10.

Organisation (Resources):

The organisation consists of the people, their training, competence, job descriptions and work processes.

This will typically involve requirements to organisation, competence and roles/responsibilities.

Materials (Resources):

Material resources include consumables, spare parts and tools required to carry out maintenance.

This will typically involve the spare part availability shall be optimized based on demand, consequence of failure, repair time and cost, and linked to the maintenance planning activity.

See Clause 11.

Documentation (Resources): Documentation in this context includes all documentation required to carry out and manage maintenance in an effective manner. This includes, but are not limited to, equipment/tag register, drawings and design details, historical maintenance data, maintenance task descriptions, spares lists.

This will typically involve the following:

- maintenance data are organized into a database where technical information, plans and historic performance are readily available for users and decision makers;
- this documentation needs to be controlled, updated and made available to the relevant user.

Management and verification: A key to good maintenance is a well organized management team taking responsibilities in implementing the principles herein and verifying the results. The management team should ensure that the maintenance work processes are followed. This will typically involve the following:

- the leaders should define roles and responsibilities and qualification requirements within the area of maintenance;
- the leaders should possess knowledge related to risk based maintenance management and make sure that the main work flow is followed;
- the leaders should monitor defined indicators (KPIs) and act upon deviations from set goals;
- in addition, the leaders should plan and institute audits of the organisation, suppliers and contractors.

Risk level (Technical condition): The risk level is a result of the operation and maintenance work done to the asset. Risk can be measured as HSE performance, barrier reliability status or related indicators.

Production assurance (Technical condition): The plant's production assurance is a result of the activities implemented to achieve and maintain a performance that is at its optimum in terms of the overall economy and at the same time consistent with applicable framework conditions. An indicator of this would be the achieved production availability.

Cost (Technical condition): Cost is here related to man cost for preventive and corrective work, spares and consumables, lost/deferred production that is under the control of the maintenance function.

6 Technical hierarchy

The technical hierarchy is a corner stone in maintenance management. It describes the technical structure of the installation by giving functional locations unique identifiers. The technical hierarchy provides an overview of equipment units that belong together technically, and shows the physical relationship between main equipment, instruments, valves, etc. The technical hierarchy should be established at an early phase to give an overview of all the tags/equipment and how they are related. The purpose of the technical hierarchy is as follows:

- show technical interdependencies of the installation;
- retrieval of tags, equipment and spare parts;
- retrieval of documents and drawings;
- retrieval of historical maintenance data from CMMS;
- planning of operations (e.g. relationships due to shutdown etc.);
- cost allocation and retrieval;
- planning and organization of the maintenance programme;
- planning of corrective work.

The level on which the maintenance objects are established is governed by practical execution and the individual need to monitor and control the different maintenance programmes. For corrective maintenance where the work orders can be assigned to any tagged equipment, the cost will be traceable to a lower level, but even this costing should be possible to summarise to the same level as for the maintenance objects used for the PM programmes.

See Annex D for detailed information and practical examples of the work process for establishing a technical hierarchy.

Reference is made to public coding standards:

- ISO 14224
- NORSOK Z-DP-002

7 Consequence classification

7.1 General

This clause describes how consequence classification should be done, its workflow and relation to maintenance programmes. Consequence classification expresses what effect loss of function can have on HSE, production and cost/other. The classification is done according to a consequence scale which is a part of the risk model, see Clause 4 and Annex C.

The consequence classification together with other key information and parameters gives input to the following activities and processes:

- selection of equipment where detailed RCM/RBI/FMECA analysis is recommended (screening process);
- establish PM programme;
- preparation and optimisation of GMCs;
- design evaluations;
- prioritisation of work orders;
- spare part evaluations.

7.2 Principles and work flow

Figure 2 shows an overall workflow related to classification. The following principles apply:

- The consequence classification is done to identify critical equipment for HSE, production and cost
- All systems and/or tags related to an installation should be classified using the same classification scale – regardless which method and standard is used for the classification.
- A functional hierarchy is established (MFs and sub functions). This is normally not stored in the CMMS but used during the classification process. See Annex D. Sub functions are linked to equipment/maintenance object in the technical hierarchy
- The classification feeds in to a common risk model used for operational decision making thus they need to be comparable.
- The static process equipment consisting of pipes, vessels, valves are normally consequence classified via an RBI analysis. The classification of HSE leakage may be done as a part of the RBI analysis or as a separate activity together with the overall classification of all functions and equipment. The containment has a dual function, i.e. a safety system with a PS and a production system with its production functions.
- Safety functions are defined via safety analysis (e.g. quantitative risk analysis) in the design or modification process. As such these systems and equipment are already identified and its function defined, normally with high consequence for HSE.
- The outcome of the classification will be a set of attributes assigned to each tag. The set of parameters should be aligned to the decision model. Examples of information to be assigned to each tag are
    - safety function identifier,
    - leakage HSE consequence,
    - functional failure/loss of function – HSE consequence,
    - functional failure/loss of function – production consequence,
    - functional failure/loss of function – cost/other consequence,
    - redundancy.

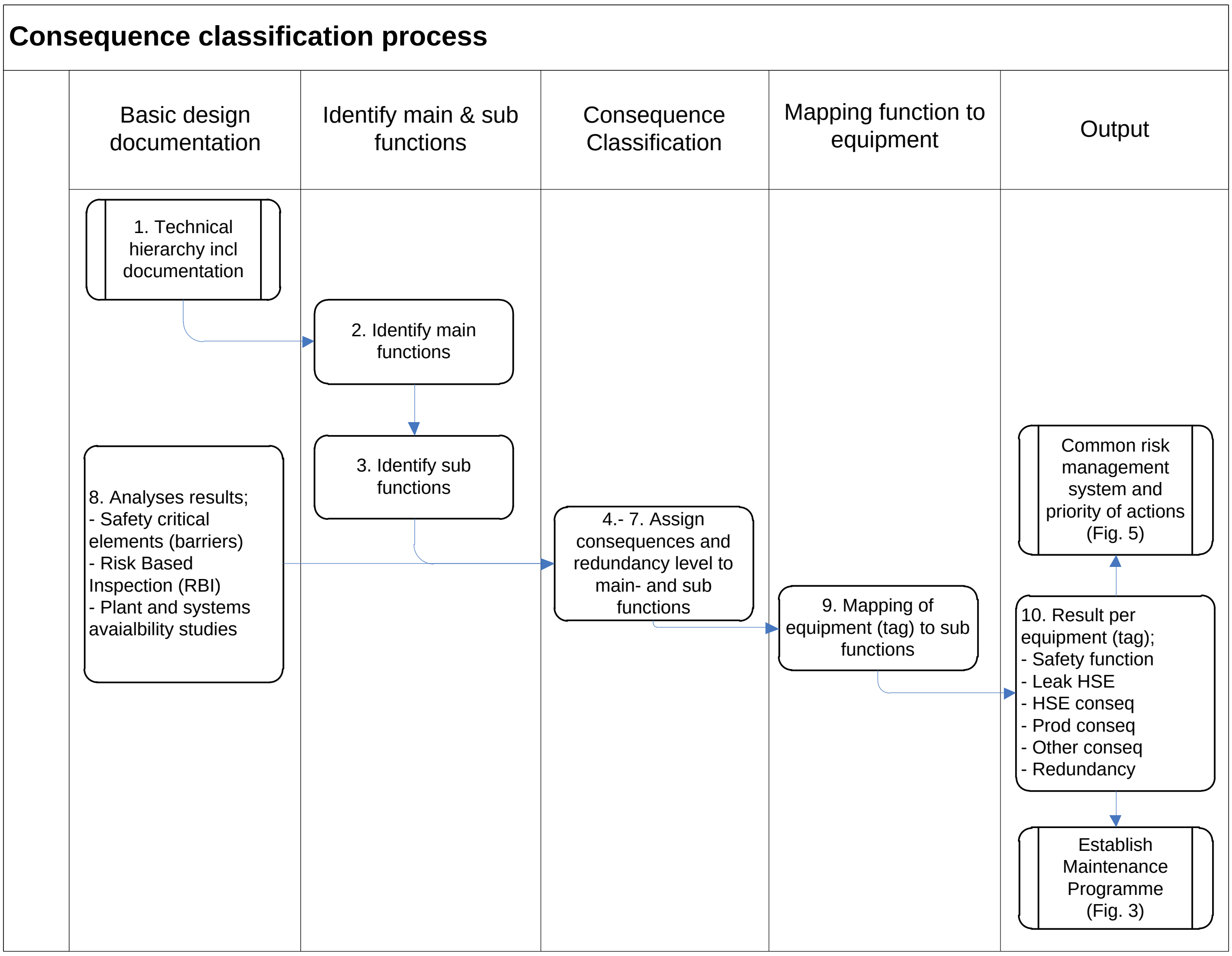


Figure 2 – Consequence classification process

7.3 Consequence classification of main and sub function

The functional classification work process is described stepwise below:

No	Step	Activity
1	Technical hierarchy	• The established technical hierarchy including documentation is used to identify systems and equipment which is subject to consequence classification.
2	Identify MFs	• Each plant system should be divided into a number of MFs covering the entire system. • The MFs are characterised by being the principal tasks in the process such as heat exchanging, pumping, separation, power generation, compressing, distributing, storing, etc. Annex A gives an overview of typical MFs for an oil and gas production plant. • Each MF is given a unique designation consisting of a number (if appropriate a tag number) and a name that describes the task and the process.
3	Identify sub functions	• MFs are split into sub functions. In order to simplify the consequence assessment, the sub function level can be standardised for typical process equipment with pre-defined terms. See Annex B. • The standard list of sub functions has to be supplemented with other sub functions relevant for the system configuration.
4	Assign MF redundancy	• MF redundancy shall be specified, see Table C.2 for example of redundancy definitions.

