BORA

Barriere- &

operasjonell risikoanalyse

Operational Risk Analysis – Total Analysis of Physical and Non-physical Barriers

H3.1 Generalisation Report
Rev 01

29 January 2007

Report No:
200254-07

Classification:
Open

BORA
Barriere- &
operasjonell risikoanalyse

P O Box 519, N-4341 Bryne, Norway
Tel: +47 5148 7880, Fax: +47 5148 7881
E-mail: post@preventor.no
Web: http://www.preventor.no

Title of report: Operational risk analysis Total analysis of physical and non-physical barriers H3.1 Generalisation Report Rev 1	Date: 31.01.2007 Number of pages/appendices:
Author(s): Stein Haugen, Safetec; Jorunn Seljelid, Safetec; Snorre Sklet, Sintef; Jan Erik Vinnem, Preventor/UiS; Terje Aven, UiS	Signature:

Client(s)/Sponsor(s): NFR/HSE/OLF	Clients ref: T-P Johnsen/R Miles/K Sandve

The objective of this report is to present a generic model for quantitative (or qualitative) analysis of the causes of process leaks. In particular the model has been developed to include not only technical causes but also provides comprehensive modeling of human and organisational causes of leaks. Initiating events that may lead to leaks have been identified from leak statistics. Barrier systems, including technical, human and organisational factors, in place to prevent these from developing into a leak have been identified and illustrated with Barrier Block Diagrams. Risk Influencing Factors (RIFs) are identified and included in the model, in order to reflect better the specific conditions on the installation. The RIFs are characterized by a weight (how important they are) and a score (what is the state of the RIF on the specific installation being considered). Through the RIFs, specific risk estimates can be established for an installation which takes into account the local conditions in a much better way than traditional QRA methodologies do.

In total, it is considered that the proposed methodology shows great promise with regard to improving the modeling of process leaks on offshore installations. This also includes possibilities for evaluating human and organisational measures to reduce risk.

Index terms, English:	Norsk:
Operational risk analysis	Operasjonell risikoanalyse
Organisational factors	Organisatoriske forhold
Human factors	Menneskelige faktorer
Leak frequency	Lekkasjefrekvens

(blank page)

Preface

The approach presented in the report results from developments, discussions and evaluations that have been developed in the period 2004-2006, within the BORA project group, and in contact with members of the BORA Steering Committee, user representatives as well as international experts. Two case studies have been conducted in 2004 and 2005. We wish to thank those from ConocoPhillips Norge and Statoil who have contributed to the case studies. The work has been completed at the end of 2006, but the updating of the final report extended into January, 2007. The authors wish to thank all those that have contributed with comments and suggestions to the preliminary drafts and reports.

(blank page)

BORA project
Operational risk analysis – Total analysis of physical and non-physical barriers
Generalisation Report – Rev. 1

Table of contents

Overview of tables

Overview of figures

0. Summary

The BORA project is a research project initiated in 2003 where the purpose of the main project was to carry out a demonstration project with a complete modeling and analysis of barriers on offshore production installations, including physical and non-physical barrier elements. The overall objective has been somewhat modified as the work progressed. The present report completes the main efforts in the project. The objective of the report is to present a generic model for quantitative (or qualitative) analysis of the causes of process leaks. In particular the model has been developed to include not only technical causes but also provides comprehensive modeling of human and organisational causes of leaks. This is an area where the risk modeling traditionally is weak in existing QRAs.

Causes of leaks have been identified from investigation reports from actual leaks that have occurred on offshore installations on the Norwegian Continental Shelf in the period 2001-2005. The causes of leaks have been classified into 6 main types of causes:

A. Technical degradation of system
B. Human intervention introducing latent error
C. Human intervention causing immediate release
D. Process disturbance
E. Inherent design errors
F. External impact

These are further broken down into more specific causes and a percentage distribution of leaks is established. For each of these causes, or Initiating Events, the barrier systems in place to prevent these from developing into a leak have been identified. Barrier Block Diagrams have been developed to illustrate and model how these barrier systems may prevent leaks from occurring. The barrier systems that have been modeled include technical, human and organisational systems.

Failure of the barrier systems has further been modeled using Fault Tree Analysis. The fault trees include technical, human and organisational factors. In order to support the quantification of leak frequencies, the report also contains generic failure data for the basic events in the fault trees.

Risk Influencing Factors (RIFs) are identified for the Initiating Events and the basic events in the fault trees, in order to reflect better the specific conditions on the installation. The RIFs are characterized by a weight (how important they are) and a score (what is the state of the RIF on the specific installation being considered). By determining the weight and score of all identified RIFs, specific risk estimates can be established for an installation which takes into account the local conditions in a much better way than traditional QRA methodologies do.

In total, it is considered that the proposed methodology shows great promise with regard to improving the modeling of process leaks on offshore installations. Testing through two cases studies have shown that this is a feasible approach and that it is particularly well suited for evaluating risk reducing measures and their potential for actually reducing risk. This also includes possibilities for evaluating human and organisational measures to reduce risk. It is also considered that the resource usage required to perform a study using this methodology represents a relatively limited increase compared to existing methods.

1. Background

1.1 The BORA project

The BORA project is a research project initiated in 2003 where the purpose of the main project is to carry out a demonstration project with a complete modeling and analysis of barriers on offshore production installations, including physical and non-physical barrier elements. Barriers both before and after unplanned events are to be included, i.e. barriers to prevent events from occurring and barriers intended to eliminate/contain the consequences of an unplanned event. The analysis takes quantitative form as far as possible, with the limitations imposed by available models and data. The analysis is performed in such a way that it will enable the identification of failures and failure combinations which entail risk. In turn, this can be used to identify the necessary measures for controlling risk and to observe the effect of modifications and configurative changes, as well as to reveal the effect on barriers during the performance of special operational activities. The analysis will contribute to giving the petroleum industry the overview and understanding of barriers which the Management Regulations require it to have.

This report presents some results from the work carried out as part of the BORA project.

1.2 Objectives of the report

The objective of the report is to present a generic risk model with leak distribution, Barrier Block diagrams, Fault Trees, Risk Influencing Factors (RIFs) and weights and how to score the RIFs. In more detail, the work can be outlined as follows, based on the scope of work that was prepared at the start of the work:

- Establish distribution of leaks on scenarios. Based on accident investigation reports, the types of work operations taking place when the release occurred and the type of initiating event that caused the release has been determined. This has been used to establish leak distributions.
- Update Barrier Block Diagrams and Fault Trees for the containment barrier function. Each release scenario has been described by a barrier block diagram (i.e. event tree) in terms of the initiating event and the barrier functions that can prevent release. This includes both technical and operational barrier functions.
- Establish RIFs and weights for all basic events. A limited set of work meetings has been possible to arrange, thus weights are presented from the case studies and the work conducted in relation to the generalization. Due to the limitations in number of work meetings, it has not been possible to cover all initiating events. However, the main focus has been on those initiating events which contribute most to total leak frequencies.
- Define what information is suited for scoring of RIFs for a specific installation. Sources of information for scoring of the RIFs have been identified and the merits of each source have been described.

1.3 Terminology

The following are the main terms being used (Ref. 1):

Barrier function:	Function in order to prevent the realization of a threat, or to reduce damage potential.
Barrier system:	Set of MTO related actions that will provide the planned barrier function.
Barrier element:	Part of a barrier system

Performance influencing factor:	Factor which may influence the performance of a barrier function or barrier system.

1.4 Structure of report

Section 2 presents an overview of the BORA methodology.

Typical work operations and equipment units are presented in Section 3

Section 4 presents the development of a basic risk model. In this section the hydrocarbon release scenarios with corresponding safety barriers are defined and described, followed by the modelling of the performance of the safety barriers in Section 5.

Frequency and probability data are presented in Section 6, including analysis of hydrocarbon leaks reported to PSA in the period 2002-2005, and human reliability data.

Case studies have been a major part of the BORA project in order to test the proposed methodology on specific problems and for different organizations. One part of the case studies has been to obtain weights of the RIFs for the individual Basic Events. The results from this work are presented in Section 7.

The adjustment of industry average probabilities/frequencies used in the quantitative analysis is presented in Section 8, and in Section 9 data sources for scoring of RIFs are presented.

Section 10 summarise the limitations, advantages and challenges in using this methodology.

1.5 Abbreviations

BBD	Barrier Block Diagram
BOPD	Barrels of Oil Per Day
BORA	Barrier and Operational Risk Analysis
CCR	Central Control Room
ESD	Emergency Shutdown
ESDV	Emergency Shutdown Valve
F&G	Fire & Gas
HEP	Human Error Probability
HOF	Human and Organisational Factors
HP	High Pressure
HRA	Human Reliability Assessment
HSE	Health, Safety and Environment
HTA	Hierarchical Task Analysis
LEL	Lower Explosion Limit
LP	Low Pressure
MTO	Man, Technology and Organisation
NCS	Norwegian Continental Shelf
P&ID	Piping and Instrument Diagram
PM	Preventive Maintenance
PPE	Personal Protection Equipment
PPL	Pipeline
PR	Performance Requirement
PS	Performance Standard
PSD	Process Shutdown
PSF	Performance Shaping Factor

QRA	Quantitative Risk Analysis
RIF	Risk Influencing Factor
RNNS	Risk Level on the Norwegian Continental Shelf, project with annual updating, see http://www.ptil.no/English/Helse+miljo+og+sikkerhet/Risikonivaa+paa+sokkelen/
SAP	Information system
SIL	Safety Integrity Level
SJA	Safe Job Analysis
SLR	Sleipner R
SPA	Safety Petroleum Authority [Norway]
TBO	Tjeldbergodden
TLP	Tension Leg Platform
TTS (TST)	Technical Safety Condition
WP	Work Permit

2. Overview of methodology

2.1 Main steps in the method

The overall methodology that has been developed is based on the work undertaken in the BORA project. The main basis can be summarized as follows:

- A literature review was undertaken to identify potential approaches and ideas for use in the development of a methodology for this project.
- A proposed methodology was developed.
- The proposed methodology was tested in several case studies.

From this, a theoretical basis has been established and experience from use has been gained, and a methodology for establishing general models for describing the risk in operations has been developed.

The overall elements of a generic risk model are illustrated in the figure below.

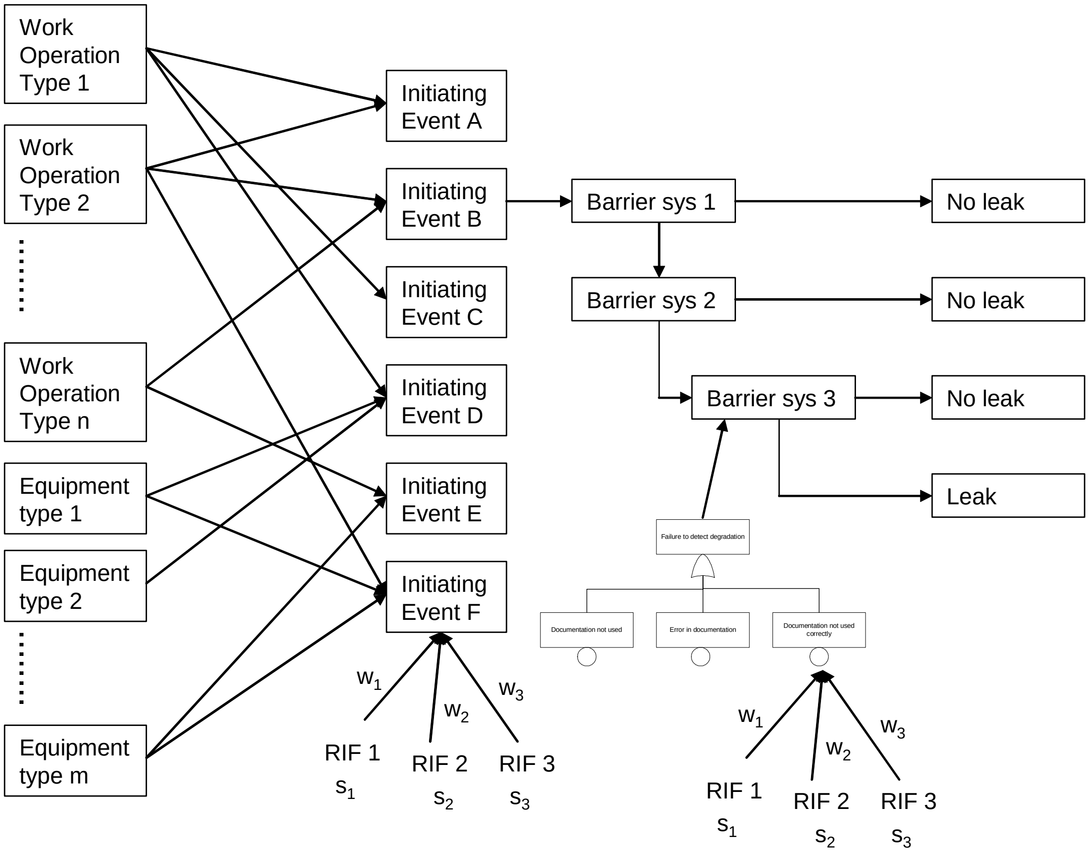


Figure 1 Illustration of a generic risk model

The elements in this can briefly be described as follows:

- The starting point for the model is a set of work operations and equipment types in hydrocarbon systems. Current QRAs will in most cases model the quantity of equipment in detail, but will not take into account platform specific characteristics of the equipment. Work operations are further taken into account to a very limited degree. An example of a work operation is “work on depressurized hydrocarbon containing equipment”.

- Various types of errors or failures during the work operations may lead to a leak. These are termed “Initiating Events”. One example is replacement of a flange gasket where the gasket may be inserted wrongly or bolts are not tightened correctly. Likewise, the equipment itself may fail due to technical causes, such as corrosion, fatigue, erosion or other degradation mechanisms.
- For each work operation, there is a certain probability that different types of Initiating Events will occur. The probability of this happening will be influenced by a set of “Risk Influencing Factors” (RIF). As an example, the probability of making an error when replacing a flange gasket may be dependent on the competence of the mechanic doing the work and the time pressure when the work is being performed. If the competence is high, the probability will be low while if the work situation is stressful the probability may increase. The importance of the RIF (how strongly the RIF influences the probability) is described by a weight (w). Further, the condition of the RIF for the specific installation being considered is described by a score (s).
- In most cases, there will be one or more barriers implemented to prevent an Initiating Event from causing a leak. These barriers are modeled using Barrier Block Diagrams (BBD). The probability of a barrier failing is usually modeled using Fault Tree Analysis (FTA). For each of the basic events in the fault tree, RIFs are also identified.

In the following, the individual steps in the model are described in some more detail. This is followed by detailed description of results and data for each step in the methodology in individual sections in the report.

2.2 Discussion of individual steps

2.2.1 Work operations and equipment units (system characteristics important for risk)

The first step in the development of the model has been to define work operations and equipment units that may cause a leak. In order to have a manageable risk model, a limited number of generic work operations are defined, covering operations which may directly cause a leak or introduce errors/weaknesses/failures in the system which may cause a leak at a later point in time. The work operations are defined in such a way that they will have as many common characteristics as possible such that the RIFs influencing the probability of making errors will be the same or very similar for all specific operations grouped together.

Further, generic equipment units or equipment packages are also defined. This could be e.g. “compressor package”. For each of these generic equipment packages, the number of flanges, valves, instrument connections etc is specified.

Based on this, an “average” platform with average leak frequencies can be established. As will be seen later in the report, a simplified approach is also proposed, using generic leak frequency data and adjusting these to take into account variations in number of work operations for a specific installation.

2.2.2 Initiating Events and BBDs

The errors or failures that may develop into a leak are termed Initiating Events (IE). The IEs are based on review of investigation reports from actual leaks that have occurred on the Norwegian Continental Shelf. The causes of the leaks have been identified and structured. Further, the IEs have been grouped according to how they are mitigated against, i.e. what barriers are in place to prevent an IE from developing into a leak. Six groups of IEs have been defined:

G. Technical degradation of system
H. Human intervention introducing latent error
I. Human intervention causing immediate release

J. Process disturbance
K. Inherent design errors
L. External impact

The event sequence following on from the initiating event is visualized in a *barrier block diagram* as illustrated in Figure 1. A barrier block diagram consists of an initiating event, arrows that show the event sequence, barrier functions realized by barrier systems, and possible outcomes. An arrow straight on indicates that a barrier system functions (i.e., fulfill its function), whereas an arrow downwards indicates failure to fulfill the barrier function. In our case, the undesirable event is release of hydrocarbons (loss of containment).

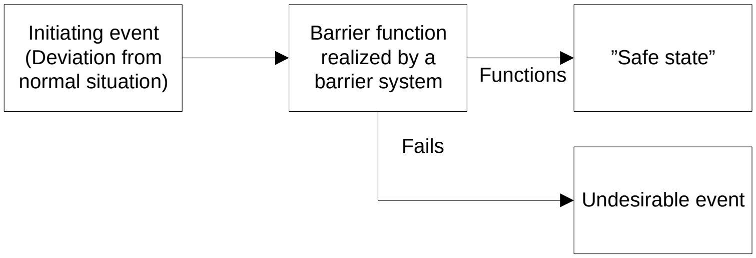


Figure 2 Illustration of a barrier block diagram.

One main purpose of a barrier block diagram is to illustrate available barrier functions intended to prevent a deviation (i.e. an initiating event) from escalating into a release, and how these functions are realized by barrier systems.

2.2.3 Modeling the performance of barrier systems

The performance of barrier systems is modeled using fault trees. In order to generalize the fault trees, the following main structure is applied where possible.

The top events in the fault trees are generally expressed as “Failure or degradation of barrier system”. More specifically, this can be related to failure to detect degradation of a system, failure to detect an error introduced in the system etc.

The causes of the top events are generally grouped into three groups of events (conceptually illustrated in the figure below):

- Inadequate or insufficient “functionality” of the barrier system. This could be simply that the barrier system is not specified or not used, that the specification of the system is not adequate (e.g. too few inspection points) or that the system is not fully functional (e.g. will inspection methods not detect all potentially critical cracks).
- Technical failures of the system – This is relevant only for technical barrier systems and will basically cover the technical “unreliability” of the system.
- Human errors – This covers human errors related to preparation for and performance of the work, e.g. errors in documentation used as basis for performing the work, failure to perform the work according to a described procedure etc.

The fault trees defined for the individual barrier systems largely follow this overall structure.

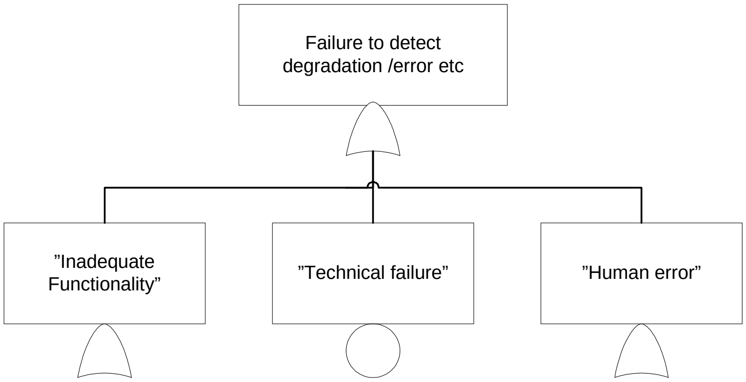


Figure 3 **Generic fault tree for modeling failure of barrier systems**

2.2.4 Assignment of industry average frequencies and probabilities

There are two sets of industry average data that go into the risk modeling:

- Initiating event frequencies
- Basic event probabilities for fault trees

The main basis for the initiating event frequencies is actual leaks that have been reported to PSA for the period 2002 to 2005. The investigation reports have been reviewed and the causes of the leaks identified. This is used to establish a breakdown of the total leak frequency on causal factors.

Technical failures can be directly linked to equipment counts, followed by adjustments based on RIF scoring for the specific installation. For operational failures, the calculation can in principle be performed as follows:

$$F_{IE} = N_{WO} \cdot P(IE|WO)$$

where F_{IE} is the frequency of the Initiating Event, N_{WO} is the number of Work operations per year and P(IE|WO) is the probability of the Initiating Event occurring when performing the Work operation. In practice, we have however also arrived at a possible simplified approach that can be used to link the number of work operations to the equipment count. This is done to enable use of the methodology even with limited availability of data on the number of operations.

The basic events in the fault trees are of a varying nature and the probabilities will therefore also have to be determined from a variety of sources. Data on technical failures will be based on platform specific information, from reliability studies of the technical systems or from other sources (in the same way as in QRAs today). Human error probabilities have however been gathered as part of this project and proposed data are presented.

2.2.5 Development of risk influence diagrams

The purpose of the risk influence diagrams is to identify and illustrate the RIFs influencing the probabilities or frequencies of the occurrences of the basic events in the fault trees. The risk influence diagrams in Appendix A were developed by members from the project team and verified in discussions with personnel from oil companies. The basis for identification of RIFs was the generic framework shown in Figure 4. A short description of each RIF is presented in Table 1.

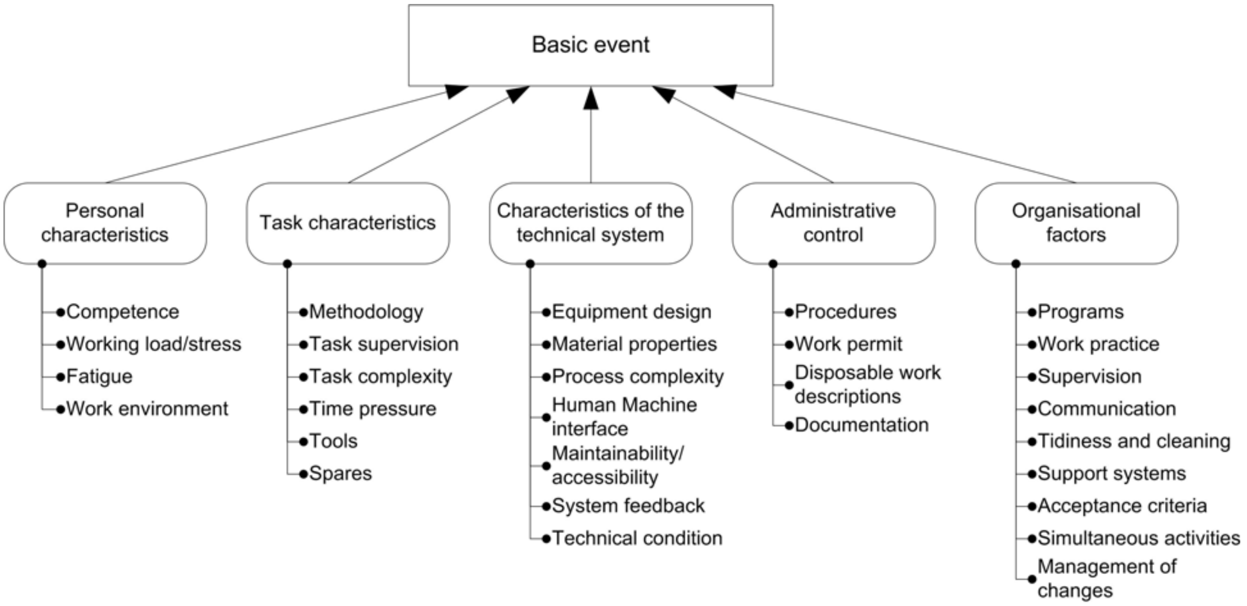


Figure 4 **Generic framework for identification of RIFs.**

The framework for identification of RIFs is based on a review, comparison, and synthesis of several schemes of classification of human, technical, and organisational (MTO) factors and experience from the case study. The schemes include classification of;

1. Causes in methods for accident investigations (MTO-analysis (ref 2) and TRIPOD (ref 3)),
2. Organisational factors in models for analysis of the influence of organisational factors on risk like I-RISK (ref 4) and WPAM (ref 5 & 6), and
3. Performing shaping factors (PSFs) in methods for human reliability analysis (HRA), like THERP (ref 7), CREAM (ref 8), SLIM-MAUD (ref 9), and HRA databases (CORE-DATA (ref 10)).

Table 1 Description of risk influencing factors (RIFs).

RIF group	RIF	Description
Personnel	Competence	Cover aspects related to the competence, experience, system knowledge and training of personnel
	Working load/stress	Cover aspects related to the general working load on persons (the sum of all tasks and activities)
	Work environment	Cover aspects related to the physical working environment like noise, light, vibration, use of chemical substances, etc.
	Fatigue	Cover aspects related to fatigue of the person, e.g., due to night shift and extensive use of overtime
Task	Methodology	Cover aspects related to the methodology used to carry out a specific task.
	Task supervision	Cover aspects related to supervision of specific tasks by a supervisor (e.g., by operations manager or mechanical supervisor
	Task complexity	Cover aspects related to the complexity of a specific task
	Time pressure	Cover aspects related to the time pressure in the planning, execution and finishing of a specific task
	Tools	Cover aspects related to the availability and operability of necessary tools in order to perform a task.
	Spares	Cover aspects related to the availability of the spares needed to perform the task.
Technical system	Equipment design	Cover aspects related to the design of equipment and systems such as flange type (ANSI or compact), valve type, etc.
	Material properties	Cover aspects related to properties of the selected material with respect to corrosion, erosion. fatigue, gasket material properties, etc.
	Process complexity	Cover aspects related to the general complexity of the process plant as a whole
	HMI (Human Machine Interface)	Cover aspects related to the human-machine interface such as ergonomic factors, labeling of equipment, position feedback from valves, alarms, etc.
	Maintainability/ accessibility	Cover aspects related to the maintainability of equipment and systems like accessibility to valves and flanges, space to use necessary tools, etc.
	System feedback	Cover aspects related to how errors and failures are instantaneously detected, due to alarm, failure to start, etc.
	Technical condition	Cover aspects related to the condition of the technical system
Administrative control	Procedures	Cover aspects related to the quality and availability of permanent procedures and job/task descriptions
	Work permit	Cover aspects related to the system for work permits, like application, review, approval, follow-up, and control
	Disposable work descriptions	Cover aspects related to the quality and availability of disposable work descriptions like Safe Job analysis (SJA) and isolation plans
	Documentation	Cover aspects related to the quality, availability, and updating of drawings, P&IDs, etc.
Organisational factors	Programs	Cover aspects related to the extent and quality of programs for preventive maintenance (PM), condition monitoring (CM), inspection, 3rd party control of work, use of self control/checklists, etc. One important aspect is whether PM, CM, etc., is specified
	Work practice	Cover aspects related to common practice during accomplishment of work activities. Factors like whether procedures and checklists are used and followed, whether shortcuts are accepted, focus on time before quality, etc.
	Supervision	Cover aspects related to the supervision on the platform like follow- up of activities, follow-up of plans, deadlines, etc.
	Communication	Cover aspects related to communication between different actors like area platform manager, supervisors, area technicians, maintenance contractors, CCR technicians, etc.
	Tidiness and cleaning	Cover aspects related to the general cleaning and tidiness in different areas on the platform
	Support systems	Cover the quality of data support systems like SAP, etc
	Acceptance criteria	Cover aspects related to the definitions of specific acceptance criteria related to for instance condition monitoring, inspection, etc.
	Simultaneous activities	Cover aspects related to amount of simultaneous activities, either planned (like maintenances and modifications) and unplanned (like shutdown)
	Management of changes	Cover aspects related to changes and modifications

2.2.6 Weighting of risk influencing factors

Weighting of the RIFs is an assessment of the effect (or importance) the RIFs has on the frequency or probability of occurrence of the basic events. The weights of the RIFs correspond to the relative difference in the frequency or probability of occurrence of an event if the status of the RIF is changed from A (best standard) to F (worst practice).

The weighting of the RIFs was done by expert judgments in work shops. The assessments of the weights were based on an individual assessment of the attendees of the workshops prior to a general discussion and a common agreement of the importance.

A five point scale (from high importance to low importance) was applied. Quantitatively, the RIFs were given relative weights on the scale 10 – 8 – 6 – 4 – 2. Finally, the weights were normalized as the sum of the weights for the RIFs influencing a basic event should be equal to 1 (see Formula 2).

An example on the weighting process (qualitative assessment) and the normalized weights are shown in Table 2.

Table 2 Example of the weighting process.

B1 Release due to incorrect blinding/isolation							
B2 3^{rd} party control of work							
E2 3^{rd} party control of work specified but not performed							
RIF	*Description*	*Importance (weight)*					Normalized weight
		High				*Low*	
Time pressure						X	0.09
Work practice		X					0.45
Supervision				X			0.27
Communication					X		0.18

2.2.7 Scoring of risk influencing factors (RIFs)

Scoring of the risk influencing factors implies to assign a score to each identified RIF in the risk influence diagrams. Each RIF is given a score from A to F, where score A corresponds to the best standard in the industry, score C corresponds to industry average, and score F corresponds to worst practice in the industry (see Table 3). The six-point scale is adapted from the TTS (Technical Condition Safety) project (ref 11).

Table 3. Generic scheme for scoring of RIFs.

Score	Explanation
A	Status corresponds to the best standard in industry
B	Status corresponds to a level better than industry average
C	Status corresponds to the industry average
D	Status corresponds to a level slightly worse than industry average
E	Status corresponds to a level considerably worse than industry average
F	Status corresponds to the worst practice in industry

There are two principally different approaches to RIF scoring and quantification:

- Specific studies tailored to the needs of the BORA methodology
- Use of existing studies where applicable, supplemented with additional studies where needed

2.2.8 Adjustment of industry average probabilities/frequencies

The industry average probabilities/frequencies used in the quantitative analysis are adjusted in order to assign platform specific values allowing for platform specific conditions of the RIFs. The industry average probabilities/frequencies are revised based on the risk influence diagrams through an assessment of the weights and score of the RIFs.

