

Criticality analysis for maintenance purposes

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

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

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

Copyrights reserved

Foreword	2
Introduction	2
1 Scope	3
2 Normative references	3
3 Definitions and abbreviations	4
3.1 Definitions	4
3.2 Abbreviations	6
4 Application of this NORSOK standard	7
4.1 General	7
4.2 Principles for risk evaluation and allocation of maintenance activities	7
4.3 Safety critical functions	8
4.4 Inspection of static process equipment	8
5 Functional hierarchy and criticality analysis	9
5.1 General	9
5.2 Necessary preconditions	10
5.3 System selection	11
5.4 Main function (MF) definition	11
5.5 Sub function definition	12
6 Documentation of the end product	13
7 Application of criticality analysis	14
7.1 Maintenance program	14
7.2 Spare parts evaluation	16
7.3 Conceptual and design evaluation	17
7.4 Prioritising work orders	18
Annex A (informative) Main function description and boundaries	19
Annex B (informative) Simplifying consequence assessment	23
Annex C (informative) Practical examples	25
Annex D (informative) Relations to other NORSOK standards	29
Bibliography	30

Foreword

The NORSOK standards are developed by the Norwegian petroleum industry to ensure adequate safety, value adding and cost effectiveness for existing and future petroleum industry developments.

The NORSOK standards are prepared to complement available international standards and 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 Subject to development and publication of international standards, the relevant NORSOK standard will be withdrawn.

These 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 preparation and publication of the NORSOK standards is supported by OLF (The Norwegian Oil Industry Association) and TBL (Federation of Norwegian Manufacturing Industries). NORSOK standards are administered and issued by NTS (Norwegian Technology Centre).

All annexes are informative.

Introduction

The purpose of this NORSOK standard is to provide requirements and guidelines for establishing a basis for preparation and optimisation of maintenance programs for new and in service facilities offshore and onshore taking into account risks related to:

- Personnel
- Environment
- Production loss.
- Direct economical cost (everything other than cost of production loss).

The result of this NORSOK standard is applicable for different purposes such as:

- Design phase.
Establishing initial maintenance manning requirements, identify hidden failures on critical equipment and selection of insurance spare parts.
- Preparation for operation.
Development of initial maintenance programs for implementation into maintenance management systems and selection of ordinary spare parts.
- Operational phase.
Optimisation of existing maintenance programs and as a guide for prioritising work orders.

1 Scope

This NORSOK standard is applicable for preparation and optimisation of maintenance programs 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.
- 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 fault modes and failure mechanisms are covered by this NORSOK standard.

This NORSOK standard covers:

- Definition of relevant nomenclature.
- Guidelines for criticality analysis, including:
- Functional breakdown of plants and plant systems in main functions and sub functions.
- Identification of main function and sub function redundancy.
- Definition of failure consequence classes.
- Assessment of the consequences of loss of main functions and sub functions.
- Assignment of equipment to sub functions and associated consequence classes.

Examples of application of the functional breakdown and the criticality analysis:

- Selection of equipment where preventive maintenance activities can be based on generic maintenance concepts.
- Selection of equipment where detailed RCM (FMECA) analysis is recommended.
- Establishment of maintenance activities and intervals, specification of resource and competence requirements, and evaluation of shutdown requirements.
- Preparation and optimisation of generic maintenance concepts.
- Design evaluations.
- Prioritisation of work orders.
- Spare part evaluations.

2 Normative references

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

DNV RP-G-101	Risk Based Inspection of Topside Static Mechanical Equipment
IEC 60300-3-11	Application guide, Reliability Centred Maintenance
OLF 066 Rev. no 01	Recommended guidelines for the application of IEC 61508 and IEC 61511 in the petroleum activities on the Norwegian continental shelf
NORSOK Z-016	Regularity management & reliability technology
NORSOK Z-013	Risk and emergency preparedness analysis

3 Definitions and abbreviations

3.1 Definitions

For the purpose of of this NORSOK standard the following terms and definitions apply.

3.1.1

can

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

3.1.2

condition based maintenance

preventive maintenance consisting of performance and parameter monitoring and the subsequent actions

NOTE - Performance and parameter monitoring may be scheduled, on request or continuously (CEN-prEN 13306).

3.1.3

condition monitoring

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

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 (prEN 13306)

3.1.5

criticality analysis

quantitative analysis of events and faults and the ranking of these in order of the seriousness of their consequences (BS 3811)

3.1.6

failure

the termination of the ability of an item to perform a required function

NOTE - After failure the item has a fault. "Failure" is an event, as distinguished from a "fault", which is a state (prEN 13306)

3.1.7

failure mechanism

physical, chemical or other processes which lead or have led to failure (prEN 13306)

3.1.8

failure rate

number of failures of an item in a given time interval divided by the time interval (prEN 13306)

NOTE 1 - This value is an approximation.

NOTE 2 - In some cases time can be replaced by units of use.

(In most cases 1/MTTF can be used as the predictor for the failure rate, i.e. the average number of failures per unit of 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.)

3.1.9

fault

state of an item characterised by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.

NOTE - A fault is often a result of a failure of the item itself, but may exist without failure (prEN 13306).

3.1.10**fault mode**

one of the possible states of a faulty item, for a given required function

NOTE - The use of the term "failure mode" in this sense is deprecated (prEN 13306).

3.1.11**failure mode**

the observed manner of failure (ISO 14224)

3.1.12**fault mode and effect analysis (FMEA)**

qualitative method of reliability analysis which involves the study of the fault modes which can exist in every sub item of the item and the effects of each fault mode on other sub items of the item and on the required functions of the item (BS 3811)

3.1.13**fault mode, effects and criticality analysis (FMECA)**

quantitative method of reliability analysis which involves a fault modes and effects analysis together with a consideration of the probability of failure modes, their consequence and ranking of effects and the seriousness of the faults (BS 3811)

3.1.14**hazard**

situation that could occur during the lifetime of a product, system or plant that has the potential for human injury, damage to property, damage to the environment, or economic loss (BS 3811)

3.1.15**hidden fault**

fault which is not evident to the operator during normal operation

3.1.16**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 - prEN 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.

3.1.17**item**

any part, component, device, subsystem, functional unit, equipment or system that can be individually considered (prEN 13306).

3.1.18**maintenance**

combination of all technical, administrative and managerial actions, including supervision 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 (prEN 13306)

3.1.19**maintenance analysis**

systematic analysis for identification and evaluation of required maintenance activities, including estimation of time and resources needed for the maintenance performance

3.1.20**maintenance management**

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

3.1.21**may**

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

3.1.22**preventive maintenance**

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 (prEN 13306)

3.1.23**redundancy**

in an item, the existence of more than one means at a given instant of time for performing a required function (prEN 13306)

3.1.24**repair time**

that part of active corrective maintenance item during which repair is carried out on an item (prEN 13306)

3.1.25**risk**

combination of the probability, (or frequency) of occurrence of a defined hazard and the magnitude of the consequences of the occurrence (BS 3811)

3.1.26**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

3.1.27**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

3.2**Abbreviations**

AFFF	aqueous film forming foam
F&G	fire and gas
FMEA	failure mode and effect analysis
FMECA	fault mode, effect and criticality analysis
HSE	health, safety and environment
MF	main function
NDT	non destructive testing
P&ID	process and instrumentation diagram
RCM	reliability centred maintenance
SIL	safety integrity level

4 Application of this NORSOK standard

4.1 General

The purpose of this NORSOK standard is to establish a basis for preparation and optimisation of maintenance programs for new and in-service oil and gas plants. This NORSOK standard describes an efficient and rational working process resulting in an optimised maintenance program based on risk analysis and cost-benefit principles.

As a basis for risk evaluations and establishment of maintenance activities, this NORSOK standard support the use of practical operation and maintenance experience, provided this experience is documented for the relevant types of plant equipment. Application of this general maintenance practice is referred to as "generic maintenance concepts", see 7.1.3. This NORSOK standard recommends that a more comprehensive RCM analysis (see IEC 60300-3-11) is carried out when relevant generic maintenance concepts are not available.