No	Step	Activity
		• In case of safety systems or protective functions with redundancy due to functional reliability or regulatory requirements, the redundancy effect should not be counted for.
5	Assign MF consequences	• The entire MF failure consequence is assessed in terms of the state where the MF no longer is able to perform its required functions. • Assuming that other adjacent functions and equipment are operating normally • In this assessment any redundancy within the function is disregarded, as the redundancy will be treated separately. • Other mitigating actions are not considered at this stage, i.e. like spares, manning, and tools. • The most serious, but nevertheless realistic effects of a function fault shall be identified according to set risk criteria. See Clause 4.
6	Assign sub function redundancy	• If there is redundancy within a sub function, the number of parallel units and capacity per unit shall be stipulated, see Table C.2 for example of redundancy definitions.
7	Assign sub function consequences	• The consequence on system/plant of a fault in a sub function is assessed with respect to HSE, production and cost according to the same principles as outlined for MF.
8	Input from other analyses	• Structures/pipelines and risers: These systems are not covered by this NORSOK standard, but the same classification systematic is proposed used. • Containment: For the tags/systems that are containment related, results from the RBI analysis are used to set the safety/environmental consequence of failure (leakage HSE). • Safety functions: Dedicated safety functions shall be identified via a risk assessment where performance requirements are defined such as reliability and survivability. In the classification process these systems are mapped to the tag hierarchy for readily identification in the CMMS system. The functional requirements are carried forward to the maintenance programme to maintain these functions, primarily in the form of functional testing.
9	Equipment mapping to function	• The equipment (identified by its tag numbers, see Clause 6) carrying out the sub functions shall be assigned to the respective sub functions. • If equipment performs more than one sub function (e.g. some instrument loops), it should be assigned to the most critical sub function. • All equipment (identified by its tag number) will inherit the same description, consequence classification and redundancy as the sub function of which they are a part. See Annex C for an example.
10	Result per equipment	• Consequence analysis should be documented according to 7.4 and the key data stored in CMMS readily available.

7.4 Documentation of consequence classification

A sound principle is to make the assessment available and traceable for updates and improvements of the results, as more information and feedback from the operation become available. As a minimum, the following should be documented:

- decision criteria;
- definition of consequence classes;
- MF description;
- sub function description;
- assignment of equipment (tags) to sub function;
- assessment of the consequences of loss of MFs and sub functions for all consequence categories, including necessary arguments for assignment of consequence classes;
- assessment of MF and sub function redundancy;
- any deviations should be documented and explained.

8 Maintenance programme

8.1 General

The purpose of a maintenance program is to control all risks associated with degradation of equipment. Maintenance includes e.g. calendar based activities, inspection, condition monitoring and testing. The program shall include activities and maintenance intervals per equipment. The classical way of establishing a maintenance programme is using RCM analysis, see IEC 60300-3-11. However, this NORSOK standard calls for using GMCs in combination with more detailed RCM methods. The generic concepts are considered an efficient way of capturing company knowledge for traditional technology where the maintenance tasks can be standardized. It is important that the generic concepts are adjusted to local operational conditions as well as the local risks associated with the plant in question.

8.2 Work flow for establishing preventive maintenance (PM) programme for new plants

The work flow for establishment of maintenance programme for new plants is described stepwise below and illustrated in Figure 3.

No	Step	Activity
1	Grouping and classification	Input to the process is the technical hierarchy and a functional grouping and functional classification of the plant in question. See Clause 8.
2	Safety functions	If the equipment is defined as a safety function, there should exist a Performance Standard and a safety requirement specification defining basic requirements including testing frequency for hidden failures. For safety functions with given availability requirements, there exists models for how to estimate testing time, see OLF 070 or IEC 61508. Further, for many safety systems there will exist additional maintenance tasks to be done like cleaning, lubrication, etc. which should be described in generic concepts for this equipment group. These data and tasks are then input to the PM programme.
3	Generic concepts	The next step in the process is to determine if there exist generic concepts for the equipment. If that is the case, the applicability and relevance of the concept should be checked as well as if there exist specific PM requirements from authority or company.
4	Adjustment of GMCs	The generic concepts should be evaluated for the actual case considering the production value of the plant (deferred production) and repair capacity (man-power, spares and tools) at hand to handle the most common failures. Any local adjustments should be in addition to the generic concept.
5	Risk analysis/ Assignment of maintenance activities	In case no GMC is applicable or the purpose of the study requires more in-depth evaluations, it is recommended that an RCM/RBI/SIL analysis is carried out according to IEC 60300-3-11 and DNV RP- G-101. Identification of relevant failure modes and estimation of failure probability should primarily be based on operational experience of the actual equipment, and alternatively on generic failure data from similar operations. Again, the task will involve both safety assessment and cost benefit to determine the maintenance tasks, as well as including authority/company requirements. See 9.3 for unsafe failure modes.
	Cost benefit analysis	Defining intervals are to a large extent based on engineering judgement The engineering judgement should be based on a form of cost-benefit assessment including the following factors: • consequences of function or sub-function failures and functional redundancy; • probability of function or sub-function failures and its function of time or frequency of PM activities; • detectability of failure and failure mechanisms, including the time available to make necessary mitigating actions to avoid critical function or sub-function failure; • cost of alternative preventive activities.
6	Developing	The above RCM/RBI/SIL analysis can be transformed to a GMC for later use on

No	Step	Activity
	generic maintenance concepts	similar equipment. Additional experience related to use of the concepts should be included.
7	Low consequence items	For equipments classified with low consequence of failure, a planned corrective maintenance strategy may be selected (run to failure). However, a minimum set of activities to prolong lifetime may also be considered. See 9.3 for unsafe failure modes.
8	Establish maintenance programme	Finally, all the maintenance tasks should be packed and scheduled considering plant production plans, resources requirements, turnaround schedule, etc to derive to the final maintenance plan.

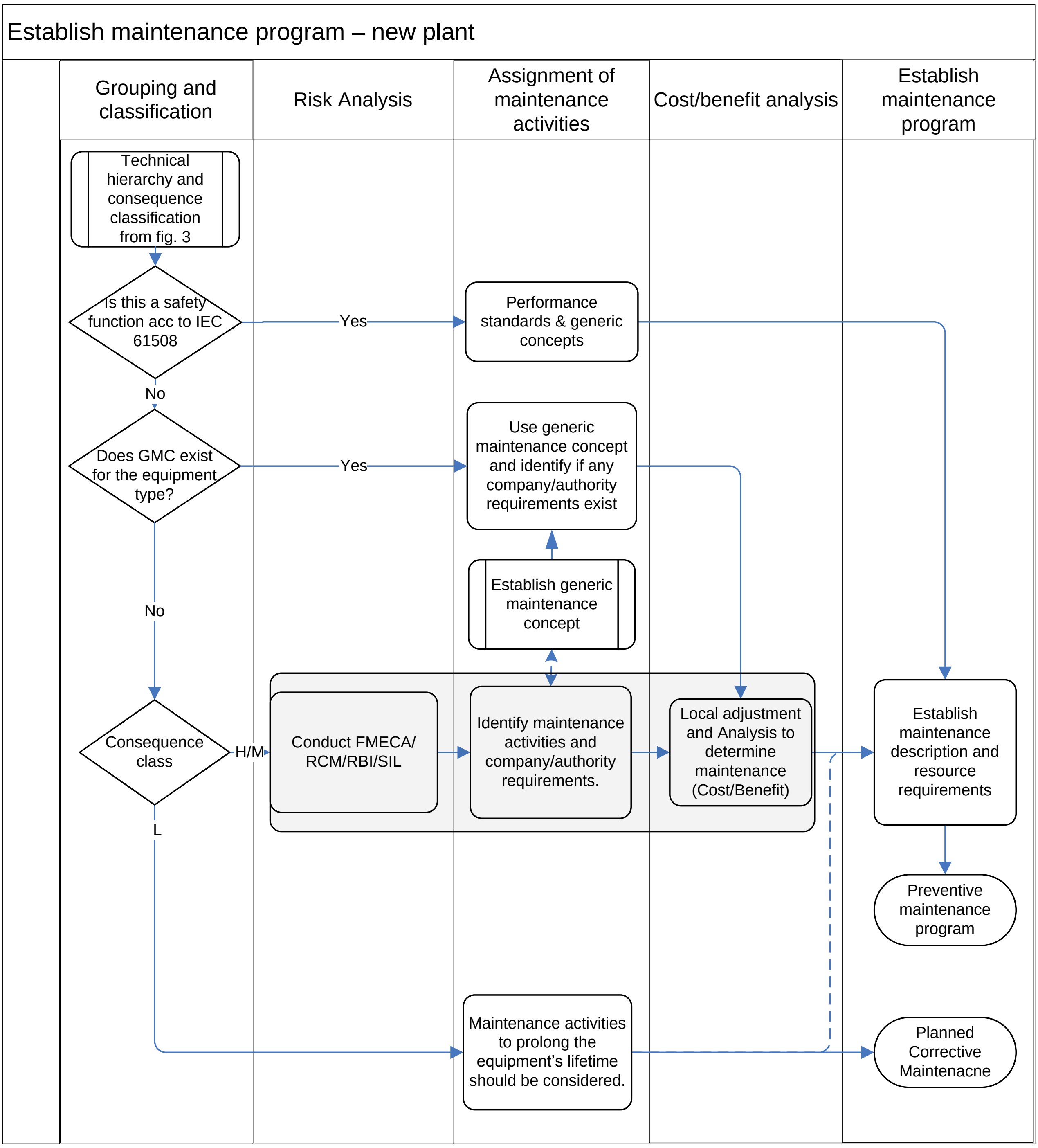


Figure 3 – Establishing maintenance programme for new plants

8.3 Unsafe failure modes

Some equipment may suffer failure modes dangerous for personnel but which do not threaten the MF of the equipment. Example is damage to electrical insulation causing short circuit dangerous for personnel touching the equipment. The short circuit is usually not considered a functional failure but represents a dangerous situation. These failure modes/causes risk shall be identified in the form of probability and consequence assigned as well as PM tasks to control the risk. This is best documented in a GMC or a RCM analysis