The following principles are used for adjustment of the industry average data:

$P_{rev}(A)$ is the "installation specific" probability (or frequency) of occurrence of event A. The probability $P_{rev}(A)$ is determined by the following procedure;

$$P_{rev}(A) = P_{ave}(A) \cdot \sum_{i=1}^{n} w_i \cdot Q_i \qquad (1)$$

where $P_{ave}(A)$ denotes the industry average probability of occurrence of event A, w_i denotes the weight (importance) of RIF no. i for event A, Q_i is a measure of the status of RIF no. i, and n is the number of RIFs. Here,

$$\sum_{i=1}^{n} w_i = 1 \qquad (2)$$

Values for w_i's are given from the weighting process. To determine the Q_i's we need to associate a number to each of the status scores A - F. The Q_i's are determined by the following way:

- Determine $P_{low}(A)$ as the lower limit for $P_{rev}(A)$ by expert judgment.
- Determine $P_{high}(A)$ as the upper limit for $P_{rev}(A)$ by expert judgment.
- Then put for i =1, 2, … n;

$$Q_i\,(s) = \begin{cases} P_{low} / P_{ave} & if\ s = A \\ 1 & if\ s = C \\ P_{high} / P_{ave} & if\ s = F \end{cases} \qquad (3)$$

where s denotes the score or status of RIF no i.

To assign values to Q_i for $s = B$, we assume a linear relationship between $Q_i\,(A)$ and $Q_i\,(C)$, and use $s_A = 1$, $s_B = 2$, $s_C = 3$, $s_D = 4$, $s_E = 5$, and $s_F = 6$. Then,

$$Q_i(B) = \frac{P_{low}}{P_{ave}} + \frac{(s_B - s_A) \cdot (1 - \frac{P_{low}}{P_{ave}})}{s_C - s_A} \qquad (4)$$

To assign values to Q_i for $s = D$ and E, we assume a linear relationship between $Q_i\,(C)$ and $Q_i\,(F)$. Then,

$$Q_i(D) = 1 + \frac{(s_D - s_C) \cdot (\frac{P_{high}}{P_{ave}} - 1)}{s_F - s_C} \qquad (5)$$

$Q_i\,(E)$ is calculated as $Q_i\,(D)$ by use of s_E instead of s_D in formula (5).

Table 4 shows some values of Q_i depending of the ratio between $P_{low}(A)$ and $P_{ave}(A)$, and $P_{high}(A)$ and $P_{ave}(A)$.

- Case 1: $P_{low}(A)/P_{ave}(A)$ = 0,5 and $P_{high}(A)/P_{ave}(A)$ = 2
- Case 2: $P_{low}(A)/P_{ave}(A)$ = 0,33 and $P_{high}(A)/P_{ave}(A)$ = 3
- Case 3: $P_{low}(A)/P_{ave}(A)$ = 0,2 and $P_{high}(A)/P_{ave}(A)$ = 5
- Case 4: $P_{low}(A)/P_{ave}(A)$ = 0,1 and $P_{high}(A)/P_{ave}(A)$ = 10

Table 4 Q_i for selected combinations of P_{low} and P_{high}.

	Case 1	Case 2	Case 3	Case 4
A	0.5	0.33	0.2	0.1
B	0.75	0.67	0.6	0.55
C	1	1	1	1
D	1.33	1.67	2.33	4
E	1.67	2.33	3.67	7
F	2	3	5	10

2.2.9 Recalculation of the risk in order to determine the platform specific risk

The final step is to calculate the risk by use of the generic model, generic data and platform specific data. The following figure illustrates the types of information that is generic and platform specific respectively:

- The structure of the model as such is generic, in the sense that there are generic work operations and equipment packages, initiating events, BBDs, fault trees and what RIFs influence the various factors.
- The generic data that go into the quantification of the model are indicated in green in the figure. This includes Initiating Event frequencies, Fault tree probabilities (Basic Event probabilities) and RIF weights.
- Platform specific data are shown in red. This includes the number of work operations per year, equipment count and platform specific RIF scores.

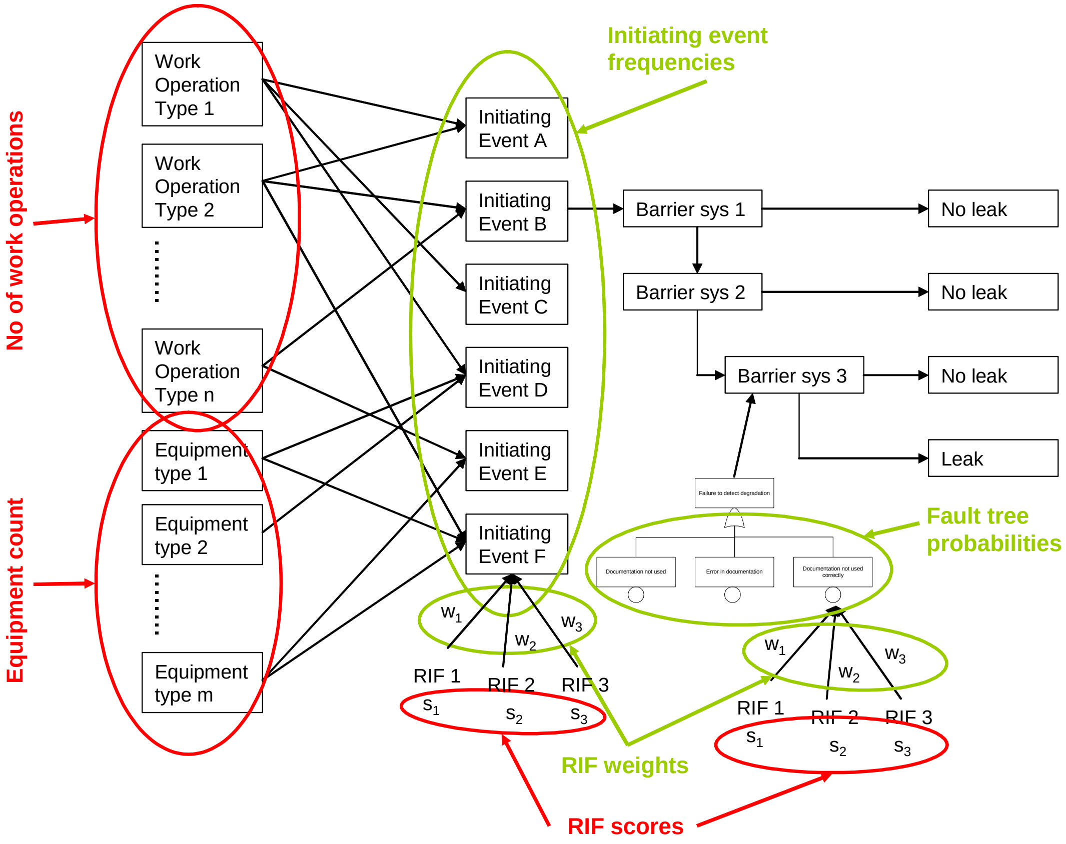


Figure 5 Generic information (green) vs installation specific information (red) used in study

2.3 Simplified approach for calculating Initiating Event Frequencies

In order to simplify the work and also to compensate for lack of data, a simplified approach to calculating Initiating Event Frequencies is also proposed. The steps in this approach may be summarized as follows:

- The total leak frequency, f_T, of the installation is established based on equipment counts or based on use of the standard equipment packages established in Section 3.3.
- This total leak frequency can be broken down on types of Initiating Events, using the information in Section 7.1.2, Figure 27 and Figure 28. This gives percentages of occurrences of different initiating events and these can be used as conditional probabilities, i.e. probability of leak being caused by Initiating event Type A1, A2 etc. This is expressed as $p(IE_{A1}|Leak)$, $p(IE_{A2}|Leak)$, etc. The frequency of each Initiating Event can than be calculated as follows:

$$f_{IE_{A1}} = f_T \cdot p(IE_{A1} \,|\, Leak)$$

These frequencies can subsequently be used in the further analysis.

This approach does not take into account the number of work operations explicitly but will still enable adjustment of the frequencies to take into account the effect of risk influencing factors. A simplified way of taking this into account is to look at the maintenance concept being applied on the installation or other specific information related to the number of work operations. If it can be argued that the activity level on the installation differs from a “North Sea average”, an adjustment factor is determined (if the number of work operations is 80% of a “typical” installation, an adjustment factor of 0.8 is applied).

3. Work operations and equipment units

3.1 Definition of typical work operations

In order to establish a suitable set of typical work operations, the starting point is to consider the types of equipment located in the process areas and what operations are being performed on this equipment. Principally, the equipment can be divided in two groups:

- Hydrocarbon containing equipment
- Other equipment and structures. This will include all sorts of equipment in the process areas such as utility equipment, safety systems, electrical equipment, structures etc.

There will be a principal difference between work operations performed on these two groups of equipment since work on the second group of equipment only indirectly can lead to a leak of hydrocarbons, e.g. due to dropped or swinging objects (external impacts). However, when performing work on the hydrocarbon containing equipment, the operation can directly lead to a release, e.g. if a wrong valve is opened.

Further, when considering hydrocarbon containing equipment, it is natural to do a further subdivision:

- Pressurized equipment
- Isolated, depressurized equipment

The errors or failures required for a release to occur in these situations will be different and are therefore natural to consider separately. We thus end up with splitting on three situations:

- Work on pressurized, hydrocarbon containing equipment
- Work on isolated and depressurized, hydrocarbon containing equipment
- Work on other equipment and structures

In the following table, typical work activities are defined. The table contains the following columns:

- **Type of activity** – This describes which of the three situations mentioned above that the work operation is relevant for and specifies more in detail the type of operation taking place.
- **Examples of activities** – Examples of activities that would be classified within the group.
- **Characteristic features of the operation** – What are the characteristic features of the activities with respect to safety?
- **Potential errors that may lead to release** – What types of failures/Initiating Events can be caused by or affected by the work operation?

Table 5 Types of activities that may be the cause of process leak

Type of activity		**Examples of activities**	**Characteristic features of the operation**	**Potential errors that may lead to release**
Work on pressurized equipment	Normal operation	· Resetting of valves after unplanned shutdown · Draining of liquid to closed drain · Use of temporary hoses · Bypass of equipment · Shut down/start up	- Part of everyday operations and work at the installation - Very limited or no preplanning of operation. - Performed by prod tech or CCR or those two in cooperation - Short duration	This may introduce latent failures that can later lead to a leak or it can lead to immediate release. Criticality of error will depend on whether the valve opens to atmosphere or not.
	PM/Inspection operations interfering with process flow	· Testing and maintenance, e.g. leak test of a valve. · Testing/calibration of equipment/instruments ·	- Limited/minor operations that require limited planning before being initiated. - Identification of correct equipment required.	May introduce latent failures that can later lead to a leak or it can lead to immediate release. Criticality of error will depend on whether the valve opens to atmosphere or not. Will also affect probability of technical failure.
	Planned opening of equipment to atmosphere	· Sampling from hydrocarbon flow in any part of the process	- Lab tech or similar samples production flow (liquid) - Limited preparation and planning, identification of valve required. - Short duration	If this takes place during normal operation, a leak is unlikely. Sampling valves may be left open when equipment is depressurized.
	External PM/inspection operations on the equipment	· Re-tensioning of bolts · External inspection and maintenance on equipment · Inspection of process equipment · Painting/surface treatment of equipment	- Part of everyday work operations - Performed by mechanic - Operation preplanned but not with particular focus on avoiding leaks - Usually short duration (within one shift) - May also be part of maintenance/-inspection campaigns	Not very likely that these operations will lead to a leak directly, but they will influence the probability of technical failures of the system/equipment.

Type of activity		**Examples of activities**	**Characteristic features of the operation**	**Potential errors that may lead to release**
Work on isolated depressurized equipment	· Isolation of major equipment units, e.g. separator, compressor etc.	· This will cover all types of activities requiring shutdown, isolation and depressurization of equipment. Examples could be replacing internal instruments, internal cleaning, replacing flanges, seals, modifications etc.	- Many valves/blindings that need to be inserted/operated, may be located in several areas/modules/deck levels - Duration over several shifts, several days - Extensive planning process before operation is started - Typically a number of (independent) activities will be combined - Often many people involved, from several disciplines - There will typically be high focus on these operations	Several possible leak situations are possible: Breakdown of isolation while work is ongoing, introduction of latent errors (that may cause a release during start-up or later) and immediate releases.
	- Isolation of small part of process, e.g. a single valve, small pipe segment etc.	· This will cover operations where it is possible to isolate only a very small part of the process to do smaller repairs/maintenance activities. Examples could be repairing or replacing a valve on a bypass line, replacing a pipe bend etc.	- A few valves/blindings that need to be inserted/operated, usually located in one area. - Duration usually only one shift - Planning process before operation is started - Prod tech and mechanic will typically be involved.	Several possible leak situations are possible: Breakdown of isolation while work is ongoing, introduction of latent errors and immediate releases.
Work in process area – not on process equipment		- Construction work - Scaffolding - Hot work (A and B) - Cleaning, painting, sandblasting - PM and modifications on equipment, incl. safety systems, utility, structures, etc	- Will cover a wide variety of operations with varying characteristics. Ranging from simple, short duration operations involving 1-2 persons to major construction work with long duration (weeks) and large number of people involved.	Affects the probability of external events causing leaks. Also a possibility of operations being performed on wrong equipment.

3.2 Typical number of Work Operations per year

It has turned out to be difficult to gather much information on this particular aspect of the model. However, some information is available form earlier work that has been performed (Ref. 12) and a summary of this is presented in the following.

First of all, the previous section showed a breakdown of operations into a total of 7 types of operations. As will be shown later in the report (Section 7.1.2), the large majority of the leaks (more than 95%) occur in relation to three types of operations:

- Work on pressurized equipment – Normal operation
- Work on depressurized equipment – Small equipment units
- Work on depressurized equipment – Major equipment units

It is therefore particularly important to have data related to these operations, while the others contribute much less and therefore are less important to cover.

In Ref 12, information has been gathered for one specific installation, Statfjord B. This is a large, integrated production platform. Work orders for one year have been studied and the number of operations of a predefined set of categories has been determined. The work operations that are of primary relevance to BORA and which were considered in this work were as follows:

- **Work on pressurized HC-containing equipment.** This involves activities on HC-equipment which contains hydrocarbons when the work in going on, e.g. inspection, calibration, draining, testing/maintenance etc. This is a category that largely coincides with our overall category "Work on pressurized equipment". However, we have split this further into four subcategories and these can not be separated out from the information provided.
- **Work on depressurized HC-equipment.** This covers all activities which require opening up the equipment, e.g. maintenance and testing, connecting new equipment etc. This matches the same category in this project, except that there is no split on small/major equipment units.
- **Planned shutdown – partial or complete.** In our categorization, this is classified as "Normal operation".
- **Changes in process conditions**, e.g. changes in pressure, temperature or composition of process flow. This is not specifically mentioned in our categorization, but this would also fall under the category "Normal operation".
- **Planned start-up – partial or complete.** In our categorization, this is classified as "Normal operation".

The table below summarizes the number of operations taking place during one year for each of these.

Table 6 Number of work operations per year (Statfjord B)

	Number of work operations per year		
	Maintenance	Modifications/-projects	Total
Work on pressurized equipment	293	5	298
Work on depressurized equipment	430	18	448
Planned shutdown	497	18	515
Changes in process conditions	0	7	7
Planned start-up	498	18	516

Some brief comments to the numbers:

- The large majority of operations are related to maintenance. For all the work categories shown in the table (except "changes in process conditions"), maintenance operations comprises more than 95% of the total number. This means that counting the number of maintenance operations will give a very good indication of the total.
- Planned shutdowns and planned start-ups naturally follow each other, and the numbers will be the same. The number of shutdowns/start-ups will also necessarily be at least as high as the number of operations on depressurized equipment. It is also not surprising to see that shutdowns/start-ups to a large degree are associated with work on equipment (87%).

In view of the fact that such a large proportion of the work is maintenance related, it is also natural to put forward the hypothesis that as long as similar maintenance concepts are applied, the number of work operations will be closely correlated with the quantity of equipment on an installation. If this is correct, it means that it may be possible to estimate the activity level on an installation from the quantity of equipment rather than by going into detail on the work operations. This is likely to be a time-saving approach since an equipment count will be performed as part of the QRA work in any case.

There may on the other hand be conditions which imply that this is too simplified. Inspection frequencies may be quite different, according to the type/quality of materials used. Use of duplex steel in process piping will usually imply a low inspection frequency, with some years between inspections. If carbon steel is used, one or two inspections per year may be required.

3.3 Typical Equipment Packages

Number of equipment units has been estimated for the following typical equipment packages:

- Separator package
- Compressor package
- Manifolds
- Metering
- Pumps
- Heat exchangers

Number of equipment units is presented for fixed and floating installations, and as a total. Information from 7 floaters and 10 fixed installations has been used when estimating the number of equipment units.

When estimating the number of equipment units belonging to each equipment unit, the equipment unit has been defined as a complete process stage. This implies that for a compressor stage, for instance, also the corresponding heat exchanger and scrubber are included. In addition, a typical amount of valves, flanges, instrument connections and piping is included in the equipment number.

In the following sections, typical equipment packages have been defined, and for each process stage a typical number of equipment has been estimated. Note that for some of the stages, isolation valves are included at the inlet and outlet of the stage. When combining stages, it is hence a risk of overestimating the number of isolation valves.

3.3.1 Separator Package

3.3.1.1 Limitations of package

A typical separator package has been defined as the separator unit with all connected piping upstream and downstream to (and including) the first actuated segregation valve. The equipment units covered within the separator stage is illustrated in Figure 6.

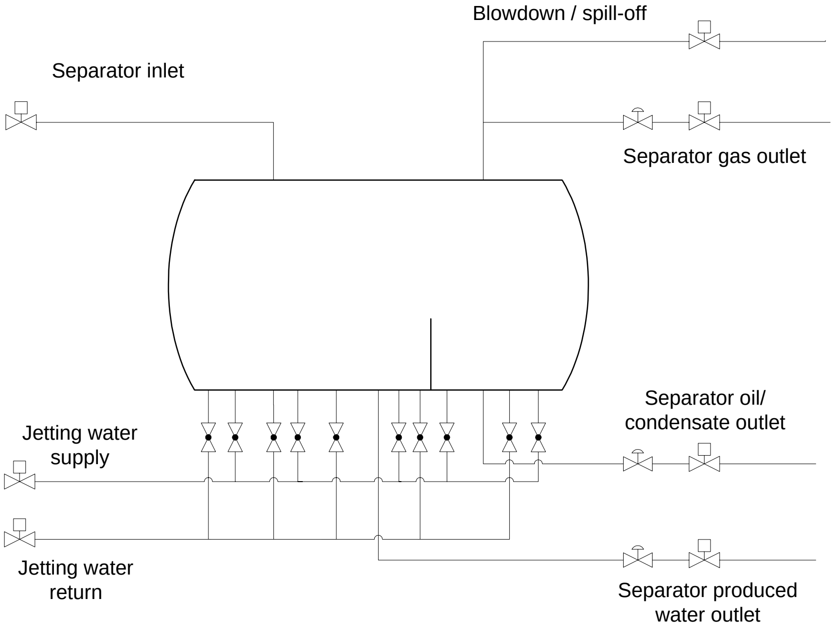


Figure 6 **Definition of separator stage**

3.3.1.2 Equipment Units included in package

Based on example studies, typical equipment numbers are estimated. The numbers are shown for fixed and floating installations in Table 7.

Table 7 Typical equipment number for a separator stage

	Number of equipment units		
Type of equipment	**Fixed**	**Floating**	**Total**
Flanges	170	90	130
Valves actuated	15	10	12
Valves manual	80	35	50
Steel piping/process piping	200	100	150
Flexible piping	0	0	0
Horizontal pressure vessels	1	1	1
Instruments	20	20	20

3.3.2 Compressor Package

3.3.2.1 Limitations of package

A typical compressor stage has been defined as the compressor unit with corresponding heat exchanger and scrubber, along with all connected piping upstream and downstream to (and including) the first actuated segregation valve. The equipment units covered within the compressor stage is illustrated in Figure 7.

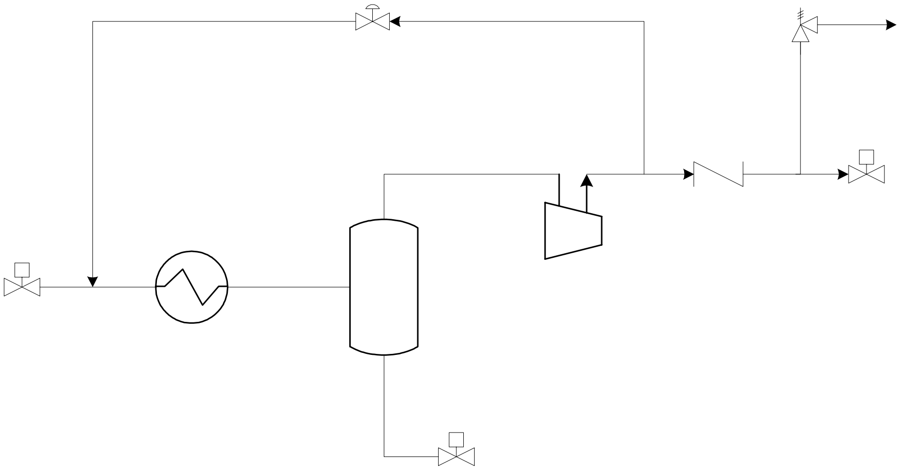


Figure 7 Definition of compressor stage

3.3.2.2 Equipment Units included in package

Based on example studies, typical equipment numbers are estimated. The numbers are shown for fixed and floating installations in Table 8.

Table 8 Typical equipment number for a compressor stage

Type of equipment	**Number**		
	Fixed	**Floating**	**Total**
Flanges	140	70	100
Valves actuated	15	10	12
Valves manual	60	30	45
Steel piping/process piping	300	100	200
Compressor, centrifugal	1	1	1
Heat exchangers	1	1	1
Vertical pressure vessels	1	1	1
Instruments	60	20	40

3.3.3 Manifolds

3.3.3.1 Limitations of package

A manifold stage is defined as the manifold itself and all supply lines from each wellhead, including the choke valve. A typical manifold stage is shown in Figure 8.

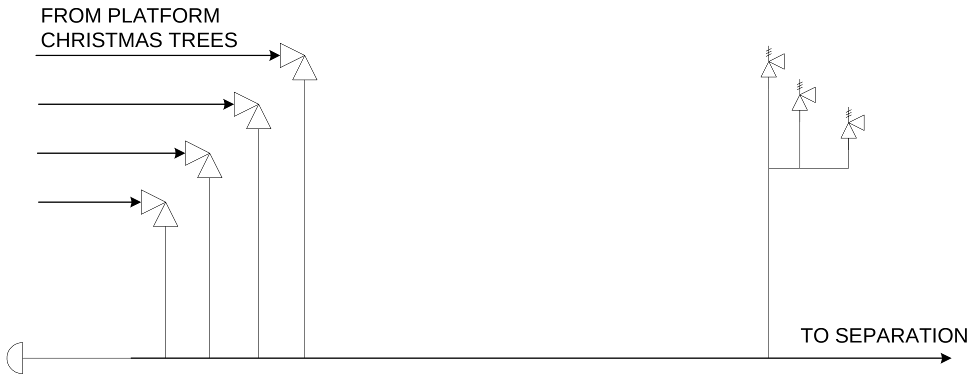


Figure 8 Definition of manifold stage

If the inlet lines to the manifold are flowlines from subsea production units in stead of platform trees, the manifold stage will have a slightly different layout. Specifically, each inlet line will typically be equipped with an actuated isolation valve.

3.3.3.2 Equipment Units included in package

Based on example studies, typical equipment numbers are estimated. The numbers are shown for fixed and floating installations in Table 9.

It should be noted that estimating the number of "typical" equipment units in a manifold stage is inherently inaccurate, as the complexity of the manifold is in direct proportion with the number of lines connected to the manifold.

Table 9 Typical equipment number for a manifold stage

	Number		
Type of equipment	**Fixed**	**Floating**	**Total**
Flanges	200	100	150
Valves actuated	10	18	15
Valves manual	90	25	55
Steel piping/process piping	300	120	200
Flexible piping	0	20	10
Instruments	40	15	25

3.3.4 Metering

3.3.4.1 Limitations of package

A typical metering package consists of a number of parallel metering units, each equipped with necessary valves and instrumentation. In addition, the metering package includes a calibration loop along with valves and piping for flow control. A typical metering unit is shown in Figure 9 (from [13]).

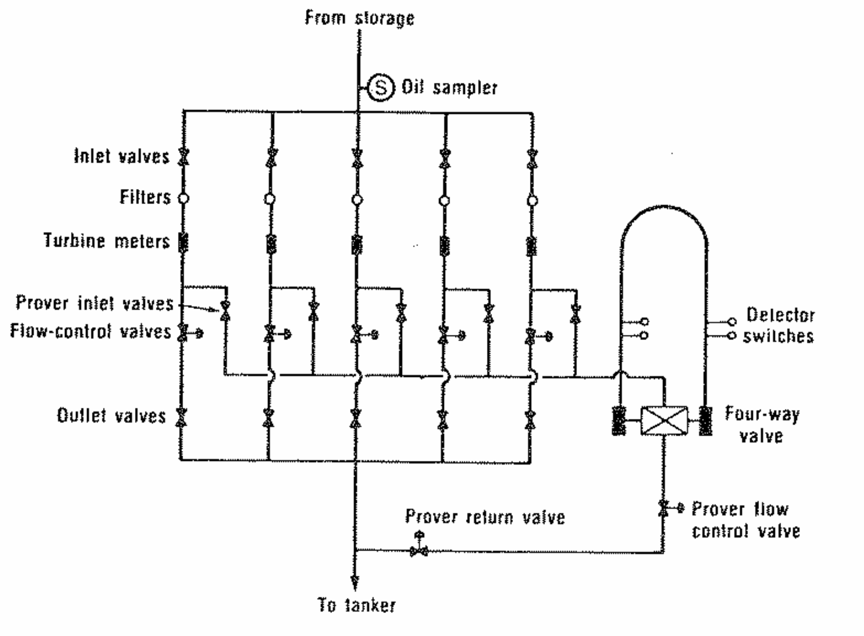


Figure 9 Definition of metering package

3.3.4.2 Equipment Units included in package

Based on example studies, typical equipment numbers are estimated. The numbers are shown for fixed and floating installations in Table 10.

Table 10 Typical equipment number for a metering package

Type of equipment	Number		
	Fixed	**Floating**	**Total**
Flanges	80	60	70
Valves actuated	12	10	11
Valves manual	40	25	35
Steel piping/process piping	160	80	120
Filters	2	2	2
Instruments	30	15	25

3.3.5 Pumps

3.3.5.1 Limitations of package

The pump stage consists of the pump itself along with a specified amount of piping, valves and flanges. Based on example studies, it is chosen to assume that a typical pump stage consists of two pumps in parallel. A typical pump stage is shown in Figure 10.

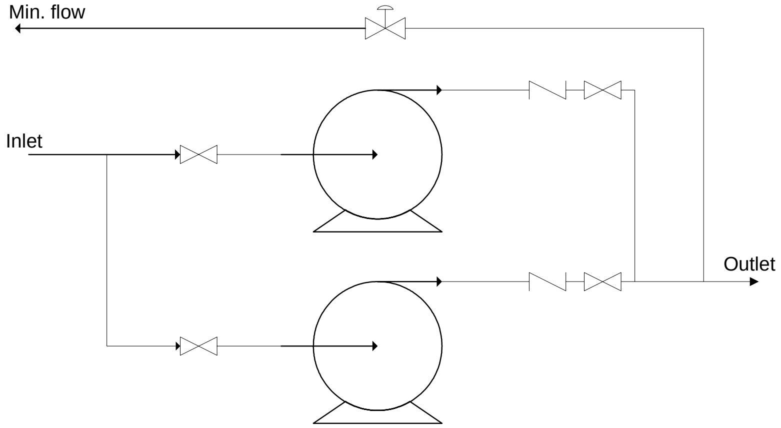


Figure 10 Definition of pump stage

3.3.5.2 Equipment Units included in package

Based on example studies, typical equipment numbers are estimated. The numbers are shown for fixed and floating installations in Table 11.

Table 11 Typical equipment number for a pump stage

	Number		
Type of equipment	**Fixed**	**Floating**	**Total**
Flanges	150	60	100
Valves actuated	20	8	15
Valves manual	20	20	20
Steel piping/process piping	100	50	75
Pumps, centrifugal	2	2	2
Instruments	20	20	20

3.3.6 Heat Exchangers

3.3.6.1 Limitations of package

A heat exchanger stage is defined as the heat exchanger itself and all piping, flanges and valves on the process medium side to (and including) the first actuated segregation valve. A typical heat exchanger stage is shown in Figure 11.

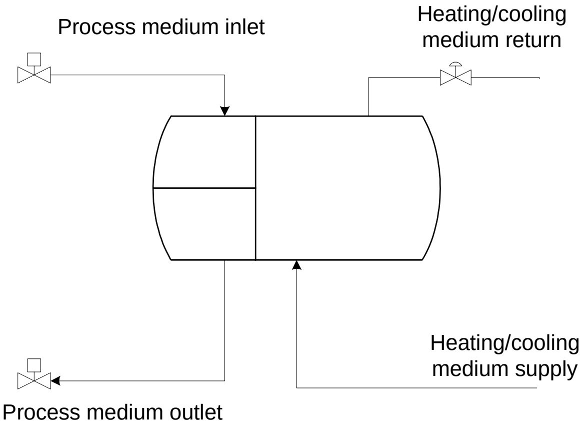


Figure 11 **Definition of heat exchanger stage**

3.3.6.2 Equipment Units included in package

Based on example studies, typical equipment numbers are estimated. The numbers are shown for fixed and floating installations in Table 12.