Application of the generic maintenance concepts is efficient for new facilities with no site-specific operational experience, and for facilities where the current maintenance program has not been established according to criteria for safe and cost-efficient operations. A more detailed RCM analysis is recommended for further optimisation of the maintenance activities for plants in-service taking into account the knowledge and experience of operation of the actual plant equipment. Both approaches, the generic maintenance concepts and the RCM analysis, are based on the principles of risk analysis for selection and prioritisation of maintenance activities. The purpose of the work and the documented practice, i.e. the availability of applicable generic maintenance concepts, decides which of the two approaches to be used.

4.2 Principles for risk evaluation and allocation of maintenance activities

Consequences and probabilities of failures are assessed independently, as:

- The consequences of system faults, loss of main functions and sub-functions, are independent of the equipment carrying out the functions.
- The actual equipment and the operational conditions affect the probability of failure.

Since the consequence of faults are independent of the equipment carrying out the functions, the consequence evaluations are carried out for each site according to the same principles irrespective of whether generic maintenance concepts or RCM analysis is applied.

The consequences of MF failures are assessed according to the effect on the plant and system level with respect to production loss and direct cost measured in downtime and monetary terms, while consequences of personal injury and environmental damage are classified according to pre-defined consequence classes and acceptance criteria. The consequences of MF failures determine the assessment of the consequences of loss of sub-functions. All relevant sub-functions should be identified to ensure that all equipment is assigned the right maintenance strategies and thus the optimal maintenance activities. This NORSOK standard provides guidelines to the definition of relevant sub-functions for typical process equipment. All tags (units) are linked to their respective sub-function and assign the same consequences as their respective sub-function.

Regarding the assessment of failure probabilities, this is implicitly expressed by the maintenance intervals documented for the different generic maintenance concepts, which again should be based on well documented operational experience and failure characteristics. In case of significant differences between the actual equipment and the equipment which has been the basis for the generic maintenance concepts, 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 impacts may influence the probability of failure and should be assessed prior to assignment of generic maintenance concepts.

In case no generic maintenance concept is applicable or the purpose of the study requires more in-depth evaluations, it is recommended that an RCM analysis is carried out. 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 which is basically the same principles applied for establishment of generic maintenance concepts.

Description of preventive maintenance activities and optimisation of intervals are not covered by this standard. However, for all practical purposes this should be based on:

- Consequences of function or sub-function failures.
- Probability of function or sub-function failures.
- Functional redundancy.
- Detectability of failure and failure mechanisms, including the time available to make necessary mitigating actions to avoid critical function or sub-function faults.
- Cost of alternative preventive activities.
- Required availability of safety critical functions.

In order to get acceptance for changes and create a basis for continuous improvements, it is necessary to involve maintenance personnel and production operators in the criticality assessment and preparation of the maintenance activities. A dynamic maintenance program 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 generic maintenance concepts are applied or the maintenance program has been developed on basis of the RCM analysis.

4.3 Safety critical functions

Requirements should be established with respect to availability, capacity and performance of safety critical functions according to OLF 066: "Recommended guidelines for the application of IEC 61508 and IEC 61511 in the petroleum activities on the Norwegian continental shelf", NORSOK standard Z-013 and NORSOK standard Z-016. Availability requirements should be used to determine the program for testing/ preventive maintenance activities and the required contingency plans in the event of failure. The inherent availability of the safety functions should be controlled and documented by observing the actual failure frequency and system downtime. The development of failure frequency and system unavailability should be used as the basis for changing of test intervals and other mitigating actions to ensure compliance with function requirements. Establishment of function requirements should be based on risk evaluations of accidental events, which will determine the safety systems and their performance.

4.4 Inspection of static process equipment

Inspection of static mechanical equipment, such as vessels and piping, is basically performed to maintain the containment function, i.e. to avoid critical leaks. In order to establish an inspection program for static mechanical equipment, it is necessary to perform more detailed evaluations than prescribed by the present standard. Selection of inspection method, location and extent of inspections, and establishment of optimal inspection intervals require knowledge of damage mechanism behaviour which depends on material properties, internal fluid compositions and the external operational environment. Similar to preparation of the preventive maintenance program, the inspection program should be based on risk evaluation of leaks with respect to personnel, environment damages and financial losses. Consequently, the present standard 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 programs, see DNV RP-G-101.

5 Functional hierarchy and criticality analysis

5.1 General

By carrying out the steps defined in the present chapter for establishing a functional hierarchy and criticality analysis, a platform for risk based decisions related to the management of maintenance activities is established. The general work process, see Figure 1, outlines systematically the breakdown of plant systems into suitable items for criticality analysis.

To better understand the practical application of the systematic breakdown of the plant systems and the criticality analysis, guidelines for establishing a maintenance program based on generic maintenance concepts or more comprehensive RCM methods are given in clause 7.

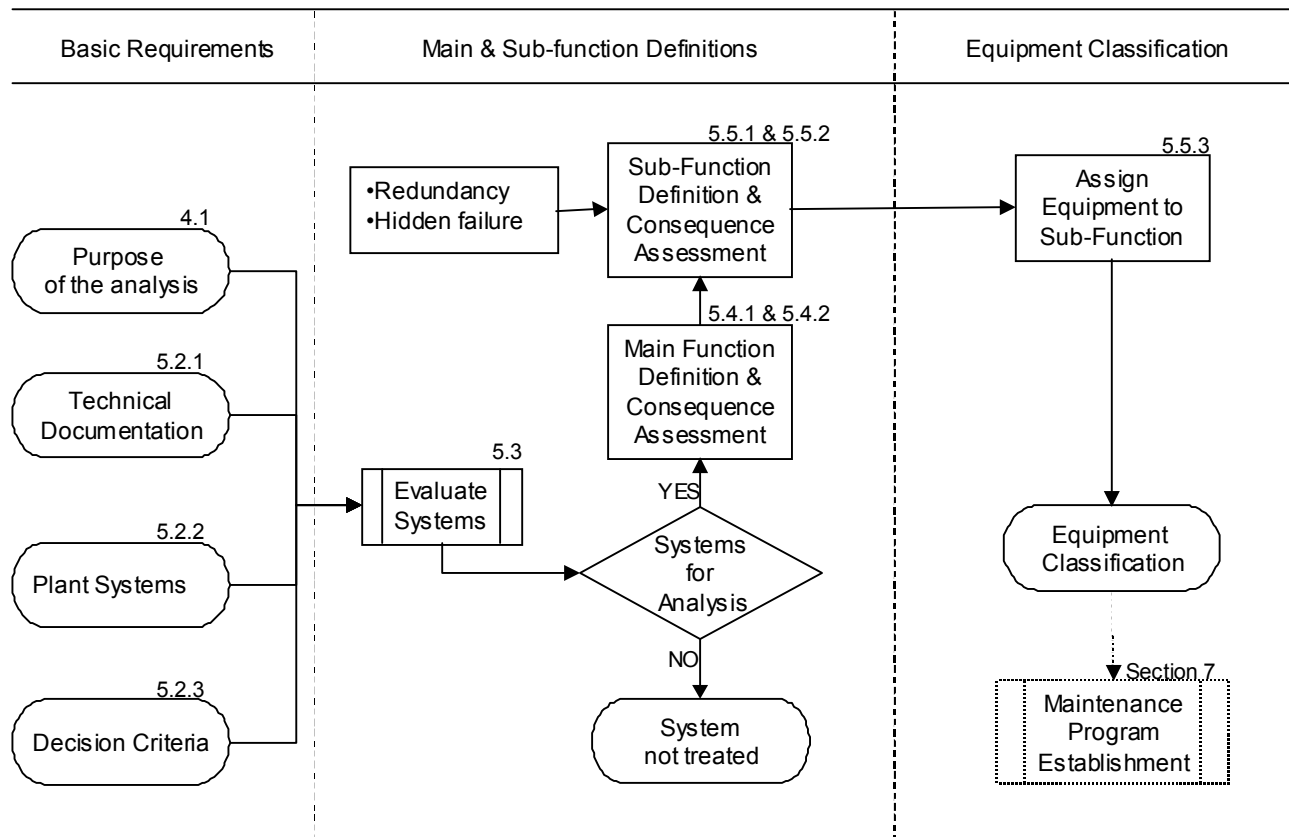


Figure 1 – Process diagram, functional structure and criticality analysis

5.2 Necessary preconditions

5.2.1 Technical documentation

Prior to start up of the criticality analysis the following technical documentation should be available:

- Technical description of the plant systems containing:
 - Detailed plant and system description.
 - Capacity requirements.
 - Operating conditions.
 - Equipment description.
- Technical drawings/diagrams containing process data, material and media codes:
 - P&ID
 - Flow diagrams.
 - One line diagrams (electrical cables and equipment).
 - Shut down logic.
 - F&G cause and effect diagrams.
 - Fire protection data sheets.

