

CONTENT

APPENDIX A	BACKGROUND FOR MINIMUM SIL REQUIREMENTS	2
APPENDIX B	EXAMPLES ON HOW TO DEFINE EUC.....	21
APPENDIX C	EXAMPLES ON HOW TO HANDLE DEVIATIONS.....	24
APPENDIX D	ESTIMATION OF PROBABILITY OF FAILURE ON DEMAND.....	29
APPENDIX E	LIFECYCLE PHASES FOR A TYPICAL OFFSHORE PROJECT.....	37
APPENDIX F	COLLECTION AND ANALYSIS OF RELIABILITY DATA	39

APPENDIX A Background for minimum SIL requirements

A.1 General

This appendix documents the background for the minimum SIL requirements as presented in Table 7.1, section 7.6, of this guideline. The formulas used in the calculations are discussed in Appendix D.

When stating minimum SIL requirements like the ones given in this guideline, one main objective should be to ensure a performance level equal to or better than today's standard. In this regard, there are certain considerations to be made in order to avoid that the stated criteria actually result in a relaxation of the safety level. Some of these considerations are discussed below:

- When using "conservative" failure rates and/or long test intervals for calculating the failure probability of a given function, the resulting PFD $\approx \lambda_{DU} \cdot \tau / 2$, becomes "high". Accordingly, a "low" SIL value will be claimed for the function, resulting in a "non-conservative" requirement in the minimum SIL table;
- Consequently, it is important that the input data fed into the calculations in this appendix are realistic both with respect to the failure rates being representative for new equipment as well as the test intervals.
- For several important safety functions, the failure probability "on demand" seem to become in the order of $1 \cdot 10^{-2}$ (e.g. $1 \cdot 10^{-2}$) when calculating the PFD using "standard" reliability data and test intervals. If this results in a SIL 1 requirement, there are two aspects to be kept in mind: (1) In such case the PFD can vary between 0.1 – 0.01 and (2) As discussed above the historical data from e.g. from OREDA and PDS might be conservative for new equipment. Therefore, as a general rule in this appendix, a SIL N requirement has been claimed when the calculated PFD is in the lower end of the interval of SIL N-1. E.g. when the estimated PDF = $1 \cdot 10^{-2}$, a SIL 2 requirement is given. This is also in line with the NPD requirement for continuous improvements.

The failure data, which are presented below and as used in the "generic quantifications", are considered to be typical values, often used in previous calculations of this type. However, it is stressed that these values should *not* be used uncritically in future calculations. Actually some of the input data may now be outdated, and more important, in actual calculations it is crucial that application specific data are applied whenever available and documented.

Another important aspect concerns the failure rate λ_{DU} , which is the rate of critical failures undetectable by automatic self-test. The λ_{DU} values applied in the example calculations assumes a certain diagnostic coverage, which is given from the applied data source (mainly PDS - see below). It is therefore important that during the process of SIL verification, the assumed diagnostic coverage factors are properly documented. This requirement will, in addition, follow from the documentation of hardware safety integrity, ref. Table 2 and 3 in IEC 61508-2, where requirements to (amongst other) diagnostic coverage (DC) and safe failure fraction (SFF) are given depending on the claimed SIL.

For the examples given here, some details are omitted, e.g. barriers, relays and signal adapters. In the final calculations, to prove compliance, all components and modules that may influence PFD of the function has to be included. In addition to the PFD requirements all other requirements has to be fulfilled, to prove compliance.

A.2 Data dossier

This section contains a collection of the reliability data used in the calculations.

With respect to the applied failure rates, these are to a large degree based upon the PDS report "Reliability Data for Control and Safety Systems, 1998 Edition" which is considered the most "up to date" database for the referred equipment.

A.2.1 Reliability Data

Table A.1 summarises the failure rates used in this appendix. λ_{DU} is here the rate of failures causing Fail-To-Operate (FTO) failures, undetectable by automatic self-test. TIF (Test Independent Failure) is the probability that a component which has just been functionally tested will fail on demand, i.e. resembling the term "systematic failure" in IEC 61508/61511

Table A.1 Applied failure rates

Component	Failure rate $I_{DU} (\cdot 10^{-6})$	TIF	Data source / comments
Pressure transmitter	0.1	$3 \cdot 10^{-4}$ ¹⁾ $5 \cdot 10^{-4}$ ²⁾	Reliability Data for Control and Safety Systems, 1998 Edition (PDS) ¹⁾ For smart transmitter ²⁾ For standard transmitter
Level transmitter	0.1		
Temperature transmitter	0.1		
Smoke detector	0.8	- *	Reliability Data for Control and Safety Systems, 1998 Edition (PDS). Coverage of self-test has increased during the last years, and in particular the rate of the flame detector now seems high. * No TIF values are given for the detectors since the definitions of F&G functions in table 7.1 assume exposed detector, whereas the TIFs given in PDS include the likelihood of the detector not being exposed.
Heat detector	0.5		
Flame detectors, conventional	2.1		
Gas detector, catalytic	0.6		
IR Gas detector, Conventional point detector	0.7		
IR Gas detector, Line	0.7		
Logic incl. I/O card (single PLC)	1.6		
XV/ESV incl. actuator	1.3		
Blowdown valve incl. actuator	1.3	$1 \cdot 10^{-6}$ ¹⁾ $1 \cdot 10^{-5}$ ²⁾	Reliability Data for Control and Safety Systems, 1998 Edition (PDS). Same failure rate for blowdown valves as for ESVs has been assumed ¹⁾ For complete functional testing ²⁾ For incomplete functional testing
X-mas tree valves - Wing valve (WV) - Master Valve (MV)	0.8		
Down Hole Safety Valve – DHSV	2.0	-	Internal SINTEF data / includes the failure modes Fail To Close (FTC) and leakage in closed position.
Solenoid / pilot valve	1.4	-	Reliability Data for Control and Safety Systems, 1998 Edition (PDS)
Circuit Breaker < 600 V	0.34	-	T-Boken: “Reliability data of components in Nordic nuclear power plants”, rev. 3
Circuit Breaker 6 KV - 10 KV	0.18	-	
Fire water pump	1 critical failure, 400 demands; Probfail to start $= 2.5 \cdot 10^{-3}$	-	OREDA 97, 1.3.1.3.
Deluge valve including actuator, solenoid and pilot valve	Prob.fail to open $= 5 \cdot 10^{-3}$	-	This value is better than the observed; but increased testing should make this value realistic.

Table A.2 Assumed test intervals

Component	Test interval (months)	Test interval (hours)	Comments / assumptions
Transmitters	12	8760	
Fire and gas detectors	12	8760	
Logic incl. I/O card (single PLC)	6	4380	6 months interval for ESD might be optimistic; OK for PDS and F&G
Topside valves (ESV/XV/blowdown)	6	4380	Taking into consideration that such valves occasionally trip. In addition to the full stroke functional testing (e.g. once every year) partial stroke testing can be performed which will reveal most failures
DHSV	6	4380	When installed these valves might be tested as often

			as each month, increasing to every third month and then to twice a year.
Solenoid /pilot valve	6	4380	
Circuit Breakers	24	17520	
Fire water pumps	-	-	NFPA requires weekly starts of fire water pumps
Deluge valve	-	-	

Table A.3 below summarises the above input data with respect to resulting PFD (probability of failure on demand), i.e.:

$$PFD = \lambda_{DU} \cdot \tau / 2.$$

When Table A.1 presents several values (as for the TIF-probability), one value within the interval is chosen in Table A.3. Finally, also some "typical" β -factors are included in Table A.3. This is partly based on the PDS Reliability Data (1998 Edition) letting $\beta \approx 2 \cdot p_2 |_2$. The PDS values for some components are combined values for random hardware and systematic failures. However, Table A.3 provides separate β -s for these two failure categories. An analysis performed for Norsk Hydro (Tune) is another source for the β -factors for random hardware failures presented in Table A.3. This Hydro analysis applied the IEC 61508 approach for calculating some β -factors. According to these data sources the suggested β -values are perhaps somewhat optimistic. All values for random hardware failures are within the range that follows from the IEC approach; i.e. $0.5\% < \beta < 5\%$ for logic, and $1\% < \beta < 10\%$ for sensors and actuators.

It is stressed that Table A.3 in no way presents "The recommended values". They are simply "typical values" to be used in the "example calculations".

Table A.3 Summary of component reliability. Values used in example calculations.

Component	Test interv. t, (months)	Fail. rate, λ_{DU} per 10^6 hrs	PFD	TIF-prob.	b-factor ⁵⁾
Pressure transmitter	12	0.1	$0.44 \cdot 10^{-3}$	$3 \cdot 10^{-4}$ ²⁾	2% (5% for TIF)
Level transmitter	12	0.1			
Temperature transmitter	12	0.1			
Smoke detector	12	0.8	$3.50 \cdot 10^{-3}$	$5 \cdot 10^{-4}$ ²⁾	5% (20% for TIF)
Heat detector	12	0.5	$2.19 \cdot 10^{-3}$		
Flame detectors, conventional	12	2.1	$9.20 \cdot 10^{-3}$		
Gas detector, catalytic	12	0.6	$2.63 \cdot 10^{-3}$		
IR Gas detector, Conv. point detector	12	0.7	$3.07 \cdot 10^{-3}$		
IR Gas detector, Line	12	0.7			
Logic incl. I/O card (single PLC)	6	1.6	$3.50 \cdot 10^{-3}$	$1 \cdot 10^{-4}$	1% (50%)
XV/ESV incl. actuator	6	1.3	$2.85 \cdot 10^{-3}$	$5 \cdot 10^{-6}$	2% (5% for TIF)
Blowdown valve incl. actuator	6	1.3 ¹⁾	$2.85 \cdot 10^{-3}$		
X-mas tree valves (WV, MV)	6	0.8	$1.75 \cdot 10^{-3}$		
Down Hole Safety Valve – DHSV	6	2.0	$4.38 \cdot 10^{-3}$	$5 \cdot 10^{-6}$ ³⁾	-
Solenoid / pilot valve	6	1.4	$3.07 \cdot 10^{-3}$	- ⁴⁾	2%-10% ⁶⁾
Circuit Breaker, < 600 V	24	0.34	$2.98 \cdot 10^{-3}$	-	-.
Circuit Breaker, 6 KV - 10 KV	24	0.18	$1.58 \cdot 10^{-3}$	-	-
Fire water pump, (fail to start)	-	-	$2.5 \cdot 10^{-3}$	-	5%
Deluge valve incl. actuator, solenoid and pilot valve, (fail to open)	-	-	$5.0 \cdot 10^{-3}$	-	-

¹⁾ Use the same FTO rate as for XV/ESV, even if this is another failure mode (here Fail-To-Open)

²⁾ Suggested TIF-probability, given exposed detector

³⁾ It is suggested to use same TIF-probability as for XV/ESV

⁴⁾ TIF-probability for pilot is included in figure for main valve/actuator.

⁵⁾ Value applies to dangerous undetectable random hardware failures (duplicated system). Values in parenthesis apply for systematic failures (TIF).

⁶⁾ $\beta=10\%$ for pilot valves on the same valve, otherwise $\beta=2\%$

A.2.2 Assumed average demand rate

In this guideline, the demand rates are not used to determine the required SIL (see section 7). However, in order to allow follow-up during operation, it is considered an advantage to have some typical or average demand rates as a basis for comparison (see section 10). As proven field data is usually missing, assumed average demand rates are therefore suggested below. As part of the requirements in section 10 of this guideline, these demand rates have to be collected separately for each installation in the future.

There are several limitations and pitfalls in using the figures presented below:

- The Cause&Effect diagram for the installation will influence strongly on the dependence between the various figures
- Some figures are given per installation, not per function. Single functions repeatedly contributing to the demand rate should be investigated
- The figures should be calibrated depending on size and complexity of the process
- Here, some average oil and gas processing installation is assumed
- As SIL (in this guideline) is independent of the demand rates, a conservative assumption will be to assume low demand rates as a basis for comparison
- Only real demands should be counted, not spurious activation

The following assumptions were made when stipulating the annual demand rates:

- It is assumed 3 demands per year for the ESD segregation. Of these 2 are manually released
- For the (one assumed) automatically initiated ESD segregation, it is assumed that
 - 20% comes from *confirmed* fire
 - 80% comes from *confirmed* gas
- The total number of exposures of *single* F&G detectors are assumed as
 - 2 fire alarms
 - 8 gas alarms
- 10 electric isolations are required as a consequence of detected fire or gas
- Blowdown is manually activated for 2 of the 3 ESD demands
- 3 isolations per well and/or riser due to ESD segregations are assumed
 - in addition, it is assumed that the installation inlet also is closed 10 times due to PSD (might be a separate/additional PSD valve depending on specific solution)
- 3 PSD segregations are assumed, all due to ESD segregation
- 21 local PSD functions (pressure, level and temperature) per platform (see table for distribution)
- 1 release of deluge due to confirmed fire or gas

Table A.4 Local safety functions - Assumed demand rates

Safety function	Assumed average demand rate per year (planned testing not included)
<i>Process segregation (through PSD)</i> (closure of several valves)	3
<i>PSD functions : PAHH/LAHH/LALL</i> (closure of one critical valve)	5/5/5 (<i>per installation</i>)
<i>PSD function: LAHH on flare KO drum</i> (detection and transfer of SD signal)	0.1
<i>PSD function: TAHH/TALL</i> (closure of one critical valve)	3/3 (<i>per installation</i>)
<i>PSD function: PALL</i> (primary protection against leakage)	NA

Table A.4(cont.) Global safety functions - assumed demand rates

Safety function	Assumed average demand rate per year (planned testing not included)
<i>ESD segregation</i> (closure of one ESD valve)	3
Depressurisation (blow down); (opening of one BD valve)	2
<i>Isolation of well;</i> (shut in of one well)	3 (per well) (10 PSD isolations of inlet per well)
<i>Isolation of riser;</i> (shut in of one riser)	3 (per riser) (10 PSD isolations of inlet per riser)
<i>Fire detection;</i> (alarm signal generated, processed and necessary action signals transmitted)	2 (<i>per installation</i>)
<i>Gas detection;</i> (alarm signal generated, processed and necessary action signals transmitted)	8 (<i>per installation</i>)
<i>Electrical isolation;</i> (signal giving action processed in F&G logic and electrical ignition sources removed)	10
<i>Deluge;</i> (fire water demand signal processed in Fire & Gas logic, start of fire pump, and opening of deluge-valve)	1

A.3 PSD functions

A.3.1 Process segregation through PSD

Definition of functional boundaries

An example of the function “*segregation of process section*” is given in figure A.1 below.

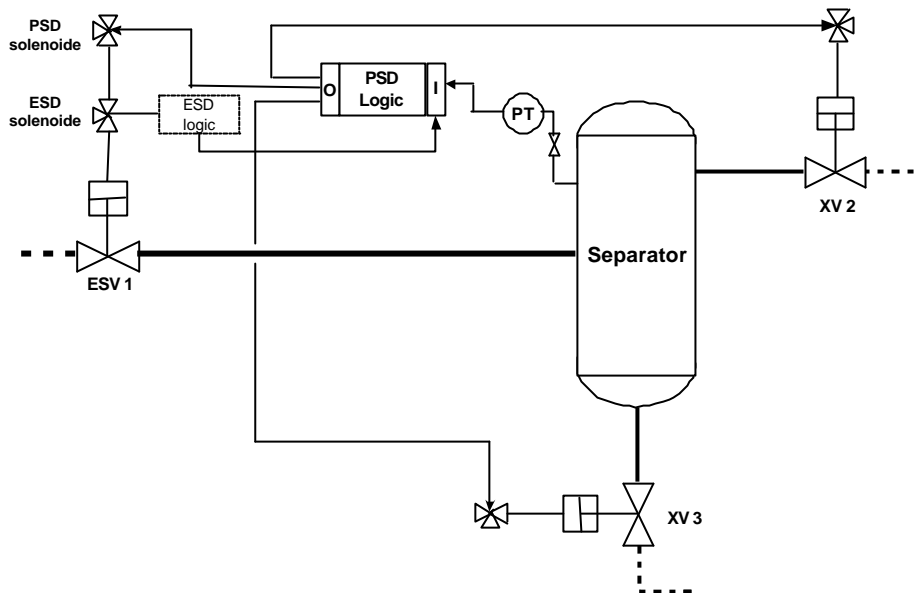


Figure A.1 Possible definition of the function “*segregation of process section through PSD*”

The function “*segregation of process section*” is here defined by the PSD system receiving and processing some signal (e.g. a PALL or a shutdown signal from the ESD system), which activates a closure of ESV 1, XV 2 and XV 3 in order to isolate the vessel.