Table 12 **Typical equipment number for a heat exchanger stage**

	Number		
Type of equipment	**Fixed**	**Floating**	**Total**
Flanges	70	70	70
Valves actuated	4	6	5
Valves manual	40	30	35
Steel piping/process piping	100	160	130
Heat exchangers	1	1	2
Instruments	9	7	8

4. Development of a basic risk model including hydrocarbon release scenarios and safety barriers

4.1 From "Release Scenarios" to "Initiating Events"

In earlier work in the BORA project (Ref 14), a set of "release scenarios" was defined based on review and analysis of actual releases that had occurred. The release scenarios were divided into seven main groups and some of these groups are divided further into sub-categories:

1. Release during maintenance of HC-system (requiring disassembling)
    a. Release due to failure prior to or during disassembling of HC-system
    b. Release due to break-down of isolation system during maintenance
2. Release due to latent failure introduced during maintenance
    a. Release due to incorrect fitting of flanges or bolts during maintenance
    b. Release due to valve(s) in incorrect position after maintenance
    c. Release due to erroneous choice or installations of sealing device
3. Release due to operational failure during normal production
    a. Release due to maloperation of valve(s) during manual operation
    b. Release due to maloperation of temporary hoses.
    c. Release due to lack of water in water locks in the drain system
4. Release due to technical/physical failures
    a. Release due to degradation of valve sealing
    b. Release due to degradation of flange gasket
    c. Release due to loss of bolt tensioning
    d. Release due to degradation of welded pipes
    e. Release due to internal corrosion
    f. Release due to external corrosion
    g. Release due to erosion
5. Release due to process upsets
    a. Release due to overpressure
    b. Release due to overflow / overfilling
6. Release due to external events
    a. Release due to impact from falling object
    b. Release due to impact from bumping/collision
7. Release due to design related failures

For all of these release scenarios, barrier block diagrams and fault trees were prepared.

During the preparation of the case studies, it was realized that a restructuring of the scenarios could be useful, mainly based on the characteristics of the barriers in place to prevent release rather than just looking at the causal factors. Further, it was also noted that these scenarios do not necessarily lead to releases because the barriers in place will in most case prevent a release from occurring. It was therefore considered to be somewhat misleading to use the term "release scenarios" and in the following we have therefore chosen to call these "Initiating Events".

The restructuring has lead to establishment of 6 groups or types of Initiating Events. Partly, the groups are similar to what has been defined earlier.

An advantage of structuring the initiating events in this way is that the same BBD can be applied to all initiating events within each group. There will obviously be differences in frequencies and probabilities for the different events, but the relevant barrier functions and barrier systems are the same and the same structure of the BBD can be applied.

The definition of initiating event is the same as is applied in the original leak scenario report, but it has been noted that some of the release scenarios that were defined in the earlier report did not follow this definition and some modifications are therefore necessary.

The six main groups are as follows:

A. **Technical degradation of system** – These are deviations which can be characterized as a (slow) degradation of the system until a release eventually occurs. In order to prevent these deviations from developing into a release, it is necessary to detect the degradation in time or to replace the deteriorating components in time. An example of this type of deviation is corrosion.
B. **Human intervention introducing latent error** – These are deviations characterized by a person performing some operation on the system and this introduces an error in the system that at some later point in time will cause a release if it is not detected. To avoid a release in these cases, means to detect the errors in time are necessary. Example of this type of deviation is “installing wrong sealing device” or “failing to isolate equipment to be worked on from the rest of the system”.
C. **Human intervention causing immediate release** – This is a special type of deviation which also involves human intervention but where the operation directly causes a release. One example could be an operator that opens a wrong valve on a system causing a release. What is special in this case is that there are no barriers between the deviation and the release (although there obviously are barriers to prevent the initial deviation from happening). No BBD is therefore developed.
D. **Process disturbance** – This covers all deviations which are “internal” to the process system, whether this is caused by the production flow (e.g. a well behaving erratically) or by a process operator error (e.g. opening or closing wrong valves). In these cases, it is the operation of the process system itself that causes the release. An example of such an initiating event would be overpressure.
E. **Inherent design errors** – Characteristic for these types of deviations are that they are not known and that it is not meaningful or possible to introduce barriers specifically to protect against these types of deviations. The best way of protecting against this is a robust design, with ample safety margins and a “defense-in-depth” strategy. Preparing a BBD will however not be of much meaning for this type of deviations.
F. **External events** – In the release scenario report, “External events” is also identified as one group. However, as pointed out in the report, these are not process related as such and in order to prevent release due to these causes, one needs to look at other types of operations than those related to the process system as such. No BBD has therefore been prepared.

In the following table, the six groups of initiating events, with all the specific events as identified earlier, are listed. The table also shows the earlier numbering from the release scenario report.

Table 13 Overview over Initiating Events

Initiating Event Type	Initiating Events	
A. Technical degradation of system	1. Degradation of valve sealing 2. Degradation of flange gasket 3. Loss of bolt tensioning 4. Fatigue 5. Internal corrosion 6. External corrosion 7. Erosion 8. Other causes	4a 4b 4c 4d 4e 4f 4g 3c
B. Human intervention introduction latent error	1. Incorrect blinding/isolation 2. Incorrect fitting of flanges or bolts during maintenance 3. Valve(s) in incorrect position after maintenance 4. Erroneous choice or installations of sealing device 5. Maloperation of valve(s) during manual operation* 6. Maloperation of temporary hoses.	1a** 2a 2b 2c 3a 3b
C. Human intervention causing immediate release	1. Break-down of isolation system during maintenance. 2. Maloperation of valve(s) during manual operation* 3. Work on wrong equipment, not known to be pressurised	1b 3a -
D. Process disturbance	1. Overpressure 2. Overflow / overfilling	5a 5b
E. Inherent design errors	1. Design related failures	7
F. External events	1. Impact from falling object 2. Impact from bumping/collision	6a 6b

* This may lead to either introduction of a latent error or an immediate release
** The Initiating Event does not correspond exactly to release scenario 1a, but is similar

4.2 Work Operations leading to Initiating Events

The Initiating Events may have different origins, in the sense that there may be several Work operations that can lead to any one Initiating Event. All combinations are however not possible. In order to structure this, a table has been prepared showing which of the Work operations may lead to which Initiating Events.

The table also contains "Quantity of Equipment" in a separate column together with the Work operations. Initiating Events marked as being associated with Quantity of Equipment are those which depend only on this factor and which are not (or at least to a limited degree) dependent on the work operations taking place. This includes technical failures and design related failures.

Table 14 Overview over Work Operations and Initiating Events

Type of Initiating Event	Work operation	Pressurised equipment				Depress. equipment		Other work in process area	Quantity of equipment
		Normal operation	PM/Inspection	Sampling	External	Major unit	Small unit		
A1	Degradation of valve sealing (PM)								X
A2	Degradation of flange gasket (PM)								X
A3	Loss of bolt tensioning (PM)								X
A4	Fatigue (insp)								X
A5	Internal corrosion (Insp)								X
A6	External corrosion (Insp)								X
A7	Erosion (Insp)								X
A8	Other								X
B1	Incorrect blinding/isolation					X	X		
B2	Incorrect fitting of flanges or bolts during maintenance					X	X		
B3	Valve(s) in incorrect position after maintenance		X			X	X		
B4	Erroneous choice or installations of sealing device					X	X		
B5	Maloperation of valve(s) during manual operation*	X	X			X	X		
B6	Maloperation of temporary hoses.	X				X	X		
C1	Break-down of isolation system during maintenance (technical)					X	X		
C2	Maloperation of valve(s) during manual operation*	X	X	X		X	X		
C3	Work on wrong equipment (not known to be pressurised)					X	X	X	
D1	Overpressure	X							
D2	Overflow / overfilling	X							
E1	Design related failures								X
F1	Impact from falling object				X	X	X	X	
F2	Impact from bumping/collision				X	X	X	X	

4.3 BBDs for groups of initiating events

4.3.1 A. Technical degradation of system

The group “A. Technical degradation of system” has been divided into two sub-groups:

- Degradation beyond acceptable limit identified during PM
- Degradation beyond acceptable limit identified during CM/inspection

Table 15 BBD description for initiating event "Degradation beyond acceptable limit identified during PM"

<table>
<tr><td colspan="2">Barrier Block Diagram description</td></tr>
<tr><td colspan="2"><i>Initiating event</i>
A. Technical degradation of system
• Degradation beyond acceptable limit identified during PM</td></tr>
<tr><td colspan="2"><i>General description</i>
These events are deviations which can be characterized as a (slow) degradation of the system until a release eventually occurs. In order to prevent these deviations from developing into a release, it is necessary to detect the degradation in time or to replace the deteriorating components in time. This can either be done by inspection or condition monitoring, or by preventive maintenance (PM).</td></tr>
<tr><td colspan="2"><i>Example of degradation mechanisms</i>
• <i>A.1 Valve sealing:</i> Mechanical or material degradation of sealing include loss of flexibility of valve stuffing box, degradation of properties of O-rings, etc. Material properties, internal environment/fluid properties etc. are influencing the degradation rate.
• <i>A.2 Flange gasket:</i> Typically degradation of material properties of gasket/seal, e.g. loss of flexibility. Material properties, internal environment/fluid properties etc. are influencing the degradation rate.
• <i>A.3 Loss of bolt tensioning</i>: Loss of bolt tensioning includes leaks from flanges, valves, instrument couplings, etc. Process conditions, use of lock-tite etc. are influencing the degradation rate.</td></tr>
<tr><td colspan="2"><i>Operational mode when failure is introduced</i>
During normal production (slow degradation)</td></tr>
<tr><td colspan="2"><i>Operational mode at time of release</i>
During normal production or during process disturbances (resulting in e.g. increased pressures)</td></tr>
<tr><td><i>Barrier functions</i>
The release may be prevented if the following safety functions are fulfilled:
• Detect degradation beyond acceptable limit
• Detect release <0.1 kg/s</td><td><i>Barrier systems (modeled in Fault Trees)</i>
The release might be prevented if the following barrier systems function:
• <i>Preventive Maintenance (PM)</i>: Planned preventive maintenance operations in accordance with a scheduled PM program. When planning and doing the PM operations different type of documentation may be required/used, e.g. instruction manuals, equipment datasheets, work procedures, work program.
• <i>Area based leak search</i>: Leak search to detect minor releases before they develop into significant leaks. This can either be done using sniffing equipment (detectors) or manual.</td></tr>
<tr><td colspan="2"><i>Assumptions</i>
• All leaks > 0.1 kg/s are reported to the PSA. The leaks have therefore split into two categories in the block diagrams, leaks < 0.1 kg/s and leaks > 0.1 kg/s.
• Area based leak search is not considered to be a barrier system for leaks exceeding 0.1 kg/s. These are assumed detected by the automatic gas detection system or by personnel in the area.</td></tr>
</table>

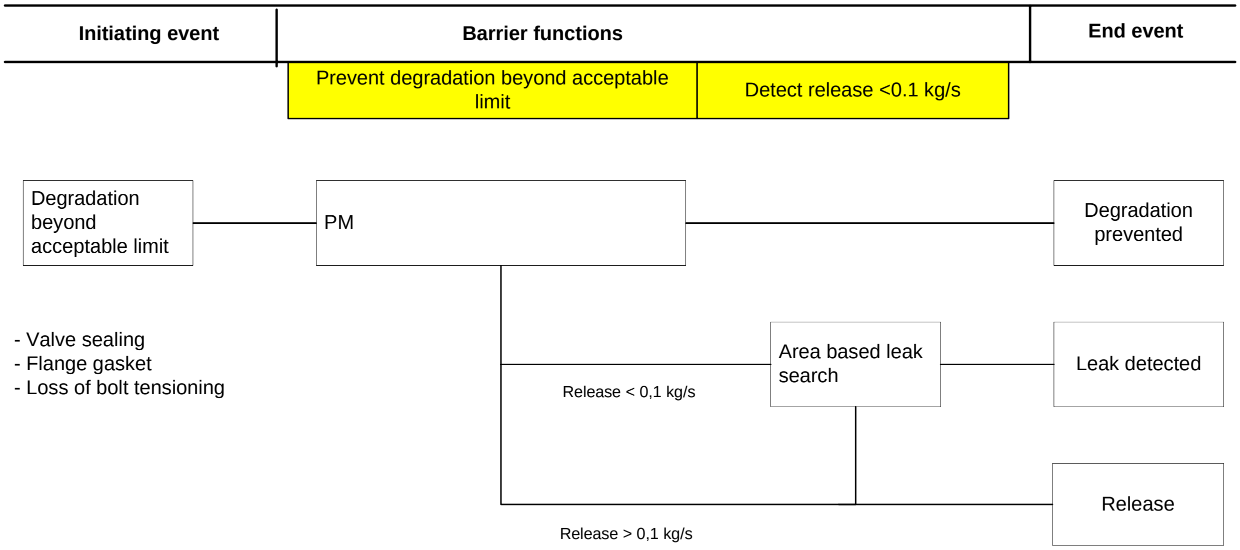


Figure 12 **BBD for initiating event "Technical degradation of systems identified during PM"**

Table 16 BBD description for initiating event "Degradation beyond acceptable limit identified during inspection and/or condition monitoring"

<table>
<tr><td colspan="2"><i>Initiating event</i>
A. Technical degradation of system
• Degradation beyond acceptable limit identified during inspection and/or condition monitoring</td></tr>
<tr><td colspan="2"><i>General description</i>
These events are deviations which can be characterized as a (slow) degradation of the system until a release eventually occurs. In order to prevent these deviations from developing into a release, it is necessary to detect the degradation in time or to replace the deteriorating components in time. This can either be done by inspection or condition monitoring, or by preventive maintenance (PM).</td></tr>
<tr><td colspan="2"><i>Example of degradation mechanisms</i>
• <i>A.4 Fatigue/crack</i>: Material properties, internal environment/fluid properties, vibration, supporting etc. are influencing the degradation rate.
• <i>A.5 Internal corrosion</i>: Corrosion resistance of material, corrosion coating, chemical injection/corrosion inhibitor, internal fluid properties etc. are influencing the degradation rate.
• <i>A.6 External corrosion</i>: Degree of passive protection, material selection, external environment etc. are influencing the degradation rate.
• <i>A.7 Erosion</i>: Typically caused by production of sand, i.e. reservoir conditions, quality of sand filters, monitoring of sand content, design of pipes etc. are influencing the degradation rate.</td></tr>
<tr><td colspan="2"><i>Operational mode when failure is introduced</i>
During normal production (slow degradation)</td></tr>
<tr><td colspan="2"><i>Operational mode at time of release</i>
During normal production or during process disturbances (resulting in e.g. increased pressures)</td></tr>
<tr><td><i>Barrier function</i>s
The release may be prevented if the following safety functions are fulfilled:
• Detect degradation beyond acceptable limit
• Detect release <0,1 kg/s</td><td><i>Barrier systems (modeled in Fault Trees)</i>
The release might be prevented if the following barrier systems function:
• <i>Condition monitoring:</i> Monitoring of equipment to detect potential corrosion/erosion/fatigue. Different type of CM tools may be used, e.g. corrosion coupon and MIC sampling. When planning and doing condition monitoring different type of documentation may be required/ used, e.g. instruction manuals, work procedures and inspection plans.
• <i>Inspection</i>: Inspection/NDT programme to detect potential corrosion /erosion. When planning and doing inspection different type of documentation may be required/ used, e.g. instruction manuals, work procedures and inspection plans.
• <i>Area based leak search:</i> Leak search to detect minor releases before they develop into significant leaks. This can either be done using sniffing equipment (detectors) or manual.</td></tr>
<tr><td colspan="2"><i>Assumptions</i>
• All leaks > 0.1 kg/s are reported to the PSA. The leaks have therefore split into two categories in the block diagrams, leaks < 0.1 kg/s and leaks > 0.1 kg/s.
• Area based leak search is not considered to be a barrier system for leaks exceeding 0.1 kg/s. These are assumed detected by the automatic gas detection system or by personnel in the area.</td></tr>
</table>

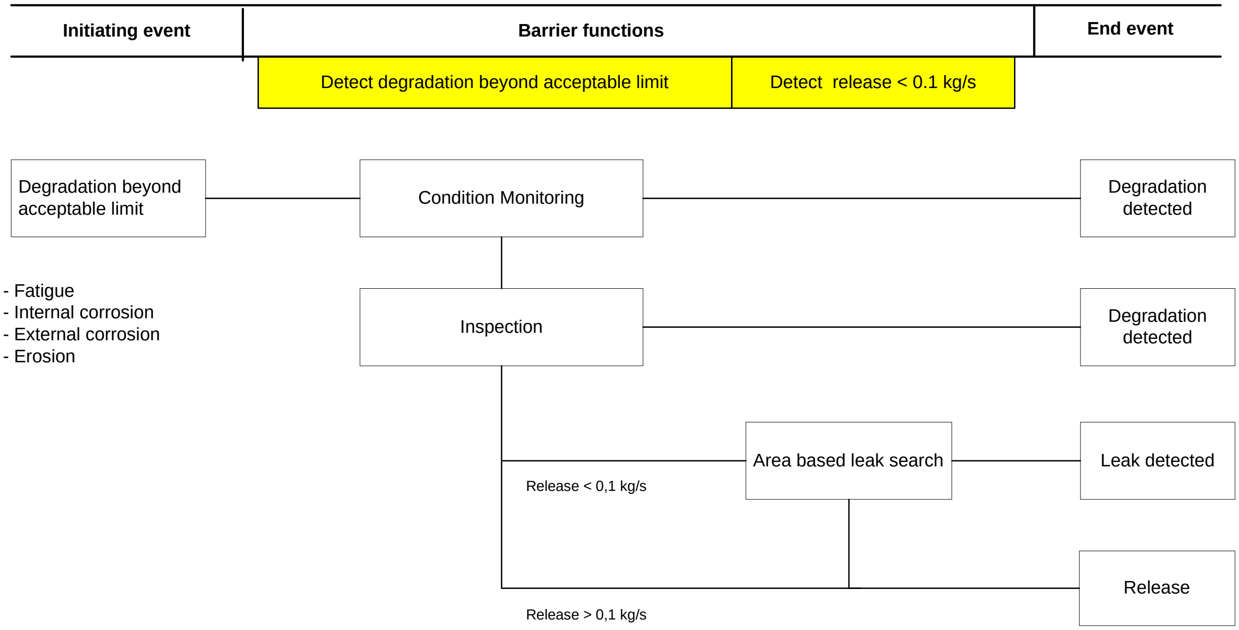


Figure 13 BBD for initiating event "Technical degradation of systems identified during inspection and/or condition monitoring"

4.3.2 B. Human intervention introducing latent error

Table 17 BBD description for initiating event "B. Human intervention introducing latent error"

<table>
<tr><th colspan="2">Barrier Block Diagram description</th></tr>
<tr><td colspan="2"><i>Initiating event</i>
B. Human intervention introducing latent error</td></tr>
<tr><td colspan="2"><i>General description</i>
These are deviations characterized by a person performing some operation on the system and this introduces an error in the system that at some later point in time will cause a release if it is not detected. To avoid a release in these cases, means to detect the errors in time are necessary.</td></tr>
<tr><td colspan="2"><i>Example of latent error</i>
• <i>B.1 Incorrect blinding/isolation:</i> Leaks due to insufficient isolation/blinding.
• <i>B.2 Incorrect fitting of flanges or bolts:</i> Leaks due to tightening with too low or too high tension, misalignment of flange faces, damaged bolts etc.
• <i>B.3 Valve(s) in incorrect position after maintenance:</i> Leaks due to valve(s) in incorrect position after maintenance (valves connected to the system undergoing maintenance)
• <i>B.4 Erroneous choice/installation of sealing device:</i> Installation of wrong type of O-ring, wrong type of gasket (e.g. incorrect material properties), missing gasket/seal in flanges etc.
• <i>B.5 Maloperation of valve(s) during manual operation:</i> Leaks due to:
o Maloperation of valve(s) while maintenance work is ongoing (valves not included in the system undergoing maintenance). Maloperation not detected before start-up or normal production.
o Maloperation of valves during normal production (not causing immediate release)
• <i>B.6 Maloperation of temporary hoses:</i> Leaks due to maloperation of temporary hoses while maintenance work is ongoing or during normal operation.</td></tr>
<tr><td colspan="2"><i>Operational mode when failure is introduced</i>
During maintenance or normal production</td></tr>
<tr><td colspan="2"><i>Operational mode at time of release</i>
During start-up after maintenance or later during normal production</td></tr>
<tr><td><i>Barrier functions</i>
The release may be prevented if the following safety functions are fulfilled:
• Detect latent error</td><td><i>Barrier systems (modeled in Fault Trees)</i>
The release might be prevented if the following barrier systems function:
• <i>Self control</i>: Formal self-control or use of checklists
• <i>3rd party control</i>: Independent control of work by other person.
• <i>Verify system status</i>: Leak test or verification of depressurized system. Leak test may be carried out in different ways, e.g. by use of Nitrogen or use of manual detectors. When planning and doing the leak test different type of documentation may be required/used, e.g. checklists, blinding/isolation plans. Verification of depressurized system may be carried out using different type of mechanical or instrumented equipment. When planning and doing the verification different type of documentation may be required/used, e.g. procedures and checklists.</td></tr>
<tr><td colspan="2"><i>Assumptions</i></td></tr>
</table>

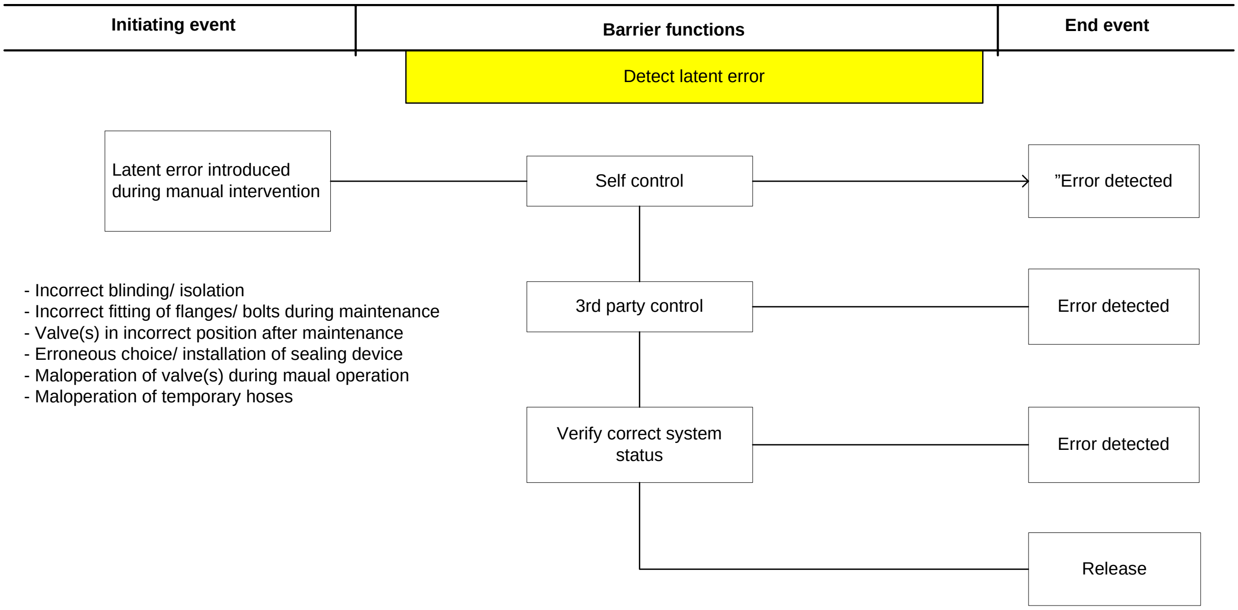


Figure 14 BBDs for Human intervention introducing latent error

4.3.3 C. Human intervention causing immediate release

Table 18 BBD description for initiating event "C Human intervention causing immediate release"

Initiating event C. Human intervention causing immediate release	
General description This is a special type of deviation which also involves human intervention but where the operation directly causes a release. One example could be an operator that opens a wrong valve on a system causing a release. What is special in this case is that there are no barriers between the deviation and the release (although there obviously are barriers to prevent the initial deviation from happening). No BBD is therefore developed.	
Example of human intervention • *C.1 Break-down of isolation system during maintenance:* Locking or labelling of valves/blindings, work permit, communication, complexity of process etc. are influencing the likelihood of fail operation. • *C.2 Maloperation of valve(s) during manual operation*: Labelling of valves, complexity of process, procedures, short time limit etc. are influencing the likelihood of fail operation. • *C.3 Work on wrong equipment, not known to be pressurized*	
Operational mode when failure is introduced During normal production	
Operational mode at time of release During normal production	
Barrier functions No BBD is developed.	***Barrier systems*** NA
Assumptions	

4.3.4 D. Process disturbance

Table 19 BBD description for initiating event "D Process disturbance"

<table>
<tr><td colspan="2"><i>Initiating event</i>
D. Process disturbance</td></tr>
<tr><td colspan="2"><i>General description</i>
This covers all deviations which are "internal" to the process system, whether this is caused by the production flow (e.g. a well behaving erratically) or by a process operator error (e.g. opening or closing wrong valves). In these cases, it is the operation of the process system itself that causes the release.</td></tr>
<tr><td colspan="2"><i>Example of process disturbance</i>
• <i>D.1 Overpressure</i>: Overpressure may be created by increased internal pressure or pressure shock.
• <i>D.2 Overflow / overfilling</i>: Principles of level senor, complexity, procedures, design, operational conditions etc. may influence the likelihood for overflow/overfilling.</td></tr>
<tr><td colspan="2"><i>Operational mode when failure is introduced</i>
During start-up, shutdown or normal production</td></tr>
<tr><td colspan="2"><i>Operational mode at time of release</i>
During start-up, shutdown or normal production</td></tr>
<tr><td><i>Barrier function</i><i>s</i>
The release may be prevented if the following safety functions are fulfilled:
• Prevent overpressure/ overfilling
• Prevent release</td><td><i>Barrier systems</i>
The release might be prevented if the following barrier systems function:
• <i>Primary protection (e.g. PSD, ….):</i> Primary protection from overpressure in a pressure equipment should be provided by a PSH protection system to shut off inflow (PSD). If a vessel is heated, the PSH sensor should also shut off the fuel or source of heat. Primary protection for atmospheric components should be provided by an adequate vent system ( ).
Primary protection from liquid overflow should be provided by an LSH sensor to shut off inflow into the component (PSD).
• <i>Secondary protection (e.g. PSV, HIPPS,….):</i> Secondary protection from overpressure in a pressure component should be provided by a PSV. Secondary protection for atmospheric components should be provided by a second vent. Alternatively an instrument based system may be used for primary and secondary protection provided it is implemented according to IEC 61508.
• Secondary protection from liquid overflow should be provided by the ESSs. Secondary protection from liquid overflow to downstream component should be provided by safety devices on the downstream component. Alternatively an instrument based system may be used for primary and secondary protection provided it is implemented according to IEC 61508.
• <i>Design margins</i>. Depending on the pressure conditions and the design, the residual strength of the steel may also prevent release.</td></tr>
<tr><td colspan="2"><i>Assumptions</i></td></tr>
</table>

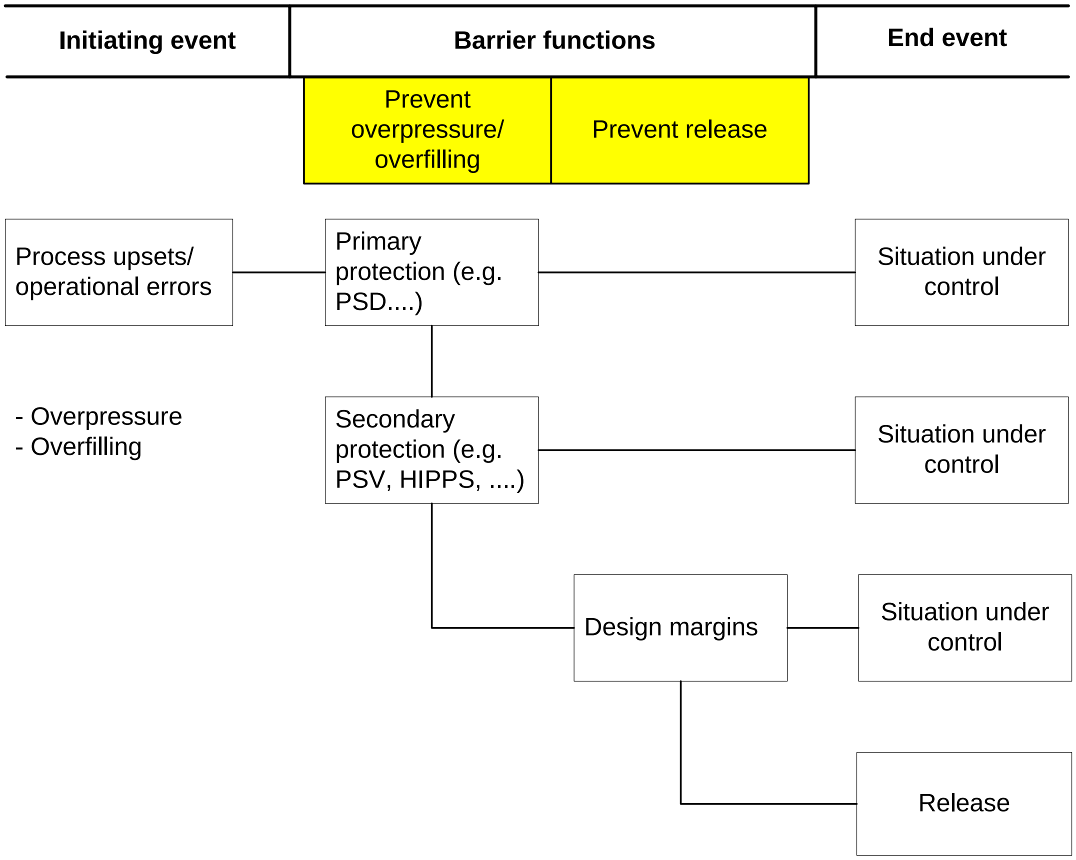


Figure 15 **BBDs for Process disturbance**

4.3.5 E. Inherent design errors

Table 20 BBD description for initiating event "E Inherent design errors"

Initiating event E. Inherent design errors	
General description Characteristic for these types of deviations are that they are not known and that it is not meaningful or possible to introduce barriers specifically to protect against these types of deviations. The best way of protecting against this is a robust design, with ample safety margins and a "defense-in-depth" strategy. Preparing a BBD will however not be of much meaning for this type of deviations.	
Example of inherent design error • *E.1 Design related failures:*	
Operational mode when failure is introduced During start-up, shutdown or normal production	
Operational mode at time of release During start-up, shutdown or normal production	
Barrier functions: No BBD is developed	***Barrier systems*** No BBD is developed
Assumptions	

4.3.6 F. External events

Table 21 BBD description for initiating event "F External events"

Initiating event F. External events	
General description In the release scenario report, "External events" is also identified as one group of scenarios. However, as pointed out in the report, these are not process related as such and in order to prevent release due to these causes, one needs to look at other types of operations than those related to the process system as such. No BBD has therefore been prepared.	
Example of external events • *F.1 Impact form falling object* • *F.2: Impact from bumping collision*	
Operational mode when failure is introduced Most likely during maintenance due to lifting restrictions during normal production	
Operational mode at time of release During start-up after maintenance	
Barrier functions No BBD is developed	***Barrier systems*** No BBD is developed
Assumptions	

5. Modeling the performance of safety barriers

5.1 Introduction

Fault trees have been developed for every barrier system. Based on the presentation and discussion in Section 4.3, fault trees have only been developed for the following Barrier Block Diagrams:

A Technical degradation of system
- Degradation beyond acceptable limit identified during CM/inspection
- Degradation beyond acceptable limit identified during PM

B Human intervention introducing latent error

For "Process Disturbance", fault trees have not been developed. The barrier systems relevant for these Initiating Events are all technical systems, which require dedicated modeling of each individual system. Generic fault trees are therefore not relevant to develop.