5.2.2 Plant systems

The systems with their boundaries should be defined and documented by the use of the engineering numbering system.

5.2.3 Decision criteria

For the criticality analysis which assess the consequences of failures and the degree of functional redundancy, the consequence classes have to be properly defined prior to performance of the analysis. The definition of the consequence classes should be done in accordance with overall company criteria for safety and environment, and reflect the actual plant operation when it comes to economical losses.

To classify the most serious effect of loss of functionality (both loss of MF and sub functions) the consequence classes defined in Table 1 should be applied, unless otherwise specified. Note that the loss of 'Production' should in monetary value comply with the corresponding cost limits specified for 'Cost' within each class.

Table 1 - General consequence classification

Class	Health, safety and environment (HSE)	Production	Cost (exclusive production loss)
High	Potential for serious personnel injuries. Render safety critical systems inoperable. Potential for fire in classified areas. Potential for large pollution.	Stop in production/significant reduced rate of production exceeding X hours (specify duration) within a defined period of time.	Substantial cost - exceeding Y NOK (specify cost limit)
Med.	Potential for injuries requiring medical treatment. Limited effect on safety systems. No potential for fire in classified areas. Potential for moderate pollution.	Brief stop in production/reduced rate of production lasting less than X hours (specify duration) within a defined period of time.	Moderate cost between Z – Y NOK (specify cost limits)
Low	No potential for injuries. No potential for fire or effect on safety systems. No potential for pollution (specify limit)	No effect on production within a defined period of time.	Insignificant cost less than Z NOK (specify cost limit)

NOTE - Loss of the sub function "Containment", i.e. external leakage, requires a separate evaluation to reflect best practice for inspection planning. This applies for consequences to health, safety and environment while the consequences to production loss and other costs are similar for all kinds of failures. Table 2 gives guidelines for assessment of the consequences to personnel safety, while 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). For consequence assessment of pollution to the open sea, reference is made to B.1 which gives guidelines for classification of external leakage. The consequence classification related to containment is intended as a prioritisation of static mechanical equipment for establishing an inspection program. See DNV RP-G-101.

Table 2 - Consequence classification for containment (external leakage)

Class	Health, safety and environment (HSE)	Production	Cost (exclusive production loss)
High	When substance is: - Hydrocarbons (highly ignitable gases and unstabilized oil) and other flammable media. - Liquid/steam, exceeding 50 °C or 10 bar. - Toxic gas and fluids. - Chemicals (see B.1)	As for production, class 'High' in Table 1.	As for cost, class 'High' in Table 1.
Med.	When substance is: - Stabilised oil, diesel and other less ignitable gases and fluids. - Liquid/steam, less than 50 °C and 10 bar - Toxic substance, small volume. - Diesel	As for production, class 'Medium' in Table 1.	As for cost, class 'Medium' in Table 1.
Low	When substance is: - Non-ignitable media. - Atmospheric gasses and fluids harmless to humans and environment. - Negligible toxic effects. - Harmless chemicals (see B.1).	As for production, class 'Low' in Table 1.	As for cost, class 'Low' in Table 1.

5.3 System selection

The first activity is to select the systems that should be included in the analysis. Ranking criteria depends on the purpose of the analysis and should be documented. Selection criteria could be based on maintenance cost, main contributors to production loss/unavailability and safety related incidents.

5.4 Main function (MF) definition

5.4.1 General

Each plant system should be divided into a number of MFs covering the entire system. The MFs are characterised by being principal tasks such as heat exchanging, pumping, separation, power generation, compressing, distributing, storing, etc. See annex A, which 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. The boundaries of the MF should be clearly defined in a P&ID or other relevant documentation. See annex A.

5.4.2 Main function (MF) redundancy

MF redundancy should be specified with respect to loss according to Table 3.

The level of redundancy within one MF is classified by the codes in Table 3.

Table 3 - Classification of redundancy (Red.)

Red.	Redundancy degree definition
A	No redundancy i.e. the entire MF 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.

5.4.3 Main function (MF) consequence assessment

Assessing the consequences of the most serious faults should preferably be carried out by personnel with experience in risk and reliability evaluations (facilitator) in collaboration with personnel experienced in operations and maintenance and with sound understanding of the production process and the technical equipment.

The entire MF is assessed in terms of the most serious effect of a fault. In this assessment any redundancy within the function is disregarded, as the redundancy will be treated separately.

The most serious (but nevertheless realistic) effect of a fault shall be identified and the influence on the performance of the MF shall be quantified (if possible) according to Table 1.

If relevant, compensating operational actions shall be described and reflected in the consequence assessment.

The time from the fault occurring, until it affects the system/plant should be estimated. See Table 1, column for 'Production'.

When the fault affects more than one of the categories (HSE, production and cost), this shall be identified and described so that it is evident from the text how the effect takes place.

5.5 Sub function definition

5.5.1 General

MFs are split into sub functions, see annex C. In order to simplify the consequence assessment and enable work to be carried out with sufficient accuracy with minimum use of resources, the sub function level can be 'standardised' for typical process equipment with pre-defined terms to cover all requirements. These sub functions are:

- Main task (term describing the task).
- Pressure relief.
- Shutdown, process.
- Shutdown, equipment.
- Controlling
- Monitoring
- Local indication.
- Manual shut-off.
- Containment
- Other functions.

The standard list of sub functions has to be completed with other sub functions relevant for the particular operation.

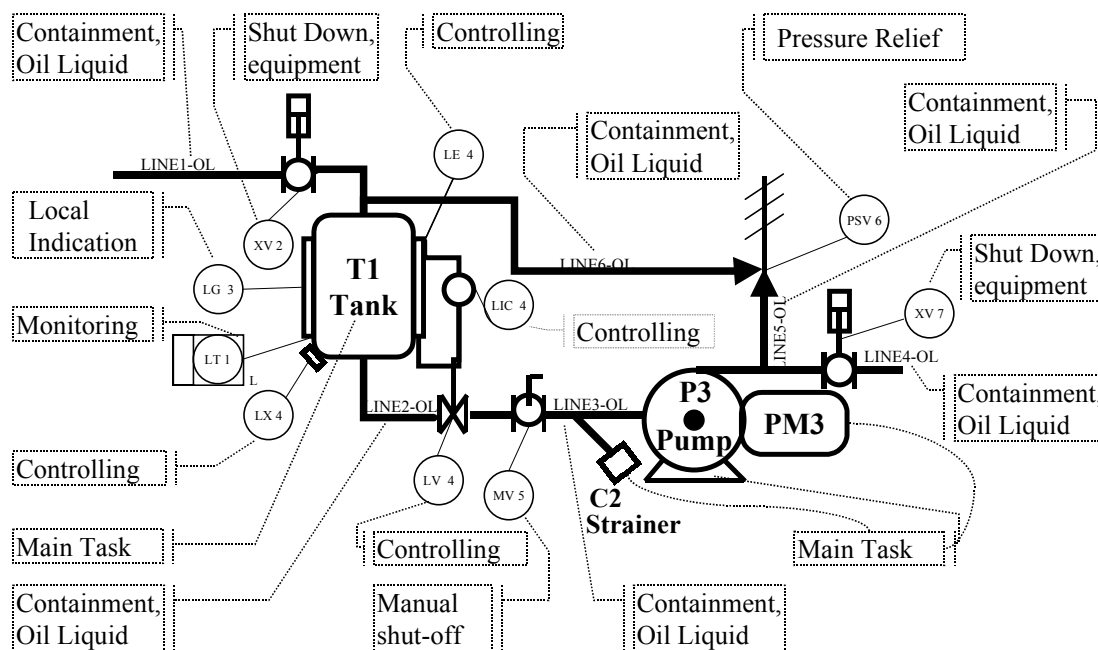


Figure 2 – Illustrates how equipment in a MF is assigned to standard sub functions

All equipment (identified by its tag number) in each instrument loop shall be assigned to one sub function. If a sub function performs multiple tasks, the equipment shall be assigned to the most critical sub function.