The CE (Conformité Européenne) marking of equipment shall include an assessment of personnel risk as part of the documentation. Relevant standard is EN ISO 12100.

8.4 Generic maintenance concept

8.4.1 General

A GMC is a set of maintenance actions, strategies and maintenance details, which demonstrates a cost efficient maintenance method for a defined generic group of equipment functioning under similar frame and operating conditions. The use of the GMC should ensure that all defined HSE, production, cost and other operating requirements are met. The concept shall include relevant design and operating conditions and should be documented by a RCM/FMECA analysis. A generic concept can be seen as a collection of best practices for a company, and as such should be maintained and updated via a controlled process as new experience and technology becomes available, see Annex D.

For safety functions: the performance requirements, the corresponding acceptance criteria and critical failure modes shall be defined on the concepts.

8.4.2 Application of generic maintenance concepts (GMCs)

Generic maintenance concepts may be developed in order to

- establish a company's minimum requirements to maintenance,
- reduce the effort in establishing the maintenance programme as similar equipments/technologies are pre-analyzed,
- ensure uniform and consistent maintenance activities,
- facilitate analysis of equipment groups,
- provide proper documentation of selected maintenance strategies,
- ensure experience transfer between plants with similar technology and operation.

Generic maintenance concepts are applicable for all types of equipment covered by this NORSOK standard.

A GMC can be utilized when

- the group of equipment has similar design,
- the equipment has similar failure modes, failure rates and operating conditions,
- the amount of similar equipment justifies the development of a generic concept.

In case of significant differences between the actual equipment and the equipment which has been the basis for the GMCs, the equipment in question has to be treated individually as a separate generic class of equipment. Basically, equipment failure modes are independent of equipment functionality, i.e. which functions the equipment supports. However, operational conditions, location and external environmental impact may influence the probability of failure and should be assessed prior to use of GMCs.

8.4.3 Preparation and documentation of generic maintenance concepts (GMCs)

The extent of documentation will differ depending on the complexity of the equipment and the risk attached. The concept should allow for adjustment of maintenance activities according to changes in the frame conditions.

The GMC should be established based on a detailed generic maintenance analysis (see Figure 3) including recommended maintenance interval and maximum allowed interval. In the local analysis, the generic concepts are adjusted to local operational conditions as well as the local risks associated with the plant in question. See Annex D for examples of how to document GMCs.

8.4.4 Local adjustments of a GMC

When a GMC is attached to a specific component/tag, the maintenance interval should be adjusted within the maximum allowed interval in GMC based on factors like

- higher or lower consequence class than described in GMC,
- different level of redundancy than described in GMC,
- operational conditions.

This local adjustment could either be done by use of adjustment factors to calculate interval, or by expertise statements.

8.5 Update maintenance programme

A maintenance programme needs updating at regular intervals. The triggers for such updating can be one or more of the following:

- the observed failure rate is significantly different from what was expected, i.e.:
  - higher failure rate is observed requiring a change in maintenance strategy or frequency – or replacement of the unit;
  - lower failure rate, or no observed damage at PM may point towards extension of intervals or omitting certain tasks.
- the operational environment has changed causing different consequence and probability:
  - less or more production;
  - change in product composition.
- cost of maintenance different from expected;
- new technology that could make the maintenance more efficient (like new methods for condition monitoring) is available;
- updated regulations;
- information from vendor;
- modifications.

The evaluation should be based on historical data and experience. A process diagram to update a maintenance programme is shown in Figure 4. If it is a safety system, an evaluation of number of failures per tests versus PS requirements should be performed. If there is a significant change in the safety system performance stated in the PS, this information should be feedback to the overall risk assessment for the plant.

For non-safety systems a cost-benefit analysis based on experience should be performed. Based on this evaluation maintenance programme and GMC (if relevant) should be updated, and implemented in the maintenance plan.

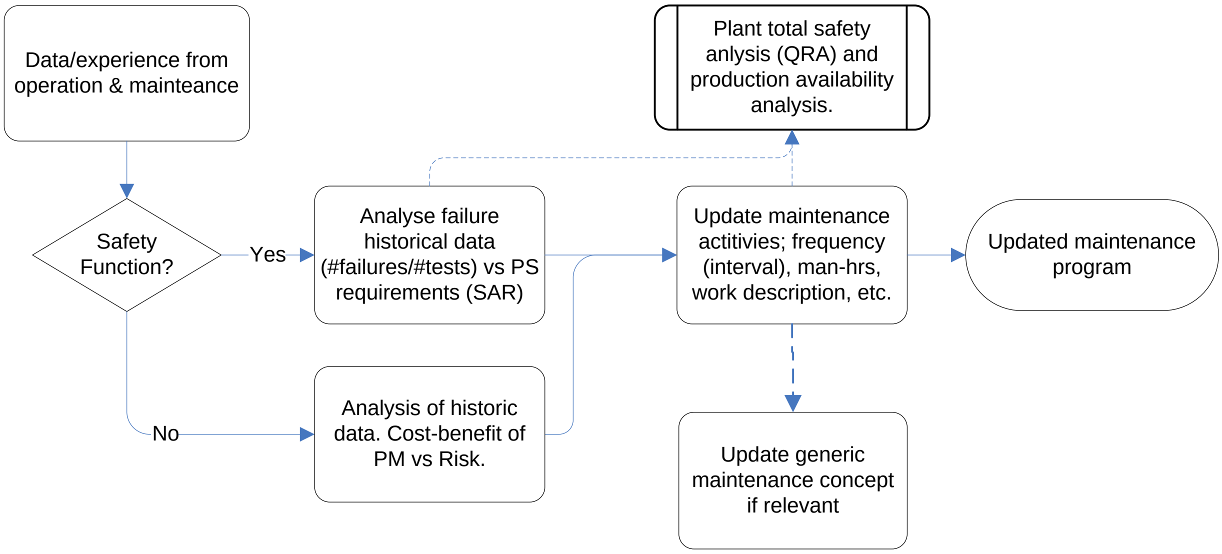


Figure 4 – Process for updating maintenance program

8.6 Maintenance programme and handling of ageing

Most maintenance programmes are based on a relatively constant failure rate not considering the ageing development that systems can suffer. However, the maintenance function should at any time have an overview of the ageing development for its components, and do maintenance and upgrading to ensure safe and reliable operation. This may require dedicated efforts beyond what is said in 9.5 when approaching the intended lifetime for the plant. Such an effort involves the following:

a) evaluate operational and degradation history. Any incidents with large degradation, abnormal operation, etc should be identified as well as any detrimental effect of modifications done to the unit. Collection and verification of system documentation and "as-build" documentation;
b) assessment of current condition/"as-is" condition;
c) evaluate the future ageing in view of the planned future operation and load planned for the asset:
   1) are there any ageing phenomena that have not been seen so far but are under development?
   2) are the safety function status and development according to requirements?
   3) will any equipment/system become obsolete so that spares no longer can be purchased?
d) based on c) decisions need to be made regarding
   1) updated/more intensive maintenance programme as well as change in spares holding strategy;
   2) replacement or modifications of single components or larger units;
   3) any operational constrains for the unit in view of ageing;
   4) dedicated analysis for e.g. structure.
e) finally, classification and maintenance programme should be updated, if relevant.

See OLF 122 for required documentation of maintenance and inspection in connection with extended lifetime.

9 Maintenance planning

9.1 Maintenance planning and scheduling

There shall exist a maintenance plan covering both preventive and corrective maintenance, and criteria for prioritisation shall be used to establish the maintenance plan. A method for prioritising maintenance should be in place. A PM program is established as described in Clause 8. This program consists of a list of maintenance activities and intervals for a plant. At certain time, e.g. 30 days before due date of an activity, a work order is generated in the CMMS system. The maintenance planner would then do the detailed planning, order material, personnel and tools for the activity.