5.2 A Technical degradation of system

5.2.1 Prevent degradation beyond acceptable limit - PM

5.2.1.1 Preventive Maintenance (PM)

Preventive Maintenance (PM): Planned preventive maintenance operations in accordance with a scheduled PM program.

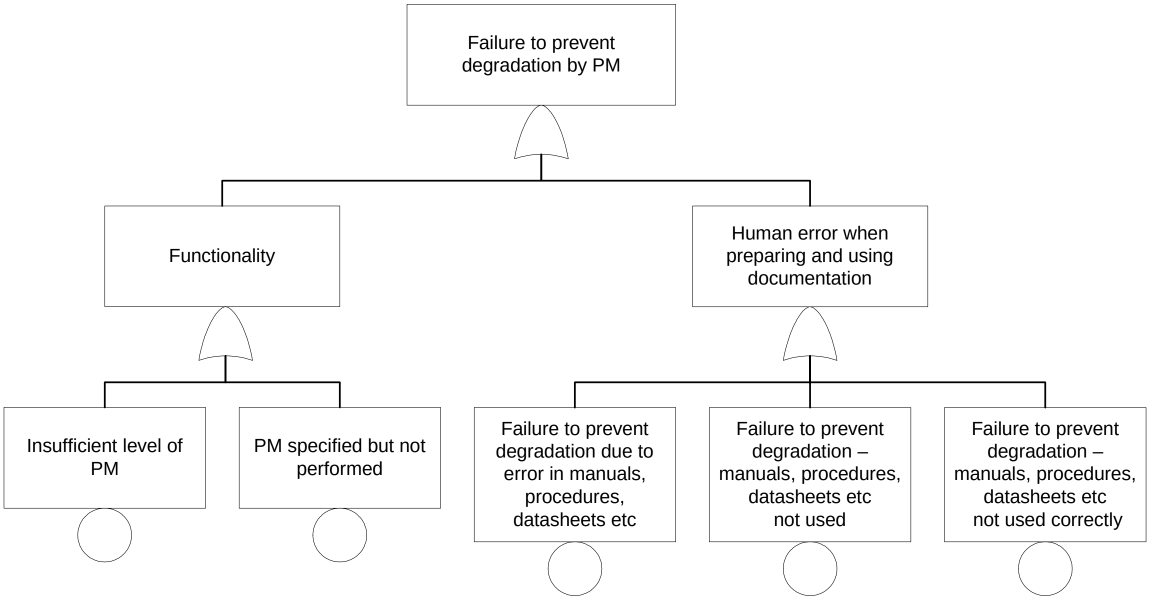


Figure 16 **Fault tree for the barrier system "PM"**

- **Functionality**: This box is covering the following factors:
    - The level of PM. PM will be performed based on PM program with predefined intervals, e.g. once every 3rd month. This means that there is a probability that degradation is not prevented even the PM program is followed.

  - PM specified but not performed.
- **Human error**: When planning and doing PM different type of documentation may be required/ used, e.g. instruction manuals, work procedures and datasheets. The barrier function "Detect degradation beyond acceptable limit" may fail due to human error:
  - Failure introduced in relevant documentation, and hence this may e.g. lead to wrong analysis of the inspection results.
  - Relevant and necessary documents not used. E.g. the operator may believe that he is familiar with the procedures and this type of analysis and fails to use the documentation.
  - Relevant documentation is used, but the operator fails to use it correctly because e.g. he may be disturbed (e.g. "errors of omission").

5.2.2 Detect release <0.1 kg/s - Area based leak search

Area based leak search: Dedicated leak search (not detection by randomly passing through the process module) to detect minor releases before they develop into significant leaks.

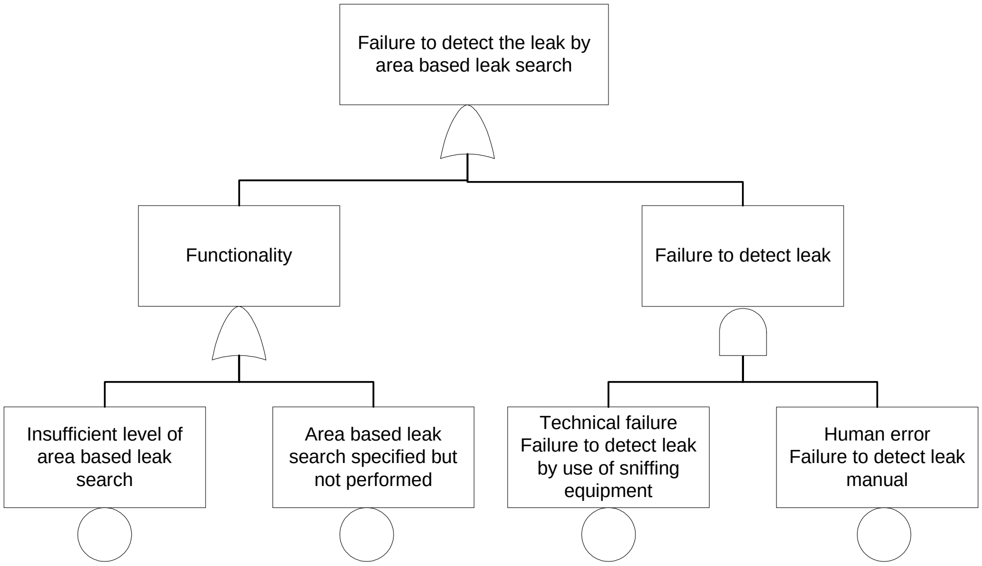


Figure 17 Fault tree for the barrier system "Area based leak search"

- **Functionality**: This box is covering the following factors:
  - The level of dedicated leak search.
  - Area based leak search not specified.
- **Failure to detect leak**: Sniffing equipment (detector) may be used. Even though the equipment is used correctly and in accordance with procedures and technical descriptions, there may be some technical failure with the equipment. The operator performing the leak search may also detect the leak.

5.2.3 Detect degradation beyond acceptable limit

5.2.3.1 Condition Monitoring

Condition monitoring: Monitoring of equipment to detect potential corrosion/erosion/fatigue. This will typically cover situation with continuous monitoring, as opposed to "Inspection", which is performed at defined intervals, often many months or years apart.

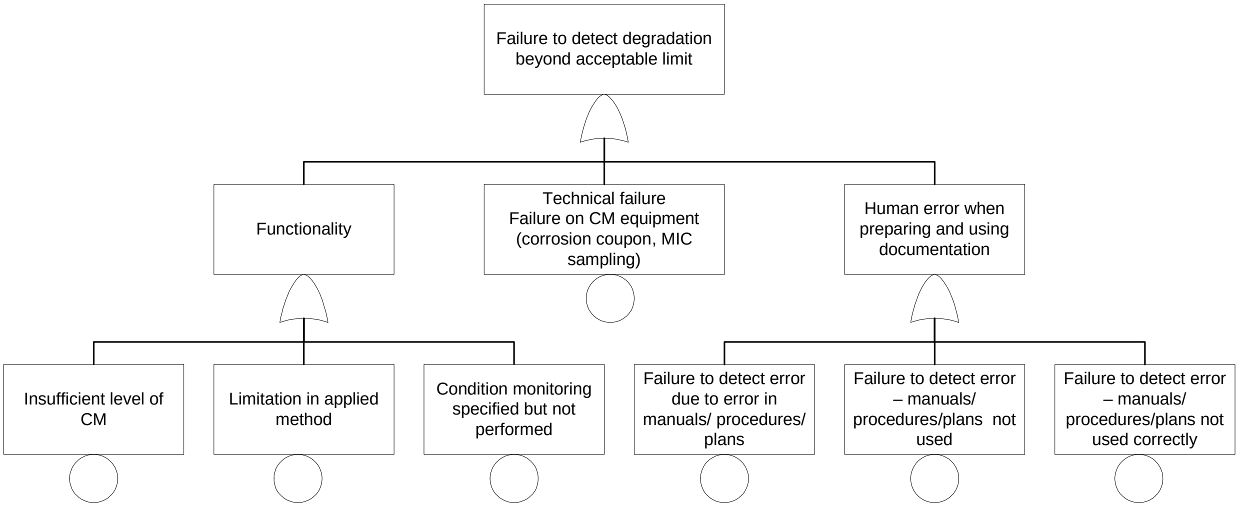


Figure 18 Fault tree for the barrier system "Condition monitoring"

- **Functionality**: This box is covering the following factors:
    - The level of CM. The CM programs will cover only a few points in a process system. This means that there is a probability that degradation is undetected, even when using CM.
    - Choice of CM method. The probability of detection of corrosion is dependent on the choice of method.
    - CM specified but not performed.
- **Technical failure**: Different types of CM tools may be used, e.g. corrosion coupons, MIC sampling, sand monitoring equipment etc. Even if the tools are used correctly and in accordance with procedures and technical descriptions, there may be some technical failure with the tools.
- **Human error**: When planning and doing condition monitoring, different types of documentation may be required/used, e.g. instruction manuals, work procedures and inspection plans. The barrier function "Detect degradation beyond acceptable limit" may fail due to human error:
    - Failure introduced in relevant documentation, and hence this may e.g. lead to wrong interpretation of the CM results.
    - Relevant and necessary documents not used. E.g. the operator may believe that he is familiar with the procedures and this type of analysis and fails to use the documentation.
    - Relevant documentation is used, but the operator fails to use it correctly because e.g. he may be disturbed (e.g. "errors of omission").

5.2.3.2 Inspection

Inspection: Inspection /NDT program to detect potential corrosion /erosion.

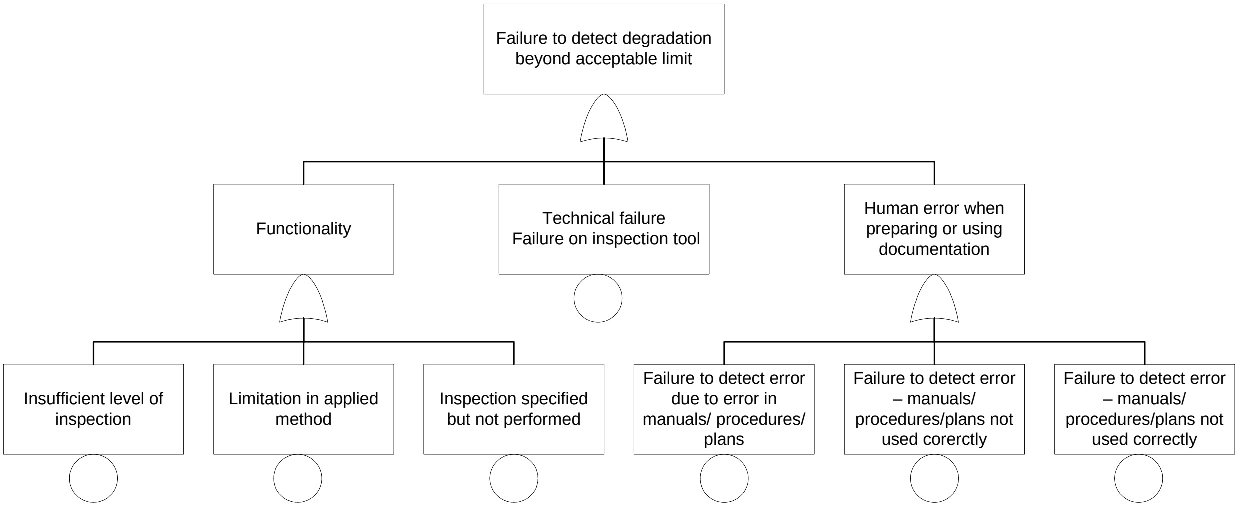


Figure 19 Fault tree for the barrier system ”Inspection”

- **Functionality**: This box is covering the following factors:
  - The level of inspection. The inspection plans will only cover a few points in a process system. This means that there is a probability that degradation is undetected, even the inspection plans are followed.
  - Choice of inspection method. The probability of detection of corrosion is dependant on the choice of method.
  - Inspection specified but not performed.
- **Technical failure**: Different type of inspection tools may be used, e.g. X-ray. Even though the tools are used correctly and in accordance with procedures and technical descriptions, there may be some technical failure with the tools.
- **Human error**: When planning and doing inspection different type of documentation may be required/ used, e.g. instruction manuals, work procedures and inspection plans. The barrier function “Detect degradation beyond acceptable limit” may fail due to human error:
  - Failure introduced in relevant documentation, and hence this may e.g. lead to wrong analysis of the inspection results.
  - Relevant and necessary documents not used. E.g. the operator may believe that he is familiar with the procedures and this type of analysis and fails to use the documentation.
  - Relevant documentation is used, but the operator fails to use it correctly because e.g. he may be disturbed (e.g. “errors of omission”).

5.2.3.3 Detect release <0.1 kg/s - Area based leak search

This is identical to the fault tree shown in Section 5.2.2 above and is therefore not repeated.

5.3 B. Human intervention introducing latent error

5.3.1 Detect latent error

5.3.1.1 Self control

Self control: Formal self-control or use of checklists

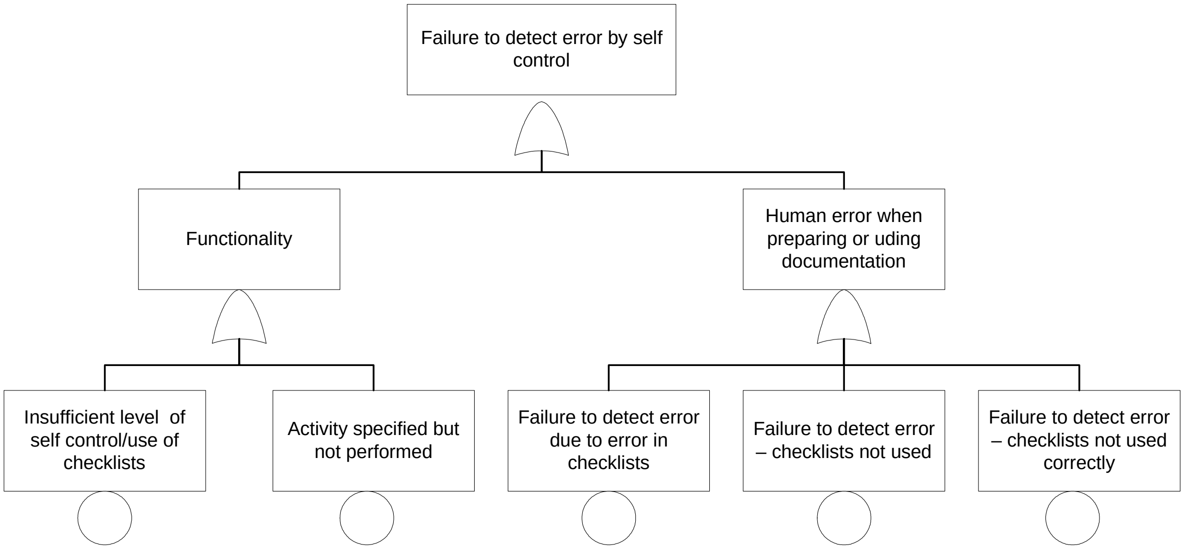


Figure 20 Fault tree for the barrier system "Self control"

- **Functionality**: This box is covering the following factors:
  - The level of self control/ use of checklists. Self control will be performed based on procedures or work practice, dependant on the activity. This means that there is a probability that latent errors are not identified.
  - Self check/ use of checklists specified but not performed.
- **Human error**: When planning and doing the activity different type of documentation may be required/ used, e.g. checklists. The barrier function "Detect latent error" may fail due to human error:
  - Failure introduced in relevant documentation, and hence this may e.g. lead to wrong analysis of the inspection results.
  - Relevant and necessary documents not used. E.g. the operator may believe that he is familiar with the procedures and this type of analysis and fails to use the documentation.
  - Relevant documentation is used, but the operator fails to use it correctly because e.g. he may be disturbed (e.g. "errors of omission").

5.3.1.2 3rd party control

3rd party control: Independent control (by other person) of work

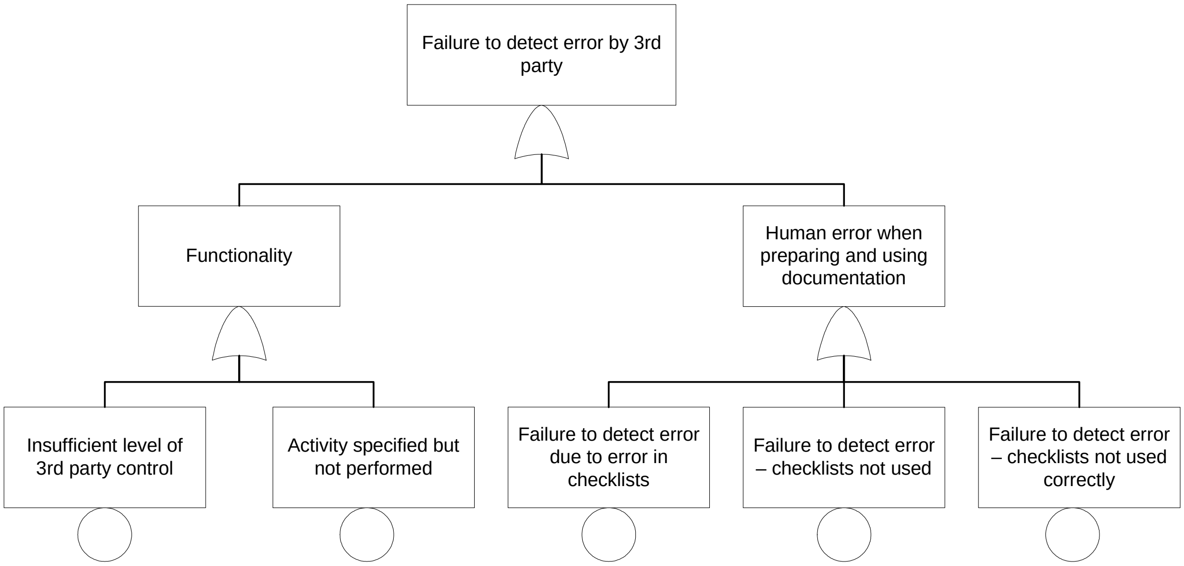


Figure 21 Fault tree for the barrier system "3rd party control"

- **Functionality**: This box is covering the following factors:
    - The level of 3rd party control. 3rd party control will be performed based on procedures or work practice, dependant on the activity. This means that there is a probability that latent errors are not identified.
    - 3rd party control specified but not performed.
- **Human error**: When planning and doing the activity different type of documentation may be required/ used, e.g. checklists. The barrier function "Detect latent error" may fail due to human error:
    - Failure introduced in relevant documentation, and hence this may e.g. lead to wrong analysis of the inspection results.
    - Relevant and necessary documents not used. E.g. the operator may believe that he is familiar with the procedures and this type of analysis and fails to use the documentation.
    - Relevant documentation is used, but the operator fails to use it correctly because e.g. he may be disturbed (e.g. "errors of omission").

5.3.1.3 Verification of system status

Verify system status: The barrier system "Verify system status" could either be verification in means of leak test or verification of depressurized system.

Leak test

Leak test may be carried out in different ways, e.g. by use of Nitrogen or use of manual detectors. When planning and doing the leak test different type of documentation may be required/ used, e.g. checklists, blinding and isolation plans.

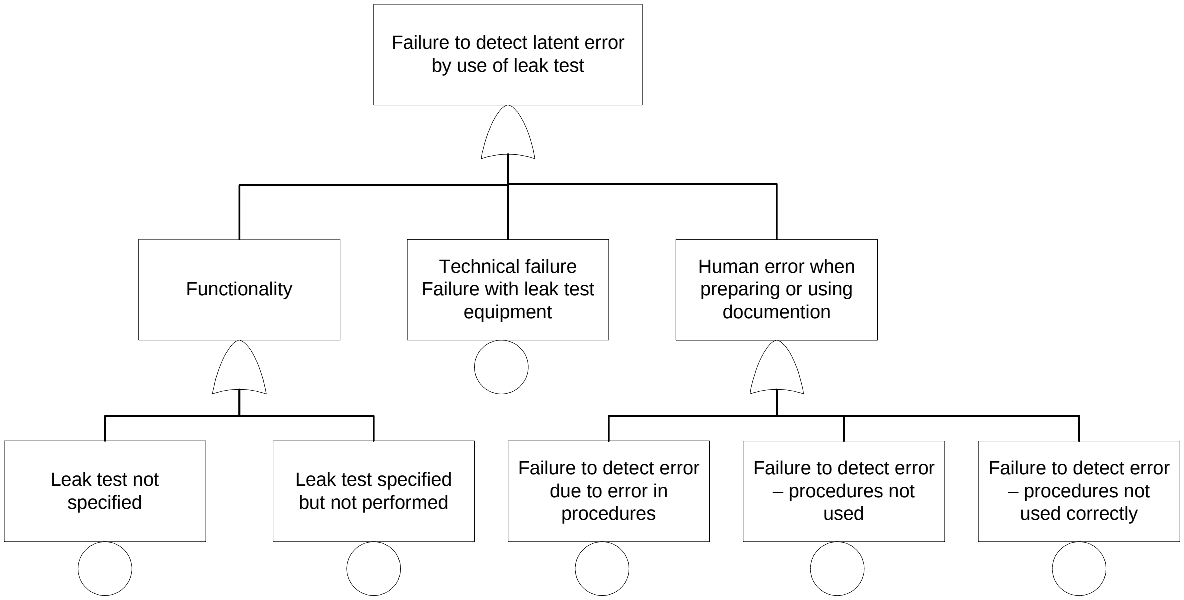


Figure 22 Fault tree for the barrier system "verification of system status – by use of leak test"

- **Functionality**: This box is covering the following factors:
    - Leak test not specified.
    - Leak test specified but not performed.
- **Technical failure**: Different type of mechanical or instrumented equipment may be used when doing the leak test. Even though the equipment are used correctly and in accordance with procedures and technical descriptions, there may be some technical failure with the equipment.
- **Human error**: When planning and doing leak tests different type of documentation may be required/ used, e.g. instruction manuals and work procedures. The barrier function "Detect latent error" may fail due to human error:
    - Failure introduced in relevant documentation, and hence this may e.g. lead to wrong analysis of the inspection results.
    - Relevant and necessary documents not used. E.g. the operator may believe that he is familiar with the procedures and this type of analysis and fails to use the documentation.
    - Relevant documentation is used, but the operator fails to use it correctly because e.g. he may be disturbed (e.g. "errors of omission").

Verification of depressurized system

Verification of depressurized system may be carried out using different type of mechanical or instrumented equipment. When planning and doing the verification different type of documentation may be required/ used, e.g. procedures and checklists.

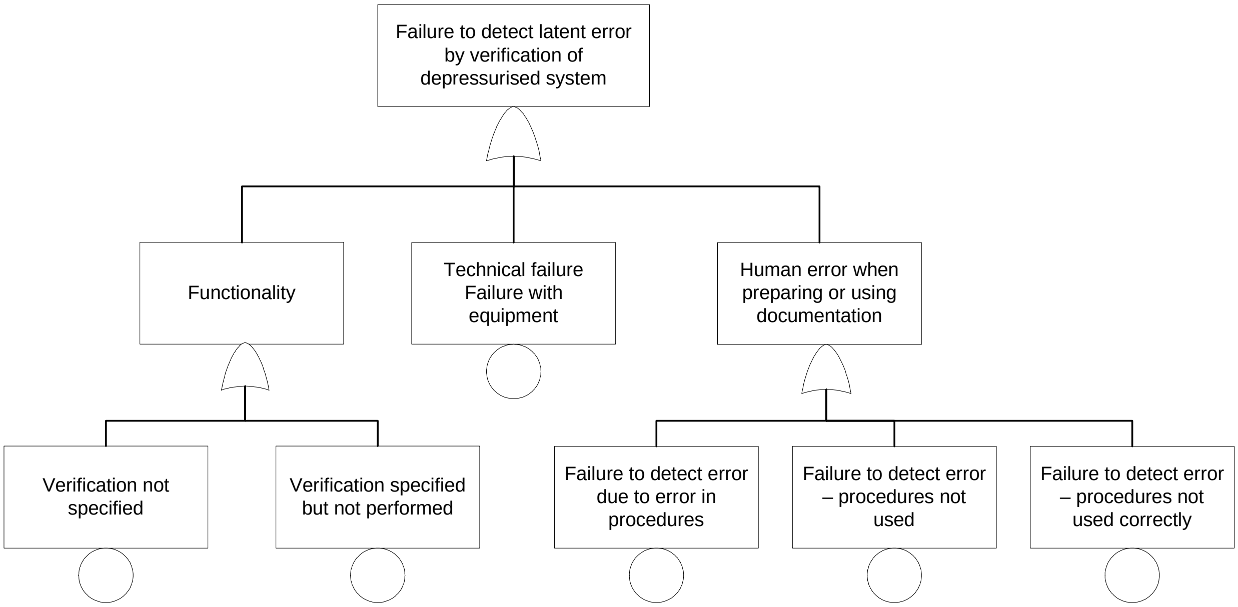


Figure 23 **Fault tree for the barrier system "verification of system status – depressurized system"**

- **Functionality**: This box is covering the following factors:
    - Verification of depressurized equipment not specified.
    - Verification of depressurized equipment specified but not performed.
- **Technical failure**: Different type of mechanical or instrumented equipment may be used when doing the verification. Even though the equipment is used correctly and in accordance with procedures and technical descriptions, there may be some technical failure with the equipment.
- **Human error**: When planning and doing the verification activity different type of documentation may be required/ used, e.g. instruction manuals and work procedures. The barrier function "Detect latent error" may fail due to human error:
    - Failure introduced in relevant documentation, and hence this may e.g. lead to wrong analysis of the inspection results.
    - Relevant and necessary documents not used. E.g. the operator may believe that he is familiar with the procedures and this type of analysis and fails to use the documentation.
    - Relevant documentation is used, but the operator fails to use it correctly because e.g. he may be disturbed (e.g. "errors of omission").

6. Risk influence diagrams

As described in section 2.2.5, the purpose of the risk influence diagrams is to identify and illustrate the RIFs influencing the probabilities or frequencies of the occurrences of the basic events in the fault trees. The basis for identification of RIFs is the generic framework for identification of RIFs shown in Figure 4.

The risk influence diagrams developed in the case studies are shown in Appendix 1. An example on a risk influence diagram for an initiating event is shown in Figure 24. Further, an example on a risk influence diagram for a basic event in a fault tree is shown in Figure 25.

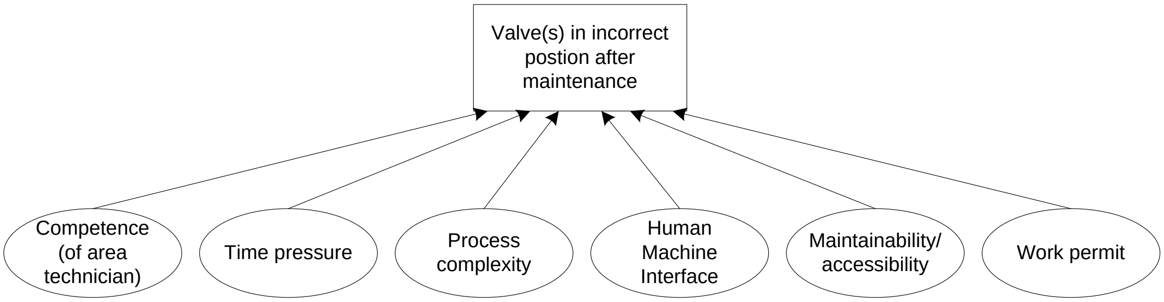


Figure 24 **Influence diagram for the initiating event.**

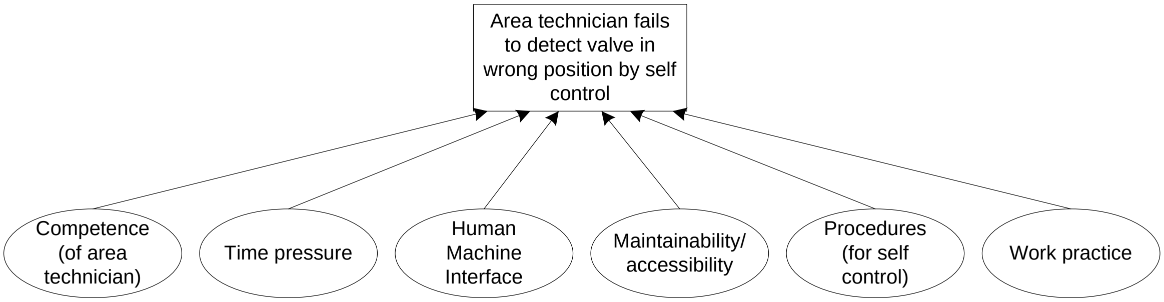


Figure 25 **Influence diagram for barrier 1 – basic event 3.**

7. Frequency and Probability data

7.1 Leak frequency

7.1.1 Data basis

The basis for establishing leak frequency distributions has been gas leaks that have been reported to PSA. Most of the leaks have also been investigated. The period that is covered is 2002 to 2005, with some few leaks from the period before that.