The standard sub functions are only to be used if relevant. When appropriate, other repetitive sub functions (i.e. lubricating, containment of different services, etc.) may be used.

5.5.2 Sub function redundancy

Identify the level of redundancy of each sub function.

If there is redundancy within a sub function, the number of parallel units and capacity per unit shall be stipulated. The redundancy shall be classified using the codes in Table 4.

Table 4 - Classification of redundancy (Red.)

Red.	Redundancy degree definition
A	No unit can suffer a fault without influencing the function.
B	One 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.

NOTE - It is recommended that each sub function shall contain maintainable equipment (identified by its tag number) with one degree of redundancy only. If this is not the case the sub functions have to be defined in a way that allows tags with common redundancy to be assigned to each of the sub functions.

5.5.3 Sub function, consequence assessment

The consequence on system/plant of a fault in a sub function is assessed with respect to HSE, production and cost (excluding production loss) according to the same principles as outlined for MF. If the sub function can suffer a fault without this being evident to the operator during normal operation this condition shall be described and identified as a hidden failure.

For safety critical functions, the failure modes and failure rates must be described in sufficient detail to be able to decide appropriate maintenance activities when assessing the consequence of loosing the function. This information should normally be part of the generic maintenance concept or documented in the FMEA/RCM analysis.

5.5.4 Equipment classification

The equipment (identified by its tag number) carrying out the sub functions shall be assigned to the respective sub functions in a one-to-one relationship, i.e. no equipment shall be assigned to more than one sub function. If equipment maintains 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) shall be assigned the same description, consequence classification and redundancy as the sub function of which they are a part.
See annex C for an example.

6 Documentation of the end product

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 from this NORSOK standard, including terminology, methodology and recommended classification of consequences and degrees of redundancy should be documented.

7 Application of criticality analysis

7.1 Maintenance program

7.1.1 Process diagram

A process diagram to establish a maintenance program is shown in Figure 3.

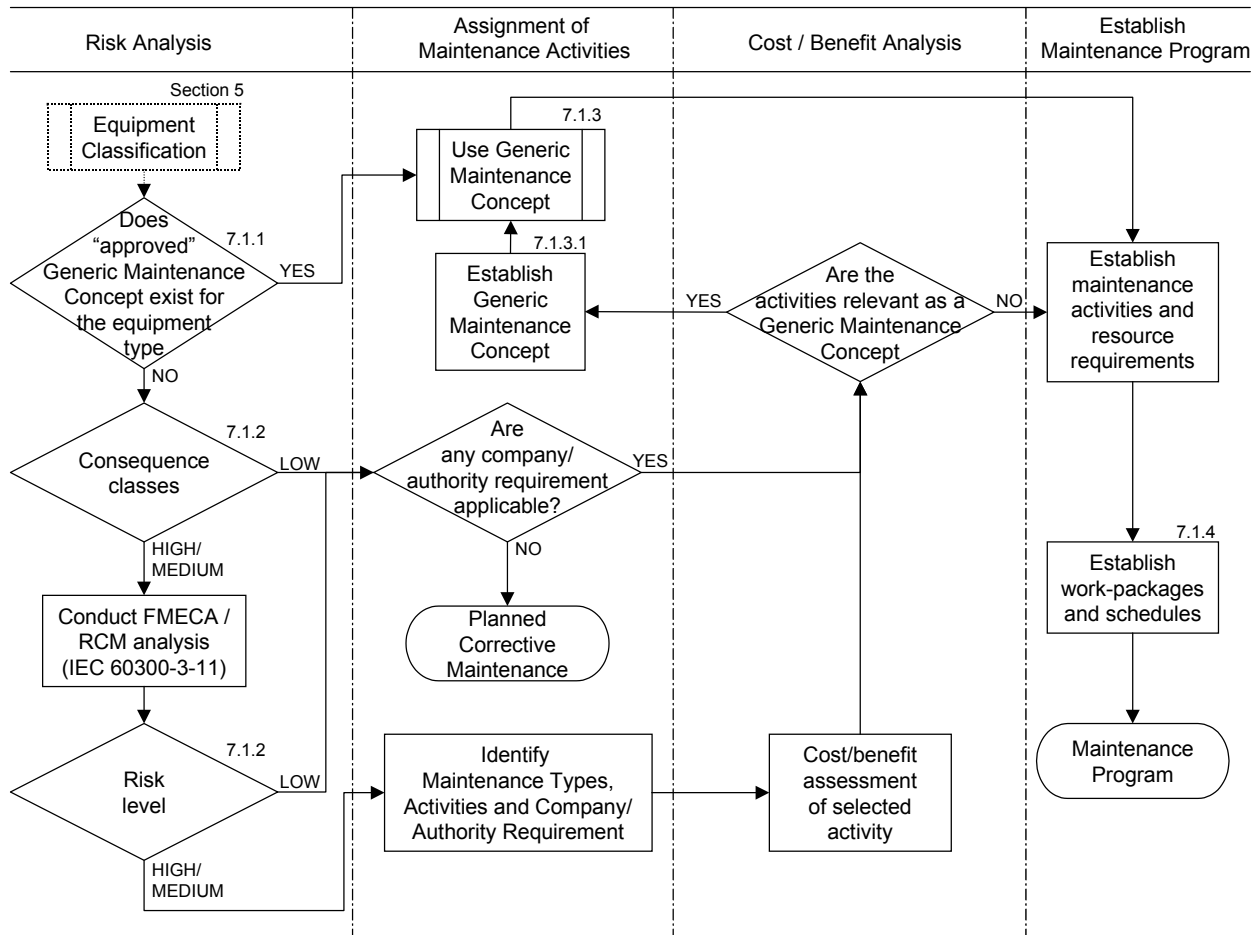


Figure 3 – Process diagram, establishing maintenance program

7.1.2 Establish preventive maintenance activities

The preventive maintenance activities could be established in two different ways:

- By use of detailed maintenance analysis (see IEC 60300-3-11).
- By use of relevant generic maintenance concepts as described below.

Both methods applies to the criticality analysis.

7.1.3 Requirement for maintenance analysis

To ensure that important equipment is maintained properly, sufficiently documented decisions are required. For equipment classified 'Low' no documentation is required. If it is classified 'Medium' or 'High' documentation should be based on a maintenance analysis.