9.2 Prioritising maintenance activities

The results from the consequence classification are useful when defining criteria for prioritising work orders – both preventive and corrective work. Preventive maintenance work orders should in principle be executed according to the given maintenance plan. Backlog related to the plan should be prioritised based on risk, i.e. probability and consequence of failure. Prioritization of corrective maintenance should be done based on the risk the failure represents, described as consequence and failure impact/probability of failure. Some companies call this process "Risk Based Work Selection", and have implemented it in their maintenance management system.shows an example of such a work flow, i.e. a selection of which corrective work orders to prioritize.

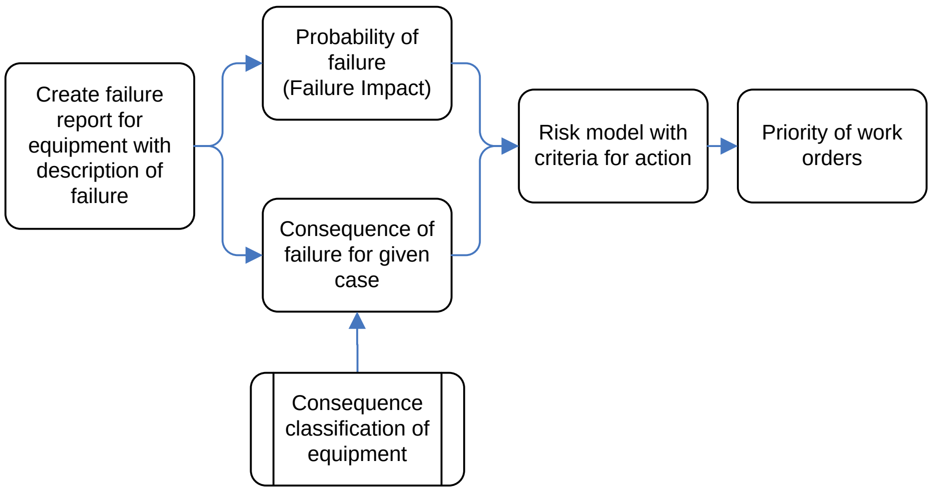


Figure 5 – Priority of corrective work orders

The process involves the following:

- assigning the consequence of failure to the case. It can be assigned via the consequence classification of equipment on overall functional level. This consequence should always be supplied by information regarding the actual failure mode, the operational state of the plant, possibilities for re-routing the process, etc. As such the process cannot be automatic, but requires involvement from personnel knowing the plant and the actual case. E.g. unsafe failure modes (see 9.3) for low consequence equipment;
- assigning the failure impact. The failure impact is a coarse probability scale, see Table 1. A time to failure scale may also be used, see Table C.3;
- for failure impact "degraded or incipient failure", a time to failure shall be assigned and used in the setting of priority (time) for the repair work;
- the risk associated with the consequence and probabilities as well as actions from this risk (priorities) shall be defined in given criteria e.g. via a risk matrix. Table C.3 shows an example of a risk model described as a risk matrix used to determine the priority;
- priority: Compensating operational actions used to temporarily maintain the function can be described as redundancy;
- compensating measures shall be in place when failure on the safety critical functions.

Table 1 – Failure impact scale

Failure impact	Definition	Note
Critical failure	Failure of an equipment unit that causes an immediate cessation of the ability to perform a required function.	Includes failures requiring immediate action towards cessation of performing the function even though actual operation may continue for a short period of time. A critical failure may result in an unscheduled repair.
Degraded failure	Failure that does not cease the fundamental function(s), but compromises one or several functions.	The failure may be gradual, partial or both. The function may be compromised by any combination of reduced, increased or erratic outputs. An immediate repair can normally be delayed, but in time such failures may develop into a critical failure if corrective actions are not taken.
Incipient failure	Imperfection in the state or condition of an item so that a degraded or critical failure may (or may not) eventually be the expected result if corrective actions are not taken	

10 Reporting, analysis and improvements

10.1 General

Reporting and analysis of maintenance performance is required in order to ensure continuous improvement. Below is described how this should be done.

10.2 Reporting

The ISO 14224 standard gives recommendations for reporting of data related to maintenance. Table 2 is extracted from ISO 14224 and lists a minimum of information recommended to be reported related to maintenance activities. For details, see ISO 14224. The need for reporting will vary between systems and has to be taken into account in order to avoid overloading of the field personnel.

Table 2 – Reporting of maintenance data

Corrective maintenance	Preventive maintenance
Failure mode Failure cause Failure mechanisms Equipment down time Spare parts used Man hours for activity Start and finish time of repair	Condition of equipment before PM work Man hours for activity Spare parts used Start and finish time

10.3 Key performance Indicators for maintenance management

Setting up the right set of KPIs facilitates people to focus and prioritise in the same direction. KPIs should be defined to support the overall goal and strategy for the operational phase.

As a minimum following KPIs should be established:

- failure fraction from functional testing of safety critical equipment;
- PM man-hours;
- corrective maintenance man-hours;
- backlog PM, total number of hours;
- backlog PM, number of hours HSE critical;
- backlog corrective maintenance, total number of hours;

- backlog corrective maintenance, number of hours HSE critical.

See ISO 14224, Annex E, and EN 15341 for examples of KPIs.

10.4 Analysis and Improvement

Based on reported maintenance data the effectiveness of maintenance shall be evaluated systematically. The organization should have established a set of key performance indicators to evaluate against – KPIs reflecting the goals and requirements for the operation, see Clause 5. For practical reasons some trigger levels should be applied above which a more detailed investigation is done aiming at finding the root-cause for the failure. The triggers can be related to

- HSE related equipment failure,
- unacceptable production losses,
- cost of single failure events in terms of downtime, repair cost or spare cost,
- number of repeated failures over a give time period for key components,
- hidden failures (exceeding requirements) detected during test,
- technical condition assessments.

Based on the event(s) the root cause(s) should be found and actions taken to avoid reoccurrence. The problem at question can be either single discipline or multidiscipline. The team should be allocated to the actual case, and will typically consist of personnel operating the equipment, maintenance engineers, and equipment experts. Basic knowledge of the most common root-cause analysis techniques is advantageous.

Finally implementation of the actions identified is a key to sustained improvement, as well as measurement of the effect via KPIs and equipment reliability data.

Learning from failure and events is a key to continuous improvement of performance of a plant and an organisation. Dedicated efforts should be done to drive this process and avoid “fire fighting” as opposed to systematic preventive work.

11 Spare parts evaluation

11.1 General

The spare part assessment defining need for spares, (number of, location and lead time) shall be based on results from the consequence classification. Further, the PM programme should state the needed spares for its activity giving estimate of the demand rate for spare parts used for PM.

The demand rate and which spare parts are needed for corrective maintenance is more challenging to estimate for a new plant. The typical sources are historical maintenance and inventory transactions, installation specific generic reliability data like OREDA®, vendor and maintenance personnel experience.

Further parameters such as procurement lead time and transportation time will have significant impact on the ultimate quantities of spare parts to be hold, their quantities as well as location.

11.2 Work flow for evaluation of spare parts

Figure 6 gives an overview of the work flow for evaluation of spare parts. Subclause 11.3 to 11.5 details the content in each box.