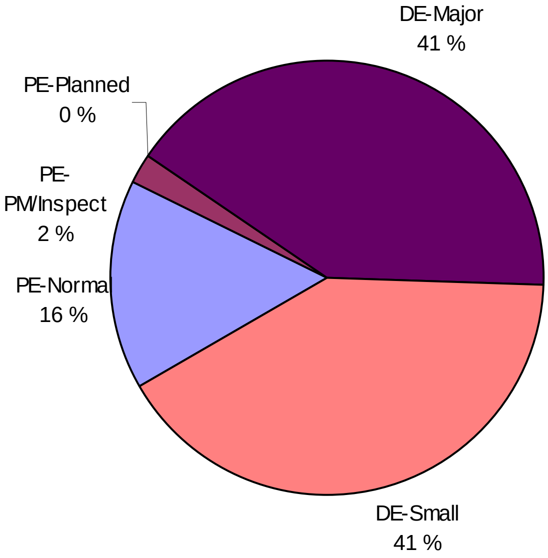
A total of 94 leaks have been classified. Reports on more leaks have been available, but not all are relevant (e.g. subsea leaks, drilling related leaks) and there are also some cases where it has not been possible to classify the leaks.

In some cases, the classification has been difficult due to unclear descriptions in the investigation reports, lack of details etc. In order to minimize the possibility of erroneous classification, some of the reports have been classified by two persons independently and compared afterwards.

Summaries of the leaks have been prepared, covering a brief description of the leak, the direct cause, where it has occurred and the leak size. In addition, a classification is provided, with regard to the type of operation that caused the leak and the type of Initiating Event that caused the leak.

7.1.2 Leak distribution

The following figure shows a breakdown of the leaks on the type of operation that was the cause of the leak.



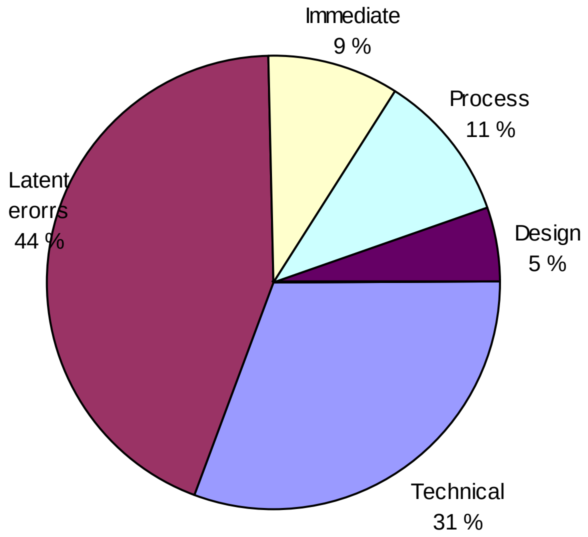
Codes:
PE-Normal – Pressurized equipment – normal operations
PE-PM/Inspect – Pressurized equipment – Preventive Maintenance/Inspection operations
PE-Planned – Pressurized equipment – Planned opening of equipment
DE-Major – Depressurized equipment – Major unit
DE-Small – Depressurized equipment – Small unit

Figure 26 Breakdown of leaks on type of operation causing the leak

No leaks have been classified as occurring during the other work operations that have been defined (External work on process equipment, Other work in the area).

The figure shows that there is roughly an equal split between leaks caused by work on pressurized equipment and depressurized equipment. With regard to work on pressurized equipment, virtually all leaks have been caused during normal operations. For depressurized leaks, there is an equal split between work on major units and small units.

The other major classification is related to what initiating events have caused the leaks. The breakdown of this is shown in the following figure.



Codes:
Manual intervention (PM & FV)

- ‘Immediate’ is a release which occurs immediately during intervention
- ‘Latent errors’ are releases that result from latent errors during interventions, and that occur after some time

‘Process’ are leaks caused by process control errors or problems

‘Design’ are leaks caused by design errors

‘Technical’ are leaks caused by technical failures

Figure 27 Breakdown of leaks on type of initiating event

The clearly most important initiating events for leaks are latent errors introduced during maintenance or other intervention in the equipment and technical failures. Together, these two causes contribute 75% of the total number of leaks. Immediate release, Process upsets and Design errors are all much less important contributors. However, it is noted that Latent errors and Immediate release, which both are related to intervention in the process equipment, together comprise more than 50% of the total. Further breakdown of the two most important causes are shown in the following. The breakdown of technical failures is shown on the left and the breakdown of latent errors on the right.

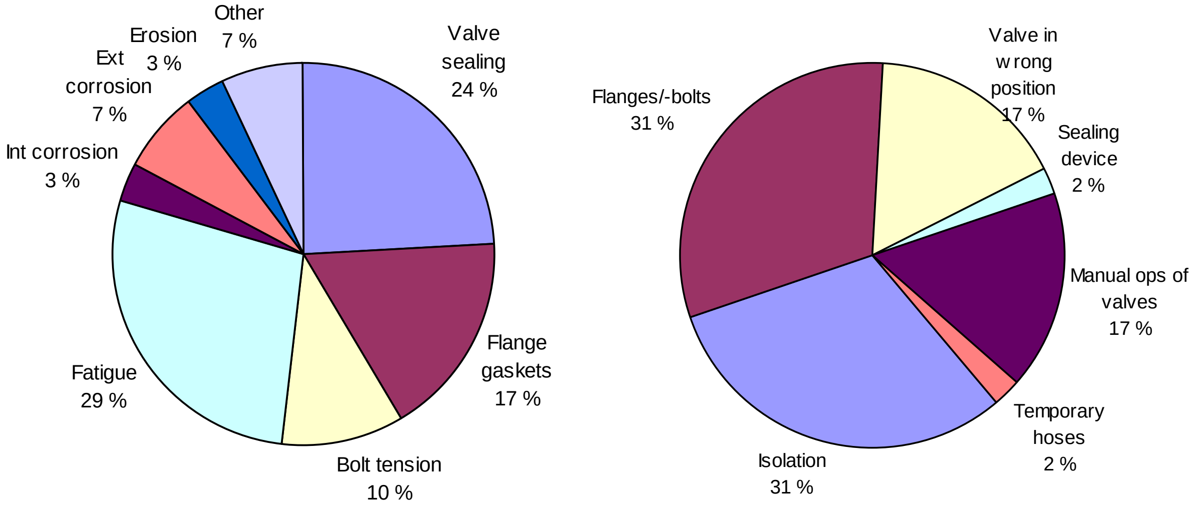


Figure 28 **Breakdown of technical failures (left) and latent errors (right)**

The breakdown of technical failures shows that fatigue is the most important single cause of leaks. Problems with valve sealing and flange gaskets then follow as the most common causes of leaks. Loss of bolt tensioning is also related to flanges, and together these three contribute 27% of the total.

One of the most common of the latent errors is also related to flanges/bolts, due to errors in fitting/installation. This comprises 31% of the total number of leaks in this category. Further, errors in blinding/isolation also comprise the same proportion of the total number of leaks. It is noted that “Valve in wrong position”, “Manual operation of valves” and “Isolation” all are related to valves and together, these three categories comprise nearly two thirds of the total number of leaks.

In addition to these breakdowns, some further analysis has also been undertaken to investigate if there are differences in the breakdown depending on the circumstances. A split between fixed and floating installations has been made and further, only leaks above 1 kg/s have been considered. The resulting distributions are compared in the figure below.

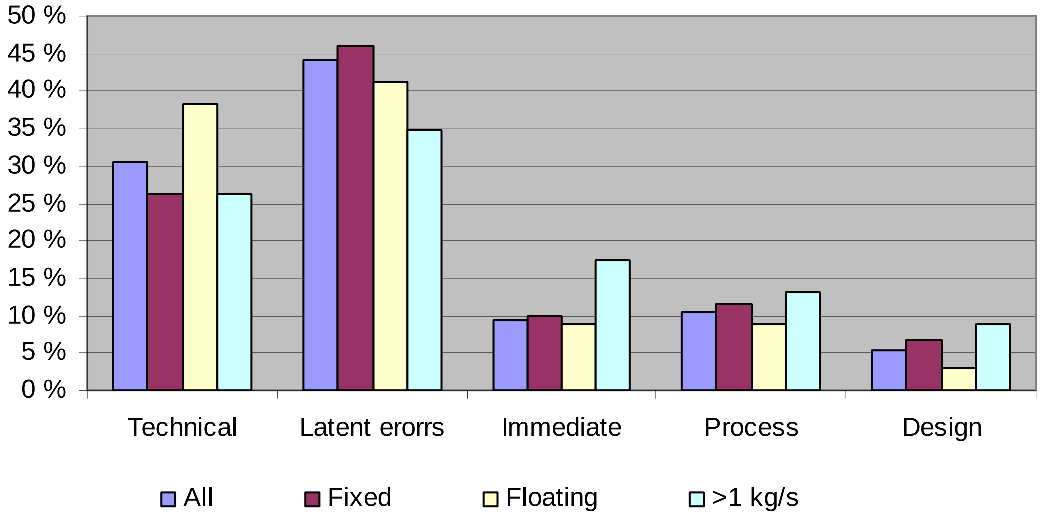


Figure 29 Comparison of breakdown of Initiating Events for different circumstances

The most striking feature of this figure is probably the small differences between the different comparisons. It is noted, however, that the proportion of leaks due to technical failure is higher on floating than on fixed installations. The number of leaks due to technical failure of flange gaskets is higher on floating than on fixed installations and this may possible be due to the motions.

A difference is also seen for "Immediate release" and releases larger than 1 kg/s, but due to the low number of leaks in this category the difference is probably not statistically significant. On the other hand, there may also be a logical explanation for this since the "immediate releases" (e.g. where someone accidentally opens a wrong valve and thus causes a release) are likely to be on average larger than leaks from e.g. flanges, technical failures etc.

7.2 Fault tree data

In order to prepare a basis for quantifying the effects of human error, a number of data sources have been reviewed and compared. The purpose of the literature search has been to establish a set of recommended data which can be applied in the modeling of barriers.

The following data sources have been reviewed:

- Swain and Guttman [15]
- Reason [16]
- Blackman and Gertman [17]
- Kirwan I [18]
- Kirwan II [19]

The total number of available data sources is rather limited, and the textbooks and reports that have been subject to review vary with respect to industrial background and scope. In addition, some of the sources are rather old (particularly [15]).Still, it is found plausible to base the fault tree data on the listed sources. The reasons for this are mainly the following:

- The purpose of the review is to establish recommended or "typical" values, or intervals of recommended values. It is not assumed that the general modeling of probability of human error can be represented by accurate values; hence it is found appropriate to base the recommended data on a compilation of a variety of data sources.
- The data listings presenting human error probability (HEP) concentrate on the fundamentals of human behavior. Hence, it is assumed that the topics of investigation are not subject to significant fluctuations over time, and that data collected over a period of time will still have relevance in human reliability modeling today.

The individual HEP values which have been assigned to the failure descriptions in the following sections are not based on a single source. Instead, information from the sources listed above is combined in order to establish "typical" HEP values. A problem related to assigning HEP values is that the generic data is not necessarily representative with respect to failure description, environment, competence etc. Therefore, the sources have been combined in a general manner, keeping the following principles in mind:

- The HEP decreases with increasing competence.
- The HEP decreases with increasing level of feed-back from the system.

This implies that the HEP values are assigned based on the premises that e.g. fitting of flanges and bolts is associated with lower failure probability than valve positioning after maintenance. A skilled operator will be able to judge whether a bolt is correctly tightened (based on experience and reading from a torque wrench), whereas valve positioning based on a list will not necessarily give the same direct "feed-back" as to whether the valve is correctly positioned. The same principle applies also for the other failure descriptions.

A comprehensive listing of the basis for the recommended HEP values is included in Appendix 2.

7.2.1 Initiating Event Data

As described earlier, some of the initiating events are associated with human error. This applies for the events which are categorized within the following groups:

B: Human intervention introducing latent error
C: Human intervention causing immediate release

Based on the data review, a set of recommended HEP values have been defined for the initiating events. These values are presented in Table 22 .

Table 22 Recommended Human Error Probability Assignments to be used for Initiating Events

Initiating Event	**Human Error Description**	**Recommended HEP Assignment**		
		Lower Assignment	**Upper Assignment**	**Average**
B. Human intervention introducing latent error	B.1 Incorrect blinding/isolation	$1 \cdot 10^{-2}$	$1 \cdot 10^{-1}$	$5 \cdot 10^{-2}$
	B.2 Incorrect fitting of flanges or bolts	$1 \cdot 10^{-3}$	$1 \cdot 10^{-2}$	$5 \cdot 10^{-3}$
	B.3 Valve(s) in incorrect position after maintenance	$1 \cdot 10^{-2}$	$1 \cdot 10^{-1}$	$5 \cdot 10^{-2}$
	B.4 Erroneous choice/installation of sealing device	$5 \cdot 10^{-3}$	$5 \cdot 10^{-2}$	$3 \cdot 10^{-2}$
	B.5 Maloperation of valve(s) during manual operation	$1 \cdot 10^{-2}$	$1 \cdot 10^{-1}$	$5 \cdot 10^{-2}$
	B.6 Maloperation of temporary hoses	$1 \cdot 10^{-2}$	$1 \cdot 10^{-1}$	$5 \cdot 10^{-2}$
C. Human intervention causing immediate release	C.2 Maloperation of valve(s) during manual operation:	$1 \cdot 10^{-2}$	$1 \cdot 10^{-1}$	$5 \cdot 10^{-2}$

7.2.2 Fault tree data

The fault trees related to barriers presented in Section 5 include elements of human error, and a data set has been prepared to assign the probability of human error. The recommended probability figures are related to the human error descriptions given in the fault trees. In Table 23 recommended HEP values are presented for failures which are related to initiating events belonging to the groups *A* and *B*.

Table 23 Recommended Human Error Probability Assignments to be used for Modeling of Barrier Fault Trees

Initiating Event	**Human Error Description**	**Recommended HEP Assignment**		
		Lower Assignment	**Upper Assignment**	**Average**
A. Technical degradation of system	Failure to prevent degradation – manuals, procedures, datasheets etc. not used	$1 \cdot 10^{-3}$	$1 \cdot 10^{-2}$	$5 \cdot 10^{-3}$
	Failure to prevent degradation – manuals, procedures, datasheets etc. not used correctly	$1 \cdot 10^{-2}$	$1 \cdot 10^{-1}$	$5 \cdot 10^{-2}$
	Failure to detect error – manuals, procedures, datasheets etc. not used	$1 \cdot 10^{-3}$	$1 \cdot 10^{-2}$	$5 \cdot 10^{-3}$
	Failure to detect error – manuals, procedures, datasheets etc. not used correctly	$1 \cdot 10^{-2}$	$1 \cdot 10^{-1}$	$5 \cdot 10^{-2}$
	Failure to detect leak manually	$5 \cdot 10^{-3}$	$5 \cdot 10^{-2}$	$3 \cdot 10^{-2}$
B. Human intervention introducing latent error	Failure to detect error – checklists not used	$1 \cdot 10^{-3}$	$1 \cdot 10^{-2}$	$5 \cdot 10^{-3}$
	Failure to detect error – checklists not used correctly	$2 \cdot 10^{-2}$	$2 \cdot 10^{-1}$	$1 \cdot 10^{-1}$
	Failure to detect error – procedures not used	$1 \cdot 10^{-3}$	$1 \cdot 10^{-2}$	$5 \cdot 10^{-3}$
	Failure to detect error – procedures not used correctly	$1 \cdot 10^{-2}$	$1 \cdot 10^{-1}$	$5 \cdot 10^{-2}$

8. RIF Weights

8.1 Overview over case studies performed

Case studies have been a major part of the BORA project in order to test the proposed methodology on specific problems and for different organizations.

One part of the case studies has been to obtain weights of the RIFs for the individual Basic Events. This has been done for all case studies through work meetings, involving operating personnel and BORA project personnel. The same list of RIFs has been applied for all case studies. However, different approaches have been used when selecting the most important RIFs, since the case studies have been worked out at different stages in the development phase. In addition different Basic Events have been used for the same initiating event.

In the following section the weights of the RIFs for the individual Basic Events from 3 case studies are presented.

8.1.1 Case study 1

Case study 1 is the first case study that has been performed and this was done as part of the model development phase.

Relevant cases were proposed by the operator based on their activity and experience with the operation of the platform. The cases that have been studied are related to flowline inspection, which is a frequently performed work operation on this installation. Flowline inspections are performed in order to reveal corrosion in the pipes, flanges and instrument fittings on the flowlines.

The quantification has been carried out for the following leak scenarios:

A5. Release due to internal corrosion
A6. Release due to external corrosion
B2. Release due incorrect fitting of flanges or bolts during maintenance
B3. Release due to valve(s) in incorrect position after maintenance

RIF selection approach for case study 1:
The weights of the RIFs for the individual Basic Events were obtained through work meetings. In practice, this was done as follows:

- The meeting participants were asked to identify the RIF having highest influence using the standard RIF list established for BORA.
- This RIF was given the weight 10
- Other relevant RIFS were identified and given lower weights, on the scale: 2-4-6-8. No maximum number of RIFs were set.
- This process was repeated for all Basic Events.

8.1.2 Case study 2

Case study 2 was also performed as a part of the model development phase.

Relevant cases have been proposed by the platform management based on their activity and experience with the operation of the platform.

- The first scenario being considered is based on a shutdown, when one of the tasks that were performed was cleaning and minor modifications to the separators. This involved isolating the separators, opening them and doing internal cleaning. The release scenario that is being considered is related to the possibility that one (or more) valves are left in the wrong position after the work is completed and that a release occurs when production is started.
- The second scenario is also identified from a situation that occurred prior to the shutdown. A problem was then identified in relation to the pipeline compressors and it was concluded that it was necessary to perform maintenance. The specific scenario is however not seen in relation to the shutdown.

The quantification has been carried out for the following leak scenarios:

B1. Release due to incorrect blinding/isolation
B2. Release due to valve(s) in incorrect position after maintenance

RIF selection approach for case study 2:
Maximum 10 RIFs were selected for each event.

The weights of the RIFs for the individual Basic Events were obtained through work meetings. In practice, this was done as follows:

- A set of tables was prepared, showing a general list of RIFs and with a 6-point scale going from “High Importance” to “Not Applicable”. One table was established for each Basic Event.
- The meeting participants were asked to rate the importance (weight) of each RIF on the scale provided. This was done by each participant in the meeting on their own.
- The resulting weights were then compared and discussed until an agreement was reached on the weight that each RIF should have.
- This process was repeated for all Basic Events.
- The scale from “High” to “Not Applicable” was converted to a scale from 5 to 0.

8.1.3 Case study 3

Case study 3 has been performed as a part of the work with the generalisation report.

Relevant cases have been introduced by the BORA team in order to test the methodology on more initiating events.

Weights have been identified for the following leak scenarios:

B1. Release due to incorrect blinding/isolation
B2. Release due incorrect fitting of flanges or bolts during maintenance
B3. Release due to valve(s) in incorrect position after maintenance
B4. Release due to erroneous choice or installation of sealing device
B6. Release due to maloperation of temporary hoses
C1. Release due to break-down of isolation system during maintenance
C2. Release due to maloperation of valve(s) during manual operation
C3. Release due to work on equipment, not known to be pressurised

RIF selection approach for case study 3:
Maximum 10 RIFs are selected for each event.

The weights of the RIFs for the individual Basic Events were obtained through work meetings. In practice, this was done as follows:

- A set of tables was prepared, showing a general list of RIFs and with a 6-point scale going from “High Importance” to “Not Applicable”. One table was established for each Basic Event.
- The meeting participants were asked to rate the importance (weight) of each RIF on the scale provided. This was done by each participant in the meeting on their own.
- The resulting weights were then compared and discussed until an agreement was reached on the weight that each RIF should have.
- This process was repeated for all Basic Events.
- The scale from “High” to “Not Applicable” was converted to a scale from 5 to 0.

8.1.4 Summary of initiating events and case studies

An overview of the initiating events and case studies is presented in Table 24.

Table 24 Overview over Initiating Events and case studies

Initiating Event Type	**Initiating Events**	**Case study**		
		1	**2**	**3**
A. Technical degradation of system	1. Degradation of valve sealing			**X**
	2. Degradation of flange gasket			
	3. Loss of bolt tensioning			
	4. Fatigue			
	5. Internal corrosion	**X**		
	6. External corrosion	**X**		
	7. Erosion			
	8. Other causes			
B. Human intervention introduction latent error	1. Incorrect blinding/isolation		**X**	**X**
	2. Incorrect fitting of flanges or bolts during maintenance	**X**		**X**
	3. Valve(s) in incorrect position after maintenance	**X**	**X**	**X**
	4. Erroneous choice or installations of sealing device			**X**
	5. Maloperation of valve(s) during manual operation			
	6. Maloperation of temporary hoses.			
C. Human intervention causing immediate release	1. Break-down of isolation system during maintenance.			**X**
	2. Maloperation of valve(s) during manual operation			**X**
	3. Work on wrong equipment, not known to be pressurized			**X**

8.2 A1: Release due to degradation of valve sealing

8.2.1 Case study 3

Table 25 Risk Influencing factors and their weights for initiating and basic events related to A1, case study 3

		A1 Release due to degradation of valve sealing									
			B1 PM					B2 Area based leak search			
RIF group	RIF	IE	E1	E2	NA	NA	E5	E1	E2	E3	E4
Personnel	Competence						0.12				0.10
	Working load/stress						0.08				0.03
	Work environment						0.12				0.10
	Fatigue						0.16				0.07
Task	Methodology							0.42			
	Task supervision										
	Task complexity										
	Time pressure			0.19					0.33		0.10
	Tools									1.00	
	Spares										
Technical system	Equipment design	0.25									
	Material properties	0.33									
	Process complexity						0.08	0.25			0.13
	HMI (Human Machine Interface)						0.08				
	Maintainability/ accessibility			0.19			0.12				0.13
	System feedback										
	Technical condition	0.42									0.10
Administrative control	Procedures										
	Work permit										
	Disposable work descriptions										
	Documentation										
Organisational factors	Programs		1.00					0.33			
	Work practice			0.14			0.12		0.33		0.10
	Supervision			0.24			0.12		0.33		
	Communication										
	Tidiness and cleaning										0.13
	Support systems			0.24							
	Acceptance criteria										
	Simultaneous activities										
	Management of changes										
		1	1	1			1	1	1	1	1

[1)] For definition of the Es (Basic events) in the table above see Section 5.

8.3 B1: Incorrect blinding/isolation

8.3.1 Work on small equipment unit

8.3.1.1 Case study 3

Table 26 Risk Influencing factors and their weights for initiating and basic events related to B1, case study 3

		B1 Release due to incorrect blinding/isolation										
			B1 Self control of work					B2 3rd party control of work				
RIF group	RIF	IE	E1	E2	E3	E4	E5	E1	E2	E3	E4	E5
Personnel	Competence	0.11			0.19	0.13	0.16			0.19	0.13	0.16
	Working load/stress						0.16					0.16
	Work environment											
	Fatigue						0.20					0.20
Task	Methodology											
	Task supervision											
	Task complexity	0.06			0.07	0.25	0.04			0.07	0.25	0.04
	Time pressure	0.06		0.11	0.07	0.06			0.09	0.07	0.06	
	Tools											
	Spares											
Technical system	Equipment design											
	Material properties											
	Process complexity	0.11			0.15	0.06	0.08			0.15	0.06	0.08
	HMI (Human Machine Interface)	0.09					0.20					0.20
	Maintainability/ accessibility	0.06					0.12					0.12
	System feedback											
	Technical condition											
Administrative control	Procedures											
	Work permit	0.06										
	Disposable work descriptions	0.11										
	Documentation	0.14			0.19					0.19		
Organisational factors	Programs		1.00					1.00				
	Work practice	0.11		0.56	0.15	0.31	0.04		0.45	0.15	0.31	0.04
	Supervision			0.33	0.11	0.19			0.27	0.11	0.19	
	Communication	0.09			0.07				0.18	0.07		
	Tidiness and cleaning											
	Support systems											
	Acceptance criteria											
	Simultaneous activities											
	Management of changes											
		1	1	1	1	1	1	1	1	1	1	1

1) For definition of the Es (Basic events) in the table above see Section 5.

8.3.2 Work on major equipment unit

8.3.2.1 Case study 3

Table 27 Risk Influencing factors and their weights for initiating and basic events related to B1, case study 3

RIF group	RIF	B1 Release due to incorrect blinding/isolation										
			B1 Self control of work					B2 3rd party control of work				
		IE	E1	E2	E3	E4	E5	E1	E2	E3	E4	E5
Personnel	Competence	0.10			0.16	0.13	0.14			0.16	0.13	0.14
	Working load/stress						0.14					0.14
	Work environment											
	Fatigue						0.17					0.17
Task	Methodology											
	Task supervision											
	Task complexity	0.10			0.09	0.25	0.03			0.09	0.25	0.03
	Time pressure	0.05		0.18	0.09	0.06			0.09	0.09	0.06	
	Tools											
	Spares											
Technical system	Equipment design											
	Material properties											
	Process complexity	0.10			0.13	0.06	0.07			0.13	0.06	0.07
	HMI (Human Machine Interface)	0.08					0.17					0.17
	Maintainability/ accessibility	0.05					0.10					0.10
	System feedback											
	Technical condition											
Administrative control	Procedures											
	Work permit	0.05										
	Disposable work descriptions	0.13										
	Documentation	0.13			0.16					0.16		
Organisational factors	Programs		1.00					1.00				
	Work practice	0.10		0.45	0.13	0.31	0.03		0.45	0.13	0.31	0.03
	Supervision			0.36	0.13	0.19			0.27	0.13	0.19	
	Communication	0.10			0.13		0.14		0.18	0.13		0.14
	Tidiness and cleaning											
	Support systems											
	Acceptance criteria											
	Simultaneous activities											
	Management of changes											
		1	1	1	1	1	1	1	1	1	1	1

[1] For definition of the Es (Basic events) in the table above see Section 5.

8.4 B2: Incorrect fitting of flanges or bolts during maintenance

8.4.1 Case study 1

Table 28 Risk Influencing factors and their weights for initiating and basic events related to B2, case study 1

		Release due to incorrect fitting of flanges or bolts during maintenance									
			B1 Self control			B2 3rd party control			B3 Leak test		
RIF group	RIF	IE	E1	E2	E3	E1	E2	E3	E1	E2	E3
Personnel	Competence	0.33			0.33			0.38			0.42
	Working load/stress										
	Work environment										
	Fatigue										
Task	Methodology										0.08
	Task supervision										
	Task complexity	0.33									
	Time pressure	0.20		0.38	0.20		0.38	0.15		0.38	
	Tools										
	Spares										
Technical system	Equipment design										
	Material properties										
	Process complexity	0.07									
	HMI (Human Machine Interface)				0.07			0.08			
	Maintainability/ accessibility	0.07			0.07			0.08			
	System feedback										
	Technical condition										
Administrative control	Procedures				0.33			0.15			0.08
	Work permit			0.23			0.23	0.15			
	Disposable work descriptions									0.23	
	Documentation										
Organisational factors	Programs		1.00			1.00			1.00		
	Work practice			0.38			0.38			0.38	
	Supervision										
	Communication										0.42
	Tidiness and cleaning										
	Support systems										
	Acceptance criteria										
	Simultaneous activities										
	Management of changes										
		1	1	1	1	1	1	1	1	1	1

[1] For definition of the Es (Basic events) in the table above see Section 5.