If the maintenance analysis has previously been performed on identical/ similar equipment (generic grouped equipment types) and documented as a generic maintenance concept, it is only necessary to carry out/document the following:

- Low consequence:
- Verify if any specific company/ authority requirements are applicable.
- Verify that simple service activities are adequate and cost beneficial.
- Medium and High:

- A maintenance analysis comprising of the following elements:
 - If specific company/authority requirements are applicable (including assumptions/requirements for/from risk analysis).
 - Dominating fault/failure modes with approximate probability.
 - Failure mechanisms with approximate probability.
 - Repair time (approximate).
 - Selected maintenance activities to reduce the probability of such failure mechanism to cause a fault - along with the interval.
 - Detectability of failure.
- Experience from using a known maintenance strategy along with periodic monitoring of the result:
 - If this alternative is used on equipment, which performs safety critical functions where a fault is not evident to the operator, the availability requirement shall be defined and the compliance verified by documented tests.
 - The percentage of periodic tests resulting in 'Fail to operate on demand' may be used as the performance indicator.
- It is also recommended to include:
 - Required competence of maintenance personnel.
 - Estimated man-hours for maintenance activities.
 - Repair time.
 - Essential spare parts and lead times.

7.1.4 Generic maintenance concept

7.1.4.1 General

A generic maintenance concept is a set of maintenance actions, 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 generic maintenance concept should ensure that all defined HSE, production, cost and other operating requirements are met. The concept shall include relevant design and operating environments. Appropriate performance indicators and the corresponding acceptance criteria shall be defined for safety critical functions.

7.1.4.2 Application of generic maintenance concepts

Generic maintenance concepts may be developed in order to:

- Reduce the effort in establishing the maintenance program.
- Ensure uniform and consistent maintenance activities.
- Facilitate analysis of equipment groups.
- Provide proper documentation of selected maintenance strategies.

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

A generic maintenance concept can be utilised when:

- The group of equipment has similar design.
- The equipment has similar failure modes and failure frequencies.
- The amount of similar equipment justifies a generic concept.

7.1.4.3 Documentation of the generic maintenance concept

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.

In addition to what is defined in requirement for maintenance analysis (see 7.1.3) the documentation should describe:

- General:
- Description of the generic equipment class.
- Physical operating and frame conditions.

- Operating experiences.
- Regulations and company requirements.
- Definition of loss of function, and a quantification of the acceptance level for safety critical functions.

7.1.5 Preparation of maintenance and inspection work packages

In order to achieve effective management of the resources used for maintenance purposes, all equipment must be arranged in a hierarchy.

A maintenance program is divided into scheduled work packages of suitable size to suit the organisation and the available resources. These packages are assigned to maintenance objects (see Figure 4) thus making them the lowest level in the hierarchy carrying the cost for the maintenance program. Hence all maintenance objects should be identified prior to establishing the maintenance program.

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 programs.

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 maintenance programs.

This information is a part of the data needed to perform an evaluation and optimisation of the maintenance strategy. If the data is linked to the lowest tag level the hierarchy will make it possible to summarise this information to the appropriate level - which could be the maintenance object or MF as shown in Figure 4.

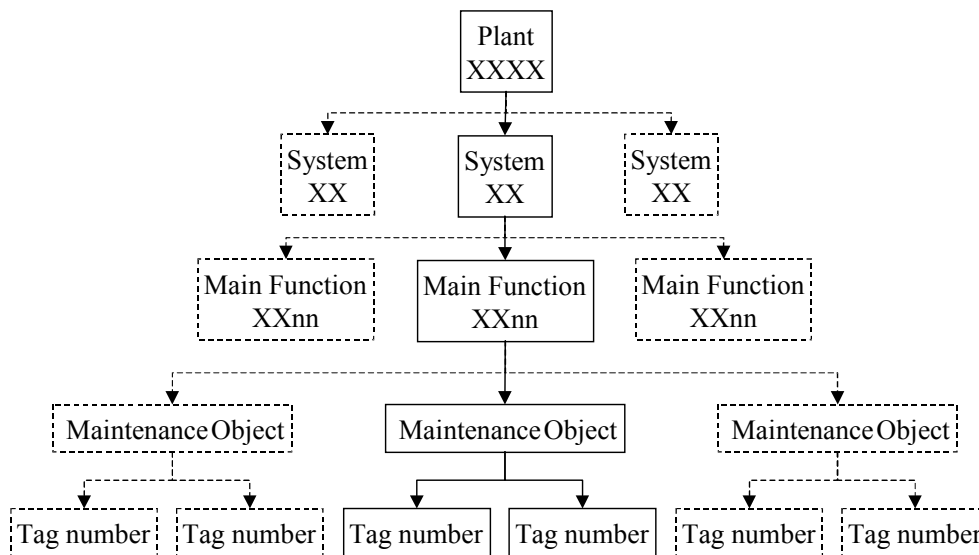


Figure 4 – Illustration of a hierarchy

7.1.6 Critical equipment without redundancy

All sub functions and associated tags that could lead to a shut down of a system (or the whole plant) can be identified by means of the data established during the criticality analysis as described in clause 5. This could be applied for prioritisation of recourses and attention towards the vulnerable equipment with respect to HSE and production.

7.2 Spare parts evaluation

7.2.1 General

The results from the criticality analysis are very useful when identifying the need for spare parts that are to be purchased along with the initial system package.

7.2.2 Insurance spare parts selection

Insurance spare parts are always

- Vital to the function of the plant, but unlikely to suffer a fault during the lifetime of the equipment.
- Supplied 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. In order to be able to identify the equipment that may contain such spare parts, the consequence of the MFs suffering a fault has to be known.

MFs to be analysed are selected by choosing those with high consequence of failure (independent of area) and no redundancy.

During the conceptual phase, it is only possible to identify main equipment. Due to the process of concurrent engineering practised to-day the documentation required to identify the content of the sub functions is usually not available until the start of the preparations for the operation.

The different failure modes, need for spare parts and the possibility of compensating with temporary solutions have to be evaluated for the equipment (identified by its tag number) in the selected MFs. Additionally the probability factor that these spare parts will be required must be established. Then the price alternatives if the spares are ordered together with the initial order - or as separate orders at a later date shall be clarified with the supplier. Finally a risk comparison will determine which spare parts should be ordered together with the initial order.

7.2.3 Ordinary spare parts selection

Selecting the ordinary spare parts for local storage can be made accurately and conveniently by using the results from the criticality analysis together with the generic maintenance concept/RCM during preparations for the operation.

All pieces of equipment are classified with respect to the consequence of a fault, and defined with a degree of redundancy. The generic maintenance concepts specifies the type of spare parts needed and the lead-time until the spare parts are available on site.

7.3 Conceptual and design evaluation

If this analysis is performed during the early design phase of the plant, the result may be utilised to provide data for supporting decisions that have to be taken in two important areas. The first one is to quantify the need for maintenance resources required for normal operation of the plant, and the second is to identify if hidden faults can occur on safety critical equipment.

- Establishing initial maintenance manning requirements:
- Initial determination of the number of people required to perform the maintenance tasks. Provided the generic maintenance concept is defined in sufficient detail for each generic type of equipment and the typical content of equipment associated with each MF is known from other plants/projects - the consequence and the degree of redundancy are vital elements when calculating the need for manning.
- Identifying hidden faults on safety critical equipment:
- Verify if any MF with no redundancy, is critical to safety - and can suffer a fault without this being evident to the operator. The identification of MFs containing this type of equipment is only appropriate if the analysis is performed early enough to influence the design.

Sub functions exposed to this selection will have redundancy class "A", the consequence of a fault will be classified as "High" with respect to HSE - and in addition they should be marked 'hidden fault' in the criticality analysis.

7.4 Prioritising work orders

The results from the criticality analysis can be useful when defining criteria for prioritising the preventive and corrective work orders.

The prioritising of corrective work orders is normally based upon a judgement of the consequence of the actual failure. This may or may not be the same failure mode that was considered to lead to the most serious consequence while performing the criticality analysis.

Data from the criticality analysis can be combined with other information to define criteria for prioritising the corrective work orders. The criteria should combine the following information:

- Classification of consequence of a fault and redundancy (or both parameters, combined with allowed down time).
- Failure mode and causes.
- Operating considerations.
- Repair time including lead time for spare parts

The criteria can also be implemented in a maintenance management system with a default priority based on:

- Classification of consequence of a fault.
- Redundancy
- Information about the seriousness of the actual failure (breakdown/no breakdown).