The function starts where the signal is generated (not including transmitter or ESD system) and ends and includes closing of all the necessary valves. The transmitter is not included as this function is most probably activated on an ESD demand. Requirement to the PT is covered by the function PAHH in A 3.2.

It should be noted that the specific valves needed for segregation depends on the situation, as some of the valves used in the segregation will be “nice to have” – while others will be essential. The hazard analysis will pinpoint the essential valves/actions and only these valves should be included in the PSD function. This is further discussed in section A.3.2 – A.3.5 below where specific process deviations are considered.

Quantification of safety function

The Reliability Block Diagram (RBD) for this function is given below. Just one Solenoid box is drawn although there shall be three in series. This is indicated by “x3” above this box. The PFD quantification is presented in Table A.5. The last column also provides the TIF for the function.

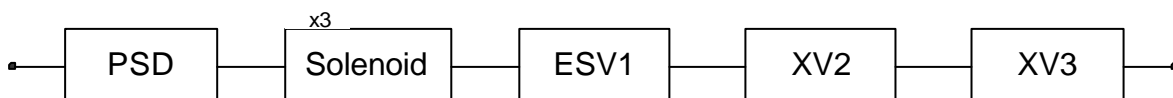


Figure A.2 RBD for Process segregation through PSD.

Table A.5 PFD for Process segregation through PSD

Component	No. of components	PFD per component	Total PFD	Total TIF
PSD logic +I/O	1	$3.50 \cdot 10^{-3}$	$3.50 \cdot 10^{-3}$	$1 \cdot 10^{-4}$
ESV/XV	3	$2.85 \cdot 10^{-3}$	$8.55 \cdot 10^{-3}$	$1.5 \cdot 10^{-5}$
Solenoid / pilot	3	$3.07 \cdot 10^{-3}$	$9.21 \cdot 10^{-3}$	-
Total Function	-	-	0.021	1.2×10^{-4}

As seen the PFD is estimated to be ≈ 0.02 , and a SIL 1 requirement seems achievable based on a pure quantitative consideration.

A.3.2 PSD functions : PAHH, LAHH, LALL, (primary protections)

Definition of functional boundaries

Figure A.3 illustrates the boundaries for the PSD functions PAHH, LAHH and LALL.

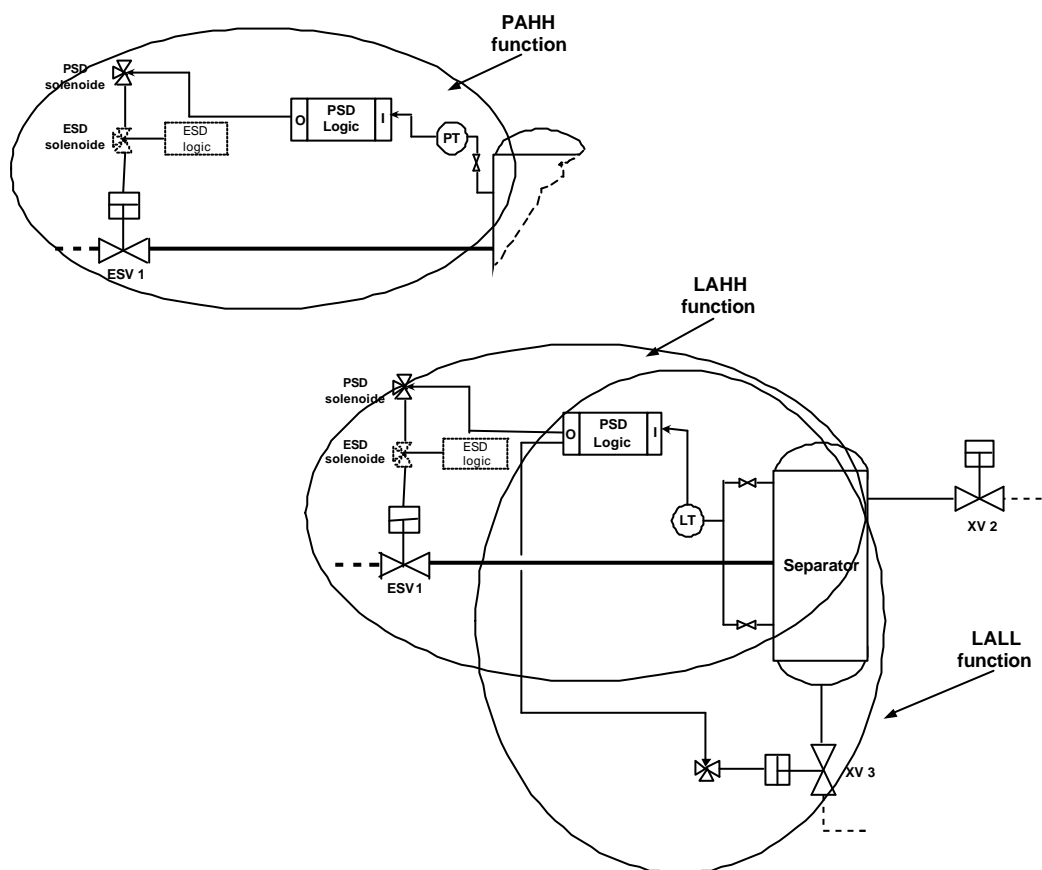


Figure A.3 Example of definition for the functions: PAHH, LAHH and LALL

It is here assumed that:

- A PAHH will only close the inlet valve(s), not the outlet valves;
- A LAHH will close the same valves as a PSHH;
- A LALL will only close the valve on the liquid outlet.

The function starts inside the process where the high pressure or level is detected, and ends within the process with closing of the valve.

It should be noted that in the above definition it is assumed that there is one common inlet valve to the separator. However, the PSD functions PAHH and LAHH might depend upon closure of several valves if there is more than one line into the separator and no common inlet valve. In such case a separate evaluation should be performed in order to evaluate whether a lower SIL requirement than given below (SIL 2) is acceptable.

Quantification of safety functions

The Reliability Block Diagram for this function is given below. The PFD quantification is presented in Table A.6. The presentation is common for all three functions: PAHH, LAHH and LALL (closure of one valve).

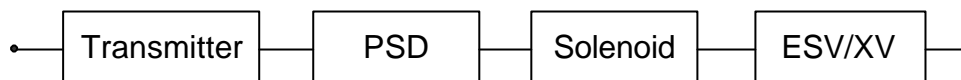


Figure A.4 RBD for PAHH, PALL and LALL.

Table A.6 PFD for Process segregation through PSD

Component	No. of components	Total PFD	Total TIF
Transmitter	1	$0.44 \cdot 10^{-3}$	$3 \cdot 10^{-4}$
PSD logic + I/O	1	$3.50 \cdot 10^{-3}$	$1 \cdot 10^{-4}$
ESV / XV	1	$2.85 \cdot 10^{-3}$	$0.5 \cdot 10^{-5}$
Solenoid / pilot	1	$3.07 \cdot 10^{-3}$	-
Total Function	-	0.010	4.1×10^{-4}

Here PFD is estimated to be $0.0099 \approx 0.01$, and a SIL 2 requirement seems achievable based on a pure quantitative consideration.

A.3.3 PSD function: LAHH in flare KO drum

Definition of functional boundaries

A LAHH in the flare KO drum shall close the feed to the vessel and will therefore generally require a closure of the inlet lines to the installation and/or to the inlet separator. Since it will normally be difficult to detect from where the overfeed originates, a LAHH in the flare KO drum will often initiate a global shutdown of the process through the PSD system and possibly also through the ESD system in order to increase the reliability of the function.

Consequently, a generic definition of the function *LAHH in flare KO drum* with respect to what is actually shut down, is difficult to give, and rather the function is defined in terms of the detection device and the processing of the signal, i.e. as illustrated in Figure A.5 below.

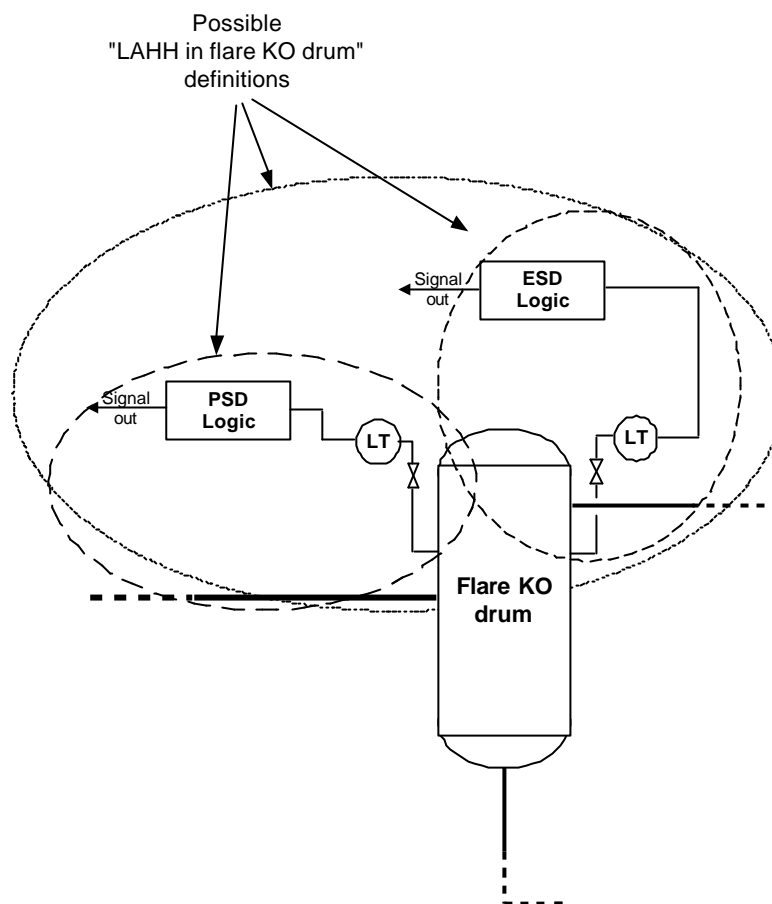


Figure A.5 Possible definitions of the function: LAHH in flare KO drum

As indicated on the figure, shutdown as a result of LAHH in the flare KO drum can be executed through the PSD system, the ESD system or through both. A possibility, not shown on the figure, could be that one common transmitter is applied to send a signal to both the PSD and the ESD system.

Hence, the function starts inside the process where the high level is expected, and ends at the unit(s) intended to perform the action (these units are not included).

Quantification of safety functions

The RBDs for this function is given below. Three different solutions of implementation are presented:

1. Shutdown executed through PSD (or ESD) alone
2. Shutdown executed through both PSD and ESD; using the same LT
3. Shutdown executed through both PSD and ESD; using separate LTs.

The PFD values for relevant single and duplicated components are presented in Table A.7. The resulting PFD values for the function are presented in Table A.8 (for all three solutions).

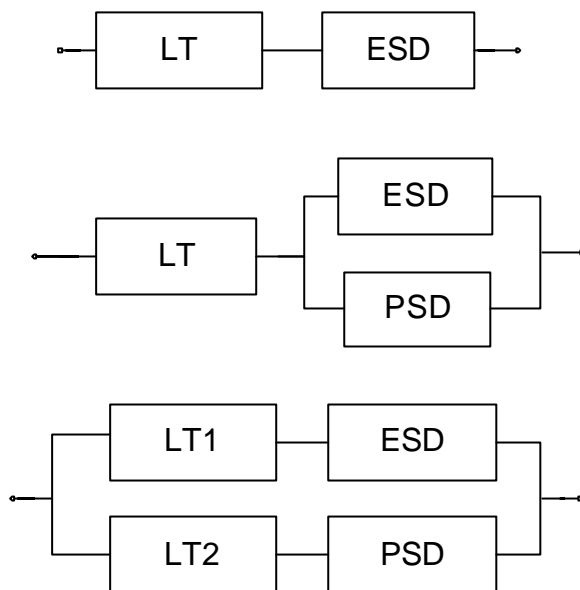


Figure A.6 RBDs for LAHH in flare KO drum (Solutions 1, 2 and 3).

Table A.7 PFD input for LAHH in flare KO drum

Component	PFD, single component	PFD, duplicated comp.	TIF, single component	TIF, duplicated comp.
LT	$0.44 \cdot 10^{-3}$	$0.88 \cdot 10^{-5}$	$3 \cdot 10^{-4}$	$1.5 \cdot 10^{-5}$
PSD/ESD logic +I/O	$3.50 \cdot 10^{-3}$	$3.50 \cdot 10^{-5}$	$1 \cdot 10^{-4}$	$5 \cdot 10^{-5}$

Table A.8 PFD results for LAHH in flare KO drum

Solution	PFD for function	TIF-probability for function
1. PSD (or ESD) alone	$3.94 \cdot 10^{-3}$	$4 \cdot 10^{-4}$
2. PSD and ESD); single LT	$0.48 \cdot 10^{-3}$	$3.5 \cdot 10^{-4}$
3. PSD and ESD; separate LTs	$4.4 \cdot 10^{-5}$	$6.5 \cdot 10^{-5}$

Thus, a SIL 3 requirement seems achievable given that the function is implemented through both the PSD and ESD system (i.e. if Solution 1 is *not* chosen).

A.3.4 PSD function: TAHH/TALL

Definition of functional boundaries

A TAHH/TALL will close the inlet valve(s) and the definition of the function will therefore resemble the definition of PAHH above (ref. Figure A.3), the only difference being that the pressure transmitter is substituted with a temperature transmitter.

Quantification of safety functions

The RBD and quantification is exactly as in Section A.3.2. Thus, the estimated total PFD for the TAHH/TALL function is $\text{PFD} \approx 0.01$, and a SIL 2 requirement seems achievable.

A.3.5 PSD function: PALL (primary protection against leakage)

Definition of functional boundaries

The PALL function is frequently applied as primary protection against leakage (in addition to gas detection) and will normally initiate a closure of both the inlet and outlet valves. Consequently, this particular PSD function is similar to the function “*segregation of process section*” as described in section A.3.1 above. Since the reliability of the low pressure detection itself is highly uncertain for all leaks except very large ones, the definition of PALL should be as for *segregation of process section*, i.e. excluding the sensor device.

Hence, the function starts inside the process where the low pressure is expected, and ends within the process with the valve.

Quantification of safety function

No special requirements apply according to this guideline. This requires that adequate automatic gas detection is provided to cover the leakage. It should, however, be noted that excluding the sensor device, the function fulfils a SIL 1 requirement.