8.5 B3: Valve(s) in incorrect position after maintenance

8.5.1 Case study 1

Table 29 Risk Influencing factors and their weights for initiating and basic events related to B3, case study 1

		Release due to valve(s) in incorrect position after maintenance						
	RIF		B1 Self control			B2 3rd party control		
RIF group		IE	E1	E2	E3	E1	E2	E3
Personnel	Competence	0.36			0.33			0.33
	Working load/stress							
	Work environment							
	Fatigue							
Task	Methodology							
	Task supervision							
	Task complexity							
	Time pressure	0.36		0.38	0.33		0.38	0.33
	Tools							
	Spares							
Technical system	Equipment design							
	Material properties							
	Process complexity	0.07						
	HMI (Human Machine Interface)	0.07			0.07			0.07
	Maintainability/ accessibility	0.07			0.07			0.07
	System feedback							
	Technical condition							
Administrative control	Procedures				0.07			0.07
	Work permit	0.07		0.23	0.13		0.23	0.13
	Disposable work descriptions							
	Documentation							
Organisational factors	Programs		1.00			1.00		
	Work practice			0.38			0.38	
	Supervision							
	Communication							
	Tidiness and cleaning							
	Support systems							
	Acceptance criteria							
	Simultaneous activities							
	Management of changes							
		1	1	1	1	1	1	1

8.5.2 Case study 2

Table 30 Risk Influencing factors and their weights for initiating and basic events related to B3, case study 2

		Release due to valve in wrong position after maintenance										
			B1 Self control of work					B2 3rd party control of work				
RIF group	RIF	IE	E1	E2	E3	E4	E5	E1	E2	E3	E4	E5
Personnel	Competence	0.13	0.21	0.17	0.16					0.15		
	Working load/stress											
	Work environment											
	Fatigue											
Task	Methodology											
	Task supervision											
	Task complexity	0.10	0.17	0.14	0.16					0.15		
	Time pressure	0.13	0.17	0.17	0.16					0.15		
	Tools											
	Spares											
Technical system	Equipment design											
	Material properties											
	Process complexity	0.13	0.17	0.14	0.16					0.15		
	HMI (Human Machine Interface)	0.10	0.04	0.03	0.08					0.04		
	Maintainability/ accessibility	0.07	0.04	0.10	0.08					0.07		
	System feedback											
	Technical condition											
Administrative control	Procedures											
	Work permit				0.04							
	Disposable work descriptions											
	Documentation											
Organisational factors	Programs											
	Work practice	0.17	0.13	0.17	0.08					0.11		
	Supervision											
	Communication	0.17	0.08	0.07	0.08					0.19		
	Tidiness and cleaning											
	Support systems											
	Acceptance criteria											
	Simultaneous activities											
	Management of changes											
		1	1	1	1					1		

B1 E1 Operator fails to detect a valve in wrong position due to error in isolation plan
B1 E2 Operator fails to detect valve in wrong position because self control/ isolation plan is not used
B1 E3 Operator fails to detect a valve in wrong position by self control/ use of isolation plan
B2 E1 No extra person (checker) involved
B2 E2 Checker fails to detect valve in wrong position because self control/isolation plan is not used
B2 E3 Checker fails to detect a valve in wrong position by self control/use of isolation plan

8.6 B4: Erroneous choice or installations of sealing device

8.6.1 Case study 3

Table 31 Risk Influencing factors and their weights for initiating and basic events related to B4, case study 3

RIF	B4 Release due to erroneous choice or installation of sealing device																
		B1 Self control of work [1]					B2 3rd party control of work [1]					B3 Leak test [1]					
	IE	E1	E2	E3	E4	E5	E1	E2	E3	E4	E5	E1	E2	E3	E4	E5	E6
Competence	0.19			0.36	0.19	0.16			0.36	0.19	0.16						0.42
Working load/stress						0.16					0.16						
Fatigue						0.20					0.20						
Methodology																	0.08
Task supervision													0.29				
Task complexity	0.12					0.04					0.04						
Time pressure	0.08		0.11		0.13			0.09		0.13			0.07				
Spares	0.19																
Equipment design	0.12													0.30			
Process complexity						0.08					0.08						
HMI (Human Machine Interface)	0.15					0.20					0.20			0.20			
Maintainability/ accessibility	0.15					0.12					0.12						
Technical condition														0.50			
Procedures				0.45	0.25				0.45	0.25							0.08
Work permit													0.29				
Programs		1.00					1.00					1.00					
Work practice			0.56		0.25	0.04		0.45		0.25	0.04		0.21				
Supervision			0.33		0.19			0.27		0.19							
Communication				0.18				0.18	0.18				0.14				0.42
	1	1	1	1	1	1	1	1	1	1	1	1	1	1			1

[1] For definition of the Es (Basic events) in the table above see Section 5.

8.7 B6: Maloperation of temporary hoses

8.7.1 Case study 3

Table 32 Risk Influencing factors and their weights for initiating and basic events related to B6, case study 3

	B6 Release due to erroneous choice or installation of sealing device																
		B1 Self control of work [1)]					B2 3rd party control of work [1)]					B3 Leak test [1)]					
RIF	IE	E1	E2	E3	E4	E5	E1	E2	E3	E4	E5	E1	E2	E3	E4	E5	E6
Competence	0.26			0.36	0.19	0.16			0.36	0.19	0.16				0.36		0.16
Working load/stress						0.16					0.16						0.16
Fatigue						0.20					0.20						0.20
Task supervision													0.20				
Task complexity						0.04					0.04						0.04
Time pressure	0.11		0.11		0.13			0.09		0.13			0.13			0.20	
Equipment design	0.21													0.27			
Process complexity	0.11					0.08					0.08			0.27			0.08
HMI (Human Machine Interface)	0.21					0.20					0.20						0.20
Maintainability/ accessibility	0.11					0.12					0.12						0.12
Technical condition														0.45			
Procedures				0.45	0.25				0.45	0.25					0.45		
Programs		1.00					1.00					1.00					
Work practice			0.56		0.25	0.04		0.45		0.25	0.04		0.33			0.50	0.04
Supervision					0.19			0.27		0.19						0.30	
Communication			0.33	0.18				0.18	0.18				0.20		0.18		
Simultaneous activities													0.13				
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

[1)] For definition of the Es (Basic events) in the table above see Section 5.

8.8 C1: Break-down of isolation system during maintenance.

Table 33 Risk Influencing factors and their weights for initiating event C1, case study 3

C1 Release due to break down of isolation system during maintenance	
RIF	IE
Equipment design	0.10
Technical condition	0.26
Procedures	0.32
Work practice	0.32
	1

8.9 C2: Maloperation of valve(s) during manual operation*

Table 34 Risk Influencing factors and their weights for initiating event C2, case study 3

C2 Release due to mal-operation of valves during manual operation	
RIF	IE
Competence	0.15
Working load/stress	0.07
Fatigue	0.11
Task complexity	0.07
Process complexity	0.19
HMI (Human Machine Interface)	0.19
Communication	0.15
Simultaneous activities	0.07
	1

8.10 C3: Work on wrong equipment, not known to be pressurized

Table 35 Risk Influencing factors and their weights for initiating event C3, case study 3

C3 Release due to work on wrong equipment (not known to be pressurized)	
RIF	IE
Competence	0.14
Working load/stress	0.07
Fatigue	0.07
Task supervision	0.03
Task complexity	0.03
Process complexity	0.14
HMI (Human Machine Interface)	0.14
Work practice	0.07
Communication	0.17
Simultaneous activities	0.14
	1

9. Scoring of RIFs

9.1 Introduction

In Section 2.2.9 it was shown that the main types of platform specific information that is required as input to the model is number of work operations, equipment count and scores for the identified RIFs. Equipment count is established from drawings and as was discussed earlier, number of work operations can be identified either from e.g. maintenance planning systems or the activity level can also be linked to the quantity of equipment. Establishing input values for the scoring of the RIFs has however not been discussed earlier and in this section, this topic will be covered. The main basis for the discussion and recommendations provided here is the conclusions that were reached in Case Study 2.

The BORA Methodology report (Ref. 20) discusses two principally different approaches to RIF scoring and quantification:

- Specific studies tailored to the needs of the BORA methodology
- Use of existing studies where applicable, supplemented with additional studies where needed

The feedback from the industry on the Methodology report was virtually unanimous, that existing studies should be used as the primary source, as far as possible. In Case study 2, it was decided to look at four different approaches for obtaining platform specific values, applying the following methods:

- Use of RNNS questionnaire data
- Use of TTS data
- Expert judgement
- Use of results from MTO investigations

Rather than combining these, quantification was performed using these four approaches individually, producing four different results. This provided useful information in several respects:

- The suitability of each individual source was investigated, both with respect to overall suitability and whether each source has particular strong and weak areas.
- Results based on different sources could be compared, to see if there were large differences or not.

In the following, use of the different data sources are discussed individually and a summary is provided at the end.

9.2 Use of RNNS data

The RNNS questionnaire data were used in the analysis as follows:

- The RNNS questionnaires were reviewed with the purpose of identifying which questions were relevant for the general RIFs. A table of RIFs and associated questions was established.
- For each RIF, the relevance of the identified questions was evaluated. The relevance was evaluated on a three-point scale (High – Medium – Low).
- The total relevance of all identified questions was also evaluated for each RIF. This was expressed in terms of %, e.g. if it was considered that the identified questions gave a complete coverage of the RIF, 100% was used. If the identified questions only partially covered the RIF, a coverage between 0% and 100% was used.

- The relevance of the individual questions was converted to numbers, using the following scale: High = 9, Medium = 4 and Low = 1. The numbers were added together and the relevance of each question was calculated as a %.

The number of relevant questions that were identified was quite high and for some of the RIFs the RNNS questions gave a reasonably good coverage of the status of the RIF. However, the questions did not cover all the RIFs. Provided RNNS questionnaire data are going to be used in the analysis, it may be considered to include questions that more specifically address all the RIFs.

The adjustment factors that were determined based on the RNNS survey did not give very large adjustments. This may mean that the approach chosen underestimates the risk variation. There may be several explanations for this:

- If we look at the individual RIFs, the adjustment varies more then when the RIFs are combined. This means that the individual variations are larger than the accumulated values used to adjust the basic event probabilities. This means that the RNNS questions tend to give varying results, with some having a better than average and some worse than average rating.
- It is however also noted that the difference between the North Sea average rating from the questionnaire and the ratings for the platform considered in Case study 2 are limited. It may be that the model that has been developed underestimates the difference that this actually means for the adjustment factors.

A sensitivity analysis showed that the variation in adjustment factors will increase if the differences are given a higher weight but the final results are in fact not very sensitive to this change. This may be an indication that the results from the RNNS questionnaire not are able to reflect the differences in a sufficiently good manner to be of use in a setting such as this.

Another possible explanation may however also be that the platform average is quite close to the North Sea average. In other words, based on the RNNS survey, this is an “average” platform and the adjustment factors would therefore be expected to be limited. In this context, it may be noted that RNNS data also were used in Case study 1 and the differences from the North Sea average were there found to be larger.

There are a number of inputs that the risk analyst has to provide in the process of using the RNNS data:

- First, the selection of relevant questions is dependent on the analyst and the choice may depend on how the analyst interprets the basic events, the RIFs or the questions posed.
- Second, the analyst has to evaluate the degree of relevance of the identified questions. Some guidance has been prepared on how to determine the relevance, but this is an area that requires further development of more precise descriptions/definitions as experience with the use increases.

In general, it is probably useful if two persons perform these two tasks independently and that the results are compared. In this way, the possibility of misunderstandings and misinterpretations is reduced.

9.3 Expert Judgment

RIF scores can also be determined through the use of expert judgement. For this purpose, a scale ranging from A to F is applied, where A is the best score and F is the poorest score. This is in accordance with the TTS rating system applied.

The following definitions are the guidelines that were used in the work meetings as a basis for to how to rate the individual RIFs.

Table 36 Rating – expert judgement

Score	Description of interpretation of score
A	Condition is significantly better than what may be considered "best practice".
B	Condition in accordance with "best practice".
C	Conditions are satisfactory, but are not in full compliance with "best practice" ("reference level"). "Average" North Sea conditions would be scored with a C.
F	Condition has significant deficiencies compared to minimum regulatory requirements and is not acceptable.

D and E have not been defined, but these were said to be intermediate levels between the definitions provided above.

The scores must be converted to adjustment factors before application, and this is done using the following scale, based on the methodology report:

A	0.1
B	0.55
C	1.0
D	2.5
E	5.5
F	10

In practical terms, the scoring was done as follows:

- Tables showing all the RIFs were prepared for each basic event that was being considered in the work meeting.
- All the participants in the meeting received a paper copy of all tables.
- Each participant was then asked to apply the scale from A to F for each RIF for the first basic event. All participants completed this task before continuing the meeting.
- The scores for each RIF was then compared and based on discussion, a "joint" score was established.
- The process was then repeated for all basic events.

The first conclusion that can be drawn from this is that the expert judgment meetings turned out to be very efficient and that this seems to be a good way of extracting scores. Although a complete record was not kept of the input from each individual participant, the overall impression is that there was limited disagreement and that it in most cases was easy to reach an agreement on what weight or score that was applicable. The main exceptions were seen when the interpretation of the RIF could be misunderstood or when the participants in the meeting interpreted the Basic Events differently.

The number of experts that participated was limited since only 2-3 operations personnel participated in the scoring. It could possibly have been useful to have a higher number of participants, but in view of the large degree of agreement between the participants this is considered to be a minor point.

The scoring was done using a 6-point scale, but there seemed a clear reluctance to use the lower end of the scale for the scoring. The lowest score recorded was D (with F being the poorest score). This may of course be a reflection of the fact that the situation at the platform was quite good. It may also be that clearer definitions of the grades would have implied that the full scale had been used.

It is also noted that none of adjustment factors calculated on basis of the expert judgment scoring was higher than 1. In other words, conditions at the platform were considered to be equal to or better than "North Sea average" for all basic events being considered. This is not to say that all scores were average or better ("D" was also used), but weighting together the contributions from different RIFs, the result was always that the adjustment factors became 1 or smaller.

Again, it is difficult to say whether this is a true reflection of the situation at this specific platform or whether it is an example of too much "optimism" from the experts. In this context it may also be noted that the platform specific leak statistics show a higher number of leaks than the average. In any case, this is an issue to be aware of in future applications.

9.4 Information from TTS reports

TTS ("Teknisk Tilstand Sikkerhet" – Technical Condition Safety) is a system for reviewing/auditing the technical safety condition of Statoils offshore installations. Other operators also use similar auditing schemes. The review is performed on a predefined set of Performance Standards (PS) and for each PS, a set of Performance Requirements (PR) has been established and these are again split in sub-requirements. The condition of the systems on an installation is measured against these requirements and the condition is rated as follows:

Table 37 Rating - TTS

Rating	Description of condition
A	Condition is significantly better than the reference level (PR)
B	Condition is in accordance with the reference level (PR)
C	Conditions satisfactory, but does not fully comply with the reference level (PR)
D	Condition is acceptable and within the statutory regulations' minimum intended safety level, but deviates significantly from the reference level (PR)
E	Condition with significant deficiencies as compared with "D"
F	Condition is unacceptable

In practice, this has been implemented as follows:

- The TTS reports are reviewed with the purpose of identifying all statements in the reports which are of relevance for the Basic Events.
- The degree of relevance of each statement is evaluated in relation to each Basic Event, on a three-point scale (High/Medium/Low). The relevance rating is converted to numbers according to the following scale: High=9, Medium=4 and Low=1. Some guidance on relevance rating is found in Table 38.
- After all statements have been evaluated, their total "coverage" of the Basic Event is evaluated and determined as a % value. This is evaluated subjectively, by the analyst. The "residual relevance" identified in this way is assumed to always have an average score.
- The score is determined from the TTS report directly or based on the judgement of the project team where the TTS report does not give a score directly. The TTS grades from A to F are used.
- The TTS scores are then converted to adjustment factors.

The calculation of adjustment is done in accordance with the methodology proposed in the method statement report, Ref. 20. Based on the rating from the TTS reports, adjustment factors are assigned as follows:

A	0.1
B	0.55
C	1.0
D	2.5
E	5.5

F	10

When the score is calculated, the ratings are multiplied with these scores to arrive at a total score for the RIF:

$$Q_i = \frac{\sum_k RR_k \cdot s_k}{\sum_k RR_k}$$

There will be some instances when several statements are identified as being relevant for one Basic Event, but where the statements essentially cover the same issue. One statement could e.g. be that "P&IDs are not up to date" (relevance rating 4), another statement "Documentation is generally not always updated" (relevance rating 1) and a third could be "Contractor is frequently behind schedule with document updates" (relevance rating 1). The first is specific, while the second and third are more general. If this is the case, only the statement with the highest relevance rating is included, i.e. a rating of a total of 4 is applied to cover all three of these statements.

Guidelines for how the relevance rating is used have also been prepared. These are provided in the table below.

Table 38 Guidelines for evaluation of relevance of statements from TTS

Relevance Rating	Description of relevance
High	Directly relevant for the basic event being considered. Example: "Routines for testing of ESDVs" will have a High relevance for the probability of failure of ESDVs.
Medium	Relevant for similar operations/equipment or partly relevant for the basic event being considered. Example: "F&G system shall be independent" has a Medium relevance for the probability of failure of the F&G Node.
Low	General comments that may be relevant. Example: "Deviations and non-conformances are reported in several systems rather than just one" is a comment that will have a Low relevance for several technical basic events since this may be an indication that it is difficult to keep track of e.g. problems with equipment

The TTS reports provide large quantities of information that could be directly related to the basic events, and not just technical failures but also operational failures. Some of the challenges related to the use of TTS can be summarized as follows:

- The quantity of information that is or may be relevant is quite large in the TTS reports. The same or similar information can often be found in several places in the reports and it is necessary to structure the information and identify key issues that are relevant to included. An example is a large number of comments related to documentation on the platform in Case study 2. The statements were partly general and partly specifically related to particular areas. Structuring this information and not doing too much double counting of the effects can be difficult.
- In the same way as for the RNNS questions, there are several elements of the analysis of the TTS data that is associated with a high degree of uncertainty. In addition to the selection of relevant information, there is also in this case the evaluation of the relevance of the statements identified.
- The TTS reports provide scores on a relatively high level, expressed through grades on the Performance Standard or Performance Requirement level. Often, the statements that are relevant for the scoring can however be found as single sentences forming only part of the total evaluation of a Performance Requirement. This means that the total grade for a PR not necessarily is representative for

the particular statement of interest and some subjective evaluation by the analyst is required. However, this is done using the same principles as are applied when performing the TTS.

In total, it is however considered that the TTS reports is the single most useful source of information that was used in the project. They provide good coverage of technical basic events and also give quite good indications of at least parts of the factors influencing the operational basic events. In particular, the data are well suited for analysis of consequence barrier systems where technical systems play an important role.

9.5 Accident Investigation Reports

The use of results from MTO investigations may also give interesting information on the status of both technical systems and organizational/operational aspects. The methodology report (Ref. 20) presents one possible approach to the use of these data, but in the case study it was chosen to use a modified method. The suggested approach was based on the assumption that if a specific cause often contributes to a release, this is an indication that the status of this particular cause is below average and that an increased probability compared to the North Sea average should be applied.

We have chosen to use the number of occurrences of each cause as a basis for the estimation of adjustment factors. It has then been attempted to identify what basic event this cause can be associated with. This gives an indication of the number of times each basic event has occurred.

This is then compared with the average basic event probabilities. By adding together the probabilities for all relevant basic events and then calculating the percentage contribution from each basic event, we also have an "a priori" distribution which gives an indication of what can be expected.

By comparing the two distributions, it is possible to identify if some of the basic event occur more or less frequently than predicted by the average probabilities. This then forms the basis for determining adjustment factors. The adjustment factors are however defined subjectively, based on inspection of the differences, and a specific rule set for doing this has not been established.

This approach is different from the others in the sense that we update the failure probabilities of the barriers directly instead of going through risk influencing factors. This is a simplification of the analysis process but it does not give the same "deep" understanding of the mechanisms that influence risk as the other approaches does. The efficiency of this method is clearly also dependent on the number of available investigation reports. If there are few reports, it is difficult to draw conclusions and it is not possible to define adjustment factors. The average probabilities will then be very little affected by the results from the reports and the results need not be very installation specific.

In order to be able to use this information in a better way, at least two approaches could have been investigated in more detail:

- By considering the total volume of investigation reports available from the Norwegian offshore operations, more comprehensive "average" distributions of contributing causes (failures of basic events) could have been established. By comparing platform specific distributions with these North Sea wide distributions, differences could be identified and used to modify average probabilities. A weakness may however be that the information from each specific installation becomes too limited to provide statistically significant differences.
- Another approach would be to use the information from the investigation reports in a more qualitative manner, identifying statements from the reports that are relevant for the basic events being considered (in a similar manner as for TTS reports). By scoring this information, this could be used to establish adjustment factors.

9.6 Combination of Data Sources

The case studies have given indications of the strong and weak sides of the different data sources and it would appear that no single data source is ideally suited for covering all aspects of an analysis such as this.

The following is summarized:

- The most extensive information can be found from the TTS reports. In particular, this provides information related to technical Basic Events, especially for the consequence barrier systems. However, the TTS reports do not only give information for technical systems; there is also information related to operational Basic Events.
- Use of Expert Judgment for the scoring of operational basic events turned out to be a very efficient process with the additional benefit that it involves operational personnel. Expert Judgment is thus a very good supplement to the TTS reports and the two data sources together give a good basis for performing the analysis.
- RNNS questionnaire information is more uncertain. The adjustment factors tend to be smaller than what is found when using the other data sources. However, this could be a useful additional data source and if more specific questions were included in future survey, the applicability of this data source could be improved.
- As regards MTO investigations, this is the most limited data source and it has also turned out to be difficult to use the data in a systematic manner. However, it is still believed that these data can be applied as a supplement to other information.

In summary, a combination of TTS data and expert judgment appears to give a good basis for establishing scores on a high level. However, the other data sources should also be applied and some further work is probably useful on finding efficient ways of utilizing this information as high level adjustment factors or for calibration/verification of the more detailed information available from TTS and Expert Judgment.

10. Recalculation of the risk

The final step is to recalculate the risk. The principles for recalculation of the risk are illustrated by an example.

Example scenario: Release due to valve(s) in wrong position after maintenance

The barrier block diagram for the example is shown in Figure 30.

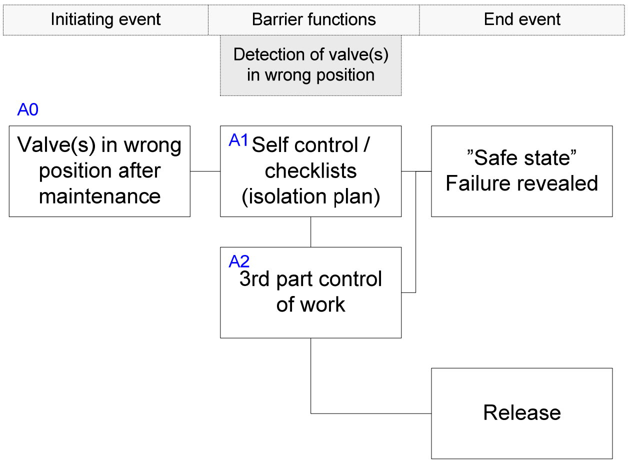


Figure 30 **Barrier block diagram for the example**

Fault trees for the barriers (A1 and A2) in Figure 30 are shown in Figure 31 and Figure 32.

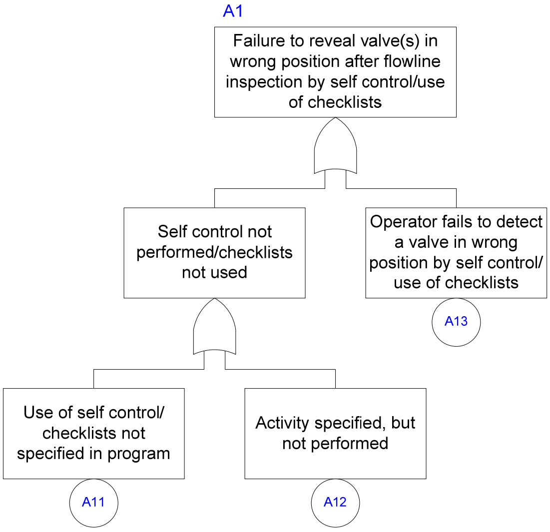


Figure 31 **Fault tree for the top event "Failure to reveal valve(s) in wrong position after maintenance by self control/use of checklists"**

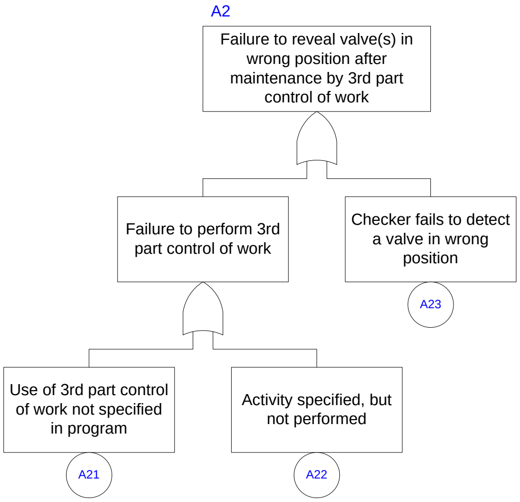


Figure 32 **Fault tree for the top event "Failure to reveal valve(s) in wrong position after maintenance by 3rd party control of work/inspection"**

Table 39 summarizes average frequencies and probabilities based on generic values as stated.

Table 39 **Scenario A - Summary of generic frequencies / probabilities**

Event notation	Event description	Assigned frequencies / probabilities
N	Number of flowline inspection per year	28
P (A_0)	Probability of valve(s) in wrong position after maintenance per maintenance operation	0.003
P (B_{A11})	Probability of failure to specify use of self control / checklists	0
P (B_{A12})	Probability of failure to perform self control when specified	0.01
P (B_{A13})	Probability of failure to detect a valve in wrong position by self control	0.33
P (B_{A21})	Probability of failure to specify 3rd party control of work in programs	1
P (B_{A22})	Probability of failure to perform 3rd party control of work when specified	0.01
P (B_{A23})	Probability that a checker will fail to detect a valve in wrong position after maintenance if control of work is performed	0.1

The risk influence diagrams for this scenario are shown in Appendix 1, section 1.5.

The weights of the RIFs are shown in Table 29.

The scoring of the RIFs used to illustrate the principles in the method are shown in Table 40

Table 40 RIFs and scores applied in the example

RIF no	RIF text	Category score
A02	**Probability of valve in wrong position**	
A21	Process complexity	C
A22	Accessibility	C
A23	HMI	D
A24	Time pressure	D
A25	Competence of area technician	C
A26	Work permit	C
A11	**Use of self control/checklists not specified in program**	
A111	Program for self control	C
A12	**Activity specified, but not performed**	
A121	Work practice	D
A122	Time pressure	D
A123	Work permit	C
A13	**Area technician fails to detect wrong position**	
A131	HMI	D
A132	Accessibility	C
A133	Time pressure	D
A134	Competence of area technician	C
A135	Procedures for self control	C
A136	Work permit	C
A21	**Use of 3rd party control not specified in program**	
A211	Program for 3rd party control	C
A22	**Activity specified, but not performed**	
A221	Work practice	D
A222	Time pressure	D
A223	Work permit	C
A23	**Checker fails to detect valves in wrong position**	
A231	HMI	D
A232	Accessibility	C
A233	Time pressure	D
A234	Competence of checker	C
A235	Procedures for 3rd party control	C
A236	Work permit	C

The results from the calculations of the leak frequency are shown in Table 41. Note that no 3rd party control of the work performed by the area technician has been required or carried out for this scenario.

Table 41 Results from calculation of the leak frequency from the example scenario.

	Industry average data	Revised data
Leak frequency	0.0283	0.0842

We may also carry out a sensitivity analysis in order to calculate the effect of introducing 3rd party control of the work (see A2 in Figure 30). Table 42 shows the revised leak frequency. The results show the effect of the risk reduction proposal, i.e., a reduction of the calculated leak frequency.

Table 42 Revised results (sensitivity analyses)

	Industry average data	Revised data
Leak frequency	0.0056	0.0270

11. Evaluation of Approach

11.1 Methodology

The approach adopted was a mix of several existing techniques and some new elements. The approach may be summarised as follows:

1) Barrier block diagrams, event trees and fault trees are used to structure human and technical barrier elements
2) Risk Influencing Factors are identified
3) Scores for RIFs are assessed
4) Average frequencies are assessed based on event trees and fault trees
5) Platform specific frequencies and probabilities are assessed based on average frequencies/probabilities, RIF scoring and weighting
6) Synthesis of frequencies and probabilities is performed according to standard probability calculus.

The structure of the approach is similar to for instance I-RISK (Ref.21) and others, but the detailed elements are different. As such the overall structure of the approach is not new, and is not particularly controversial.

Barrier block diagrams have been prepared for all leak scenarios, based on barrier elements according to common practice. These may be considered as default barrier diagrams, which may need to be adjusted if the operational barriers on a specific platform are not according to common practice.

The derivation of the RIF structure has been based on a comprehensive review of existing structures and relevant studies. It is considered that existing studies, methodologies and results are sufficient as basis for identification of risk influencing factors.

The scoring of RIFs has been inspired by the TTS/TST verification schemes used by several oil companies operating on the Norwegian Continental Shelf. Categories have therefore been defined from A (best practice in the industry) to F (worst practice in the industry), see further description in Section 2.2.7. Two approaches were considered:

- Scoring of generic RIFs based mainly on available data. One of the conclusions from the initial work in the BORA project with methodology development was that the approach had to allow existing data to be used.
- Scoring of specific RIFs based on more detailed assessments (e.g. expert judgment), but also based on available data where suitable (especially TTS/TST for “technical” RIFs).

Initially, it was assumed that existing data in some cases could be sufficient basis for scoring. It has been found that a combination of these two approaches is the only viable option.

The assessment of average frequencies and probabilities has received limited attention in the current activity, because it is not considered to be a critical aspect for the methodology. Assessment of such average frequencies and probabilities will imply use of existing approaches and data, which may be available from operational data, previous QRA studies and SIL analyses.

A substantial part of the approach is the assessment of installation specific frequencies and probabilities based on the RIF scoring. The suggested approach is discussed in Section 2.2.8 above. The two fundamental aspects are as follows, performed for each RIF and each probability:

- Transformation of scoring to quantitative status
- Assessment of quantitative weights (importance)

The transformation of scoring to quantitative status and the assessment of quantitative weights requires input from expert judgment, because none of these are available from existing sources. This expert input also offers an opportunity to compensate to some extent for aspects that for instance not are covered by available data sources. The experience with expert sessions is that this is an efficient way to create this input.

It was intended at some point that the methodology should recommend default weights to be used when it was infeasible to perform expert sessions. Default weights needed a minimum number of case studies to be established, in order to have a sufficiently broad basis for these values. It turned out that it was impossible to have access to a sufficient number of installations for which such case studies could be conducted, and no default values are therefore provided.