NOTE - It should always be possible to overrule the default priority manually based on actual operation considerations.

Annex A (informative) Main function 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.. 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	F&G
Distributing	(Main/emergency) power, hydraulic, tele
Drying	Air, gas
Expanding	
Filling	Lubrication oil
Filtering	
Fire Fighting	Sprinkler, deluge, water spray, foam, AFFF, 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 are shown on Figure A.1 and Figure A.2.

The MF shall cover the entire plant system, and the boundaries should be decided taking into consideration the possibility of isolating the MF for maintenance. If appropriate for establishing boundaries suitable for inspection purposes, the unique line numbers should be included in one MF.

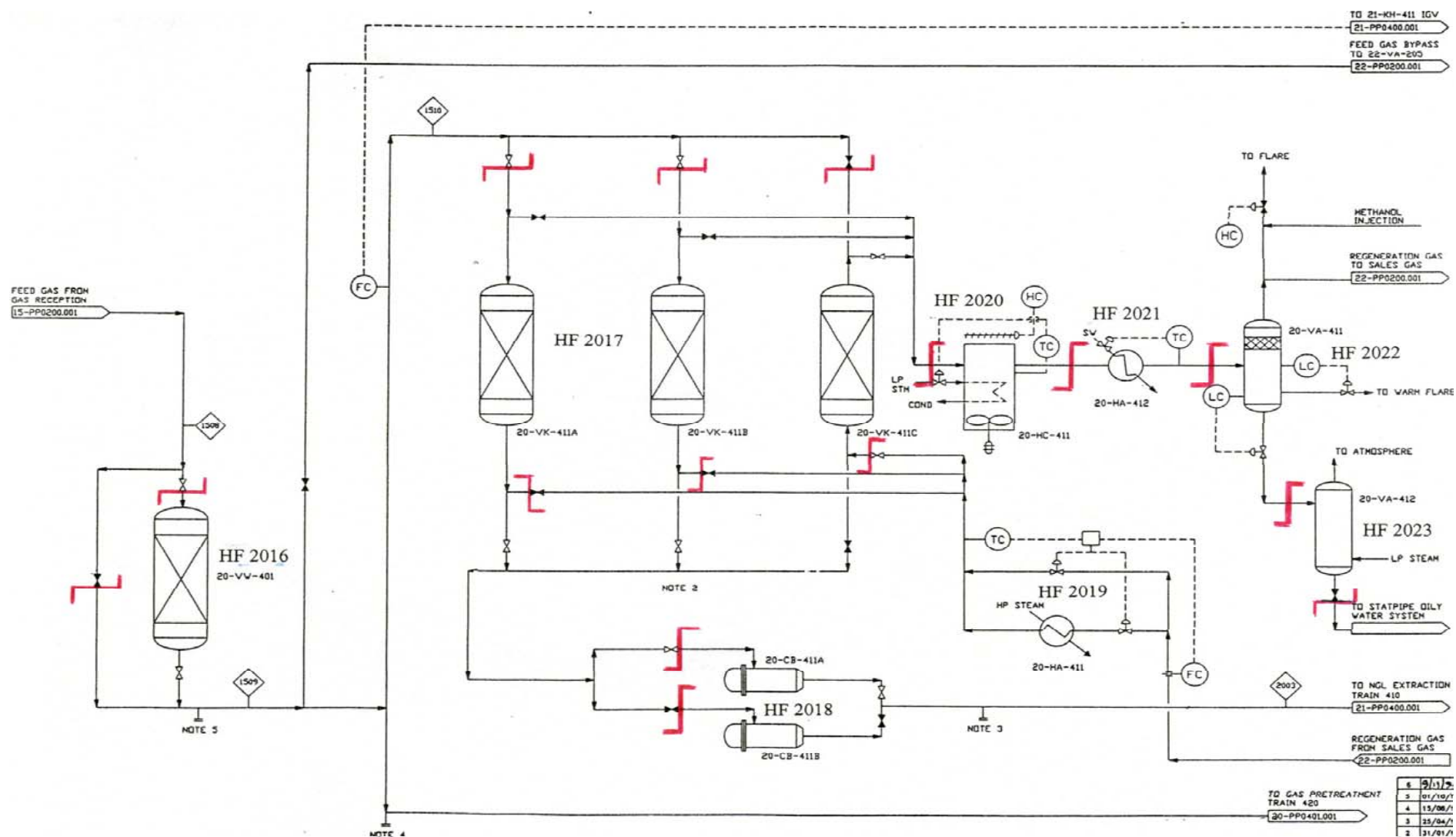


Figure A.1 – Flow diagram showing borderlines between Main Functions (HF2017, F2020)