A.4 Segregation through ESD with one ESD valve

Definition of functional boundaries

Isolation of an ESD segment occurs on demand from the ESD system, i.e. on detection of HC leaks or a fire on the installation. The number of ESD valves to close in such a situation will vary from case to case. Hence, a general definition of the ESD segregation function is difficult to give. It has therefore been decided to define an ESD sub-function in terms of:

- the ESD node
- one Emergency Shutdown Valve (ESV) including solenoid and actuator

This definition is illustrated in Figure A.7 below:

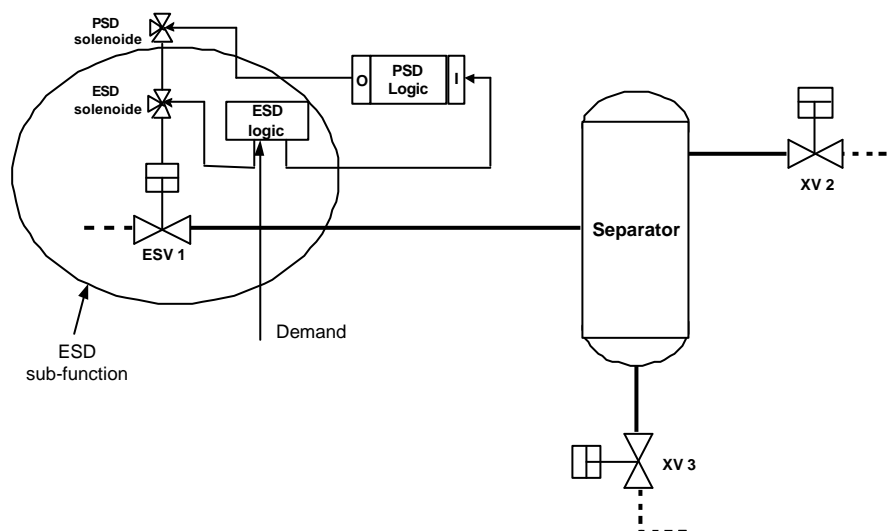


Figure A.7 Definition of the ESD sub-function

As seen from Figure A.7, the ESD sub-function is defined as closure of one valve through the ESD system. In order to increase the reliability of the sub-function, it will also be possible to include activation of the ESV through the PSD-system by a separate PSD solenoid.

The function starts at the unit giving the demand (unit not included), and ends within the process with the valve.

Quantification of safety functions

The Reliability Block Diagram for this function is given below. The PFD quantification is presented in Table A.9.

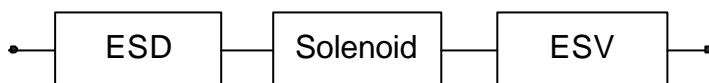


Figure A.8 RBD for ESD sub-function (Segregation through ESD with one ESD valve).

Table A.9 PFD for Segregation through ESD

Component	No. of components	Total PFD	Total TIF
ESD logic + I/O	1	$3.50 \cdot 10^{-3}$	$1 \cdot 10^{-4}$
ESV	1	$2.85 \cdot 10^{-3}$	$0.5 \cdot 10^{-5}$
Solenoid / pilot	1	$3.07 \cdot 10^{-3}$	-
Total Function	-	0.009	1.1×10^{-4}

Here PFD is estimated to be 0.009, and based on a pure quantitative consideration a SIL 2 requirement seems achievable for this ESD sub-function.

A quantitative risk analysis should be conducted to verify that the minimum SIL-requirement gives an overall acceptable risk when all the ESD valves are taken into consideration. The following should then be considered:

- number of ESD-valves needed to isolate each fire area
- scenarios where the system is demanded (e.g. leak and fire scenarios)
- process conditions (pressure, temperature) and duration of leaks and fires.
- common cause failures
- etc.

A.5 Blowdown

Definition of functional boundaries

The sub-function blowdown includes:

- the ESD node
- one blowdown valve (BDV) incl. solenoid and actuator

The function starts at the unit giving the demand (unit not included), and ends with the inventory having free access through the BDV.

The probability of successful manual blowdown activation is not included in the definition of the function. Figure A.9 illustrates the sub-function “blowdown”.

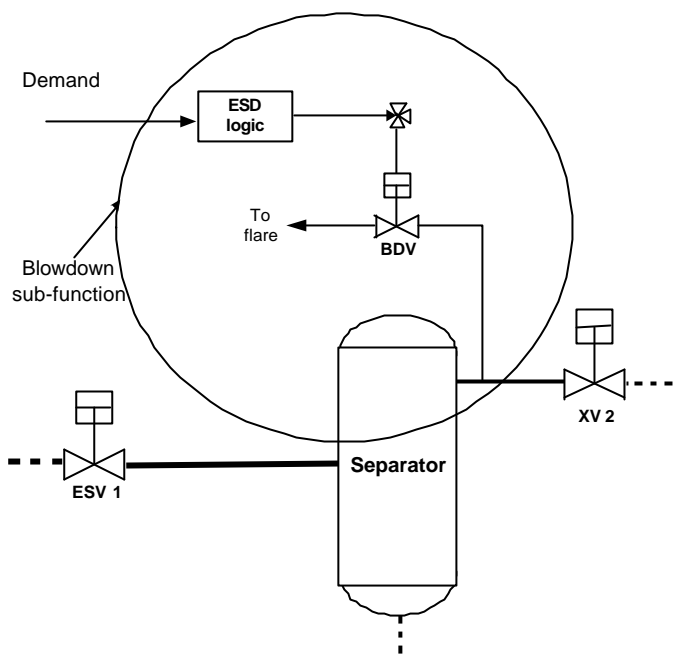


Figure A.9 Definition of the sub-function “blowdown”

Quantification of safety function

The Reliability Block Diagram for this function is given below. The PFD quantification is presented in Table A.10.

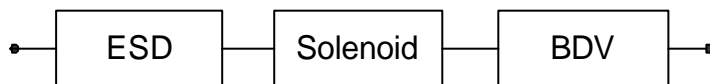


Figure A.10 RBD for sub-function blowdown

Table A.10 PFD for Blowdown

Component	No. of components	Total PFD	Total TIF
ESD logic + I/O	1	$3.50 \cdot 10^{-3}$	$1 \cdot 10^{-4}$
BDV	1	$2.85 \cdot 10^{-3}$	$0.5 \cdot 10^{-5}$
Solenoid / pilot	1	$3.07 \cdot 10^{-3}$	-
Total Function	-	0.009	1.1×10^{-4}

Here the PFD is estimated to be 0.009 and based on a pure quantitative consideration a SIL 2 requirement seems achievable for the Blowdown sub-function.

A quantitative risk analysis should be conducted to verify that the minimum SIL-requirement gives an overall acceptable risk. The following should be considered:

- number of blowdown-segments in each fire area
- scenarios where the system is demanded (fire scenarios)
- process conditions (pressure, temperature) and duration of fires.
- common-cause failures

A.6 Isolation of well

Definition of functional boundaries

The isolation function concerns only the ESD functions related to the isolation, not the overpressure protection realised through the PSD system.

The sub-system *isolation of well* is defined as the system needed to isolate one well. For a standard production well, the sub-system consists of the following:

- ESD node
- Wing valve (WV)
- Master Valve (MV)
- Downhole safety valve (DHSV)
- Solenoid valves

All valves (WV, MV & DHSV) are assumed hydraulically fail-safe, and one of the valves electrically fail-safe. There may exist additional means for removing the hydraulic power to the valves.

The function starts at the unit where the demand is initiated (unit not included), and end with the valves shutting in the well.

Depending on the scenario having triggered the demand for isolation, one of the three valves will be sufficient to isolate the well. However, in the event of a fire in the wellhead area, the well should be isolated by the DHSV.

The well or inlet to the platform will also be isolated due to PSD demands, but these are not included in this function. Depending on for example the event and C&E, this may cause a demand on the same valves or other valves.

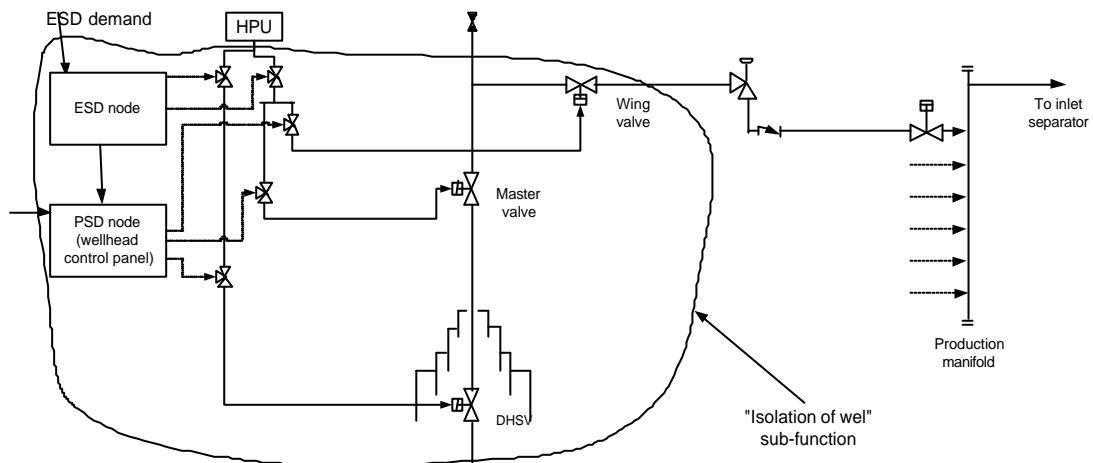


Figure A.11 Definition of the sub-function “isolation of well”

Quantification of safety functions

The function “isolation of one well”, can be represented by a Reliability Block Diagram as shown in Figure A.12 below. The illustrated solution is to have separate solenoids for the MV, the WV and the DHSV (activated by PSD), and one solenoid (activated directly by ESD) to remove hydraulic power to all three valves. Note that this RBD is slightly simplified.

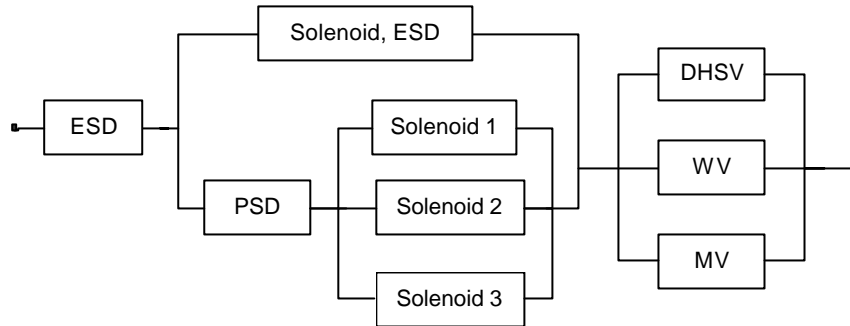


Figure A.12 RBD for “failure to isolate one well”

The calculations are presented in Table A.11, and the result in Table A.12. The quantifications assume common cause failure between the master and the wing valve, but not between MV/WV and DHSV. The essential contribution is from the ESD-system. In addition, the quantification here gives a small contribution from common cause failures of the solenoids, (as the IEC model gives the same result for common cause failure, irrespective of whether there is a 1oo2, 1oo3 or 1oo4 configuration).

Table A.11 PFD input for isolation of one well

Component	PFD, single component	PFD, duplicated comp.	TIF, single component	TIF, duplicated comp.
ESD/PSD logic +I/O	$3.50 \cdot 10^{-3}$	-	$1 \cdot 10^{-4}$	-
Solenoid	$3.07 \cdot 10^{-3}$	$6.14 \cdot 10^{-5} \text{ } ^1)$	-	-
MV /WV	$1.75 \cdot 10^{-3}$	$3.50 \cdot 10^{-5}$	$5 \cdot 10^{-6}$	$0.3 \cdot 10^{-6}$
DHSV	$4.38 \cdot 10^{-3}$	-	$5 \cdot 10^{-6}$	-

¹⁾ The standard β -factor model used here gives (essentially) same result for the 1oo4, 1oo3 and 1oo2 voting (cf. Appendix D). A more refined modelling would give a better value for 1oo3 with a factor 3.

Table A.12 PFD results for isolation of one well.

Solution	PFD for function	TIF-probability for function
1. Separate solenoids for MV, WV and DHSV. Additional "ESD solenoid" to remove hydraulic power to valves,	$3.6 \cdot 10^{-3} \text{ } ^1)$	$1 \cdot 10^{-4}$

¹⁾ Would be $3.5 \cdot 10^{-3}$ if the more refined β -factor model for 1oo3 (1oo4) voting of solenoids was applied.

Here PFD is estimated to be 0.0036, and based on a pure quantitative consideration SIL 2 requirement is achievable for the isolation of a single well. By introducing a redundant ESD-logic (1oo2 voting), the example calculation would give $\text{PFD} = 4 \cdot 10^{-5}$, and SIL 3 is clearly achievable.

Since isolation of the well is considered a crucial safety function, and since three valves are available for isolation, a SIL 3 requirement has been stated. As observed, this can be achieved by introducing redundancy with respect to safety in the ESD logic.

A quantitative risk analysis should be conducted to verify that the minimum SIL-requirement gives an acceptable risk when the total number of wells are taken into consideration. The following should be considered:

- Number of wells
- Production / injection wells with or without gas-lift
- Wells in connection with special operations, such as wireline, coiled tubing, workover, testing, cleanup, etc.

A simplified example of how a verification of the stated SIL 3 requirement can be performed using QRA, is given in Appendix C.2.

A.7 Isolation of riser

Definition of functional boundaries

Isolation of the riser occurs on demand from the ESD system, i.e. on detection of HC leaks or fire on the installation. The sub-function *isolation of riser* is defined as the function needed to isolate one riser:

- the ESD node
- one Riser Emergency Shutdown Valve (ESV) including solenoid and actuator

The sub-function starts at the unit where the demand is initiated (unit not included), and ends with the valve closing towards the riser. The sub-function is illustrated in Figure A.13 below.

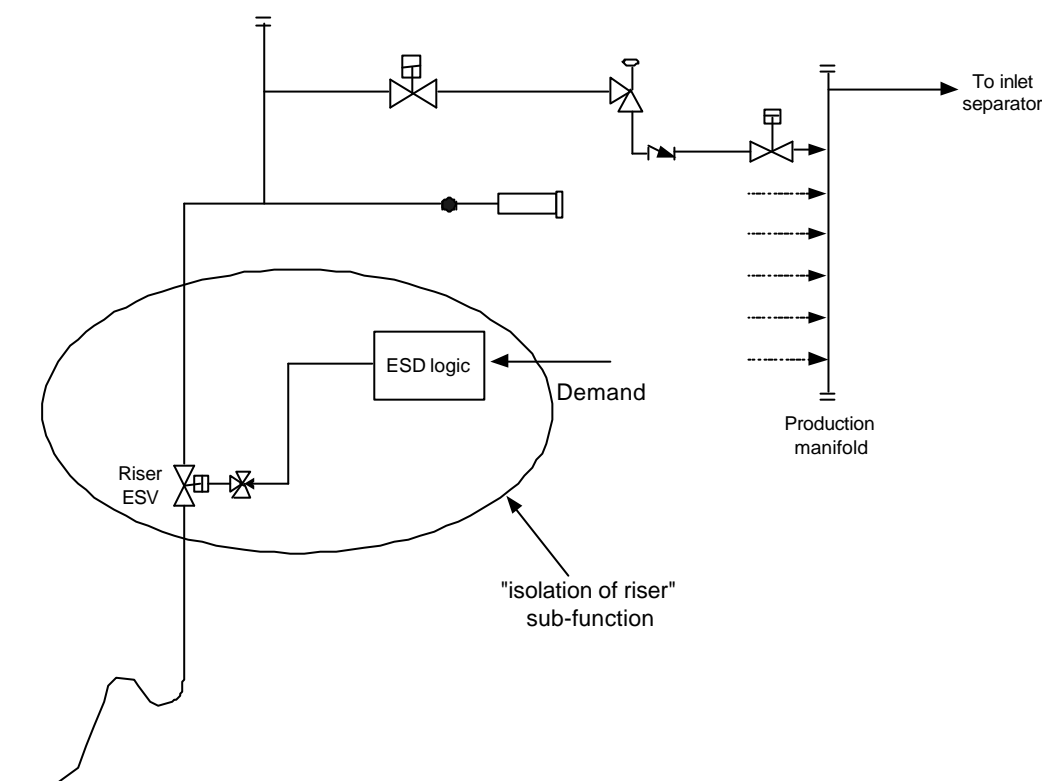


Figure A.13 Definition of the sub-function “isolation of riser”

Quantification of safety functions

The RBD and calculations will be exactly as for “Segregation through ESD”, see Section A.4. Thus the calculated $PSD = 0.009$, and hence by considering isolation of one riser only, SIL 2 is achievable.