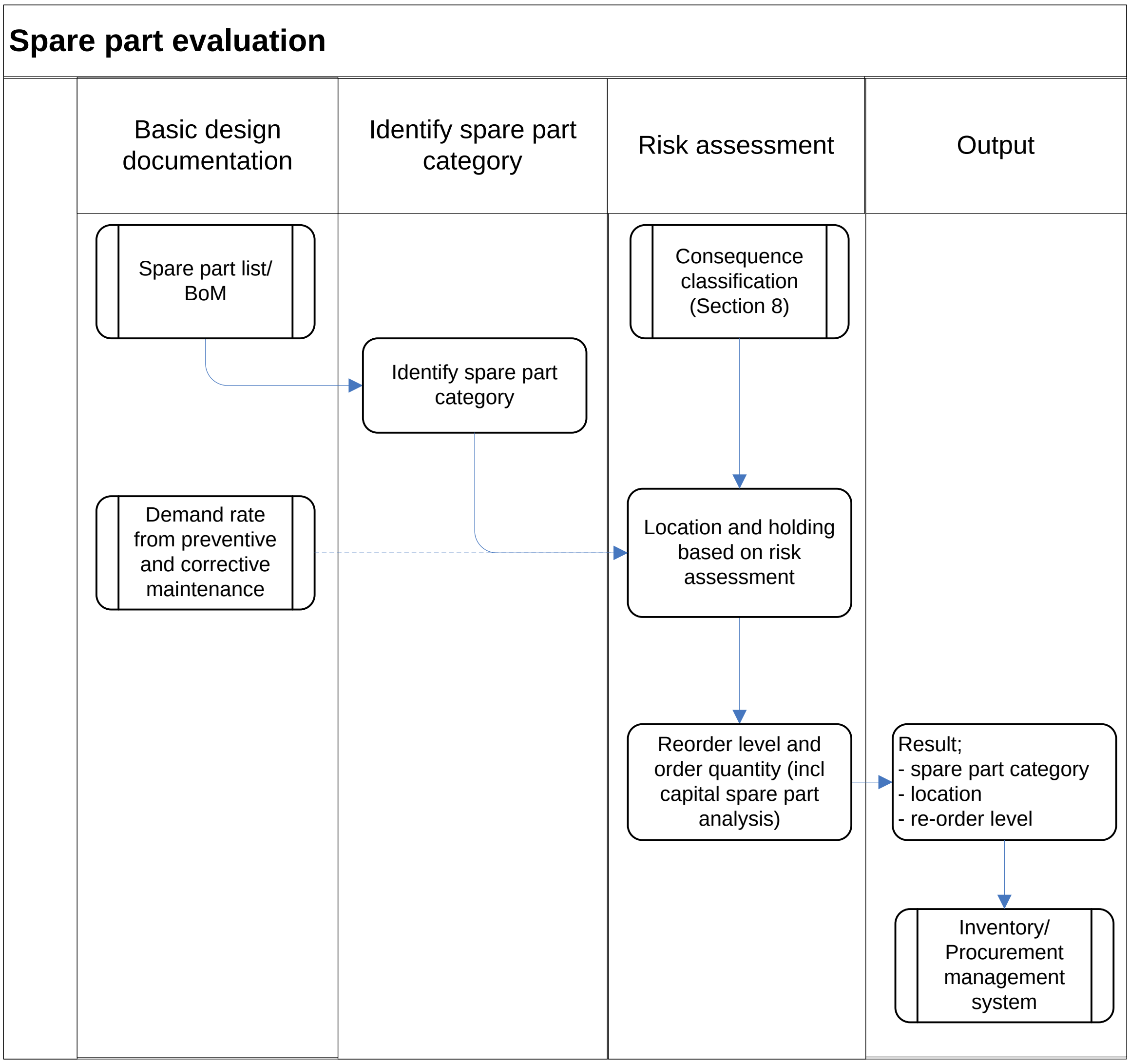


Figure 6 - Evaluation of spare parts

11.3 Spare part categories

Spare parts can be categorised as follows:

- capital spare parts:
    - vital to the function of the plant, but unlikely to suffer a fault during the lifetime of the equipment;
    - delivered with unacceptably long lead time from the supplier and usually very expensive;
    - often these spare parts are characterised by a substantially lower cost if they are included with the initial order of the system package.
- operational spare parts;
  Spare parts required to maintain the operational and safety capabilities of the equipment during its normal operational lifetime.
- consumables.
  Item or material that is not item specific and intended for use only once (non-repairable).

11.4 Location and holding

Spare parts are normally held at various locations. Determining the optimum location for a spare part can be done by use of a risk model where the dimensions are consequence of not having the spare parts in place and the demand rate. See Annex C, for an example of a risk matrix for use to determine location. Demand rate can be estimated from preventive and corrective maintenance. The consequence of not having the spare part in place can be established for this purpose, or by use of the functional classification, see Clause 7.

11.5 Reorder level and order quantity

The re-order level and order quantity are important parameters to control that spare parts are available without under- or overstocking. Traditional inventory methods and formulas can be used to estimate these parameters for operational spare parts and consumables. Capital spare parts are evaluated case by case based on a risk assessment. The output is a level of spare parts which incurs the minimum combination of costs and risks.

Reorder level is based on demand rate and delivery time, adjusted by a safety factor due to uncertainty. Order quantity is estimated based on demand rate, cost per order, and holding cost.

12 Personnel and resources

In order to get quality in the programme development, acceptance for changes and create a basis for continuous improvements, it is necessary to involve maintenance personnel and production operators in the risk assessment and preparation of the maintenance activities. A dynamic maintenance programme requires proper documentation of the evaluations for future adjustments and improvements according to new experience and changes of operational conditions. This applies irrespective of whether GMCs are applied or the maintenance programme has been developed on basis of the RCM/RBI/SIL analysis. The following type of personnel/experience should be involved:

- maintenance personnel with specific experience from different type of systems/equipment. Typically this will involve mechanical, instrument, electrical and corrosion/inception qualification on senior level;
- maintenance planners and/or maintenance supervisors;
- operation and process personnel with process/production experience handling the production impact of a failure;
- personnel with specific experience related to risk assessment and maintenance analysis – often acting as facilitators driving the process;
- maintenance engineers.

The above personnel may be employed by the operating organisation, by vendors or consultants.

Annex A
(informative)
Main function (MF) description and boundaries

Descriptions of MFs should aim to describe an active function (i.e. 'Pumping' instead of 'Pump'). Descriptions commonly used for MFs are shown in Table A.1. Normally a further specification is required to describe the MF sufficiently. If relevant, the availability, capacity and performance should be specified.

Table A.1 – Examples of MF descriptions

MF description	Sub title, examples
Accumulation	Instrument/plant air, heating/cooling medium
Cementing	
Circulating	Heating/cooling medium
Compressing	Gas export/injection
Cooling	
Detecting	Fire and gas
Distributing	(Main/emergency) power, hydraulic, tele
Drying	Air, gas
Expanding	
Filling	Lubrication oil
Filtering	
Fire fighting	Sprinkler, deluge, water spray, foam, aqueous film foaming foam, hydrants
Generating	(Main/emergency) power
Heating	
Injecting	Chemicals, gas, water
Life Saving	Mob, lifeboat, basket, raft, escape chute
Lifting	Deck crane, personnel, goods
Logging	Well, production, mud
Manoeuvring	
Metering	Fiscal (gas/oil), CO_2
Pumping	Oil/gas export, bilge, seawater
Regenerating	Glycol
Scrubbing	
Separating	Production, test, cyclone- (water/sand/oil), centrifuge
Storing	Chemicals, potable water, lubrication/seal oil
Transferring	Oil/gas pipe (riser)

Examples displaying the MF HF2020 (along with others) with boundaries marked on a flow diagram, and the same MF with boundaries marked on the more detailed P&ID is shown on Figure A.1 and Figure A.2.

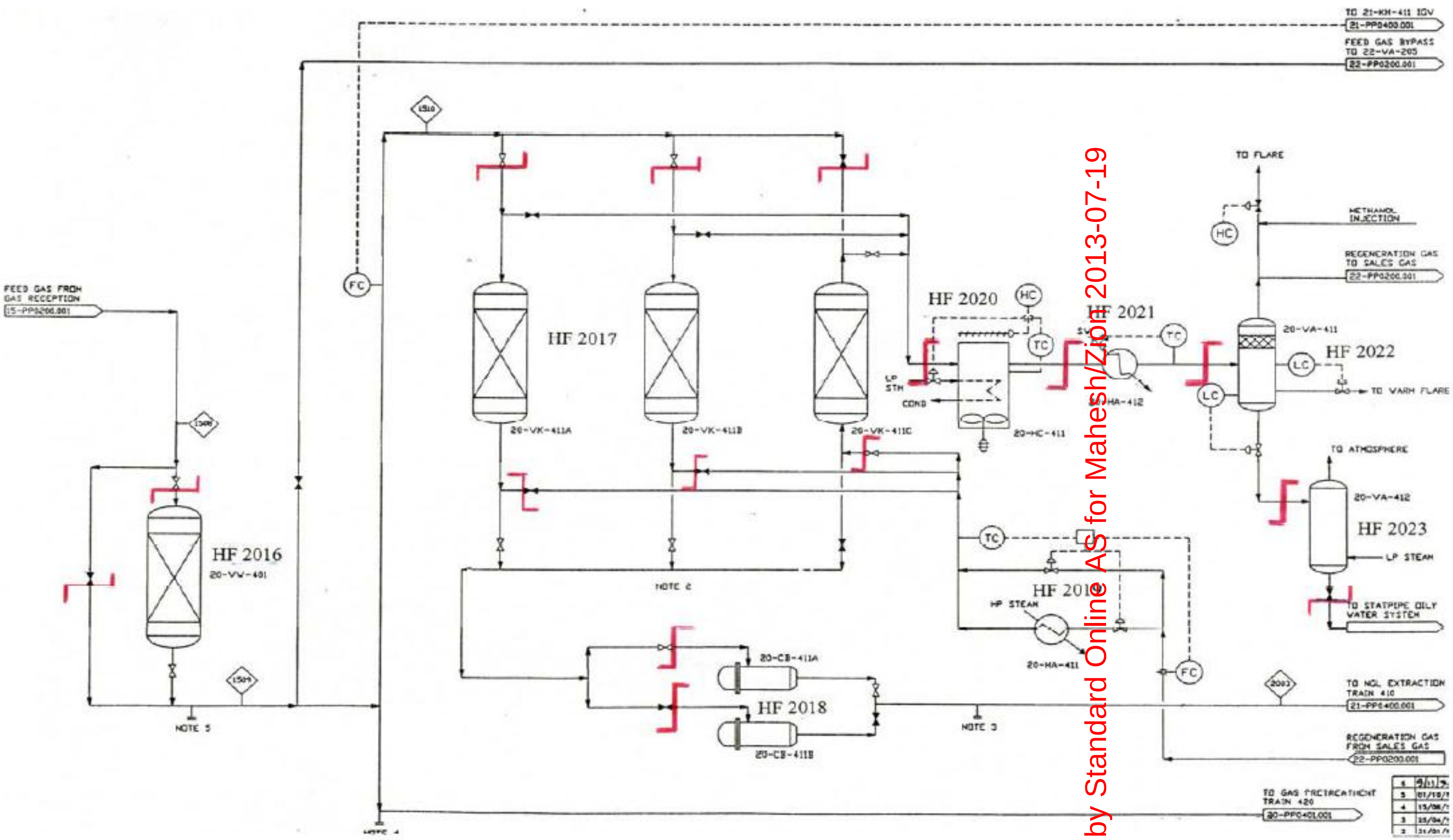


Figure A.1 – Flow diagram showing borderlines between MFs (HF2017, HF2020)