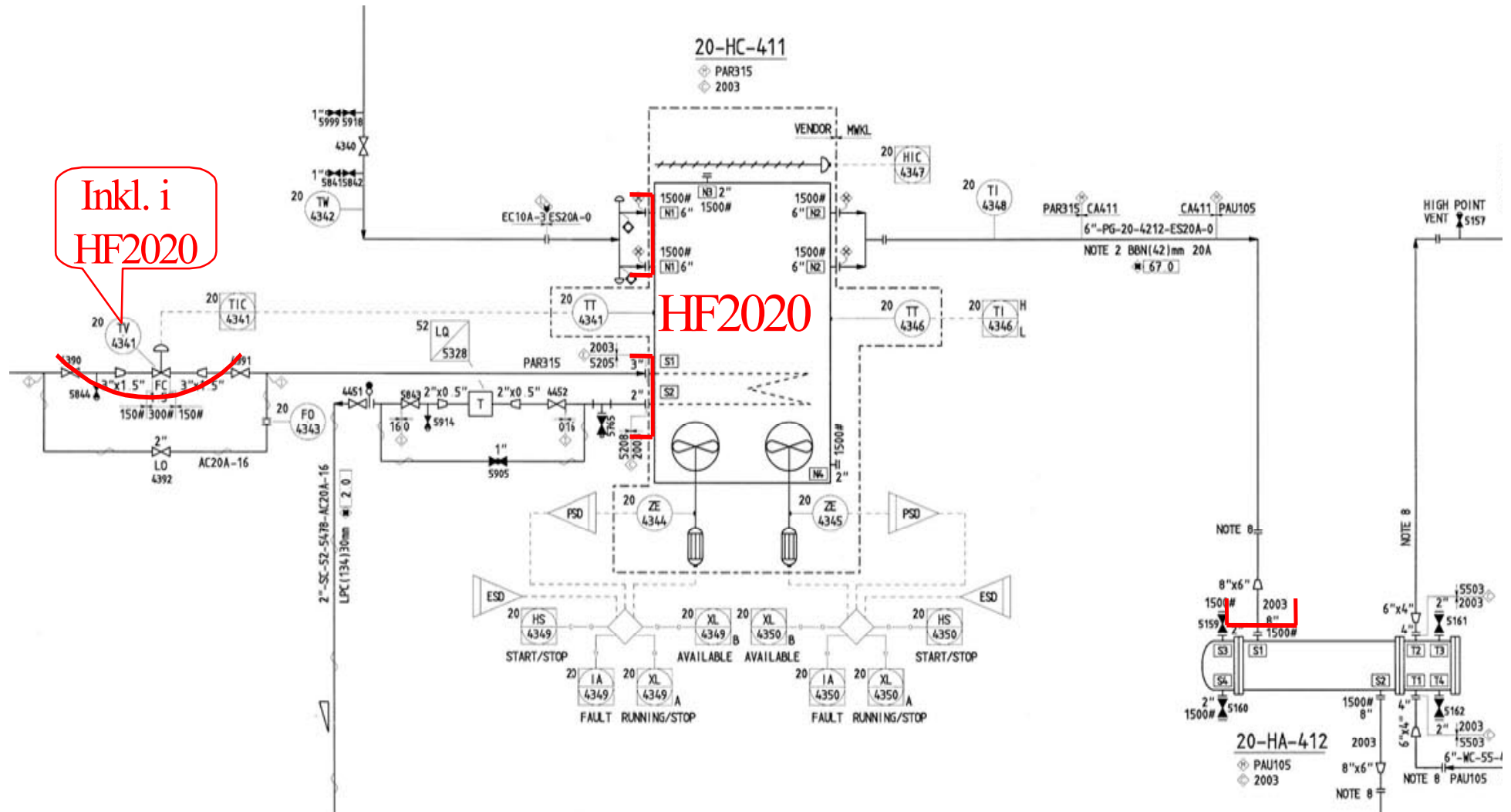


Figure A.2 – P&ID showing borderlines for MF HF2020

Annex B (informative) Simplifying consequence assessment

B.1 Consequence assessment of the standard sub functions

The consequence assessment of the MF already performed may be used as a basis for (default) 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	Assessing loss of function	Red. degr.	HSE	P	C
Main task	Red.: Will inherit the MF-redundancy. HSE/ production/cost: Will inherit the MF - consequence assessment .	MF	MF	MF	MF
Pressure, relief	Red.: No redundancy for the failure mode 'Fail to operate on demand'. HSE: Potential for serious personnel injury. Prod.: Will inherit the MF consequence assessment if time to repair exceeds 4 hours. Cost: Will lead to substantial cost, exceeding 1 MNOK	A	H	MF	H
Shut down, process	Red.: No redundancy for the failure mode 'Fail to operate on demand'. HSE: Potential for serious personnel injuries. Potential for fire in classified areas. Potential for moderate or large pollution. Prod.: Will inherit the MF consequence assessment if time to repair exceeds 4 hours. Cost: Will lead to substantial cost, exceeding 1 MNOK.	A	H	MF	H
Shut down, equipment	Red.: No redundancy for the failure mode 'Fail to operate on demand'. HSE: Potential for injury requiring medical treatment. Limited effect on safety systems controlling hydrocarbons. No potential for fire in classified areas. Prod.: No effect on production. Cost: Will lead to cost between 0,1 – 1 MNOK.	A	M	L	M
Controlling	Red.: Will inherit the MF – redundancy. HSE: Will inherit the MF consequence assessment. Prod.: Will inherit the MF consequence assessment if time to repair exceeds 4 hours. Cost: Will inherit the MF consequence assessment.	MF	MF	MF	MF
Monitoring	Red.: Will inherit the MF – redundancy. HSE: Potential for injury requiring medical treatment. Limited effect on safety systems controlling hydrocarbons. No potential for fire in classified areas. Potential for moderate pollution. Prod.: No effect on production within a period of 12 hours. Cost: Will lead to insignificant cost less than 0,1 MNOK.	MF	M	L	L
Local indication	Red.: Will always inherit the MF – redundancy. HSE: No potential for: Injury, fire or effect on safety systems. No potential for pollution. Prod.: No effect on production within a period of 12 hours. Cost: will lead to insignificant cost less than 0,1 MNOK.	MF	L	L	L
Manual shut-off	Red.: Will always inherit the MF redundancy. HSE: Will always inherit the MF - consequence assessment.	MF	MF	MF	MF

Standard sub function	Assessing loss of function	Red. degr.	HSE	P	C
	Prod.: Will inherit the MF consequence assessment if time to repair exceeds 4 hours. Cost: Will always inherit the MF consequence assessment.				
Containment	Red.: No redundancy (normally) for loss of containment. HSE/ production/cost: See Table 2	A	H/L	MF	H/L

The abbreviations in Table B.1 mean:

A = redundancy A (see Table 4)

C = cost

H = criticality class "High"

H/L = criticality "High" or "Low"

L = criticality class "Low"

M = criticality class "Medium"

MF = main function

P = production

RED = Redundancy

PROD = Production

B.2 Effect of pollution

Examples of consequence classification caused by pollution:

Potential for large pollution

Hydrocarbons : > **100 m3**

Chemical group 1 : > **200 litres**

Chemical group 2 : > **1 m3**

Chemical group 3 : > **10 m3**

Potential for moderate pollution

Hydrocarbons : **1 – 100 m3**

Chemical group 1 : **25 – 200 litres**

Chemical group 2 : **0.25 – 1 m3**

Chemical group 3 : **1 – 10 m3**

No potential for pollution exceeding

Hydrocarbons : < **1 m3**

Chemical group 1 : < **25 litres**

Chemical group 2 : < **200 litres**

Chemical group 3 : < **1 m3**

NOTE - The chemical groups referred to are different types of chemicals which are divided into groups depending on their ability to harm the environment and/or human life. The types of chemicals and the consequence of a leakage to the environment may differ from case to case, e.g. offshore/ land, open air/confined area.

Annex C

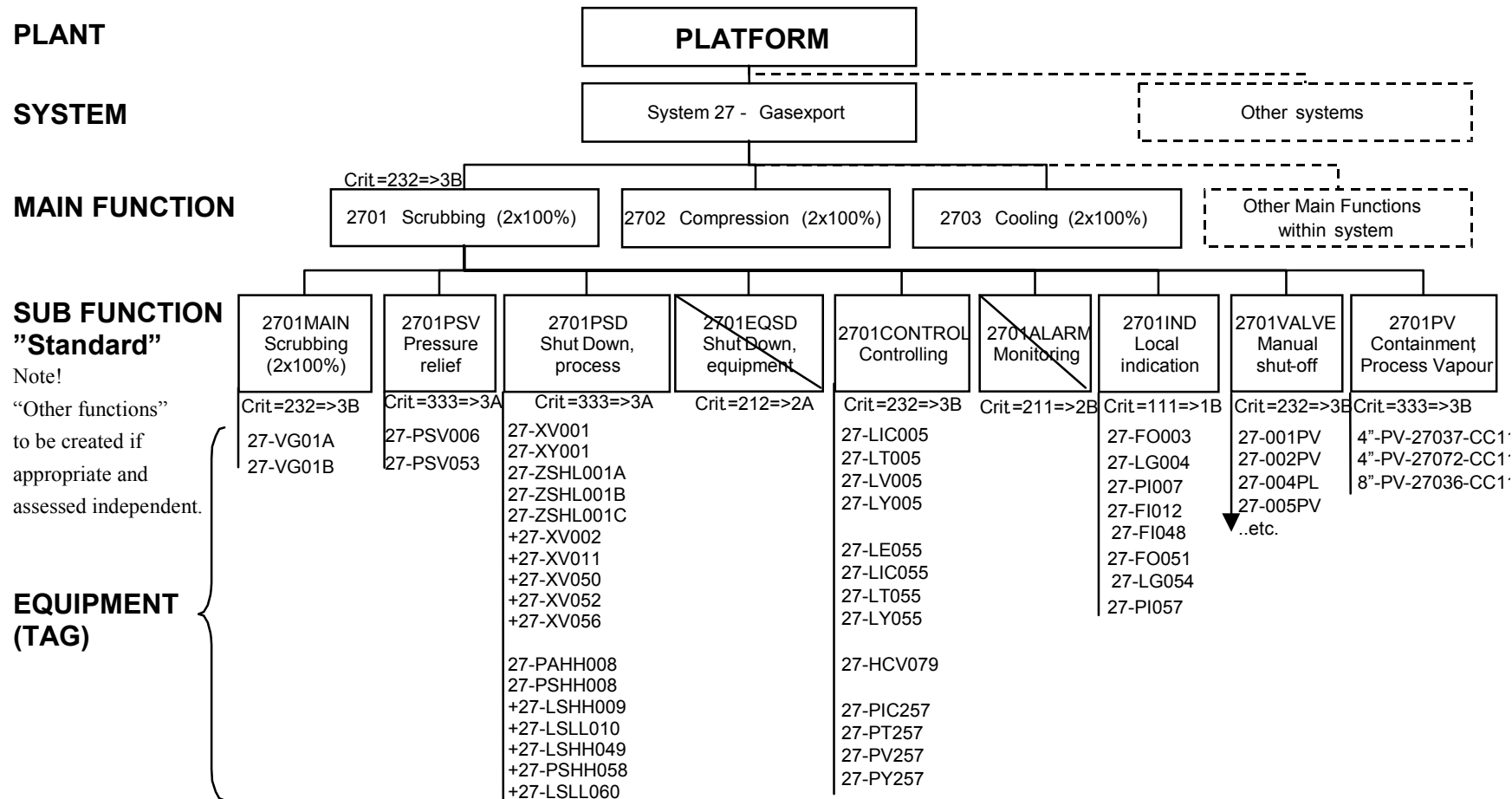
(informative)

Practical examples

C.1 Functional hierarchy

The plant system 27 (gas export) is shown in Figure C.1 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.