A quantitative risk analysis should be conducted to verify that the minimum SIL-requirement gives an acceptable risk. The following should be considered:

- number of risers
- fluid (gas, oil or condensate)
- process conditions (pressure, temperature)
- size/length of riser/flowline

A.8 Fire detection

Definition of functional boundaries

The Fire & Gas detection system consists mainly of detectors and Fire&Gas logic solvers. Fire detection is generally based on three principles, i.e. smoke detection, heat detection and flame detection:

- For smoke detection the sub-function starts when the smoke has entered the detection chamber, and ends with the signal given from the F&G system.
- For heat detection the sub-function starts when the radiation has entered the detection chamber, and ends with the signal given from the F&G system.
- For flame detection the sub-function starts when the flames are present at the detection device, and ends with the signal given from the F&G system.

Note that the fire detection sub-function is defined in terms of one single detector.

Quantification of safety functions

The RBD is presented in Figure A.14. The PFDs for the three cases, *smoke detection*, *heat detection* and *flame detection* are presented in Table A.13. This indicates that SIL 2 may be realistic, but the present quantification gives a PFD > 0.01 for flame detection (based on conservative data).

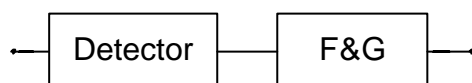


Figure A.14 RBD for fire detection sub-function

Table A.13 PFD and TIF results for fire detection.

Function	PFD for function ¹⁾	TIF-probability for function
1. Smoke detection	0.007	$6 \cdot 10^{-4}$
2. Heat detection	0.006	
3. Flame detection	0.013	

¹⁾ Failure data for detectors and logic are considered conservative. Diagnostic coverage for fire detectors have increased during the last years.

If a fire-central or some other logic's is used to interface between the detector and the F&G, this has to included in the calculations.

A.9 Gas detection

Definition of functional barriers

Gas detection is in general based on two different principles; point detection and line detection:

- For point detectors the function starts when the gas has entered the detection chamber, and ends with the signal given from the F&G system.
- For line detectors the function starts when the gas has entered the beam, and ends with the signal given from the F&G system.

The F&G detection system will have different actions based on configuration of the logic. There are different actions depending on where the gas is detected, and typically for new platforms (signal is given at 20% of LEL);

- 1ooN detectors will give an alarm in CCR.
- 1ooN detectors in non-hazardous areas will give electrical isolation of this area.
- 2ooN in any area will give electrical isolation and stop production.

Here, the gas detection sub-function is defined in terms of one single detector.

Quantification of safety function

The RBD for a single gas detector is identical to that for fire detection (Figure A.14). The quantification for gas detection is given in Table A.14.

Table A.14 PFD and TIF results for gas detection sub-function (i.e. single detector)

Function	PFD for function	TIF-probability for function
1. Catalytic detector	0.006	$6 \cdot 10^{-4}$
2. IR gas detector, conven. point det.	0.007	
3. IR gas detector, line detector	0.007	

From the table it is seen that a SIL 2 requirement is achievable.

It should be noted that in Appendix D.7, some example calculations have been performed for different types of gas detection voting configurations.

A.10 Electrical isolation

Definition of functional barriers

The SIL-requirement applies for the subsystem needed for electrical isolation given signal from F&G node, i.e:

- F&G node
- Circuit breakers / relay

The function starts at the unit initiating the demand (unit not included), and ends when the equipment is isolated.

Electric isolation is initiated from by F&G detection system. There are different actions depending on where the gas is detected. On new platforms, 1ooN detection in non-hazardous area gives electrical isolation of this area, while 2ooN in any area isolates this area or shut down main power.

Quantification of safety function

The RBD is presented in Figure A.15, for the case of 6 circuit breakers (CB). The PFD values are presented in Table A.15, using data for 600V circuit breakers. In this case it is not straightforward to achieve SIL 2. Using the data from Table A.3 would allow only 2 CB to get SIL 2. Of course, test interval < 24 months would help. Observe that the CB of 6KV has a lower PFD. To conclude, the SIL 2 requirement can be achieved if only a few circuit breakers need to open.

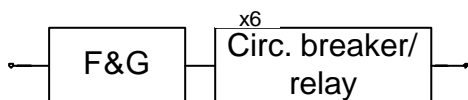


Figure A.15 RBD for Fire detection

Table A.15 PFD results for Electrical isolation. Example with 6 circuit breakers

Component	No. of components	PFD per component	Total PFD	Total TIF
F&G logic + I/O	1	$3.50 \cdot 10^{-3}$	$3.5 \cdot 10^{-3}$	$1 \cdot 10^{-4}$
Circ. Breaker (600V)	6	$2.98 \cdot 10^{-3}$	$17.9 \cdot 10^{-3}$	
Total Function	-	-	0.05	1×10^{-4}

A.11 Deluge

Definition of functional boundaries

The system boundaries includes the fire water demand signal processed in the fire pump logic, start of fire pumps, and opening of one deluge-valves (given confirmed fire).

- F&G node
- The nozzles, water intake, strainers, ring main etc. are not included but are assumed covered by inspection and maintenance program.
- The pump system consists of 2x100 % capacity pumps

The function starts at the unit initiating the demand (unit not included), and end when there is flowing water through the deluge valve.

Quantification of safety function

The RBD is presented in Figure A.16. The resulting PFD calculations are given in Table A.16. These quantifications indicate that SIL 2 can be achieved.

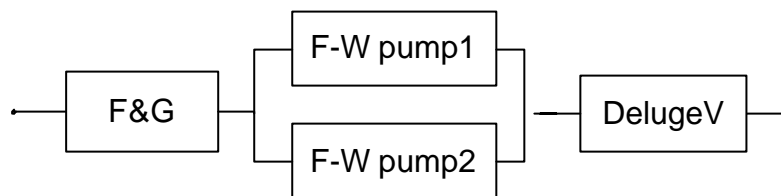


Figure A.16 Reliability block diagram for deluge function

Table A.16 PFD results for deluge

Component	Voting	PFD per component	System PFD	System TIF
F&G logic + I/O	1oo1	$3.5 \cdot 10^{-3}$	$3.50 \cdot 10^{-3}$	$1 \cdot 10^{-4}$
F-W pump	1oo2	$2.5 \cdot 10^{-3}$	$0.13 \cdot 10^{-3}$	-
Deluge valve	1oo1	$5.0 \cdot 10^{-3}$	$5.00 \cdot 10^{-3}$	-
Total Function	-	-	0.009	5.1×10^{-4}

APPENDIX B Examples on how to define EUC

IEC 61508 does not give any particular requirements as to how the EUC should be defined. Hence, it is entirely within the hands of those who wish to claim conformance to the standard to define the scope and boundary of the system to be considered. The important point will be that the EUC boundaries are clearly defined and in a manner such that all the relevant hazards to be considered in later lifecycle stages can be identified and described.

However, since definition of EUC is an important aspect of IEC 61508, section 7.3.1 and 7.3.2 of the guideline briefly discuss how EUC can be defined for local and global safety functions respectively. In this appendix, an example of a possible EUC definition is given for each type of these safety functions.

B.1 Definition of EUC for local safety functions

With respect to identification of hazards against which the local safety functions will protect, this is normally done through the HAZOP and SAT analyses. Consequently, an appropriate EUC definition would be parallel to the definition of process components applied in ISO 10418 (i.e. API RP 14C), i.e. the definition should include the process unit and associated piping and valves.

Consider a process with a high-pressure separator for a two-phased separation of oil and gas. A simplified schematic of the separator is shown in figure B.1 together with an indication of possible EUC definition. Protection of the separator is designed according to ISO 10418, with a primary and secondary barrier against undesirable events. The local safety functions for the separator are implemented through the PSD system and the PSV.

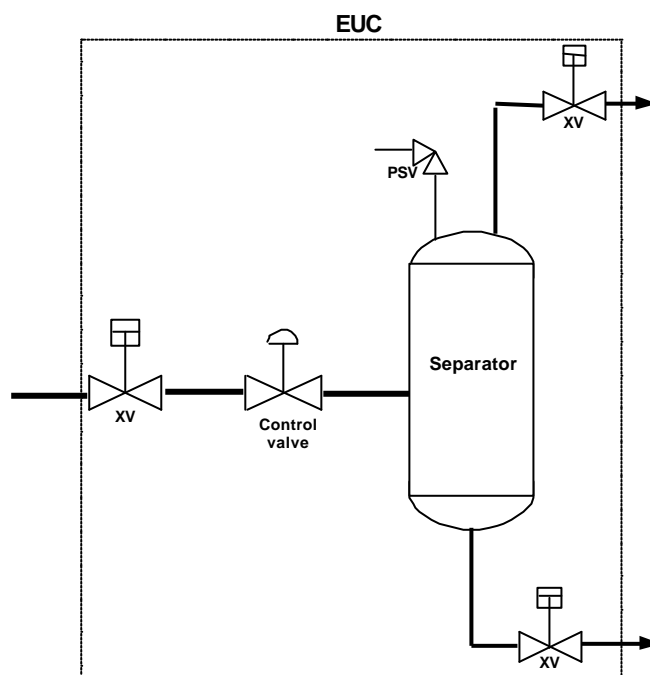


Figure B.1 Example of EUC definition for local safety functions

Hence, for this example the EUC boundaries are defined in terms of the PSD valves, which are used to isolate the separator during different PSD scenarios (ref. Appendix A.3).

B.2 Definition of EUC for global safety functions

Global safety functions on an offshore installation may include the following functions:

- Emergency shutdown function;
- Blowdown function;
- Electrical isolation function;
- Fire and Gas detection function; and
- Fire fighting function.

The purpose of these functions will be to prevent abnormal conditions, e.g. a process leakage, from developing into a major hazardous event, and further to control and mitigate the effects from such an event.

Typically, the installation will be divided into several fire areas. For process areas, emergency shutdown valves will usually be located within and at the boundaries of the fire area, e.g. next to a firewall, in order to prevent an escalation of the event from one area to another.

Hence, when considering fire and explosion events, a fire area seems an appropriate definition of the Equipment Under Control (EUC). This is illustrated in Figure B.2 below.

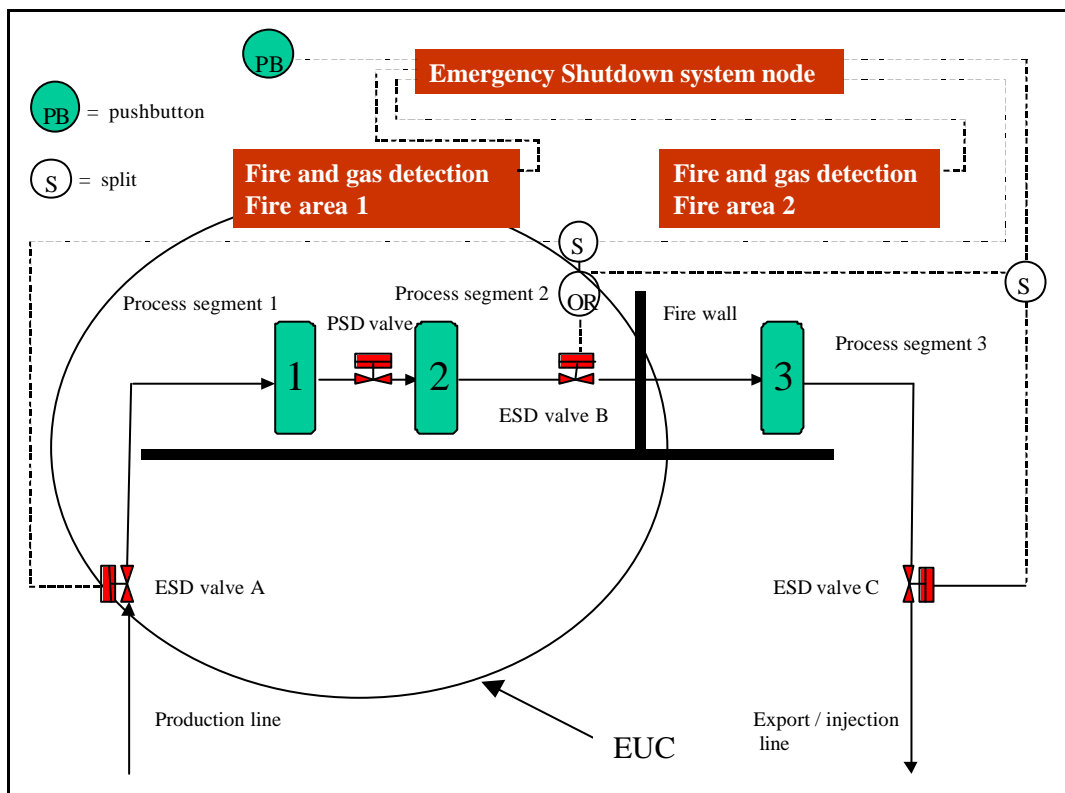


Figure B.2 Example of EUC definition for global safety functions

For this example, the EUC comprises process segments 1 and 2, whereas process segment 3 has been separated from segment 2 by a firewall and is therefore here considered as a separate EUC.

One important motivation for defining the EUC in terms of a fire area, will be the associated possibility of defining an acceptable EUC risk as required by IEC 61508/61511. With respect to acceptance criteria, the operators will have different types, which often will have the format of:

- an overall acceptance criteria for the installation (e.g. given in terms of an acceptable Fatal Accident Rate, FAR) and;
- different criteria related to the main safety functions, such as loss of escape routes, safe haven and evacuation means, as well as criteria related to loss of structural integrity and escalation of the event.

Whereas the overall FAR criterion will normally not be very suitable for defining acceptable EUC risk, the escalation criterion appears to be more applicable. This criterion would e.g. typically be defined in terms of the acceptable annual frequency for escalation of an event to another area. For the above example, the acceptable EUC risk could for example be defined as follows: *For a fire or explosion event originating in process segment 1 or 2, i.e. within the EUC, escalation to another area on the installation shall not occur with an accumulated frequency above $1 \cdot 10^{-4}$ per year.*

It should be noted that when using the minimum SIL table as given in section 7.6 of the guideline, EUC definition and the definition of an acceptable EUC risk will mainly apply to the handling of deviations.

When defining the EUC as indicated above, this may well include several process segments and several blowdown sections connected by process shutdown valves. Furthermore, with respect to electrical isolation, the extent of actual isolation will vary considerably depending on where gas is detected and will also interact closely between the different areas. For the above example (Figure B.2), gas detection in process segment 3 would e.g. typically initiate electrical isolation both in this area and in the EUC under consideration.

If found more suitable, it might be considered to define the EUC in terms of several fire areas, e.g. all the hazardous areas on the installation as one EUC, and another EUC as the non-hazardous areas. As indicated initially in this chapter, the important point will be to define EUC in a manner such that all relevant hazards can be identified.