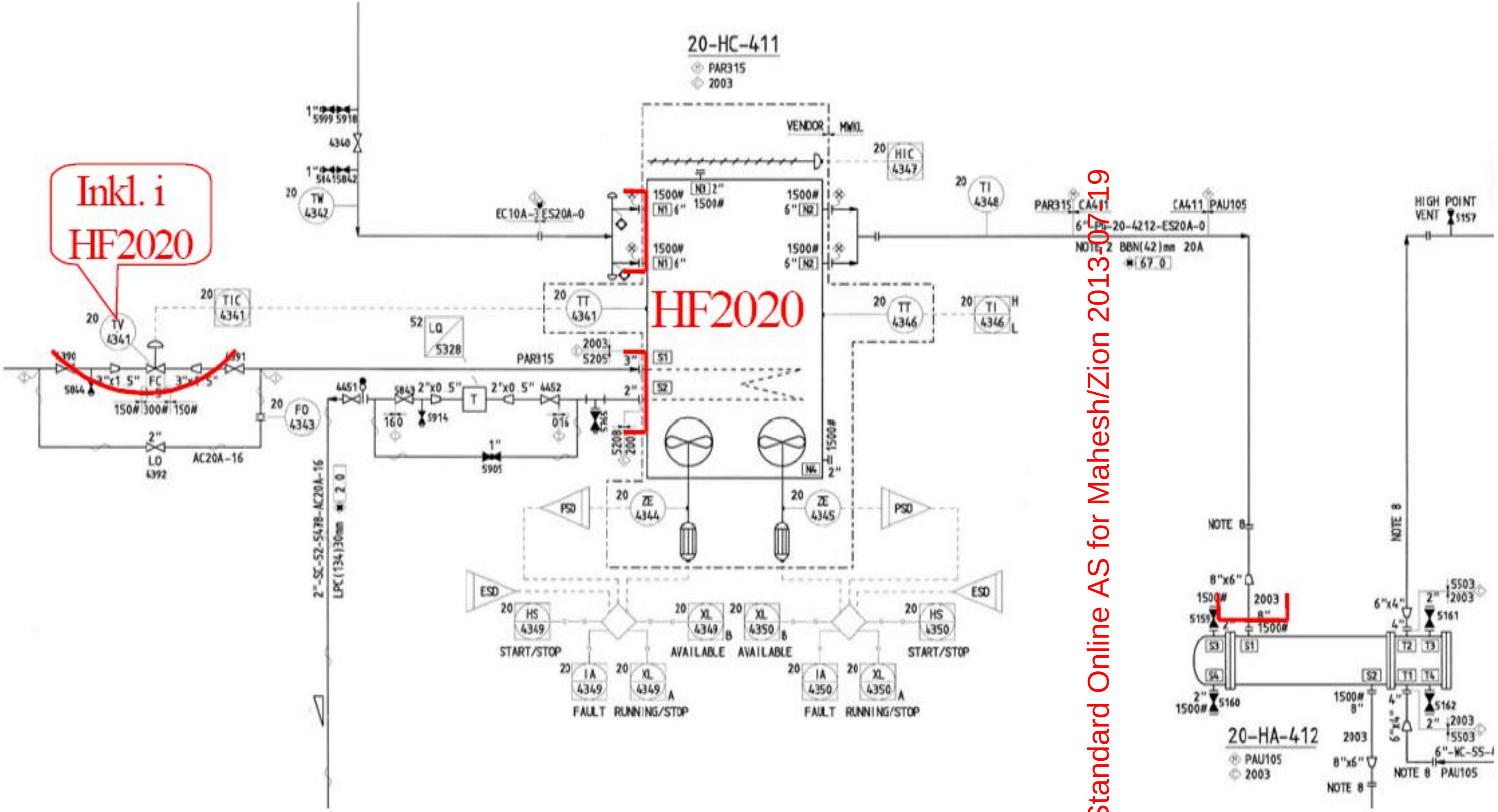


Figure A.2 – P&ID showing borderlines for MF HF2020

Annex B
(informative)
Simplifying consequence assessment of standard sub functions

The consequence assessment of the MF already performed may be used as a basis for establishing the consequence assessment for the standard sub functions. It is recommended that these evaluations are verified by experienced process personnel and adjusted individually, if needed.

An example of guidelines for the standardised sub functions for one project is shown in Table B.1.

NOTE – 'Other functions' have to be assessed independently.

Table B.1 – Project guideline example of consequence assessment of standardized sub functions, based on the MF consequence assessment

Standard sub function	Classification of loss of function				Comment
	RED	HSE	PROD	Other	
Main task	MF	MF	MF	MF	
Pressure, relief	Configu ration	H	L	L	**RED:** No redundancy for the failure mode 'Fail to operate on demand'
Shut down, process	A	H	L	L	**RED:** No redundancy for the failure mode 'Fail to operate on demand'.
Shut down, equipment	MF	M	L	MF	**Other:** Inherits the highest consequence from the MF
Controlling	MF	MF	MF	MF	
Monitoring	MF	M	L	L	
Local indication	MF	L	L	L	
Manual shutoff	MF	(MF)	(MF)	(MF)	

HSE/PROD/Other	See examples and definitions in Annex C
H/M/L	Consequence “High”, “Medium” or “Low”
MF	Will inherit MFs
RED	Redundancy, see definition in Table C.2.
( )	Reduce with one level from MF

Annex C
(informative)
Risk assessment criteria

C.1 Risk assessment using risk matrix

An example of a risk decision matrix is shown in Table C.3 for use in consequence classification, maintenance planning, inspection planning and for prioritising work orders. The risk matrix used for maintenance purposes should be harmonized with risk matrices used for evaluation of risk in other areas within a company. Table C.3 uses three classes for consequences, four for probabilities and four classes for risk. However, the company is free to choose the number of classes, and it is not necessary to use the same number of classes for consequences as for probabilities. It should also be mentioned that often the risk scale (low, medium, high) or the colour scheme (red, yellow, green) implicitly introduces risk acceptance criteria, thus should be carefully selected. ISO 14224, Table C.1 gives another example of failure consequence classification.

C.2 Risk decisions based on risk assessment

As important as the risk scale is the use of the risk for decision making. Table C.1 shows a set of criteria for prioritising time to repair connected to corrective work. The scale for time to repair should be based on company standard for maximum allowable time to complete repair and the mean time to failure.

Example: A failure is observed and the development time to critical failure (full functional outage) for this function is expected to be 2 years (corresponding to category 3 on the probability scale in Table C.3). The time to repair should be some fraction of this time, like 9 months for the highest consequence C3 and 18 months for the lower consequence C1.

Table C.1 – Example of priority of time to repair based on risk

Risk	Priority/time to repair	Comment
H	5 days	Always highest priority for safety function failure.
M	30 days	
L	180 days	
VL	360 days	

Table C.2 – Example of redundancy definitions

RED	Redundancy degree definition
A	No redundancy i.e. the entire system is required to avoid any loss of function.
B	One parallel unit can suffer a fault without influencing the function.
C	Two or more parallel units can suffer a fault at the same time without influencing the function

Table C.3 – Example of risk matrix used for consequence classification and for decisions

Freq. cat.	Freq. per year (*), (**)	Mean time between failure (year)	RISK		
F4	> 1	0 to 1	M	H	H
F3	0,3 to 1	1 to 3	M	M	H
F2	0,1 to 0,3	3 to 10	L	M	H
F1	< 0,1	Long	L	L	M
			Loss of function leading to:		
Consequence category			**C1**	**C2**	**C3**
Consequence safety			No potential for injuries. No effect on safety systems.	Potential for injuries requiring medical treatment. Limited effect on safety systems.	Potential for serious personnel injuries. Render safety critical systems inoperable.
Consequence containment			Non-flammable media Non toxic media Natural/normal pressure /temperature media	Flammable media below flashpoint Moderately toxic media High pressure/ temperature media (>100 bar/80 °C)	Flammable media above flashpoint Highly toxic media Extremely high pressure /temperature media
Consequence, Environment; restitution time (***)			No potential for pollution (specify limit) < 1 month	Potential for moderate pollution. 1 month – 1 year	Potential for large pollution. > 1 year
Consequence production			No production loss	Delayed effect on production (no effect in x days) or reduced production	Immediate and significant loss of production
Consequence other			No operational or cost consequences	Moderate operational or cost consequences	Significant operational or cost consequences

(*) Based on failure mode
(**) Typical failure rate ref OREDA(®: 1-100 * 10^-6 for rotating equipment (0.01-1 1/yr)
(***)The consequences to the external environment differ significantly depending on the chemical composition of the released substance, volume and the recipients (open sea, shore, earth or atmosphere). Here restitution time is used as a common denominator.

C.3 Risk assessment of spare parts

An example of consequence classes which can be used to determine the optimum location for spare parts is given in Table C.4. Input from the consequence classification can be used or modified for this purpose. The consequence classes combined with demand rate gives location of spare parts as shown in Table C.5.

Table C.4 – Example of consequence classes for spare parts

Consequence	Description
High	Equipment of a system that shall operate in order to maintain operational capability in terms of safety, environment and production.
Medium	Equipment of a system that have installed redundancy, of which either the system or its installed spare must operate in order to maintain operational capability in terms of safety, environment and production.
Low	No consequence for safety, production or environment.