Explanation: Crit.= Criticality expressed as 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 C.1 – Functional hierarchy, example with standard sub functions

C.2 Documenting the result

A typical example of a criticality analysis of a MF (2701 Scrubbing), with standard sub functions listed, is shown in Figure C.2. 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 as defined in 5.4.1, for the relevant operating mode.

Z008	CRITICALITY OF MAIN FUNCTION AND ITS FUNCTIONS	21-feb-00 Page 1 of 1
------	--	--------------------------

System: 27 - GAS PIPELINE COMPRESSION, METERING AND TRA**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-F027-P-*E-001-01 rev: B last updated: 21.02.00

Critical failure which affects system in 0 hours with 100% reduction.			Criticality			
Failure mode	System effect	Installation effect	S	P	C	H
Virker ikke	System is shut down/ is not available. Max. 4 hours (valver/instrument failure).	Gasproduction is shut down and flared. CO2 tax (100.000 - 1 mill. NOK), and environmental consequence. Oilproduction to be maintained acc to tariff quotas.	2	3	2	N
Virker feil	Reduced condensate separation	No immediate effect	1	1	1	N

Function	Description	reductio	Crit. time	PU*Cap>Re	Does't work	Works improperly	Criticality
2701MAIN	Scrubbing	100%	0	2*100>B	232-N	111-N	232>3
2701ALARM	Monitoring	0%	168	2*100>B	211-Y	111-N	211>2
2701CONTRO	Controlling	100%	0	2*100>B	232-N	111-Y	232>3
2701IND	Local Indication	0%	720	2*100>B	111-N	111-Y	111>1
2701PSD	Shutdown, Process	100%	0	2*100>A	333-Y	111-N	333>3
2701EQSD	Shutdown, Equipment	100%	0	2*100>A	212-Y	111-N	212>2
2701PSV	Pressure Relief	100%	0	2*100>A	333-Y	111-N	333>3
2701VALVE	Manual Shut-Off	100%	0	2*100>B	232-N	-	232>3
2701PV	Containment, Process Vapour	100%	0	2*100>A	333-N	-	333>3

Figure C.2 – Consequence assessment of a MF. The example is shown with some key data and the classification of the sub functions listed below

Annex D (informative) Relations to other NORSOK standards

Analyses for safety, reliability and maintenance are related. The following NORSOK standards deal with these issues as depicted in Figure D.1:

- NORSOK standard Z-008
The purpose of the standard is to provide requirements for effective planning and execution of criticality analysis for maintenance purposes - and guidelines for establishing a basis for preparation and optimisation of maintenance taking into account risks related to personnel, environment, production loss and direct economical cost.
- NORSOK standard Z-013
The purpose of the standard is to establish requirements for effective planning, execution and use of risk and emergency preparedness analysis. Also the use of risk acceptance criteria is covered, thus the standard covers some aspects of risk assessment.
- NORSOK standard Z-016
The purpose of the standard is to establish requirements to planning, executing and use of reliability technology. The standard focuses on regularity management and analysis of facilities and operations, as well as availability and reliability at system or equipment level, and qualified application of reliability and maintenance data.

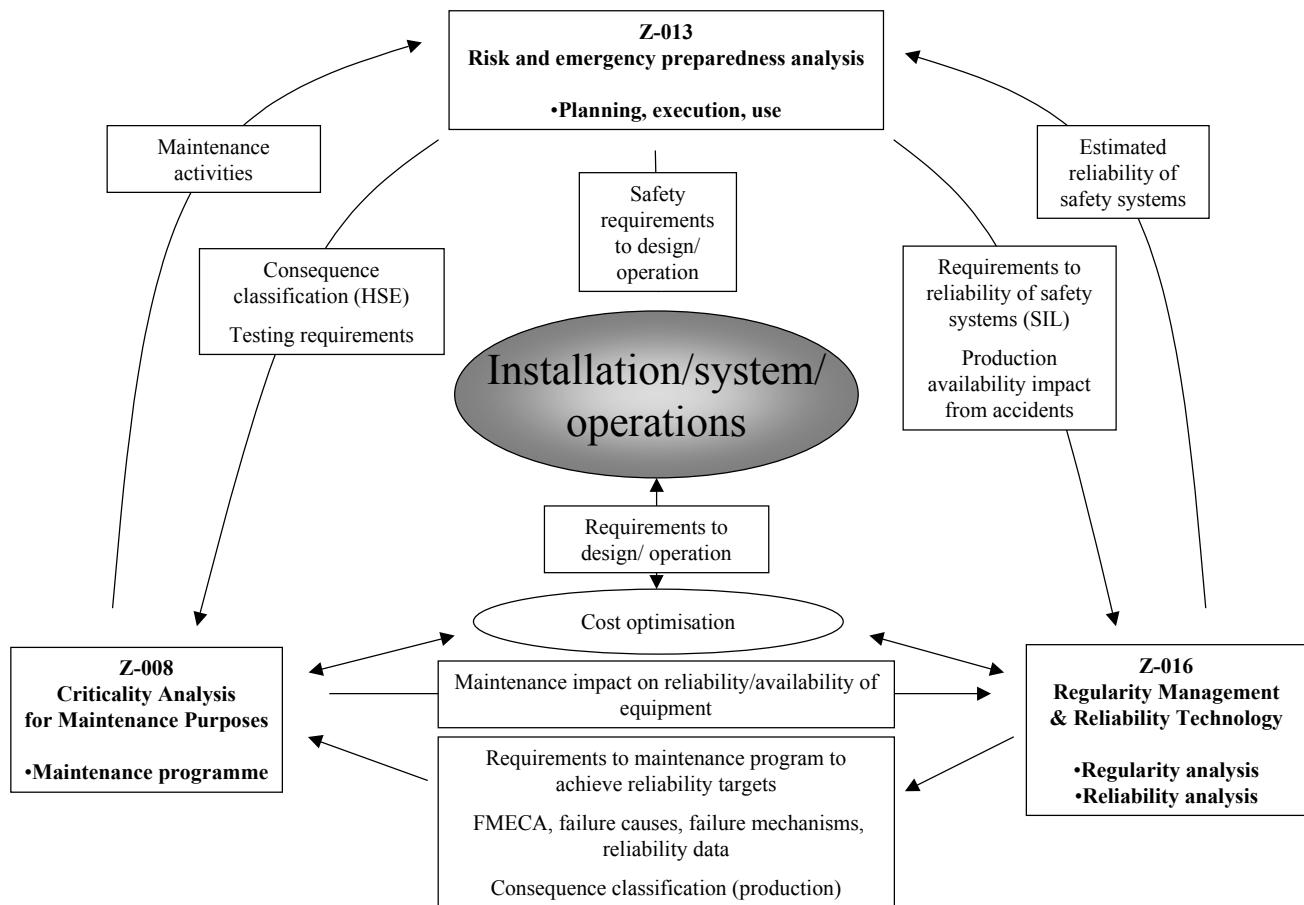


Figure D.1 – Relations between NORSOK standards Z-008, Z-013 and Z-016

Bibliography

- | | | |
|----|-----------------|--|
| 1. | NORSOK S-CR-002 | Health, safety and environment during construction |
| 2. | NORSOK S-001 | Technical safety |
| 3. | NORSOK Z-DP-002 | Coding system |