APPENDIX C Examples on how to handle deviations

This appendix includes a brief description of a recommended methodology for handling a functional deviation from standard API RP 14C design, where insufficient PSV capacity has been compensated by choosing a HIPPS solution.

Furthermore, the appendix includes a simplified example on how Quantitative Risk Analysis (QRA) can be applied in order to verify that the SIL requirement to “isolation of well” is sufficient to fulfil the stated acceptance criterion.

C.1 Example 1 – SIL requirement to HIPPS function

Assume a separator as shown on figure C.1 below, without sufficient PSV capacity to protect against certain process situations. I.e. overpressure is here the defined hazard. Furthermore, a HIPPS solution is being considered in addition to the available PSD function.

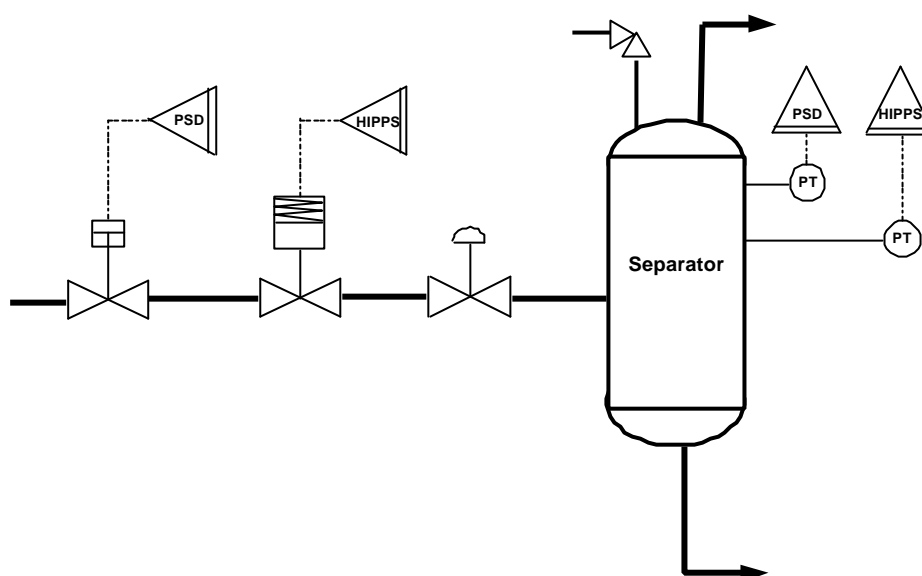


Figure C.1 Overpressure protection of separator

The following quantitative method could be applied for determining required SIL for this HIPPS function:

1. Define the EUC and its control system
2. Define exactly the overpressure scenario(s) to be considered and appropriate acceptance criteria. The latter might be expressed as an acceptable upper frequency for exceeding the test pressure of the separator, e.g. 1×10^{-5} per year
3. Consider which additional safety functions are available to protect the separator against the defined overpressure scenario(s). This could be the PSD function (if confirmed to be sufficiently quick), manually initiated ESD (depending on available operator response time), partial PSV (might provide some protection by reducing speed of pressure build-up), etc.
4. Estimate the frequency from events with a potential to cause a demand on the defined overpressure protection functions. Consider including risk reduction caused by the influence from the EUC control system, keeping in mind that failure of control system may be a potential cause for the demand in the first place (common cause)
5. Roughly estimate the effect of the identified safety functions other than HIPPS, in terms of potential risk reduction
6. Estimate resulting (residual) requirement on HIPPS function in order to achieve stated acceptance criteria.

This method will in addition to providing SIL requirement on the HIPPS function also result in quantitative requirements for the other available safety functions.

C.2 Example 2 – Verification by QRA of a stated Safety Integrity Level

C.2.1 Risk acceptance criteria

Regulatory requirements

Section 9 of “Styringsforskriften” (currently available in draft revision only) stipulates that operators (or parties responsible for operation of an installation) in the petroleum industries shall define acceptance criteria for risk in the petroleum activities. In addition, Section 9 in “Innretningsforskriften” stipulates that accidental (or environmental) loads should not cause impairment of a main safety function with a frequency exceeding $1 \cdot 10^{-4}$ pr. year. Main safety functions are defined in Section 6 of the same regulation to be;

- prevention of escalation of accidental events in order to prevent personnel outside the immediate vicinity of the area affected by the accident from being injured
- maintaining the structural integrity of load bearing construction for the time required to evacuate the installation
- protect rooms of importance for mitigating the accidental events for the time required to evacuate the installation
- keep at least one escape route open from each area in which personnel can be located until evacuation to a safe haven and rescue of personnel have been carried out

Personnel risk

Generally, risk acceptance criteria used by operators on the Norwegian continental shelf define an upper limit on the acceptable risk, using varying measures for risk to personnel, environment and assets. The overall risk acceptance criteria are normally not split pr. accidental event. This allows for some degree of flexibility, i.e. it is possible to tolerate a higher risk from process accidents, as long as this is compensated by reduction in the risk from other accident categories in order to ensure that the total risk level is acceptable. The ALARP principle is widely used, implying that the risk should be reduced to a level “as low as reasonably practicable”. ALARP is normally demonstrated using cost/benefit evaluations with risk reducing measures being implemented when e.g. the cost of averting a fatality are not prohibitively high.

Material damage risk / safety functions

The NORSOK standard Z-013 (currently under revision) specifies that “*a frequency 1×10^{-4} per year for each type of accidental load has been used frequently as the limit of acceptability for the impairment of each main safety function. Sometimes one prefers an overall frequency summing up all accidental load types. For these purposes an overall frequency of 5×10^{-4} per year has been used as the impairment frequency limit*”.

The 1×10^{-4} criteria may be derived from “innretningsforskriften”, and can be used as a basis for SIL determination. It should be noted that several operators on the Norwegian continental shelf have elected to use an overall 5×10^{-4} criteria, not setting a level for the maximum risk contribution from each accidental event. It should also be noted that the interpretation of how the risk acceptance criteria are to be applied may vary between the different operators.

Risk acceptance vs. SIL requirements

SIL requirements can influence both the likelihood (process control/PSD) and consequence (ESD) of an accidental event, and it seems reasonable to expect a certain consistency between the SIL requirements and the overall risk acceptance criteria. Where this guideline specifies SIL requirements for subfunctions, quantitative risk analyses should be applied to ensure that the overall risk is acceptable when compared to the established acceptance criteria. In general, setting “standard” safety integrity levels may be compared to setting a “standard” level of risk acceptance. Such “standard” criteria will not take into consideration elements that may be considered in a QRA, e.g;

- Installation (structural) design and layout
- Process design and layout
- Process plant size / capability
- ESD / PSD philosophy
- Maintenance standards

In order to verify whether or not the standard Safety Integrity Levels will result in an acceptable overall risk level, a more detailed analysis is required. Example calculations are given below.

C.2.2 Isolation of production wells

General – application of acceptance criteria

The guideline specifies that the subsystem “isolation of one well” should meet a minimum safety integrity level of SIL 3. The following high-level example is intended to demonstrate whether or not this is adequate in order to meet an overall risk acceptance criterion. Reference is also made to Annex C of IEC 61511-3 for additional examples.

The acceptance criterion to be applied in the following example is that *any single accidental event should not contribute to the frequency of escalation (breach of firecell integrity) with a frequency exceeding 1×10^{-4} pr. year.*

Assumptions

The installation considered has a process layout as indicated in Figure C.2 below. This includes;

- Five production wells with “standard” wellhead configuration.
- A wellhead area segregated from other areas with a H-120 fire division
- A production manifold located in the wellhead area, separated from the oil and gas separation process by an ESD valve.

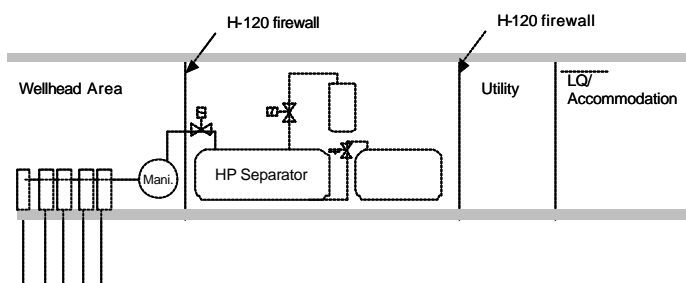


Figure C.2 - Example Wellhead / Process layout

For the purpose of this example it is assumed that any fire originating in the production manifold will have duration less than 120 minutes should isolation be successful. The fire will then not threaten the firewall separating the process and wellhead areas. However, failure to isolate the segment (failure to shut in wells) will result in the fire duration exceeding 120 minutes, with a high likelihood of failure of the firewall.

General

To limit inventory available to feed any leak, all wells must be shut in, and the ESD valve downstream the production manifold must close. Closing in wells can typically be achieved by closing at least one of the following valves;

- DHSV
- Upper master valve
- Production wing valve

Note that the DHSV is the only valve that can prevent flow to surface in the event of damage to the wellheads. A minimum SIL of 3 has been set for isolation of each well, in accordance with specifications given in this guideline. Section A.6 indicates that this is achievable with current day technology. This SIL requirement is used to establish a probability of isolation failure for further use in the risk model.

Simplified event tree analysis

In order to evaluate the annual frequency of failure of the firewall due to fires from the production manifold, an event tree approach is used. For the purpose of this example it is assumed that depressurisation of the HP separator segment is successful, resulting in failure to close the ESDV upstream of the HP separator not being a critical failure with respect to the firewall integrity. The critical aspect will then be whether or not it is possible to shut in the wells. An example event tree is given in Figure C.3.

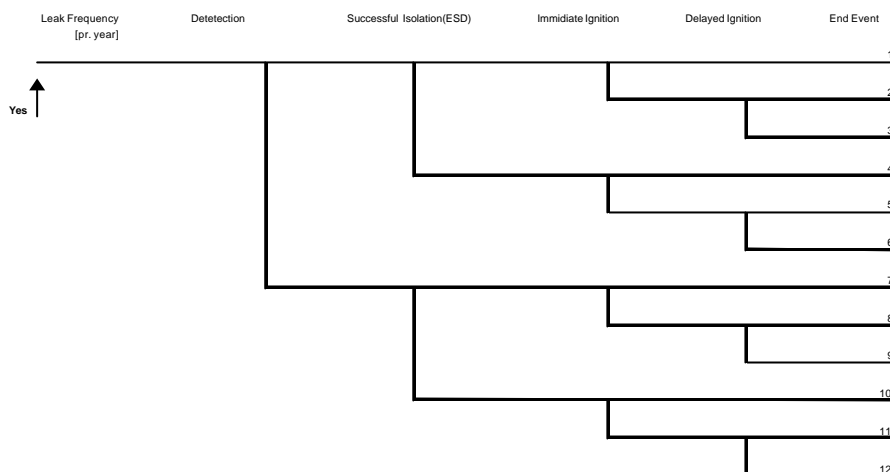


Figure C.3 - Example event tree

The above event tree takes into account the following branch probabilities;

- Detection: Likelihood of successful gas detection
- Successful Isolation (ESD): Likelihood of successful isolation of the fire cell
- Likelihood of ignition: Likelihood of immediate or delayed ignition of the released hydrocarbon inventory

The above event tree is simplified, i.e. it does not take into account all factors normally considered in a full QRA event tree. As an example, the NORSOK Z-013 standard requires event tree analyses to take into account;

- leak cause, source and location
- leak rate, volume and duration
- leak medium (e.g. gas/oil)
- effectiveness of shutdown system on leak volume
- gas spreading/dispersion
- probability of ignition, time of ignition
- probability of explosion in the event of ignition, effect of explosion
- effectiveness of fire-fighting system
- effectiveness of blowdown system
- accident escalation
- escape possibilities and evacuation system
- distribution of personnel

In order to produce a quantitative example using the above event tree, the following input is used:

- A leak in the production manifold (or associated piping) is assumed to occur with a frequency of, say, $5 \cdot 10^{-3}$ pr. year¹.
- The likelihood of immediate ignition of the leak is assumed to be in the order of 10%, with a 2.5% and 5% likelihood of delayed ignition for scenarios with successful and unsuccessful ESD, respectively².
- The manifold area is assumed covered by a sufficient amount of gas detectors
- With “isolation of well” being a SIL 3 function, the probability of failure to isolate one or more well in a wellhead area with five producing wells can be approximated by $(1-0.999) \times 5 = 0.005$.

Using the above data and assumptions in the example event tree, the quantitative example will be as indicated in C.4 below.

¹ This example considers one release scenario only. It should be noted that available data indicate that the majority of leaks will be of a very limited size and can be considered not to have a significant escalation potential (naturally, this will depend on the layout of the installation).

² Here, a detailed QRA would take into account ignition sources in the wellhead area and possibly use a time-dependent ignition model to determine installation-specific ignition probabilities.

Leak Frequency [pr. year]	Detection	Successful Isolation (ESD)	Immediate Ignition	Delayed Ignition	End Event	Frequency [pr. year]	P(Escalation)	F(Escalation) [pr. year]
5.00E-03	0.9	0.995	0.1		1	4.48E-04	0.00	0.00E+00
	4.50E-03	4.48E-03	4.48E-04		2	1.01E-04	0.25	2.52E-05
			4.03E-03	0.025	3	3.93E-03	0.00	0.00E+00
		0.005	0.1	1.01E-04	4	2.25E-06	0.95	2.14E-06
		2.25E-05	2.25E-06	0.975	5	1.22E-06	0.95	1.15E-06
			2.03E-05	3.93E-03	6	1.90E-05	0.00	0.00E+00
	0.1	0	0.1	0.94	7	0.00E+00	0.00	0.00E+00
	5.00E-04	0.00E+00	0.9	1.90E-05	8	0.00E+00	0.25	0.00E+00
			0.00E+00	0.00E+00	9	0.00E+00	0.00	0.00E+00
		1	0.1	0.00E+00	10	5.00E-05	0.95	4.75E-05
		5.00E-04	5.00E-05	0.9	11	2.25E-05	0.95	2.14E-05
			4.50E-04	2.25E-05	12	4.28E-04	0.00	0.00E+00
				4.28E-04				
						5.00E-03		9.74E-05

Figure 1 - Example event tree with assumed figures included³

The above example indicates that the acceptance criterion of $1 \cdot 10^{-4}$ per year with respect to escalation can be met, but with small margins, using a SIL 3 requirement for isolation of well. It should be noted that several other options for risk reduction exist, that could be considered had the above approach indicated that the risk was unacceptable, or if the margin to the acceptance criterion is considered to small, e.g.

- Reduction of number of leak sources in the manifold system (lower leak frequency)
- Reduction or improved maintenance of potential ignition sources (lower ignition probability)
- Improved gas detection
- Improved fire protection on firewall (lower probability of escalation)
- change of layout in wellhead area to reduce explosion overpressure (lower probability of escalation)

³ I should be stressed that all numbers in the event tree (leak frequency and branch probabilities) are *installation specific*, and that the above numbers are to be considered examples only.

APPENDIX D Estimation of probability of failure on demand

D.1 Relation between PFD used in the IEC-standards and CSU used in the PDS-model

First, we give the following definitions, related to *safety unavailability* (SU) as defined in the PDS method (cf. refs. /1/ and /2/):

CSU = Critical Safety Unavailability. The probability that the safety system due to an *unrevealed* fault will fail to automatically carry out a successful safety action on the occurrence of a hazardous/accidental event. Using the notation of IEC this parameter includes contributions both from *random hardware failures* (in particular *undetectable dangerous failures*) and *systematic failures* (cf. TIF).