Table C.5 – Example of risk matrix for spare parts

Consequence / Demand rate	Low	Medium	High
First line spare parts, frequently used.	Minimum stock at site	Minimum stock at site and any additional spare parts at central warehouse	Adequate stock at site
Not frequently used.	No stock	Central warehouse, no stock at site	Central warehouse and minimum stock at site if convenient
Capital spare parts. Seldom or never used.	No stock	No stock	Holding optimized by use of risk assessment case by case

Annex D
(informative)
Practical examples

D.1 Technical hierarchy

The level of detail with regards to tagging is in many ways a deciding factor to ensure that the equipment will receive the adequate maintenance. On the Norwegian Continental Shelf there is an industrial heritage of tagging to a detailed level where even instrumentation and equipment in support of MFs and sub functions are tagged The tagging is to be consistent from drawings, the actual equipment in the installation and the CMMS and is an important part of documenting the equipment through its life cycle.

Figure D.1 illustrates the workflow to establish a technical hierarchy.

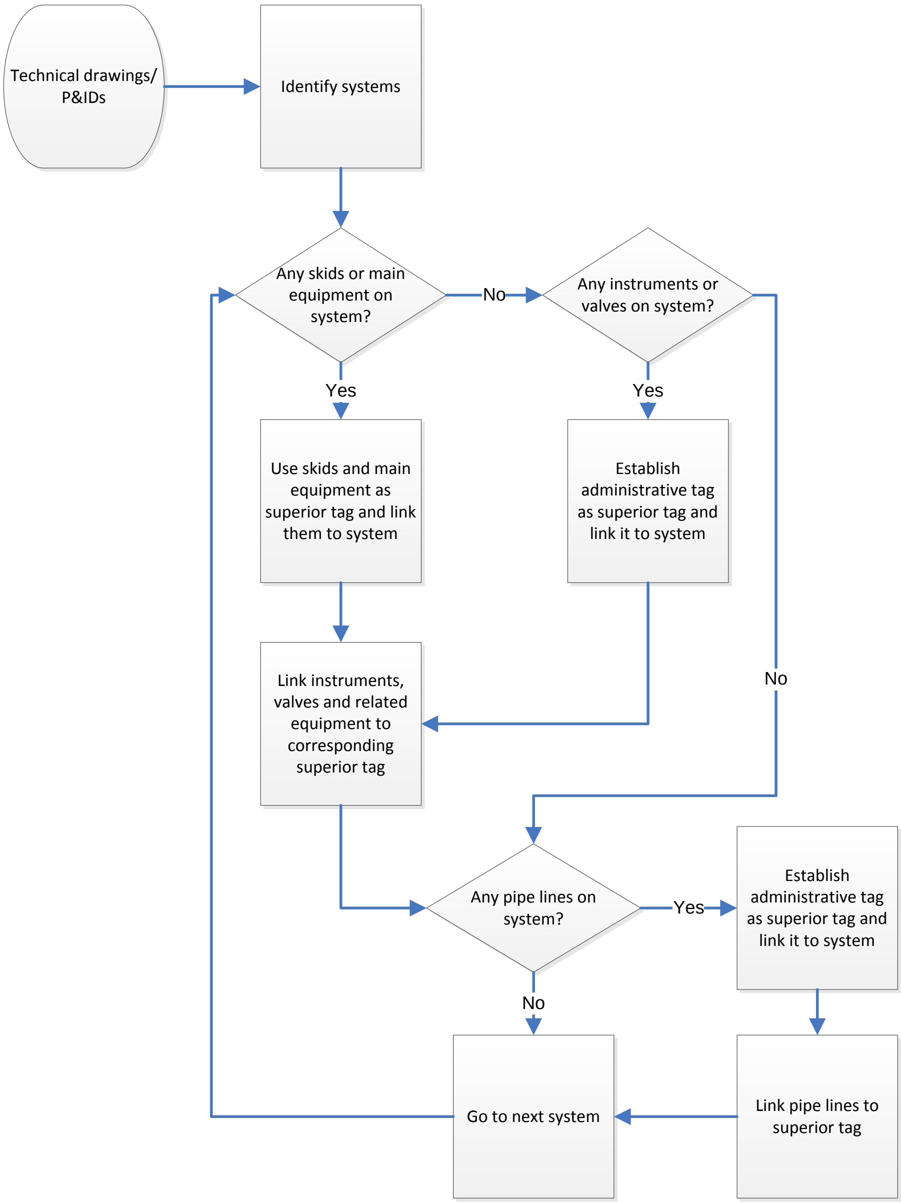


Figure D.1 – Work process technical hierarchy

To establish a technical hierarchy it is necessary with a set of technical drawings, e.g. flow and one-line diagrams, P&IDs etc. and a list of tags and a tool for linking tags to each other.

The top of the technical hierarchy normally starts with the installation code with the system numbers listed in Figure D.2. The usage of system numbers may vary from plant to plant NORSOK Z-DP-002 uses system numbers between 00 and 99. Other standards like SFI [Ship research institute of Norway (Skipsteknisk Forskningsinstitutt)] would have a 3 digit numbers as system numbering, but the principles may be similar.

Technical drawings can be used to identify skids, packages and main equipment that can work as a superior tag for the connected instruments, valves and other kinds of equipment. There can be several levels beneath a level, e.g. a skid that contains 2 pumps with electric motors. The skid will then be the top level, the pumps will be the 2nd level, and the electric motors will be the 3rd level to the corresponding pump. Each level can hold corresponding instruments and valves. See Figure D.2.

Start with a system by identifying skids and main equipment. Then link all the skids and main equipment that will be used as a superior tag to the system number in the tree structure. Next step is to identify the instruments, valves and other kinds of equipment on the system and connect them to the corresponding skid or main equipment. If there are no skids or main equipment, but only e.g. instruments or valves, then administrative tags should be established to form the level above. The instruments, valves and other kinds of equipment are then linked to the administrative tags. In instrument loops one of the components can represent the whole loop e.g. a transmitter or valve, while the rest of the loop lie beneath.