It should be feasible to integrate the BORA approach with a typical QRA approach applied for production installations in the petroleum industry. It will substantially improve the assessment of hydrocarbon risk in QRA studies in the operations phase and provide valuable knowledge about causal factors influencing the risk of hydrocarbon leaks. It may also be applied for QRA studies during engineering of new installations, based on some assumptions.

The consideration of dependencies among the RIFs is based on a simplistic approach. It has been argued by some that the approach should preferably be made more sophisticated. It may be argued that the common treatment of dependencies of technical components in fault tree analysis (through α-factors and similar) is not much more advanced.

A more fundamental issue is whether the true mechanisms that may cause such dependencies are well known at all, when it comes to HOF aspects. If the mechanisms are not well known, or the data is non-existent, it is not appropriate to spend a lot of effort on development of sophisticated models.

A key aspect with regard to usability of the method that has been developed is the resource usage that is required to perform a study with this method. If the work involved is too extensive, it is unlikely that the method will be commonly applied except possibly for very specialised applications. However, based on the experience from the case studies and the subsequent work with the generalisation of the methodology, it would appear that it is possible to conduct a study with relatively limited additional use of resources compared to a more “standard” offshore QRA approach. The main additional information that needs to be collected is basis for weighting and scoring of RIFs and this has been found to be possible to do quite efficiently in work meetings. It is therefore considered fully feasible to implement this methodology also in practical applications.

11.2 Use of Results for Decision-Making

The purpose of a modelling and analysis as described above is to provide decision support on the need for safety measures, choosing between alternative measures, etc; in other words; on prioritisation and optimisation of resources. This decision support is obtained by

- Gaining more knowledge and insights related to risks and factors influencing risks and the performance of the barrier systems
- Identifying possible failures and failure scenarios that induce risk
- Identifying safety critical activities and systems
- Assessing the effect on risk and barrier performance of activities, changes and implementation of measures

The analysis contributes to obtaining the overview of barrier performance as required by the PSA’s Management regulations.

These points are all of general character. Next the question would be to address to what extent the proposed analysis approach is able to meet these expectations. The BORA Project Plan, /22/, listed a number of application areas for operational risk analyses:

- Provide a basis for determining the effect of operational factors, measures and decisions which influence leak probability. Examples of this could be:
  - inhibiting of safety systems / functions, for example in PSD
  - quality and scope of maintenance and inspection
  - competence and training of operators
  - complexity of systems and processes
  - management, implementation and control of work processes
  - the effect of postponing or omitting a particular maintenance or inspection activity
  - the effect of not performing SJA before a maintenance activity is carried out
  - the work permit system
  - the effect of a high level of activity / many simultaneous activities
  - the effect of reducing the number of process operators

The success of the methodology is dependent on whether or not it is capable of discriminating between different levels relating to the parameters shown here.

The aspects listed above are fairly general, like ‘the work permit system’, or ‘the effect of reducing the number of process operators’. These issues may be addressed through RIF scoring based on available data, and a further reflection of specific aspects may be achieved through the assessment of weights (importance).

It is nevertheless required that the resolution in the analysis is concurrent with analysis objectives, i.e. that factors considered in the analysis are at least as detailed as the factors that are addressed in the decision-making. The experience from the case studies has demonstrated that it is feasible to have such assessments that have the sufficient depth in order to address issues like those outlined above.

The analysis results express a synthesis of knowledge in the form of hard data and expert judgments. A natural question to consider is then how is it possible to have confidence in the numbers produced, given the many complex phenomena covered and the many assumptions made? The results must be extremely uncertain or arbitrary?

Our answer to this is; the analysis is a tool for synthesis of the knowledge available, and represent the analysis group’s best judgments based on the facts and evaluations made on the issues by experts and others having knowledge about the phenomena being studied. The results provide decision support – not hard recommendations on what is the best decision. It is always necessary to see the analysis results in a context, where considerations are made in relation to the limitations and constraints of the analysis. Decisions need to be taken, and decision-makers need a decision basis. The BORA tool is developed to provide such a basis, a valuable input in the decision process, as it addresses risk and the factors influencing risks. The numbers produced are not the most important results of the analysis, but the message derived from a systematic analysis using numbers to ensure consistency and completeness.

12. References

1 Together for Safety: "*Definition of barriers*"

2 Bento, J.-P., *Menneske - Teknologi - Organisasjon Veiledning for gjennomføring av MTO-analyser*. Kurskompendium for Oljedirektoratet, Oversatt av Statoil,, Oljedirektoratet, Stavanger, Norway, 2001.

3 Groeneweg, J., Controlling the controllable: The management of safety, DSWO Press, Leiden, The Netherlands, 1998.

4 Bellamy, L. J., Papazoglou, I. A., Hale, A. R., Aneziris, O. N., Ale, B. J. M., Morris, M. I. and Oh, J. I. H., *I-RISK - Development of an Integrated Technical and Management Risk Control and Monitoring Methodology for Managing and Quantifying On-Site and Off-Site Risks*. Main Report. Contract No: ENVA-CT96-0243, 1999.

5 Jacobs, R. and Haber, S., *Organisational processes and nuclear power plant safety*, Reliability Engineering and System Safety. 45 (1994) 75 - 83.

6 Davoudian, K., Wu, J.-S. and Apostolakis, G. E., *Incorporating organisational factors into risk assessment through the analysis of work processes*, Reliability Engineering and System Safety. 45 (1994) 85-105.

7 Swain, A. D. and Guttmann, H. E., *Handbook of human reliability analysis with emphasis on nuclear power plant applications: Final report* NUREG CR-1278, SAND80-200, Sandia National Laboratories Statistics Computing and Human Factors Division, Albuquerque, 1983.

8 Hollnagel, E., *Cognitive reliability and error analysis method: CREAM*, Elsevier, Oxford, 1998.

9 Embrey, D. E., Humphreys, P., Rosa, E. A., Kirwan, B. and Rea, K., *SLIM-MAUD: An approach to assessing human error probabilities using structured expert judgment*, Department of Energy, USA, 1984.

10 Gibson, H., Basra, G. and Kirwan, B., *Development of the CORE-DATA database*, Paper dated 23.04.98, University of Birmingham, Birmingham, United Kingdom, 1998.

11 Thomassen, O. and Sørum, M., *Mapping and monitoring the technical safety level*. SPE 73923, 2002.

12 C Torjussen: "*Activity indicator for gas leaks – which data are available and how can we make use of them*", Master thesis at Høgskolen i Stavanger, 2003

13 Asheim, A: *Petroleumsproduksjon og prosessering på plattformen,* TANO A/S, 1985.

14 Sklet, S & Hauge, S., "*Safety Barriers to prevent release of hydrocarbons during production of oil and gas*", SINTEF report, STF38 A04419, 15.9.2004

15 Swain, AD and Guttmann HE: *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications,* U.S. Nuclear regulatory commission report NUREG/CR-1278, SAND80-020, August 1983

16 Reason, J: *Managing the Risks of Organizational Accidents,* Ashgate Publishing Company, Burlington, 1997.

17 Blackman, HS and Gertman, DI: *Human Reliability and Safety Analysis Data Handbook,* John Wiley & Sons, 1994.

18 Kirwan, B: *A Guide to Practical Human Reliability Assessment,* Taylor & Francis Ltd., 1994.

19 Kirwan, B: *Human Factors & Human Reliability in Offshore Systems,* Course arranged at SINTEF, Trondheim, May 11-13 1998.

20 Aven, T., et.al. "*Operational risk analysis, Total analysis of physical and non-physical barriers, H2.1 Methodology for Analysis of HOF Factors*", Draft 1, Rev 0

21 Papazoglou IA, Bellamy LJ, Hale AR, Aneziris ON, Post JG, Oh JIH. *I-Risk: development of an integrated technical and Management risk methodology for chemical installations*. Journal of Loss Prevention in the process industries, 16 (2003) 575 – 591, Elsevier

22 Operational risk analysis, *Total analysis of physical and non-physical barriers, Plan for main project (pre-project report)*, BORA-project report 200254-03, 16.10.2003

(blank page)

BORA
Barriere- &
operasjonell risikoanalyse

Operational Risk Analysis – Total Analysis of Physical and Non-physical Barriers

H3.1 Generalisation Report
Appendix 1
Risk Influence Diagrams

29 January 2007

1. Risk Influence Diagrams

1.1 Introduction

Risk influence diagrams are used to illustrate the RIFs influencing the different initiating events or basic events. Risk influence diagrams for different scenarios were developed during the case studies and are presented in this appendix.

1.2 Scenario A1 Release due to degradation of valve sealing

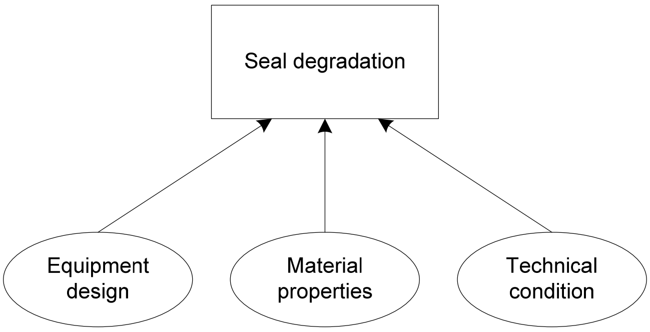


Figure 1 Influence diagram for the initiating event.

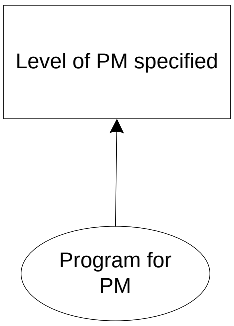


Figure 2 Influence diagram for barrier 1 – basic event 1.

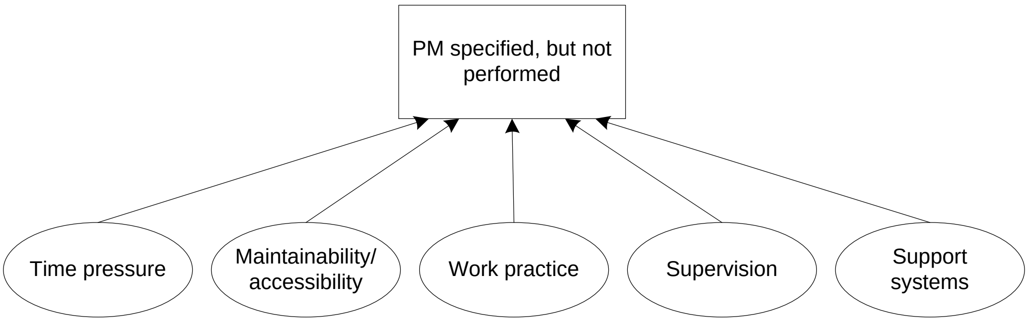


Figure 3 Influence diagram for barrier 1 – basic event 2.

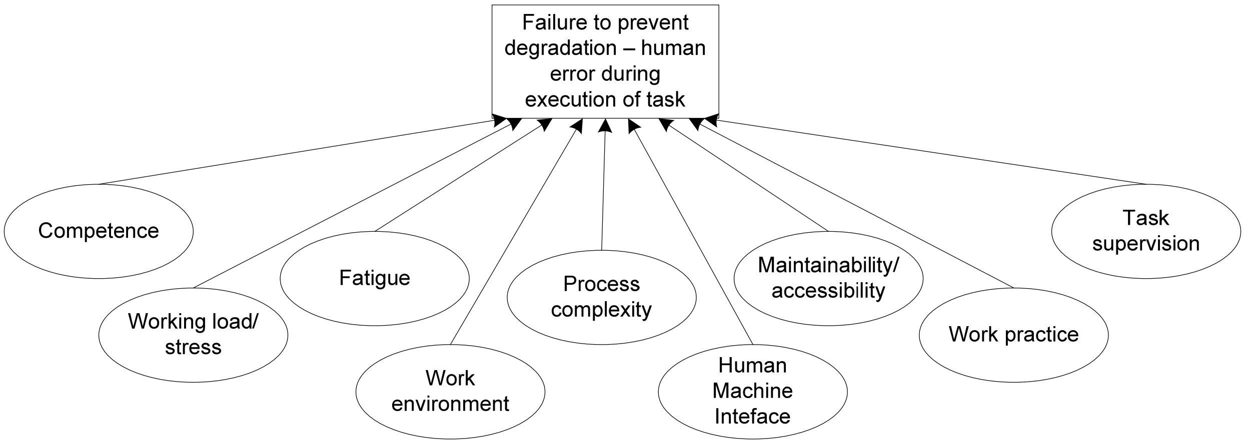


Figure 4 Influence diagram for barrier 1 – basic event 3.

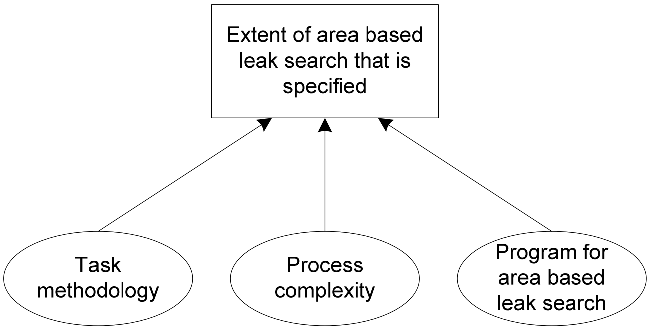


Figure 5 Influence diagram for barrier 2 – basic event 1.

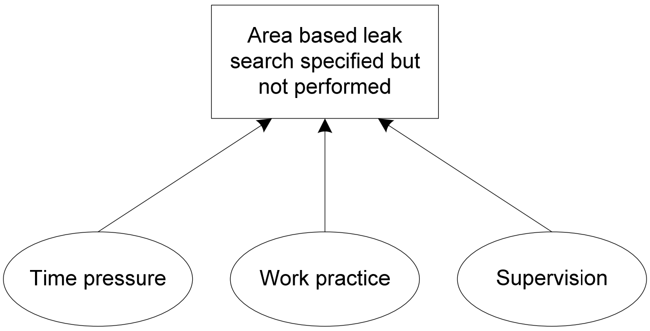


Figure 6 Influence diagram for barrier 2 – basic event 2.

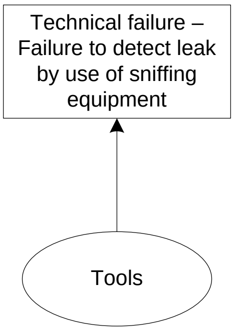


Figure 7 Influence diagram for barrier 2 – basic event 3.

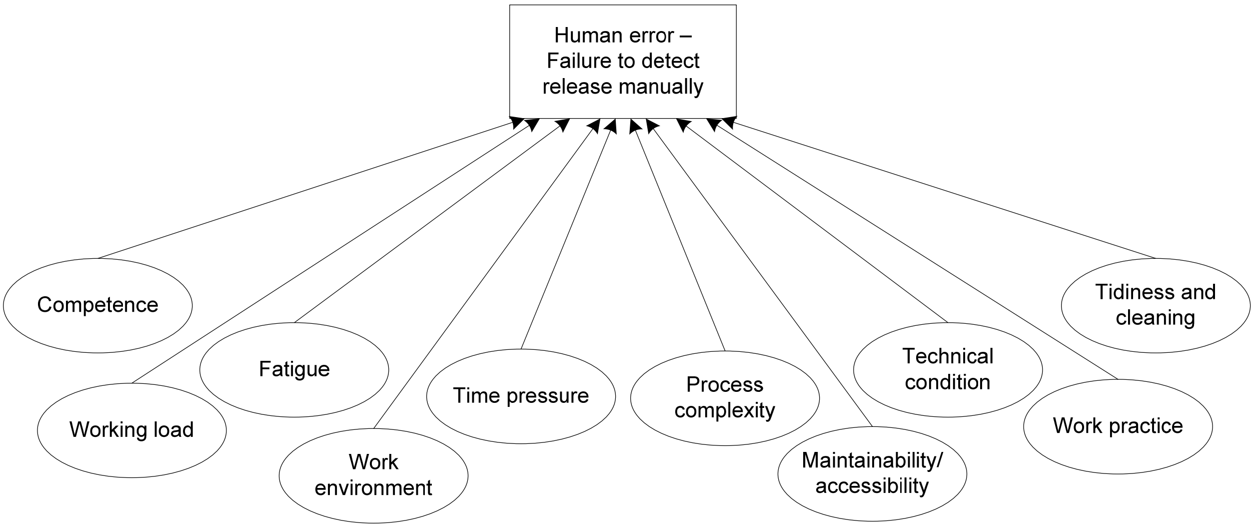


Figure 8 Influence diagram for barrier 2 – basic event 4.

1.3 Scenario B1 Release due to incorrect blinding/isolation

1.3.1 "Small" job (e.g. isolation of flowline)

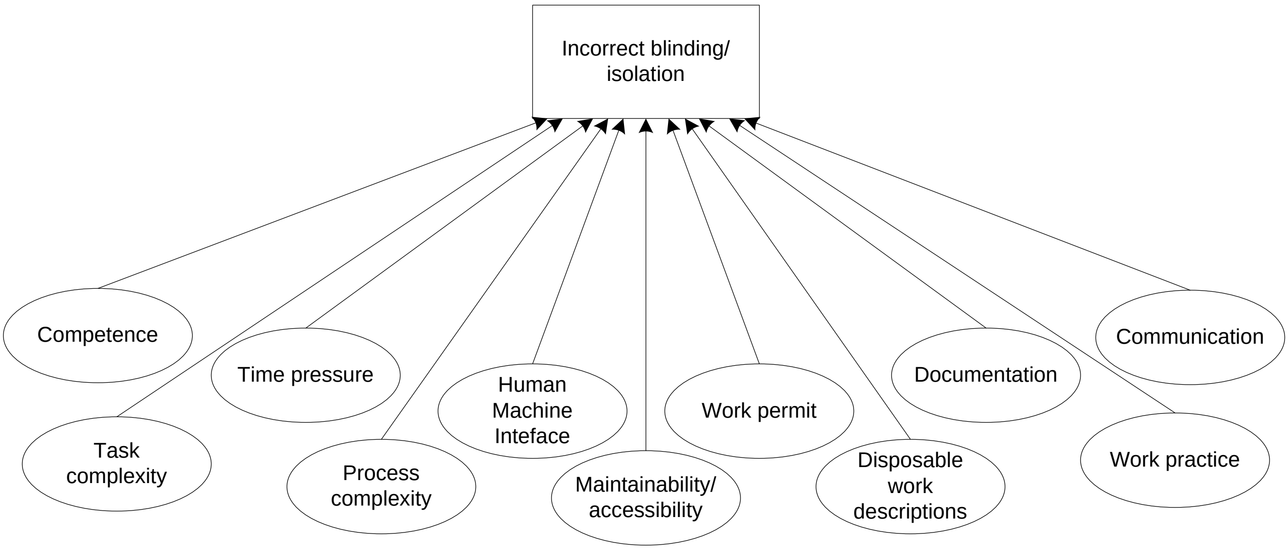


Figure 9 Influence diagram for the initiating event.

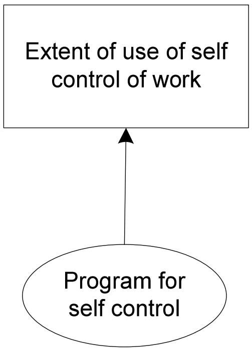


Figure 10 Influence diagram for barrier 1 – basic event 1.

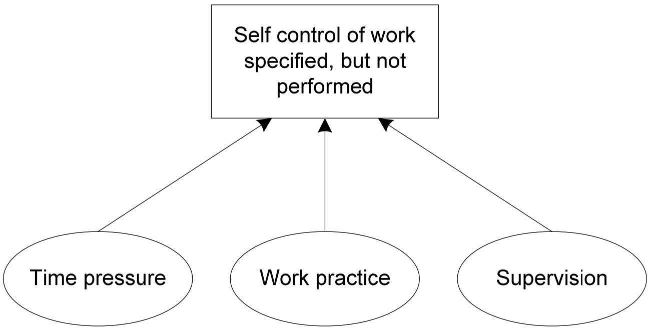


Figure 11 Influence diagram for barrier 1 –basic event 2.

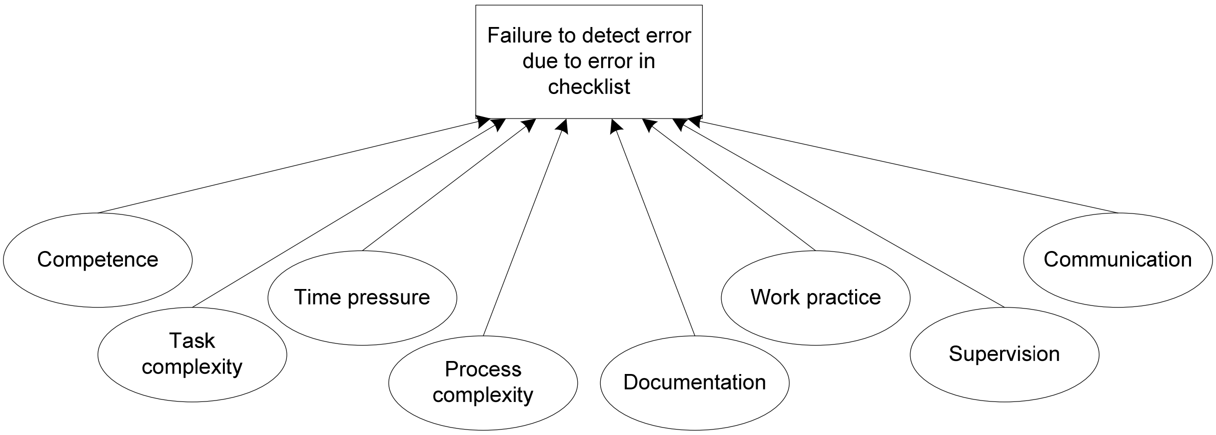


Figure 12 Influence diagram for barrier 1 – basic event 3.

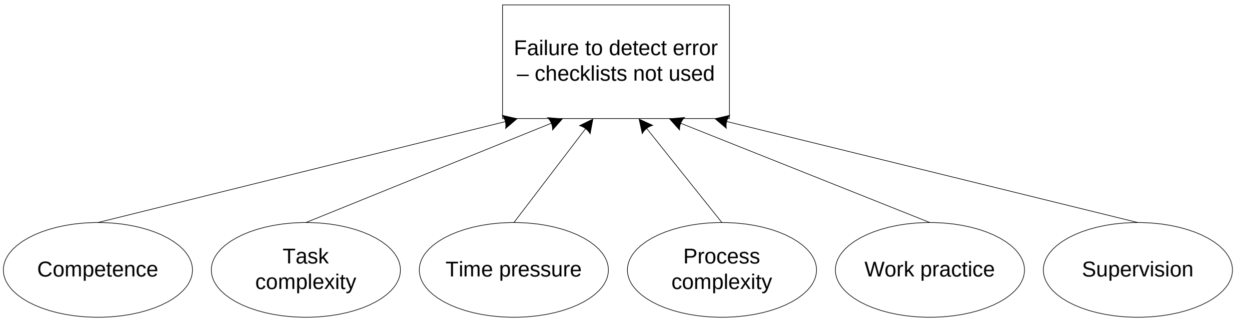


Figure 13 Influence diagram for barrier 1 – basic event 4.

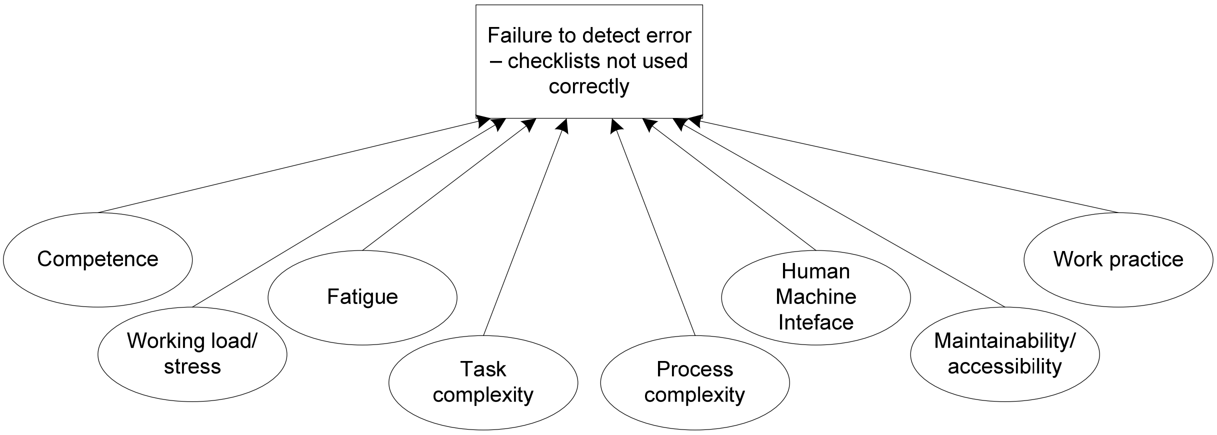


Figure 14 Influence diagram for barrier 1 – basic event 5.

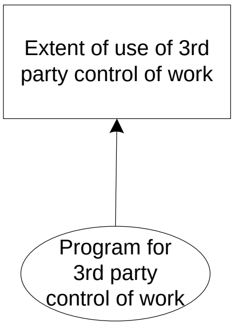


Figure 15 Influence diagram for barrier 2 – basic event 1.

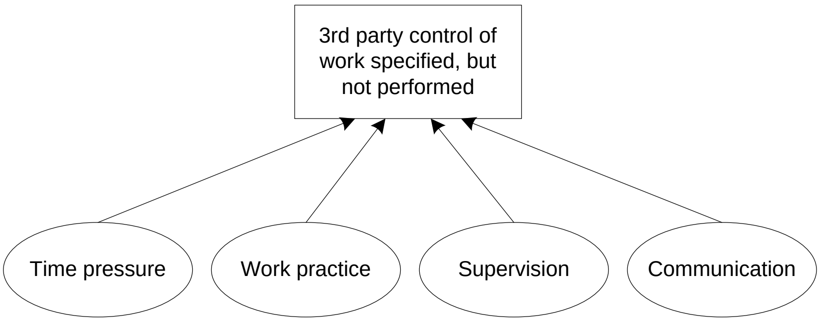


Figure 16 Influence diagram for barrier 2 – basic event 2.

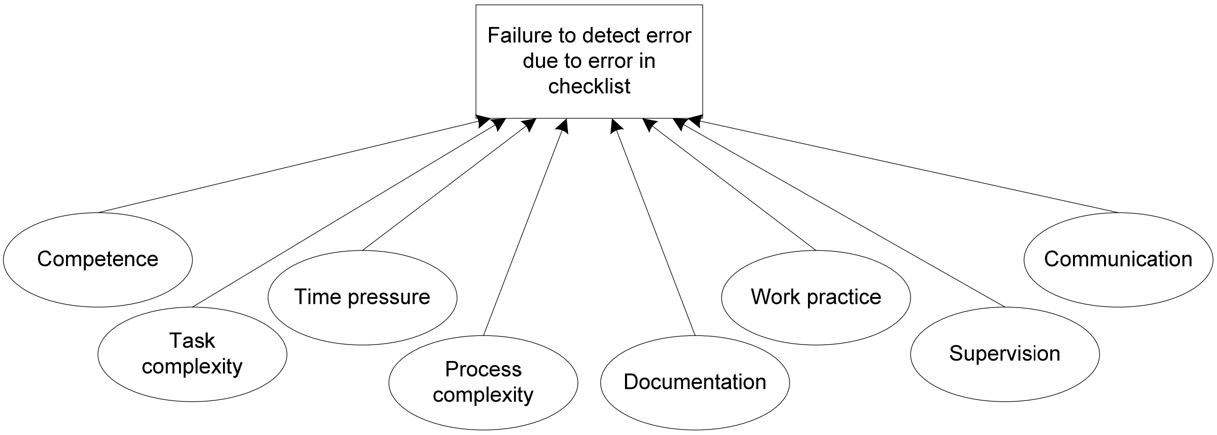


Figure 17 Influence diagram for barrier 2 – basic event 3 (identical as self control)

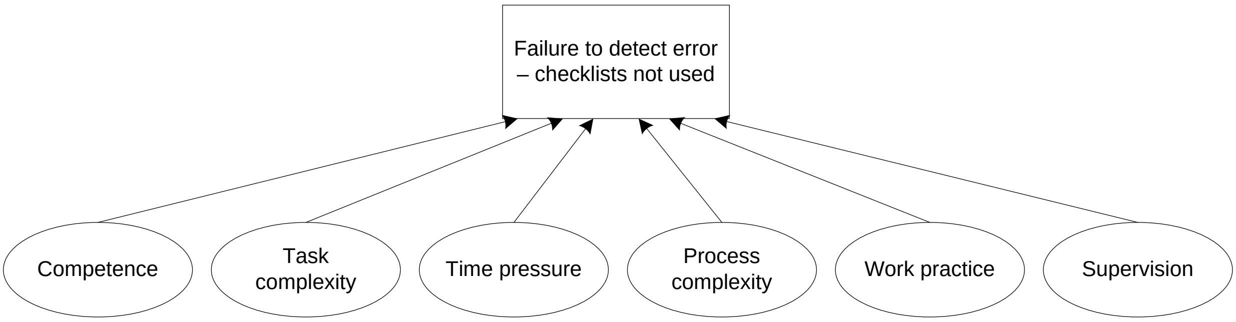


Figure 18 Influence diagram for barrier 2 – basic event 4 (identical as self control)

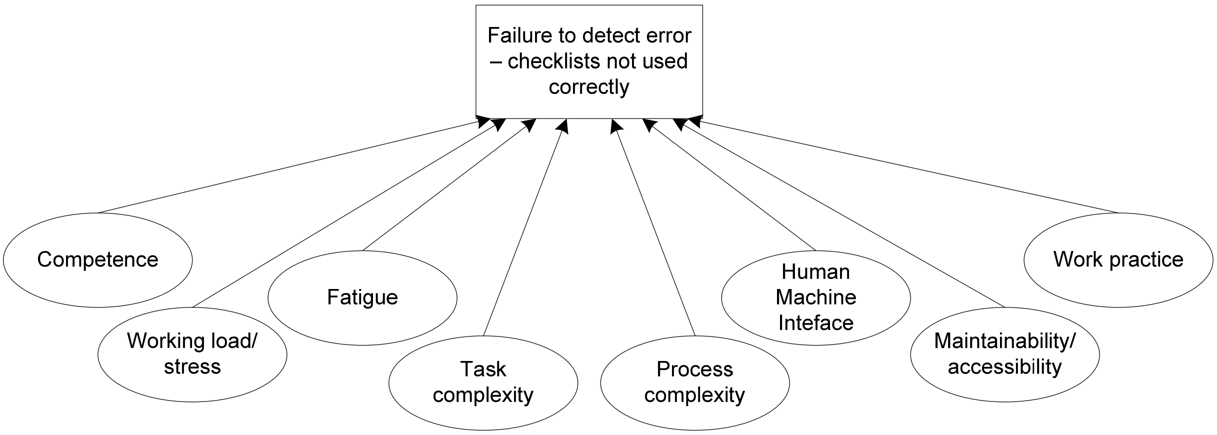


Figure 19 Influence diagram for barrier 2 – basic event 5 (identical as self control)

1.3.2 "Major" job (e.g. maintenance of separator)

All the influence diagrams for scenario B1 – "major" job are equal with the influence diagrams for scenario B1 – "small" job presented in subsection 1.3.1 except from two basic events (see Figure 20 and Figure 21).