NCU = Non-Critical Unavailability. The probability that the safety system due to a *revealed* fault or inhibition will fail to automatically carry out a successful safety action on the occurrence of a hazardous/accidental event. In PDS there are two contributions to NCU: ¹⁾ Failures that are detected cause unavailability due to repair, ²⁾ Inhibition due to functional testing being carried out. Thus we may write $NCU = NCU_1 + NCU_2$

TIF = The probability of Test Independent Failures. This is the probability that a component that has just been functionally tested will fail on demand (applies to FTO failures only). Essentially, TIF represents a quantification of what in IEC 61508 is referred to as *systematic failures*.

CSU₁ = Critical safety unavailability due to unrevealed hardware failures. This is the part of CSU which is not related to systematic failures, and so depends on the period of functional testing, τ ; (e.g. for a single system, $CSU_1 = \lambda \cdot \tau / 2$). The notation CSU₁ is introduced here and was not used in PDS.

Thus, in PDS there are three contributors to SU, see Fig. D1. In this method the main measure for SU is $CSU = CSU_1 + TIF$, while NCU is a "secondary" measure. In IEC 61508 the parameter PFD is used as a measure for SU:

PFD = Probability of Failure on Demand. Includes unavailability both to unrevealed failures (cf. CSU) and to revealed failure (cf. NCU). However, there are limitations: PFD does *not* include contributions from systematic failures (cf. TIF) and from inhibition during functional testing (cf. NCU₂).

So PFD is quite different from CSU used in PDS. The PFD will not include contribution from systematic failures (TIF), and we may write:

$$PFD = CSU_1 + NCU_1$$

So CSU₁ is the common part of CSU and PFD. To get a good overview of the safety performance of your system we claim that all above elements of SU should be quantified separately. Now, the following topics should be investigated:

1. How are failures classified in IEC and PDS? What is the difference?
2. How is CSU₁ quantified in PDS and IEC, respectively?
3. How should NCU be quantified?
4. What are the arguments for quantifying the TIF probability, also when IEC 61508 is applied?
5. What is the recommended synthesis of IEC and PDS? That is, what is the recommended approach for SU quantification, adhering to IEC, but at the same time not losing the aspects of the PDS method, that are important for a realistic evaluation of safety systems?

Safety unavailability concepts

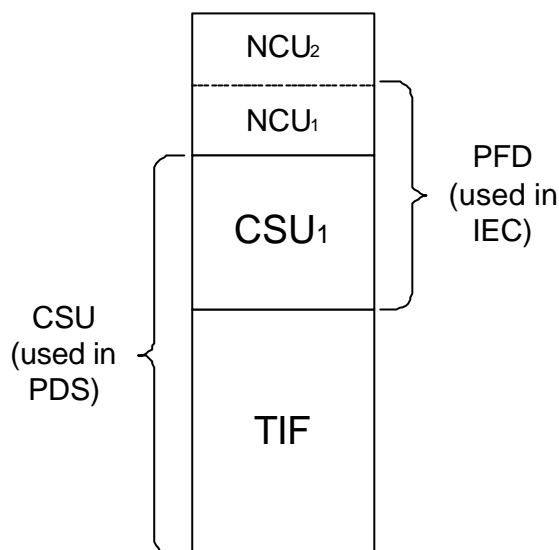


Figure D.1 Relation between CSU (used in PDS) and PFD (used in IEC 61508)

These topics are treated below. It is attempted to adhere to the IEC method and notation. The standard gives rather complex (but approximate) formulas for PFD (without providing proper arguments for these). When the expressions for PFD in IEC are split to give separate expressions for CSU₁ and NCU₁ we do *not* agree on all the formulas obtained. So the expressions for CSU₁ and NCU₁ presented below, will differ somewhat from those that can be derived from the IEC standard.

Further, the presentation below apply β -factors and *not* p-factors (as used in PDS). We restrict so far to treat the voting logics 1oo1, 1oo2, 2oo2 and 2oo3.

The following notation apply:

MTTR: Mean Time To Repair for a component

τ : Time interval between proof tests (denoted T₁ in IEC 61508)

λ : Component failure rate

β : beta-factor for common cause failures (IEC)

The component failure rate is split as follows:

IEC notation	PDS notation	Description
$\lambda_D = \lambda_{DU} + \lambda_{DD}$	I^{FTO}	Rate of dangerous failures (fail-to-operate failures) per hr, $I^{FTO} = I_{un\ det}^{FTO} + I_{det}^{FTO}$
$\lambda_S = \lambda_{SU} + \lambda_{SD}$	I^{SO}	Rate of safe failures (spurious operation failures) per hr, $I^{SO} = I_{un\ det}^{SO} + I_{det}^{SO}$
λ_{DU}	$I_{un\ det}^{FTO}$	Rate of undetected dangerous failures per hr (i.e. rate of failures which lie outside the coverage of the diagnostic tests)
λ_{DD}	I_{det}^{FTO}	Rate of detected dangerous failures per hr (i.e. rate of failures which are detected by the diagnostic tests)
λ_{SU}	$I_{un\ det}^{SO}$	Rate of undetected safe failures per hr (i.e. rate of failures which lie outside the coverage of the diagnostic tests)
λ_{SD}	I_{det}^{SO}	Rate of detected safe failures per hr (i.e. rate of failures which are detected by the diagnostic tests)

Note 1:

The formulas given below will follow (as closely as possible) the "spirit" of the IEC; in particular by applying the β -factor model, and considering both CSU_1 and NCU_1 . However, the formulas provided in Appendix B of IEC 61508-6 are rather complex and are not well documented. Thus in Table D1 below new formulas are provided, for CSU_1 following the PDS handbook /1/, (but replacing p-factors with β -s).

Note 2:

For NCU_1 the handbook /1/ does not provide results. However, the formulas for a kooN-voting given in Table D2 below are rather simple, just expressing the probability of all N "lines" being unavailable due to repair of a dangerous failure. The decision to restrict to dangerous failures again follows the IEC standard. However, it is a question whether also the unavailability due to repair of *safe detected* (SD) should be included. Often, the detection of these failures will prevent a shut-down and the repair also for these are online, and thus contributing to the NCU_1 .

Note 3:

As already stated, the IEC approach does not include unavailability due to functional testing. This seems inconsistent, as the unavailability due to repair *is* included. However, following IEC, we ignore unavailability due to testing in formulas below. This contribution could easily be added to NCU as Δ/τ , where Δ is the inhibition period for functional testing of the system; (this contribution to SU would usually be added to the function not to each element?).

Note 4:

The formulas below assume degraded operation by detection/repair of failures. So for instance when a failure is detected on a duplicated system, this failure is repaired on-line, and the system is degraded to a 1oo1 system. On line repair is carried out also on a single system.

Note 5:

All formulas are actually approximations, valid when τ is not too big. For instance a main term, like $\lambda_{DU} \cdot \tau / 2$ is actually an approximation for $(1 - \exp(-\lambda_{DU} \cdot \tau)) / (\lambda_{DU} \cdot \tau)$.

D.2 Failure classification.

The PDS method gives a well-defined and rather detailed failure classification, see Figure D2 below (from /2/).

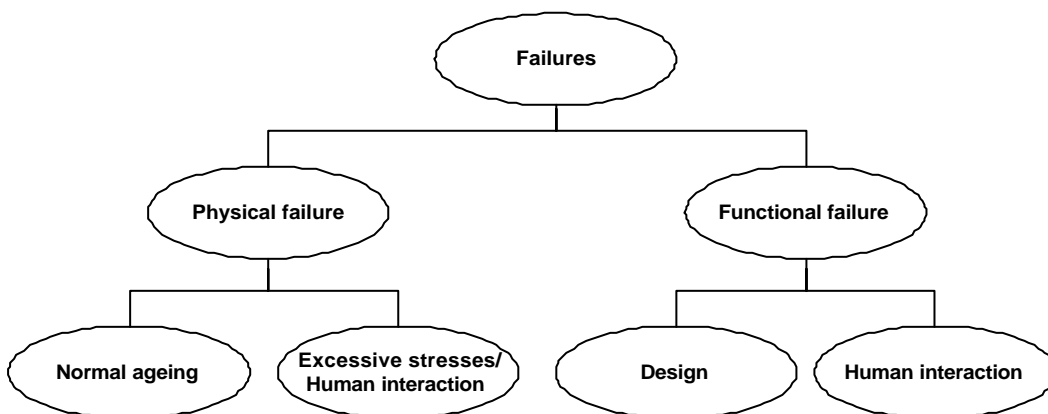


Figure D.2 Failure classification in PDS.

The IEC standard classifies failures into two main categories:

- Random hardware failures
- Systematic failures

The definitions are not so detailed. However, it is the impression that "random hardware failures" is more or less identical to "physical failures", and that "systematic failures" is more or less identical to "functional failures". The SU caused by the first category (Random hardware failures) is quantified in IEC (by PFD), while the SU caused by systematic failures is not quantified here. Thus, the PFD will *not* include unavailability due to e.g.:

- Failure of detector to react due to "wrong" location of detector
- Failure of detector to discriminate between true and false alarm
- Failure due to software error
- Unavailability of system due to erroneous inhibition

To make the definitions of safety unavailability in PDS and IEC respectively compatible, and to avoid too much confusion, we here specify TIF to entirely relate to functional failures (=systematic failures) and CSU₁ entirely to relate to physical failures (=random hardware failures), see Fig. D2 above.

Observe that a category that we could call "Maintenance induced hardware failures" (during periodic testing) falls outside this classification. These are physical failures, but will not be covered by the CSU₁ - formula, as the rate of maintenance induced failures increases with increasing test frequency.

D.3 Calculation of CSU₁

The contribution CSU₁ comes from dangerous undetected (DU) failures that occur with rate λ_{DU} (and are detected in manual tests with interval τ). For redundant systems we also have a contribution to CSU₁ where one unit is unavailable due to a repair. According to the IEC formulas we restrict to Dangerous failures (with rate λ_D). However, we should rather include also some Safe failures as these also may result in an on-line repair(?) The formulas for CSU₁ are given in Table D1.

Table D1 Formulas for CSU₁. The approximate PDS formula corresponds to the term in bold. However, in the PDS method, p-factors are used instead of a b-factor.

Voting	Formula for CSU ₁	Comment
1001	$1_{DU} \times \tau / 2$	Agrees with PDS
1002	$b \times 1_{DU} \times \tau / 2 + [(1-\beta) \cdot \lambda_{DU} \cdot \tau]^2 / 3 + 2 \cdot (1-\beta)^2 \cdot \lambda_{DU} \cdot (\tau/2) \cdot \lambda_D \cdot MTTR$	The approximate PDS formula only applies the first term, caused by common cause DU failures (with p-factors instead of β). The 2 nd term corresponds to two independent DU failures, and the 3 rd term represents that one unit has a D (being repaired), and the other has a DU failure.
2002	$[b + 2 \times (1-b)] \times 1_{DU} \times \tau / 2 + 2 \cdot (1-\beta)^2 \cdot \lambda_{DU} \cdot (\tau/2) \cdot \lambda_D \cdot MTTR$	The approximate PDS formula only applies the first term, caused by DU failures (with p-factors instead of β). The 2 nd term represents that one unit has a D and the other a DU failure.
2003	$b \times 1_{DU} \times \tau / 2 + [(1-\beta) \cdot \lambda_{DU} \cdot \tau]^2 + 6 \cdot (1-\beta)^2 \cdot \lambda_{DU} \cdot (\tau/2) \cdot \lambda_D \cdot MTTR$	The approximate PDS formula only applies the first term, caused by common cause DU failures (with p-factors instead of β). The 2 nd term corresponds to two independent DU failures, and the 3 rd term represents that one unit has a D and another a DU failure.

D.4 Calculation of NCU

When maintenance activity is done while the plant is operating, the safety system is set in the off-line state. The time that the safety system is in off-line state is in IEC included as a part of *total PFD*, and this contribution can become significant if shorter time interval between proof tests is practised.

Table D2 Formulas for NCU₁. Main term in bold

Voting	Formula for NCU ₁ (not identical to formulas in IEC)	Comment
1001	$l_D \times \mathbf{MTTR}$	Component repaired
1002	$b \times l_D \times \mathbf{MTTR} + [(1-\beta) \cdot \lambda_D \cdot \mathbf{MTTR}]^2$	Repair of both components, either due to a common cause failure or both having an independent failure.
2002	$b \times l_D \times \mathbf{MTTR} + [(1-\beta) \cdot l_D \cdot \mathbf{MTTR}]^2$	Repair of both components, due to a common cause failure or both having an independent failure.
2003	$b \times l_D \times \mathbf{MTTR} + [(1-\beta) \cdot l_D \times \mathbf{MTTR}]^3$	Repair of all three components, due to a common cause failure or all three having an independent failure.

Table D2 presents formulas for the unavailability due to repair (NCU₁). As stated above NCU₂ = Δ / τ could be used as a formula for unavailability during testing. Here Δ is the inhibition time during testing.

D.5 Why should we quantify TIF?

In the PDS - projects it was well documented that unavailability of most safety functions are caused by "systematic failures", i.e.

- Failure of detector to react due to "wrong" location of detectors
- Failure of detector to discriminate between true and false alarm
- Insufficient functional test procedure
- Human error during functional test:
 - leave in by-pass
 - wrong calibration
- Failure due to software error

These are the main elements of the TIF-probability. In the PDS it was strongly argued that it is not very sensible to quantify the contribution of hardware failures, leaving out the *major* contributor to the SU. It is true that it may be more difficult to quantify the TIF-probability. However, the PDS project succeeded in providing generic values, and for the TIF of gas detectors an approach for obtaining "plant specific" TIF was also developed, see /3/. It is also possible to establish simpler approaches, e.g. along the lines of obtaining "plant-specific" β's as presented in IEC 61508.

Regarding the quantification of TIF, we observe that

1. the TIF probability is closely linked to the application ("plant"), and
2. objective data for TIF is often lacking, so that quantification to a larger extent must be based on "subjective" data,

Hence, there are strong arguments for quantifying the TIF probability *separately*, and not just give the "total" CSU. It is much more informative to have both CSU₁ and TIF, than just having the sum CSU.

D.6 Recommended approach for quantification of SU when IEC 61508 is used

Four elements of SU were identified in Section D1. Below we give the "short version" of the definitions:

- CSU₁ = Safety unavailability due to *unrevealed* "random hardware failures"
- CSU₂= TIF = Safety unavailability due to (unrevealed) "systematic failures". We actually assume all systematic failures by definition to be unrevealed.

- NCU_1 = Safety unavailability due to *revealed* "random hardware failures", i.e. safety unavailability due to repair (of detected failures)
- NCU_2 = Safety unavailability due to functional testing.

Below, some recommendations regarding the approach for quantification of SU for safety systems are summarised:

1) Dependence on operating philosophy

The operating philosophy (degraded operation, on-line repair, etc) should be explicitly stated. The present formulas are based on the assumption that on-line repair is always carried out; also for a single (1oo1) safety system. Additional formulas should be used when other assumptions apply.

2) Data requirements

The quantifications require data on failure rates (split on dangerous/safe and undetected/detected), coverage, β -factor and test interval τ . As far as possible the data should be "plant specific", cf. the IEC approach for obtaining the β -factor.

3) Dependent failures

Regarding the handling of common cause failure (dependent failures), the use of the β -factor model was rejected in PDS. The reason is that this model is very bad for comparing say 1oo2, 1oo3 and 2oo3 votings. For instance from Table D1 it is seen that the main (bold) term for the 1oo2 and 2oo3 votings are identical! If the comparison between these voting logics shall in any way be meaningful, there should be different β 's for each voting. So either a model with p-factors should be used, *or*, alternatively and approach using β -values that depend on the voting logic! This point is illustrated in Section D.7 below.

As stated above, the IEC approach to find "plant-specific" β -factors is a good principle, and should be adopted in the future. Note that there is no problem in adopting this approach also to p-factors, (cf. theme of PDS-forum 2000, see /4/).