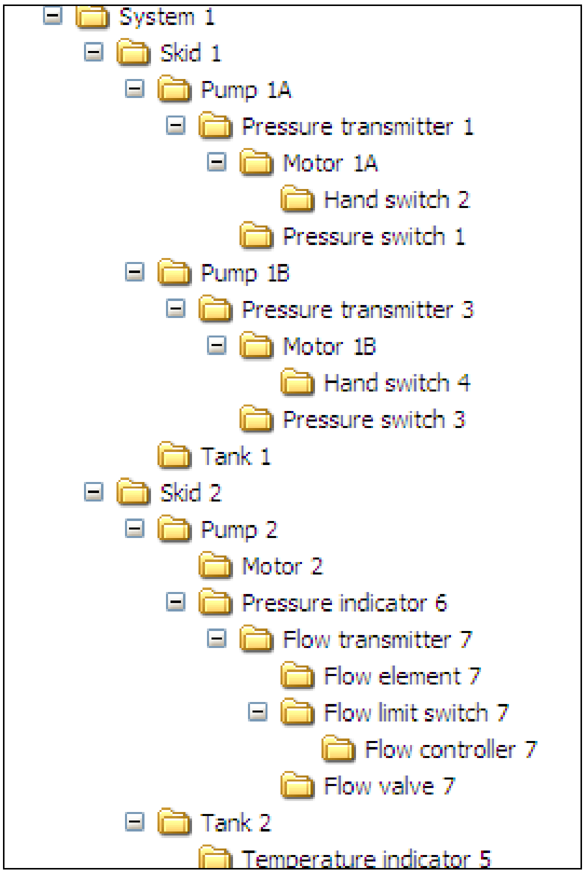


Figure D.2 – Technical hierarchy

D.2 Functional hierarchy

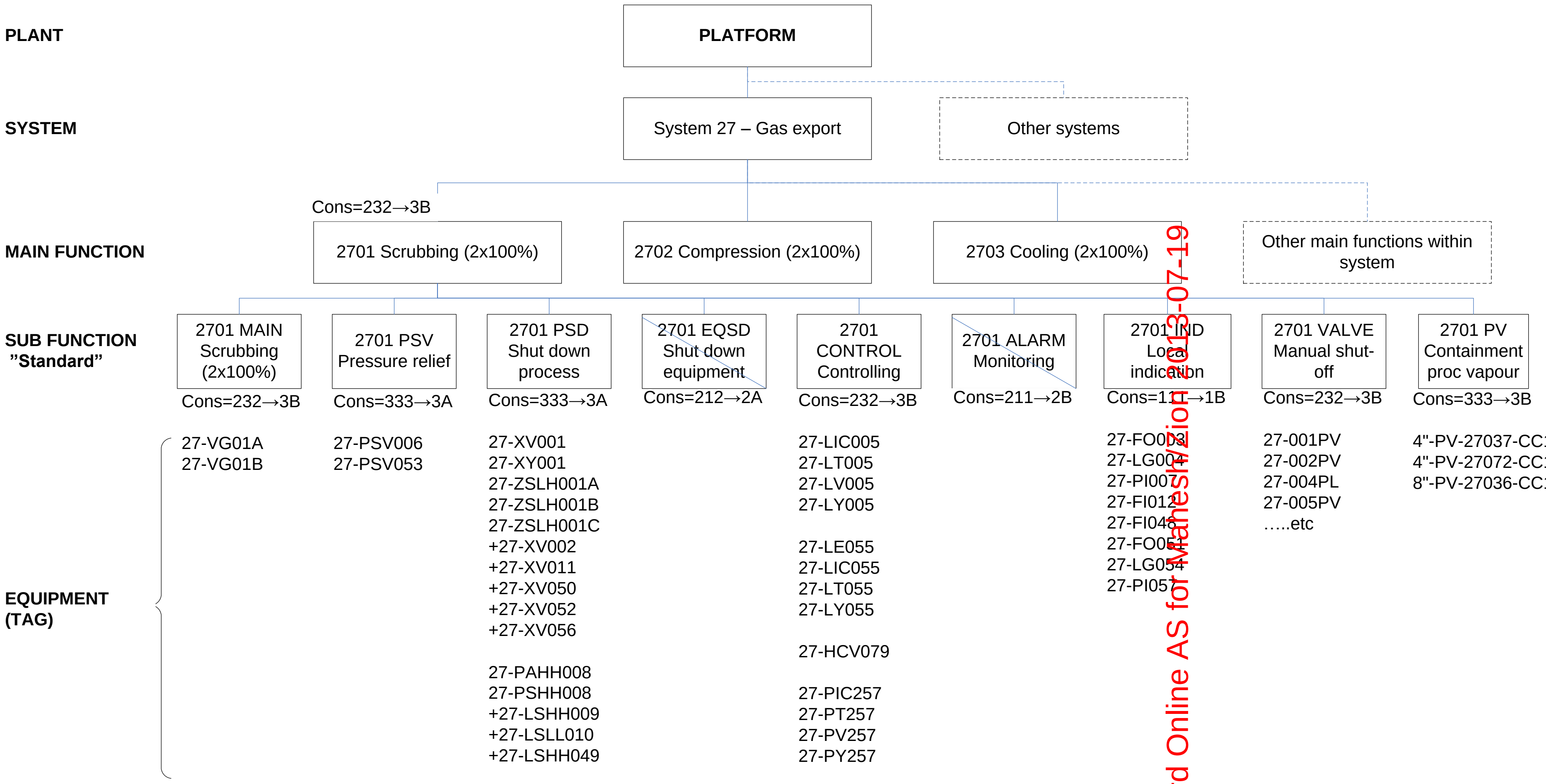
The functional hierarchy is a logical diagram linking all the plant functions noted as MF and sub functions, see Annex A. The level of detailing of the functional hierarchy may vary, but usually 2 to 3 levels are sufficient.

The plant system 27 (gas export) is shown in Figure D.3 in a schematic diagram of a plant (platform) which has been broken down into equipment identified by its tag number. The defined MFs covering part of this system and the standardised sub functions for one of these MFs are illustrated as an example.

Each tag within one sub function is given the same classification because a fault on any of these units (identified by the tag numbers) will cause the same consequence on the MF.

D.3 Documentation of consequence analysis

A typical example of a consequence analysis of a MF (2701 Scrubbing), with standard sub functions listed, is shown in Figure D.4. This MF consists of two parallel units, each able to perform 100 % of the scrubbing function in relevant operating mode. Although this example identifies 100 % redundancy for this MF, redundancy is ignored at this time. For the purpose of determining the consequence class all MFs should be considered as single, irrespective of their design redundancy. A fault which prevents the MF from operating will affect the system (Gas export) immediately (within ‘0’ hours) with a 100 % loss of functionality. This time is called ’Critical time in the list of sub functions. The consequence classification is 3 (high), 2 (medium) and 1 (low). The degree of redundancy is set by characters A, B or C for the relevant operating mode. The degree of redundancy for sub-functions is set based on number of PUs and capacity (Cap: 50 %, 100 %).



Explanation: Cons = Consequence. Figures: 3=High, 2=Medium, 1=Low HSE, Production and Cost respectively. Last result is a combination of the highest Consequence and Redundancy degree (A – No spare, B – One spare, C – Two or more spares) in operational phase.

Figure D.3 – Functional hierarchy, example with standard sub function and classification

Z-008	CONSEQUENCE OF MAIN FUNCTIONS AND ITS FUNCTIONS

System 27. GAS EXPORT AND METERING

Main Function: 2701	**SCRUBBING**		Parallel Unit 2	Capacity per unit: 100	Redundant grade B
Documents	Doc A: C-F027-P-*P-002-01	Doc. B: C-F027-P-*E-001\004-01	PID: C025-C-FO27-P-*E-001-01	Rev: B	Last updated: 21.02.00

Critical failure which affects system in 0 hours with 100 % reduction			Classification			
Failure mode	System effect:	Installation effect	S	P	O	H
Does not work	System in shut down/is not available. Max. 4 hours (valve/instrument failure).	Gas production is shut down and flared. CO_2 tax (100.000 – 1 mill. NOK), and environment consequence. Oil production to be maintained according to tariff quotas.	2	3	2	N
Works improperly	Reduced condensate separation	No immediate effect	1	1	1	N

Function	**Description**	Reduction	Crit. time	PU*Cap>Re	Does not work	Works improperly	Classification
2701 MAIN	Scrubbing	100 %	0	2*100>B	232-N	111-N	232>3
2701 ALARM	Monitoring	0 %	168	2*100>B	211-Y	111-N	211>2
2701 CONTRO	Controlling	100 %	0	2*100>B	232-N	111-Y	232>3
2701 IND	Local indication	0 %	720	2*100>B	111-N	111-Y	111>1
2701 PSD	Shutdown, Process	100 %	0	2*100>A	333-Y	111-N	333>3
2701 EQSD	Shutdown, Equipment	100 %	0	2*100>A	212-Y	111-N	212>2
2701 PSV	Pressure relief	100 %	0	2*100>A	333-Y	111-N	333>3
2701 VALVE	Manual shut-off	100 %	0	2*100>B	232-N	-	232>3
2701 PV	Containment, Process Vapour	100 %	0	2*100>A	333-N	-	333>3

Table key

Classification (S: Safety; P: Production; O: Other)
3: High
2: Medium
1: Low
Hidden failure (H)
Y: Yes
N: No

Figure D.4 – Consequence assessment of a MF. The example is shown with some key data and the classification of the sub functions listed below

D.4 Documentation of generic maintenance concept (GMC)

A GMC is a set of maintenance actions, strategies and maintenance details, which can be seen as a collection of best practices for a company. The GMC should be defined by a structured RCM analysis where failure modes and failure causes are identified.

All tags should be linked to a relevant GMC and should be available for reference directly in the CMMS. Use of dummy concepts should be restricted to a minimum and only linked to tags where a detailed generic maintenance analysis has revealed no need for any maintenance activity. Equipment which is part of an instrument loop, but no concept is applicable, should be linked to same concept as the superior tag, i.e. instrumented valve.

Each concept shall specify which type of equipment the concept is covering and which type of equipment that is excluded. Each concept should be detailed at such level that it provides sufficient information, as keywords or by a short description, about relevant maintenance activities and intervals of such activities in order to maintain the equipments intended function. It should be avoided to specify maintenance activity at the concept which is not relevant for the actual functional location which the concept are linked to.

The table below shows the final result and not the documentation of the entire process.

Generic maintenance concept

Equipment class:	*Pump*
Equipment type:	*Centrifugal*
Dominating failure mode	*Spurious stop*
Operating and frame conditions for concept:	*25-500 KW*
Responsible:	*Mechanical static equipment leader*
Revision:	*Rev1, 22.09.2009*
Comments:	

Sub unit	Activity	Activity description	Ref. to maint.doc.	Discipline	Req. from Gov/Comp?	Shu own?	Generic Interval	
Pump unit	Visual check	Brief routine check for leak, dirt, noise, vibration	xx-yy-zz	Oper.	N	N	1	1
Control and monitoring	Monitoring	Evaluate vibration data	xx-yy-zz	Mech.	N	N	6	6
Lubrication system	Replace	Replace oil	xx-yy-zz	Mech.	N	Y	6	12
Etc.								

D) Discipline
M) Requirement from Government/Company
N) Shutdown required to undertake repair, and possibly production shutdown depending on redundancy and HSE requirements

Equipment class	ISO 14224 provides a recommended structure for equipment class
Equipment type	ISO 14224 provides a recommended structure for equipment type
Dominating failure mode	The dominating failure mode used in the maintenance analysis. ISO 14224 provides recommended failure modes.
Operating and frame conditions	Physical operating and frame conditions for the concept
Responsible	Responsible person/discipline for this concept
Revision	Revision number

Sub unit	ISO 14224 provides a recommended structure for sub unit
Consequence class	Consequence class for maintainable item from consequence classification
Redundancy Activity	Redundancy for maintainable item from consequence classification Preventive maintenance activities
Activity description	Description of PM activities
Ref to main doc	Reference to detailed description of maintenance activity
D) Discipline	Craft/competence (e.g. Mech: mechanic, El: electric, Oper: operator)
M) Requirement from government/company	Regulations and company requirements. For safety functions:
	Safety critical failure with connected testing interval SIL requirement (acceptance level)
N) Shutdown required	Need for equipment shutdown
Generic Interval	Generic maintenance interval established based on consequence classification, operating conditions etc.
Interval unit	Months, years, hours etc.