4) Various contributions to SU

As discussed above there are various contributions to SU. Which of these should be quantified?

As a *minimum* CSU_1 should *always* be quantified. However, the importance of systematic failures is well documented (cf. Section D5). The IEC approach of *not* including the quantification of this contribution to SU, will represent a significant step backwards, as compared to the present practise (PDS-method). Just a qualitative evaluation of systematic failures necessarily means that there will be less focus on these essential contributions. However, providing separate values for CSU_1 and $CSU_2 = TIF$, and not only giving the sum CSU (as in PDS), seems a good idea.

So, in conclusion, it is *recommended* that all the four above elements of SU should be calculated as part of an overall evaluation of the safety system. Then also PFD (as defined in IEC today) is directly found by adding two of these contributions. However, it is considered unfortunate that PFD mixes the unavailability due to revealed and unrevealed failures, and in the long run this should be changed.

5) Quantification formulas

The formulas for quantification of PFD given in IEC are very complex. "All" such formulas are actually approximations. However, it is strongly suspected that the IEC formulas are by no means the most sensible approximations. The formulas presented above (Sections D3-D4) are significantly simpler, and are recommended as a sounder basis for the quantifications. Whether only the main term corresponding to dependent failures (as used in PDS) or also the contributions from independent failures should be included, must be decided for each application, based on the data.

In the quantification of unavailability due to repair, not only the rate, λ_D but also (part of) the rate of safe failures, λ_S will often apply. This will require a modification of the formulas given above.

D.7 Example quantification

In this section, some quantifications of k-out-of-N (kooN) votings are carried out, assuming that the β -factor for a kooN-voting is

$$\beta_{kooN} = \beta \cdot C_{kooN}$$

Here β is the β -factor given in Table A.3, and C_{kooN} is a "correction factor" taking into account the applied voting logic, see /4/. Since the β -values in Table A.3 apply for 1oo2, it follows that $C_{1oo2} = 1$. Table D.3 presents the suggested C-factors, which will give results in line with the PDS method (applies for small and moderate β -s, say $\beta \leq 10\%$.)

This approach will for instance give that PFD for a 1oo3 voting is significantly lower than for 1oo2, which again has a PFD significantly lower than for 2oo3. The standard β -factor model, as described in IEC 61508-2, will lack this feature, as the dominant term in all three cases will be $PFD_{kooN} \approx \beta \cdot \lambda_{DU} \cdot \tau / 2$ rather than

$$PFD_{kooN} \approx \beta_{kooN} \cdot \lambda_{DU} \cdot \tau / 2$$

which is used in the present quantification. The N-out-of-N votings are not covered in Table D.3, but for these cases

$$PFD_{NooN} \approx N \cdot \lambda_{DU} \cdot \tau / 2$$

is a suitable approximation.

Table D.3 Modification factor for b, accounting for voting logic.

Voting	1oo2	1oo3	2oo3	1oo4	2oo4	3oo4
C_{kooN}	1.0	0.3	2.4	0.15	0.8	4.0

Table D.4 PFD and TIF for gas detectors, 1ooN voting logics (Data from Table A.3).Component	1oo2		1oo3	
	PFD	TIF	PFD	TIF
Gas detector, catalytic	$1.3 \cdot 10^{-4}$	$1 \cdot 10^{-4}$	$0.4 \cdot 10^{-4}$	$0.3 \cdot 10^{-4}$
IR Gas detector, conventional	$1.5 \cdot 10^{-4}$		$0.5 \cdot 10^{-4}$	
IR Gas detector, line				

Table D.5 PFD and TIF for gas detectors, 2ooN voting logics (Data from Table A.3).

Component	2oo2		2oo3		2oo4	
	PFD	TIF	PFD	TIF	PFD	TIF
Gas detector, catalytic	0.005	$2 \cdot 10^{-4}$	$3.2 \cdot 10^{-4}$	$2.4 \cdot 10^{-4}$	$1.1 \cdot 10^{-4}$	$0.8 \cdot 10^{-4}$
IR Gas detector, convent.	0.006		$3.7 \cdot 10^{-4}$		$1.2 \cdot 10^{-4}$	
IR Gas detector, line						

Tables D.4 and D.5 have been prepared as a basis for evaluation of / choice between the kooN votings for gas detectors. The tables give the PFD and TIF for the detectors only. Data for the F&G logic solver ($PFD = 3.5 \cdot 10^{-3}$) is the dominant term, and has to be added when the function is considered.

D.8 References

/1/ Reliability Prediction Handbook; Computer-Based Process Safety Systems. SINTEF report STF75 A89023.

/2/ Reliability Quantification of Computer-Based Safety Systems. An Introduction to PDS. SINTEF report STF38 A97434.

/3/ Reliability Data for Control and Safety Systems. 1998 edition. SINTEF report STF38 A98445.

/4/ Beta-factor model in IEC61508 and p-factors in PDS. SINTEF report. In preparation.

APPENDIX E Lifecycle phases for a typical offshore project

INVESTMENT STUDIES

The Feasibility Phase

The Feasibility phase is the first phase after the decision is made to establish a field development project.

The Concept Phase

This phase starts when a decision is made to substantiate further field development and ends when a decision is made whether or not to prepare a plan for development and operation (PDO).

The Pre-Execution Phase (PDO-phase)

This phase starts when one field development concept is selected and the decision is made to prepare the PDO. It is completed when the PDO is sent to the authorities, the main contractor is selected.

INVESTMENT PROJECT EXECUTION

Detail Engineering and Construction Phase

This part of Project Execution starts with the final decision to execute the project and by the award of the main contract(s), and ends when the facilities are mechanically complete (pre-commissioning).

The Final Commissioning and Start-up Phase

This part of Project Execution starts when systems or parts of systems are mechanically completed (pre-commissioning), and is concluded when all systems are handed over to Operations and finally accepted by the Customer.

OPERATION AND DE-COMMISSIONING

The Operational Phase

This phase starts when the installation is handed over and accepted by Operations.

The De-commissioning Phase

This phase starts with the decision to shut down the field and remove the installation.

Lifecycle phases as described in IEC 61511 with reference to typical offshore project

Risk Analysis and Protection Layer Design

This activity will start in the concept phase and continue during start of detail engineering. Concludes with a risk analysis report. When major modification, the report to be updated.

A new risk analysis will normally be conducted when the installation have been some years in operation.

Allocation of Safety Functions to Protection Layers

This activity starts in the pre-execution phase and concluded with a report (specification) in the detail engineering phase.

Safety Requirements Specification for the Safety Instrumented System

This activity starts in the pre-execution phase and concluded with a report (specification) in the detail engineering phase.

Design and Engineering of Safety Instrumented System

This activity starts in the pre-execution phase and concludes in the detail engineering phase.

Installation, Commissioning and Validation

This activity starts in the construction phase and concludes with the final commissioning.

Operation and Maintenance

This activity is taking part in the operational phase.

Modification

This activity is taking part in the operational phase.

Decommissioning

This activity is taking part in the decommissioning phase

APPENDIX F Collection and analysis of reliability data

F.1 Introduction

Collection and analysis of reliability data is an important part of the maintenance management loop. For a new installation only generic reliability parameters are available (e.g. from OREDA or PDS data⁴). By proper collection and analysis of the reliability data for a given site, it is possible to establish site specific reliability parameters, and thus establish a maintenance program that is adapted to the actual reliability performance of that site. Further collection and analysis is an important means to ensure reliability growth during the lifecycle of an installation. By proper collection and analysis of failure causes, it is possible to eliminate systematic failures by implementing measures against these failure causes. On the other hand, if this systematic approach fails it is likely that reliability performance is impaired to an unacceptable level.

This appendix gives minimum requirements for collections of reliability data where failure modes and failure causes are important variables to include. Note that information on failure modes and failure causes also will be required in the coming regulations by the Norwegian Petroleum Directorate (see § 17 “Innsamling og tilgjengeliggjøring av data” in “styringsforskriften”). This appendix does not require that pre-defined code-lists etc should be used. It is, however, highly recommended that the oil and gas industry adopts the same taxonomy, code lists etc such that the learning processes within the industry, and the feedback loops to the manufactures can be maximised. Unless there are explicit strong arguments, the structure in ISO 14224 should be followed.

Figure F1 indicates important aspects of a maintenance management loop. The numbers in some of the boxes correspond to the numbers used in the IEC 61508 life cycle.

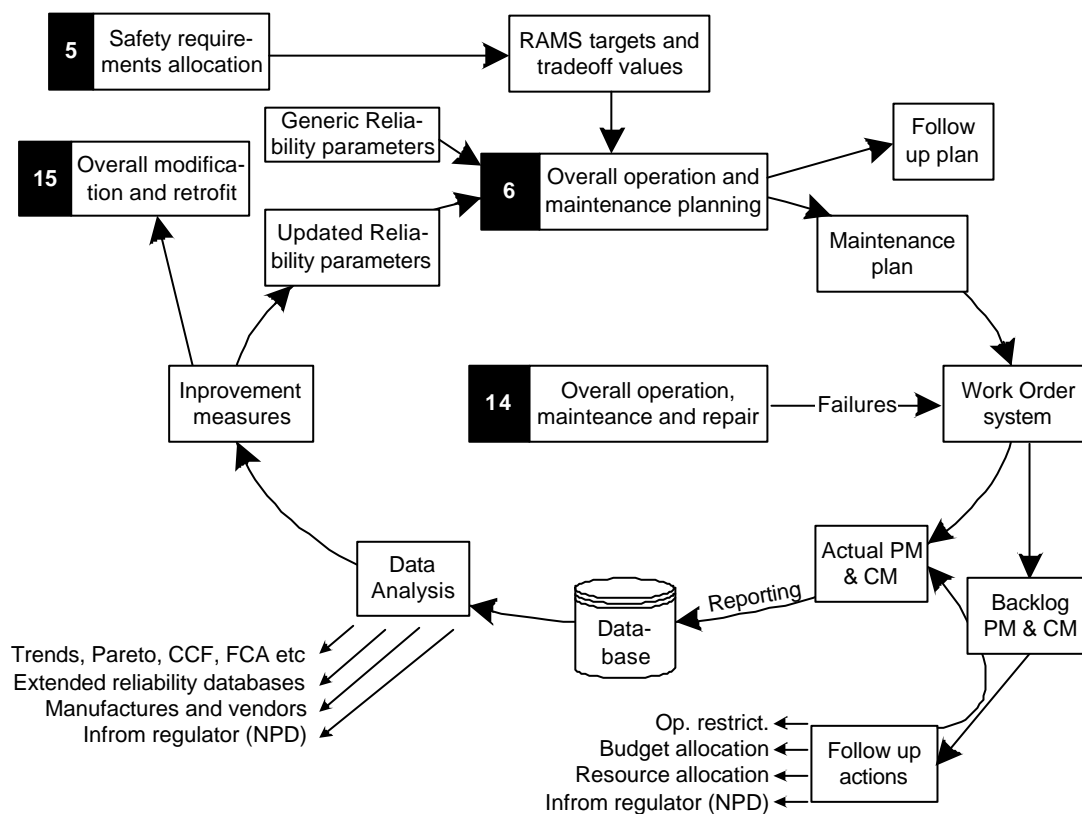


Figure F1 Maintenance management loop

When the initial maintenance program is established, i.e. “6 Overall operation and maintenance planning”, only generic data is available. Section F.4 gives guideline for how generic data could be used when the initial maintenance program is set up. There is large uncertainty whether the generic data will be relevant for the actual installation. Therefore a conservative estimate for the initial failure rate should be used (I_{IMP} in Figure F2). However, if a

⁴ The OREDA Data Handbook is published every 3-4 years. The OREDA[®] Database is available to most operators on the Norwegian Continental Shelf. See Hansen & Vatn 1999 for PDS Reliability data

systematic failure cause analysis is performed it is possible to argue that the new installation will expire a lower failure (I'_{IMP} in Figure F2), and hence maintenance intervals could be increased. The loop in Figure F1 also illustrates that reliability data should be collected and analysed to improve the overall performance. Based on a proper failure cause analysis, it will be possible to implement measures to eliminate some of these failure causes. But a systematic failure cause analysis could also be used to argue improved reliability performance (I_{UP2} in Figure F2) at an earlier stage than what is possible with only “statistical evidence” (I_{UP1} in Figure F2). The exact procedures for estimating these parameters are shown later on, but the principal issues are shown in Figure F2.

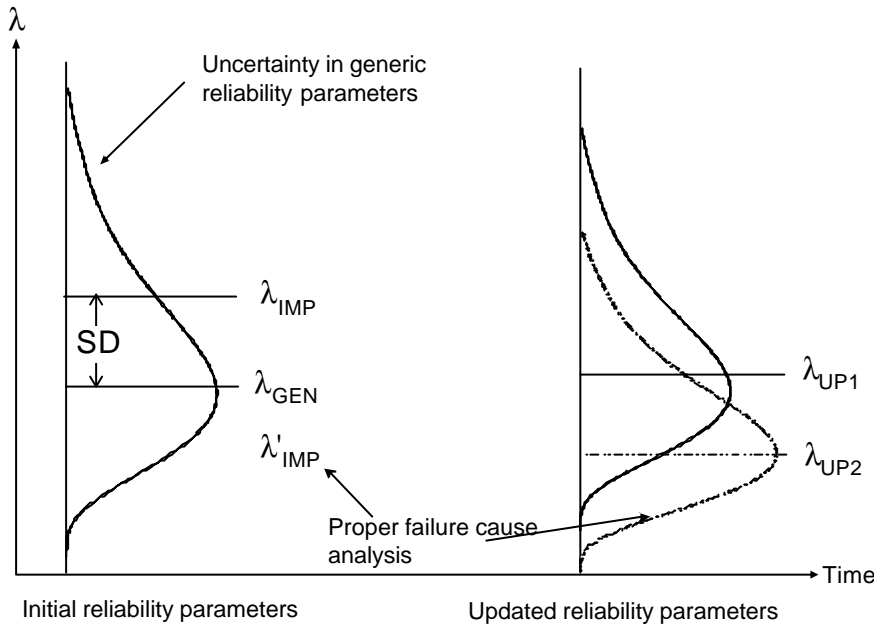


Figure F2 Failure rate estimates in different situations

F.2 **5** Safety requirements allocation

This activity is covered in the main part of this guidelines.

F.3 RAMS targets and trade-off values

Input to this stage is the SIL requirements from “**5** safety requirements allocation”. The SIL requirements are defined at a very generic level, and installation specific conditions are not taken into account. In order to use the SIL requirement for maintenance optimisation it is necessary to introduce a SIL correction factor: CF_{SIL} . The following parameters should at least be considered:

Df: change in demand rate for the safety function

DC: change in consequence of a safety function failure on demand

I_{SIL} : Inappropriate SIL value. When the SIL was selected in the first place, the interval levels of 10 may give unreasonable results

Table F1 shows proposed values for the correction factor in different situations.

Table F1 Correction factors for SIL requirements

CF_{SIL}	Conditions for adjustment
0.2	Two or more factors significant negative
0.4	One factor significant negative
1	No significant factors, or cancelling effects of factors
3	One factor significant positive
5	Two or more factors significant positive

For a given SIL requirement, i.e. SIL N , the PFD value to use in maintenance optimisation is given by

$$PFD^A = CF_{SIL} \times 10^{-N} \tag{F1}$$

F.4 Generic reliability parameters used in the definition of initial maintenance program

Appendix D presents the formulas for calculating the PFD for a given set of reliability parameters. This section gives a procedure for selecting appropriate initial values for the failure rate. The presentation is for a general failure rate, say I , and does not consider specifically the various elements, i.e. I_{DD} , I_{DU} , I_{SD} and I_{SU} .

Since a generic failure rate represents an “average” installation, the actual failure rate is expected to deviate from the generic failure rate. Now introduce:

I_{Gen} = Generic failure rate, i.e. found in OREDA, or PDS data

SD_I = Standard deviation, i.e. the standard deviation in the population from which the generic failure rate is estimated.

I_{IMP} = failure rate to use in establishing the initial maintenance program

Situation 1: No special analysis of the generic failure rate:

In this situation we add the standard deviation to the generic failure rate:

$$I_{IMP} = I_{Gen} + SD_I \tag{F2}$$

Situation 2: Failure causes are taken into account:

Assume that information about the failure causes’ contribution to the generic failure rate is available, i.e. based on the available information we may write:

$$I_{Gen} = I_1 + I_2 + \dots + I_n \tag{F3}$$

where the index $i = 1, 2, \dots, n$ runs through the n different failure causes. Further assume, that we have plant specific information that relates to the failure causes we may expect for the new installation, we may then adjust the generic failure rate according to equation (F4):

$$I'_{Gen} = \gamma_1 I_1 + \gamma_2 I_2 + \dots + \gamma_n I_n \tag{F4}$$

where γ_i , $i = 1, \dots, n$ are correction factors obtained from Table F2.

Table F2 Correction factors, γ based on failure cause analysis

γ	Explanation/situation
0.1	The failure cause is eliminated, or not relevant
0.5	Measures to prevent the failure cause are implemented
1.0	No specific conditions indicate that anything is changed for the failure cause
1.5	Failure cause not considered
2	The situation indicate that the conditions are extra bad for this failure cause
5	The situation is significant worse with respect to this failure cause

The failure rate to use in the initial maintenance program is then:

$$I_{IMP} = I'_{Gen} + I'_{Gen} SD_I / I_{Gen} \tag{F5}$$

F.5 **6** Overall operation and maintenance planning

A maintenance program shall be established, which includes written procedures for maintaining, testing, and repairing the SIS to maintain the required integrity level. This program shall be designed to reveal faults that are not automatically detected by the SIS. Consideration needs to be given to non-availability during routine testing and the effect of mean time to repair on the overall availability of the system. SIS maintenance shall include, but not be limited to, the following:

- Regularly scheduled functional testing of the SIS;
- Regular inspection of field equipment to ensure that there is no observable deterioration, for example: corrosion or mechanical damage, damaged cabling or terminations, ineffective heat tracing, blockage of fire and gas detectors etc.;
- Regularly scheduled preventative maintenance, as required (e.g., replacement of ventilation filters, lubrication, battery replacement, calibration, etc.);
- Repair of detected faults, with appropriate testing after repair.

Several approaches and methods exist for establishing a maintenance program. Among these are RCM, RBI and TPM.

Vendor manuals that describe the SIS maintenance and testing requirements (e.g., battery maintenance, fuse replacement, etc.) may be included in the maintenance procedures.

For the following discussion, it is important to identify the type of preventive maintenance, and frequency of maintenance actions. We will only consider the situation with safety systems activated with a “low” demand rate according to IEC 61508. Further we consider the situation of functional testing with time between tests equal to t , see Appendix D. From Appendix D, we also find the relation between PFD and the parameters I , b and t i.e.

$$PFD = PFD(I, b, t) \quad (F6)$$

To fulfil the acceptance criteria, we therefore must satisfy:

$$PFD^A = PFD(I, b, t) \quad (F7)$$

Solving equation (F7) with respect to t gives the maintenance interval.

Note that maintenance planning usually focuses on establishing type and amount of preventive maintenance. It is, however, strongly recommended that the anticipated corrective maintenance is planned with respect to the need for spare parts, procedures for work permit, required skill of maintenance staff, etc.

F.6 Maintenance plan

The main results of the “6 Overall operation and maintenance planning” activity is a set of proposed maintenance activities, and recommended intervals between these activities. A necessary basis for implementing these results is that the organisational and technical maintenance support functions are available. A major issue is therefore to ensure the availability of the maintenance support functions. The maintenance actions are typically grouped into maintenance packages, each package describing what to do, and when to do it.

Experience has showed that many accidents are related to maintenance work. When implementing a maintenance program it is therefore of vital importance to consider the risk associated with the execution of the maintenance work. Checklists could be used to identify potential risk involved with maintenance work:

- Can maintenance people be injured during the maintenance work?
- Is work permit required for execution of the maintenance work?
- Are means taken to avoid problems related to re-routing, by-passes etc.?
- Can failures be introduced during maintenance work?
- etc.

Task analysis, see e.g. Kirwan & Ainsworth (1992), may be used to reveal the risk involved with each maintenance job. The result of these analyses should be documented as a part of the maintenance plan.

If a SIS function needs to be bypassed while the process is in a hazardous state, administrative controls and written procedures shall be provided to maintain the safety of the process. Particular attention should be put on resetting any inhibits or overrides that may be necessary during testing, inspection and maintenance of the SIS.

Functional testing procedures:

A documented functional test procedure, describing each step to be performed, shall be provided for each SIS.

The functional testing procedures shall include, but not be limited to, verifying the following:

- Operation of all input devices including primary sensors and SIS input modules;
- Logic associated with each input device;
- Logic associated with combined inputs;
- Trip initiating values (set-points) of all inputs;
- Alarm functions;
- Speed of response of the SIS when necessary;
- Operating sequence of the logic program;
- Function of all final control elements and SIS output modules;
- Computational functions performed by the SIS;
- Timing and speed of output devices;
- Function of the manual trip to bring the system to its safe state;
- Function of user diagnostics;
- Complete system functionality;

- The SIS is operational after testing.

F.7 Follow-up plan

The follow-up plan should as a minimum cover the following items:

- Safety aspects of maintenance work;
 - Who is responsible for following up the results from e.g. task analysis
 - Methods for following up, e.g. formal review, arbitrary checks etc
 - Frequency for follow up actions
 - Budget for follow up actions
- Identification of database concept for collecting and analysing reliability data (also includes data about the technical condition of the equipment);
 - Who is responsible for development and maintenance of the database system
 - What system for quality assurance of the reporting is used, and who is responsible
 - Budget for reporting and quality assurance
- System for following up the “backlog”;
 - Who is responsible
 - What should trigger immediate actions (e.g. number of critical PM jobs exceeds a predefined number)
 - The frequency of ordinary investigation into the “backlog”
- Data analysis;
 - Who is responsible for the analysis
 - What type of analyses
 - Frequency of analysis
 - Budget for analysis
- Continuous improvement;
 - Who is responsible for systematic improvement work
 - Who is responsible for treating ad-hoc suggestions, and event-based need for improvement measures
 - Budget for evaluating proposed measures
 - Responsible for resource allocation when measures are to be implemented
- Updating maintenance plan;
 - Who is responsible updating the maintenance plan (intervals, etc)
 - Frequency of updating the plan

F.8 Work Order system

The work order system is the mean for making the maintenance plan operational. In addition to implementing the maintenance plan, the Work Order system should also handle corrective maintenance.

F.9 Actual PM & CM

In principle, the work order system defines the maintenance to be exceeded, and when to do it. The actual maintenance being carried out is, however, another story.

F.10 Backlog PM & CM

In this context we will use the term ‘backlog’ for all scheduled preventive and corrective maintenance that is not performed at due date. It does not exist a unique expression for measuring the backlog. In *Figure F1* the “backlog” box is a “virtual” entity, and the measurable backlog is defined within the “work order system”.

F.11 Follow-up actions (backlog)

It is of outmost importance to define the responsible persons or organisation units for the backlog follow-up. There are two main sources for action:

- Automatic triggering from the “backlog system”, e.g. number of critical PM jobs exceeds a predefined number
- Systematic analysis of the backlog at predefined intervals

Independent of the source, the following items should be considered:

- Any operational restrictions, e.g. shut down of part of operation, restrictions on “hot work”, etc.;
- Whether the regulator should be informed;

- What are the causes for the large backlog, e.g. lack of money, lack of adequate personnel, pressure from production unit to postpone maintenance work, organisational problems etc.;
- What could be done to overcome these problems;
- A plan, responsible persons, and due dates for bringing the backlog under control.

F.12 Reporting

All maintenance work (functional testing, preventive maintenance, and corrective maintenance) shall be reported into an electronic maintenance database. The information to report depends on the type of maintenance work, i.e.

Verification report for functional testing shall include

- Date of inspection;
- Name of the person who performed the test or inspection;
- Serial number or other unique identifier of equipment (loop number, tag number, equipment number, user approved number, etc.);
- Results of inspection/test (“as-found” and “as-left” condition);
- Details of any faults found and a link to the corresponding corrective maintenance report;
- Any identification of erroneous test procedures, increased risk during inspection etc, should be reported.

Preventive maintenance report (PM) shall include

- Date of PM;
- Name of the person(s) who performed the PM work;
- Serial number or other unique identifier of equipment (loop number, tag number, equipment number, user approved number, etc.);
- Maintenance activity;
- Any need for corrective maintenance work.

Corrective maintenance report (CM) shall include

- Date of failure detection;
- Date of CM;
- Name of the person(s) who performed the CM work;
- Serial number or other unique identifier of equipment (loop number, tag number, equipment number, user approved number, etc.);
- Failure mode, i.e. Safe detected (SD), Safe undetected (SU), Dangerous detected (DD) and Dangerous undetected (DU);
- Failed part;
- Failure cause;
- Method of detection, e.g. PM, functional testing, inspection, self test etc.;
- Corrective action;
- Recommended action to eliminate the failure cause.

F.13 Database

The database used in Figure F1 is a conceptual term. A reliability database may be realised as a part of the work order system. It is essential that the database system allows for storing the information as required in this appendix.

F.14 Data Analysis

It is essential that the scope of the data analysis is agreed upon. As a minimum the analysis should include:

- A proper failure cause analysis (FCA);
- Investigation into the failure reports to identify common cause problems (CCF);
- Updated reliability data, see Appendix F.18 below. If assumption about reliability performance (e.g. SIL requirements) are not met, this shall be formally treated.

The analysis group should also identify the need and relevance of:

- Reporting to the regulator;
- Feedback to the manufactures and vendors;
- Reporting to generic databases, e.g. company specific, or OREDA.

F.15 Improvement measures

Based on the systematic failure cause analysis, improvement measures should be identified. Improvement measures should be evaluated in a cost-benefit setting as long as the SIL requirements could be met. If the actual reliability performance threatens the SIL requirements, implementation of improvement measures are mandatory. Each

improvement measure should be evaluated wrt whether it should be treated as a “modification or retrofit” according to the IEC 61508 lifecycle or not.

F.16 **15 Overall modification and retrofit**

If an improvement measure is classified as a “modification” or “retrofit”, the IEC 61508 life cycle process should be followed.

F.17 Updated reliability parameters

This section present methods for updating reliability data in the lifecycle of a product. The principal situation is as follows:

- Only the failure rate, I , is considered in this presentation. Similar approaches could be developed for e.g. the b factor;
- From the generic data, or previous updates of the failure rate, we have an uncertainty distribution for the failure rate. This distribution is either expressed by a mean and a standard deviation, or by the two parameters a and x in the Gamma distribution (se below);
- Since the last update of the failure rate we have observed one or several components over a period of time equal to t . In this period we have observed totally X failures (with the failure mode of interest). In some situations we have also implemented measures to eliminate one or more failure causes.

Expressing the uncertainty distribution of the failure rate

At any point of time in the life cycle of a product it will be uncertainty about what the “actual” value of the failure rate is. We want to quantify this uncertainty. There are three situations.

1. The uncertainty is given by the parameters a and x in the Gamma distribution. In this situation we observe that the expected value of the failure rate is $E = a/x$ and the standard deviation is given by $SD = a^{1/2}/x$.
2. The uncertainty is given by the mean value E , and the standard deviation SD . In this situation we may obtain “corresponding” a and x by letting $x = E/SD^2$, and $a = x \cdot E$.
3. We have estimates for the mean, E , and “upper” and “lower” bounds, i.e. I_U , and I_L . In this situation we calculate $\text{Log}_{10}(I_U/I_L)$, and obtain a from Table F33, and $x = \alpha/E$.

Table F3 Estimates for a in the uncertainty distribution

$\text{Log}_{10}(I_U/I_L)$	0.4	0.5	0.6	0.8	1	1.5	2	2.5	3	3.5	4
a	10	8.5	6	3.7	2.4	1.25	0.85	0.7	0.5	0.45	0.4

Thus, we are able to express the uncertainty distribution of the failure rate by the parameters α and x in all situations above.

Updating the failure rate when failure causes are not available

If information about failure causes are not available, the failure rate is updated using a simple method, e.g.

$$\hat{I} = \frac{a + X}{x + t} \tag{F8}$$

where α and x are the parameters in the uncertainty distribution, X the number of failures in the observation period, and t is the exposure time. The uncertainty parameters could also be updated by

$$\begin{aligned} a &= a + X \\ x &= x + t \end{aligned} \tag{F9}$$

and the new parameters α and x could be used for the next update of the failure rate.

Updating the failure rate when failure causes are analysed, and compensating measures against the failure causes are implemented

In situations where failure cases are analysed, and appropriate measures are implemented we could take credit of this as indicated below.

Now, assume that the failures are classified according to the failure cause, and assume that we could group in $i = 1, \dots, n$ different failure causes. Prior to any measures we then have:

$$X = X_1 + X_2 + \dots + X_n \quad (F10)$$

If compensating measures are implemented we could estimate a future “equivalent” to this number by:

$$X' = g_1 X_1 + g_2 X_2 + \dots + g_n X_n \quad (F11)$$

Where $\gamma_i, i = 1, \dots, n$ are correction factors due to the anticipated effect of implemented measure.

The values of the parameters γ_i could be obtained from Table F4.

Table F4 Adjusting the number of future failures when means are implemented

γ	Explanation/situation
0.75	The measure is expected to have a certain effect on the given failure cause
0.5	The measure is expected to have a significant effect on the given failure cause
0.25	The measure is expected to have a significant effect on the given failure cause, and we are able to explicit describe the content of the measure, and the anticipated effect
0.1	The measure is expected to eliminate the failure cause. For such a judgement the measure should be documented complete, and it should be explained how the measure will eliminate the actual failure cause

When the different measures are implemented, a best estimate for the future failure rate is given by equation (F12):

$$\hat{I} = \frac{a + X'}{x + t} \quad (F12)$$

Note that equation (F12) will give a lower failure rate estimate than equation (F8). However, in order to use equation (F12) it is required an explicit judgement of the failure causes, and how implemented measures could eliminate or reduce the failure cause. This will also require a certain quality level of the collection and analysis of reliability data. The uncertainty parameters could also be updated by equation (13):

$$\begin{aligned} a &= a + X' \\ x &= x + t \end{aligned} \quad (F13)$$

and the new parameters α and x could be used for the next update of the failure rate.

Note that in this section we recommend to use the “best estimate” for the failure rate as input to the maintenance optimisation, where as in the initial phase we “added” one standard deviation to the failure rate.

F.18 References

- G. K. Hansen and J. Vatn. Reliability Data for Control and Safety Systems. 1998 Edition. Technical Report STF38 A98445, SINTEF Industrial Management, N-7465 Trondheim, Norway, 1998.
- ISO 14224. *Petroleum and natural gas industries - Collection and exchange of reliability and maintenance data for equipment*. International Standards Organisation, 1999.
- B. Kirwan and L. K. Ainsworth. *A Guide to Task Analysis*. Taylor & Francis, London, 1992.
- OREDA-97. *Offshore Reliability Data*. Distributed by Det Norske Veritas, P.O.Box 300, N-1322 Høvik, Norway, 3 edition, 1997. Prepared by SINTEF Industrial Management. N-7465 Trondheim, Norway