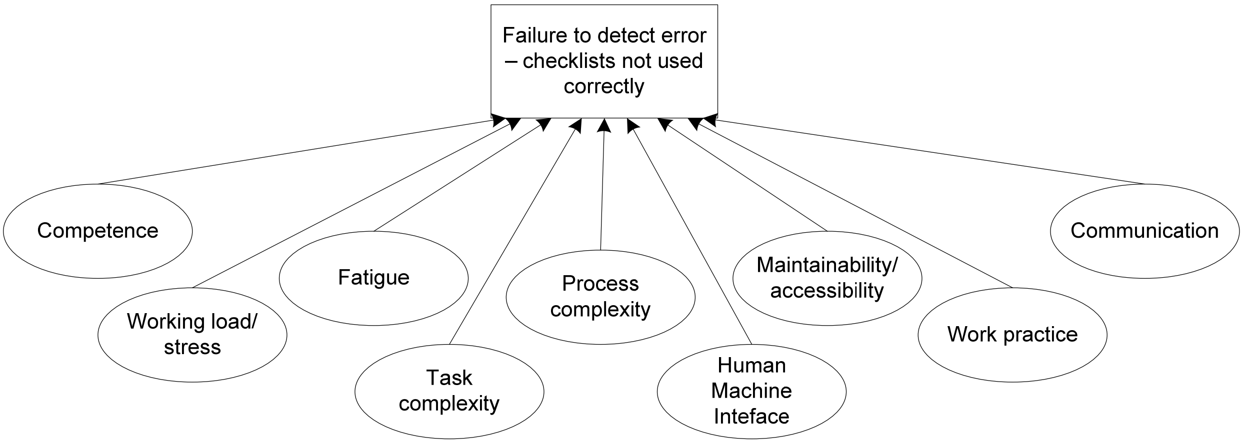


Figure 20 Influence diagram for barrier 1 – basic event 5.

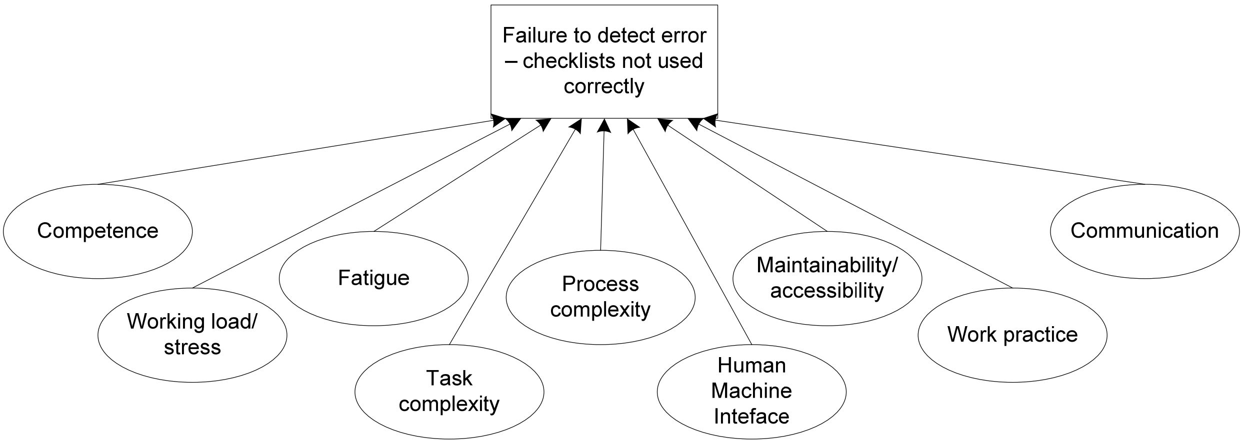


Figure 21 Influence diagram for barrier 2 – basic event 5.

Table 1 RIFs and their weights for initiating and basic events related to the containment function, Scenario A

RIFs	**Description**	**Initiating and basic events**						
		A_0	B_{A11}	B_{A12}	B_{A13}	B_{A21}	B_{A22}	B_{A23}
Process complexity	System complexity, no of valves, complex routing of plant, etc.	4	4	4	4	-	-	4
Task complexity	Many steps to be performed, unusual activity, etc.	3	4	4	4	-	-	4
Maintainability/ Accessibility	Access to valves, space to perform work, etc.	2	1	3	2	-	-	2
Human-Machine-Interface	Labeling – permanent and temporary valve marking, position feedback from valves, etc.	3	1	1	2	-	-	1
Time pressure	Actual time pressure, perceived time pressure, simultaneous activities, etc.	4	4	5	4	-	-	4
Competence	Experience from Heidrun, training, system knowledge, use of contractors, etc.	4	5	5	4	-	-	4
Communication	Communication between different parties involved in operation (CCR, Prod Tech, Mechanics)	5	2	2	2	-	-	5
Work permit	System for WP and use of WP, signatures on WP, etc.	0	0	0	1	-	-	0
Work practice	Procedures followed, same practice across shifts, etc.	5	3	5	2	-	-	3
Documentation, drawings		-	-	-	-	-	-	-

[1] For this specific scenario a checker will always be involved
[2] A checker is only involved if they use isolation plan

A_0 = Valve left in wrong position after maintenance
B_{A11} = Operator fails to detect a valve in wrong position due to error in isolation plan
B_{A12} = Operator fails to detect valve in wrong position because self control/ isolation plan is not used
B_{A13} = Operator fails to detect a valve in wrong position by self control/ use of isolation plan
B_{A21} = No extra person (checker) involved [1]
B_{A22} = Checker fails to detect valve in wrong position because self control/isolation plan is not used [2]
B_{A23} = Checker fails to detect a valve in wrong position by self control/use of isolation plan

1.4 Scenario B2 Release due to incorrect fitting of flanges or bolts during maintenance

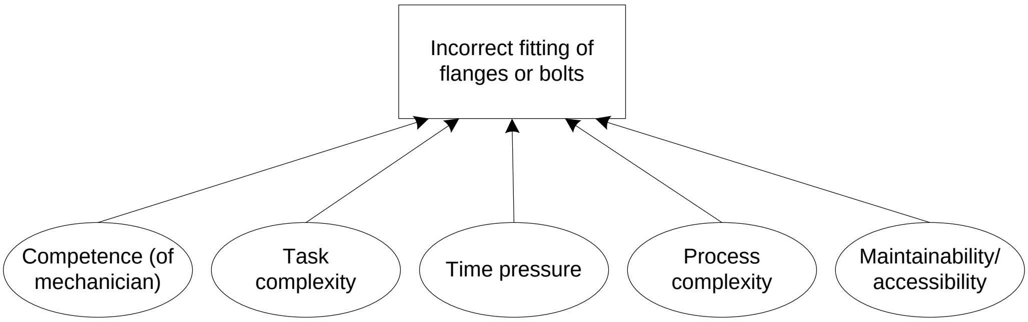


Figure 22 Influence diagram for the initiating event.

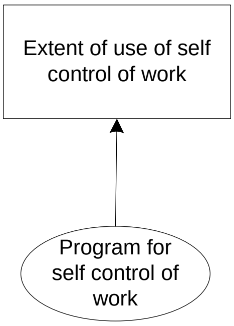


Figure 23 Influence diagram for barrier 1 – basic event 1.

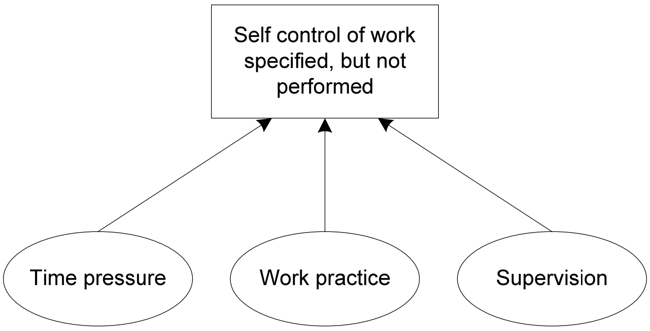


Figure 24 Influence diagram for barrier 1 – basic event 2.

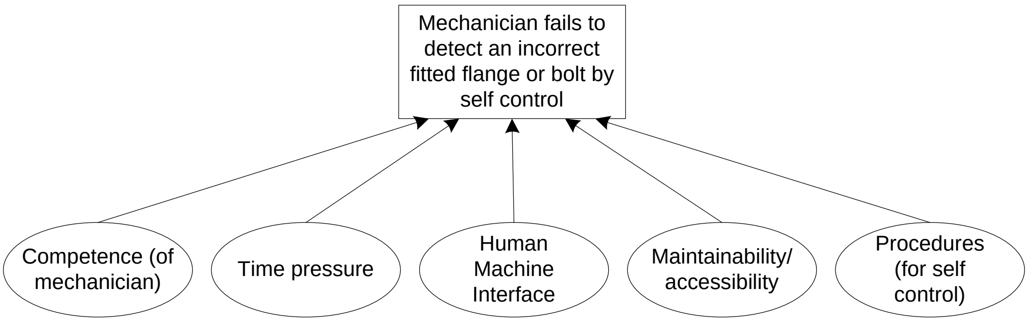


Figure 25 Influence diagram for barrier 1 – basic event 3.

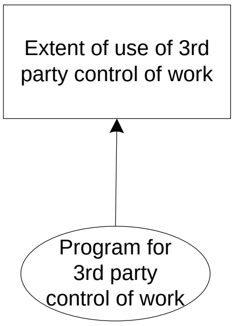


Figure 26 Influence diagram for barrier 2 – basic event 1.

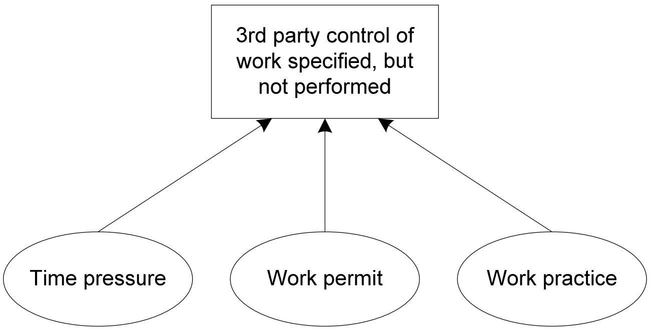


Figure 27 Influence diagram for barrier 2 – basic event 2.

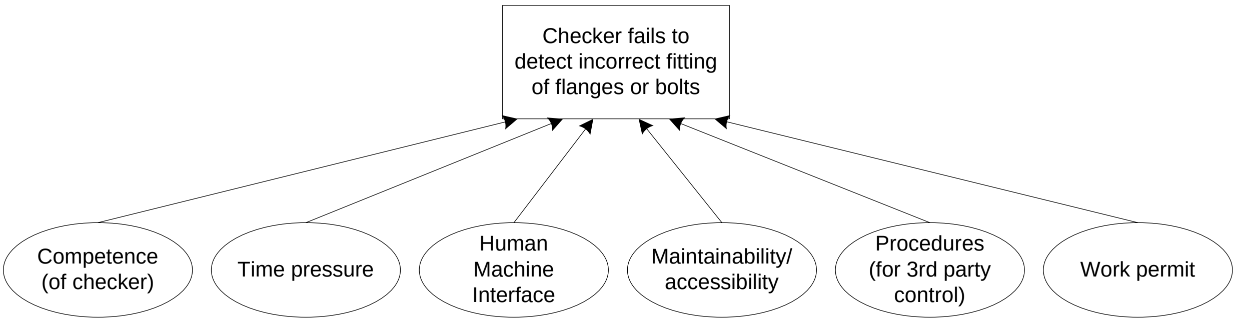


Figure 28 Influence diagram for barrier 2 – basic event 3.

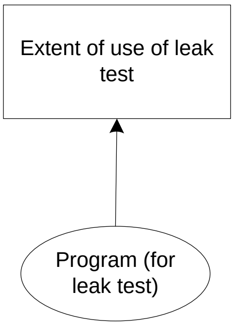


Figure 29 Influence diagram for barrier 3 – basic event 1.

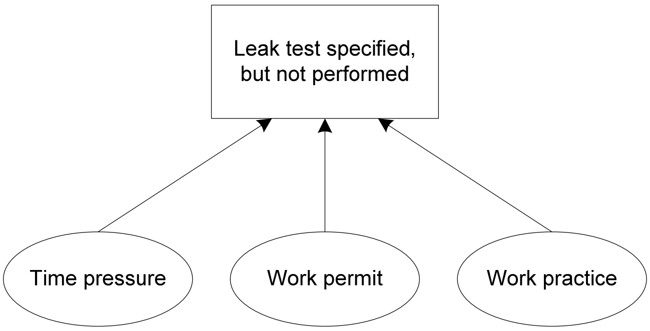


Figure 30 Influence diagram for barrier 3 – basic event 2.

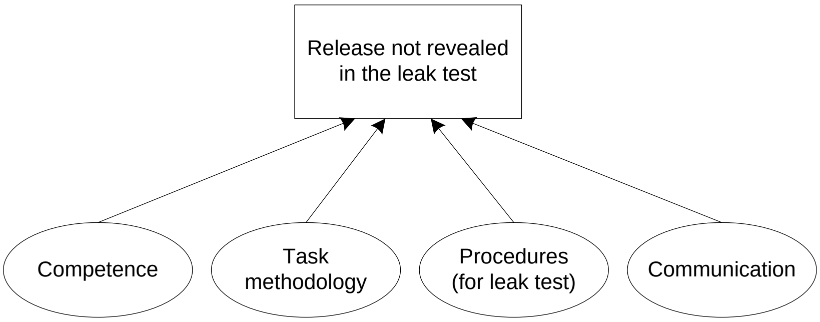


Figure 31 Influence diagram for barrier 3 – basic event 3.

1.5 Scenario B3 Release due to valves(s) in incorrect position after maintenance

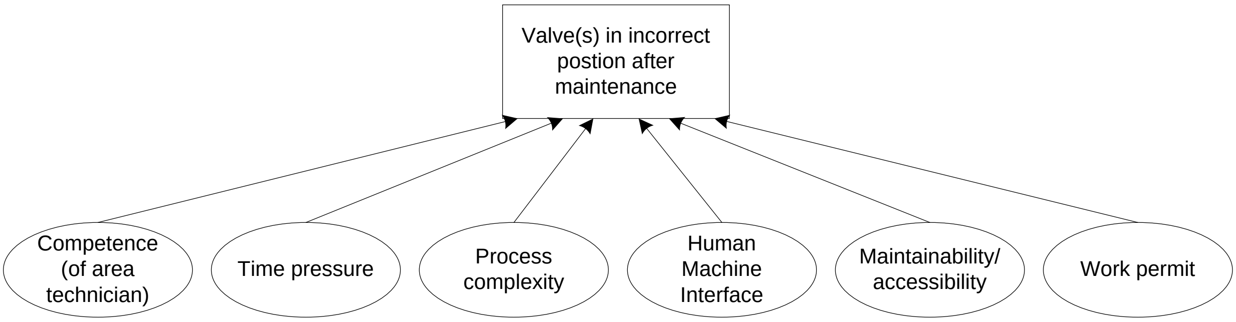


Figure 32 Influence diagram for the initiating event.

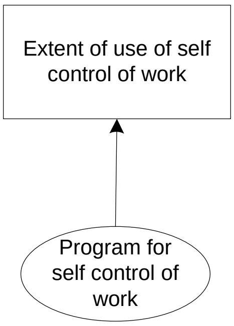


Figure 33 Influence diagram for barrier 1 – basic event 1.

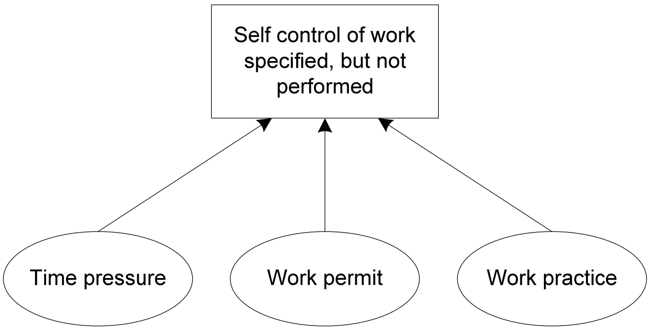


Figure 34 Influence diagram for barrier 1 – basic event 2.

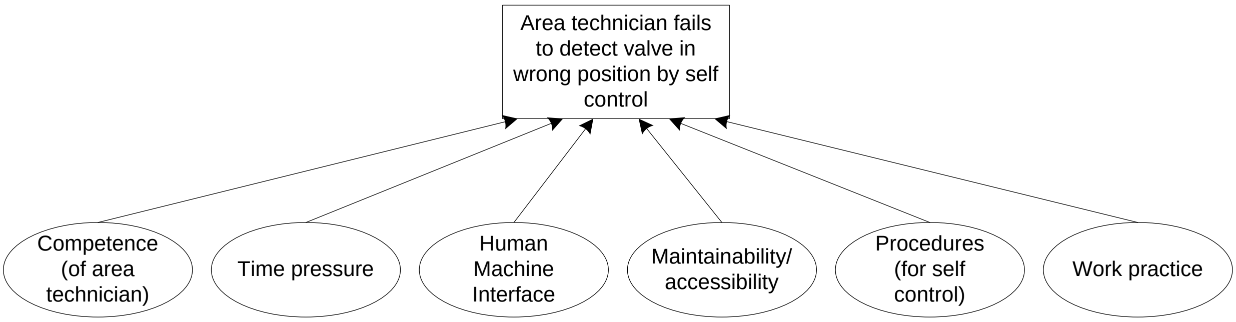


Figure 35 Influence diagram for barrier 1 – basic event 3.

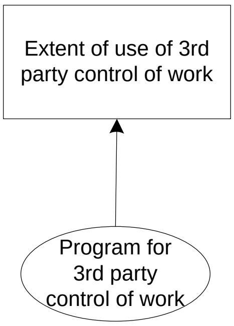


Figure 36 Influence diagram for barrier 2 – basic event 1.

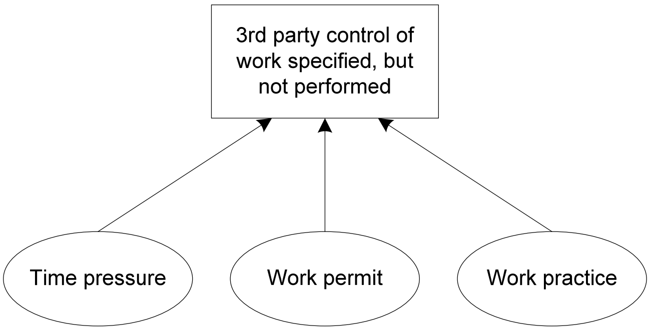


Figure 37 Influence diagram for barrier 2 – basic event 2.

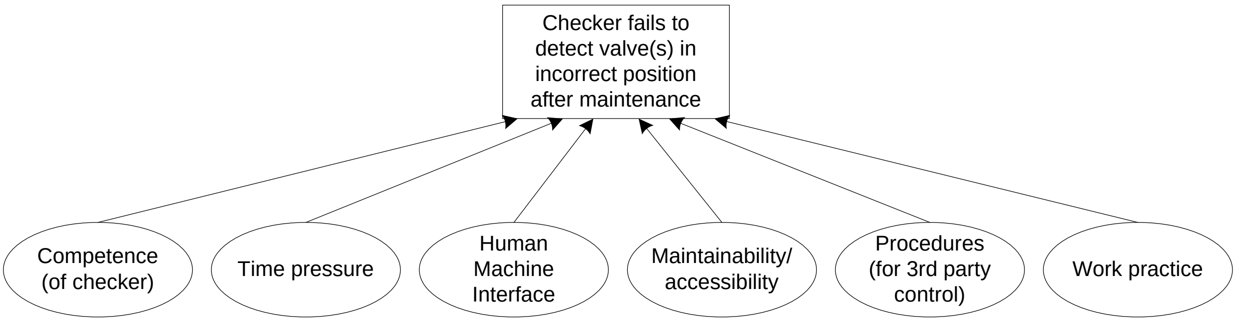


Figure 38 Influence diagram for barrier 2 – basic event 3.

1.6 Scenario B4 Release due to erroneous choice of installation of sealing device

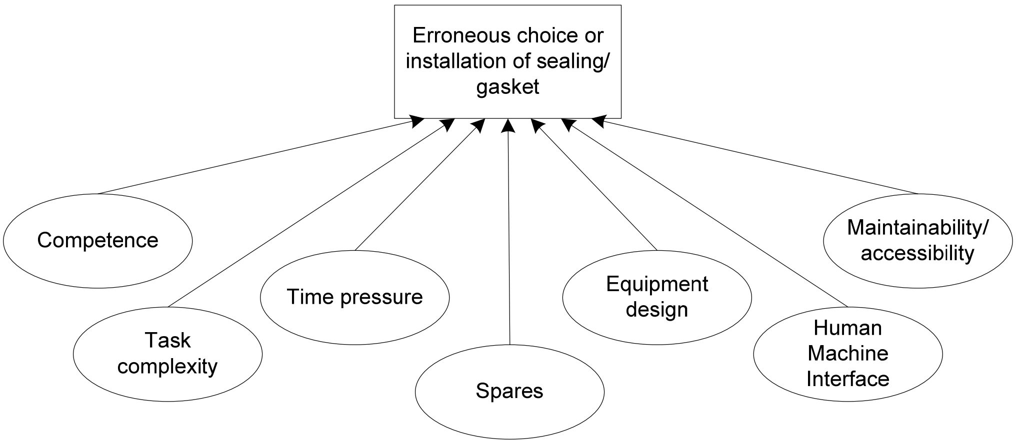


Figure 39 Influence diagram for the initiating event.

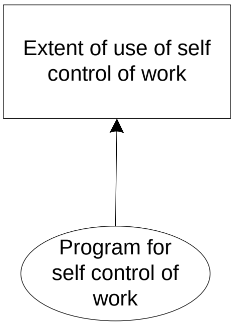


Figure 40 Influence diagram for barrier 1 – basic event 1.

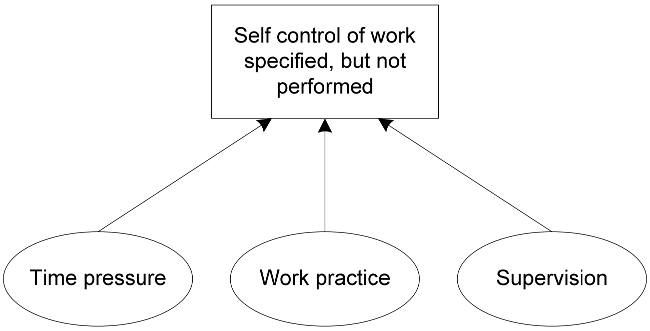


Figure 41 Influence diagram for barrier 1 – basic event 2.

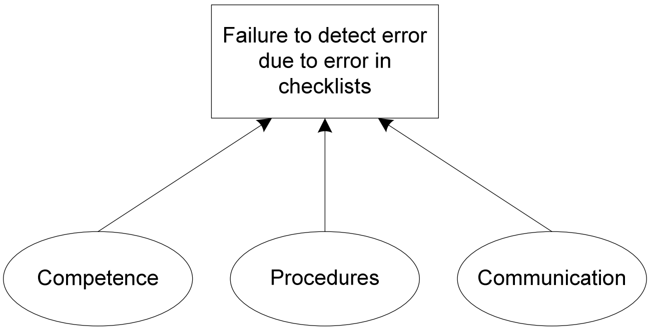


Figure 42 Influence diagram for barrier 1 – basic event 3.

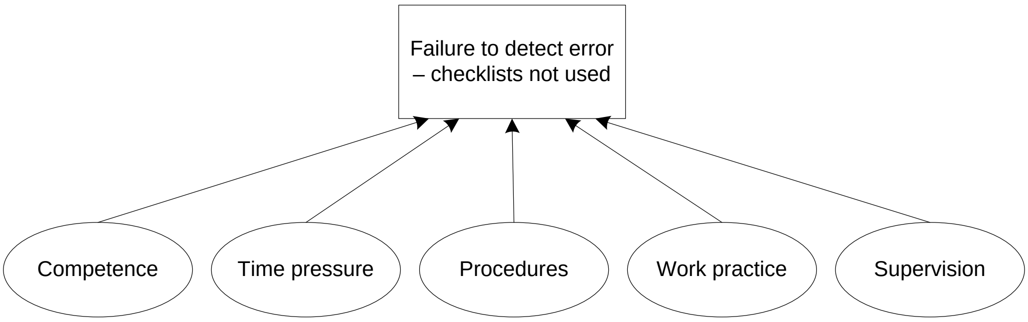


Figure 43 Influence diagram for barrier 1 – basic event 4.

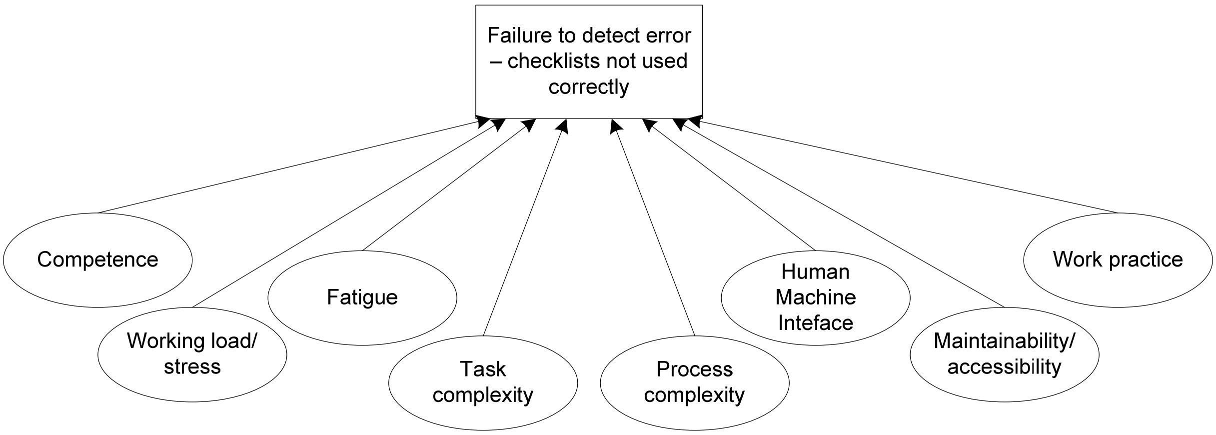


Figure 44 Influence diagram for barrier 1 –basic event 5.

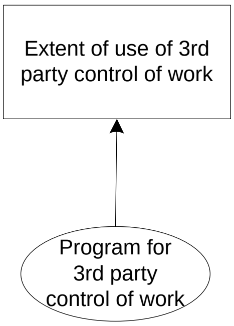


Figure 45 Influence diagram for barrier 2 – basic event 1.

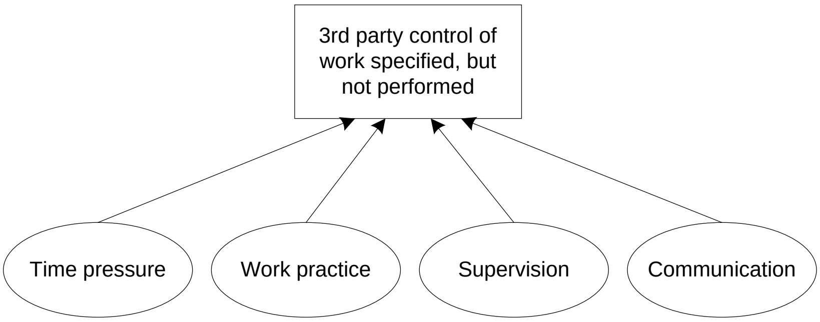


Figure 46 Influence diagram for barrier 2 – basic event 2.

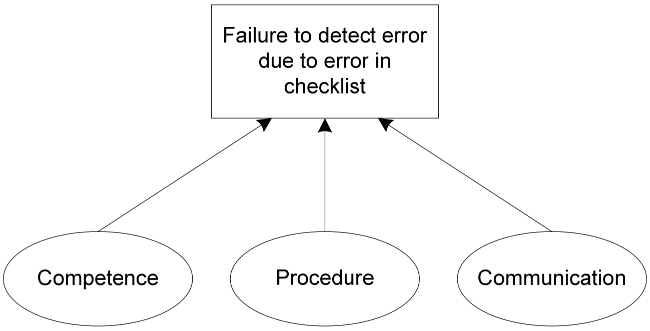


Figure 47 Influence diagram for barrier 2 – basic event 3.

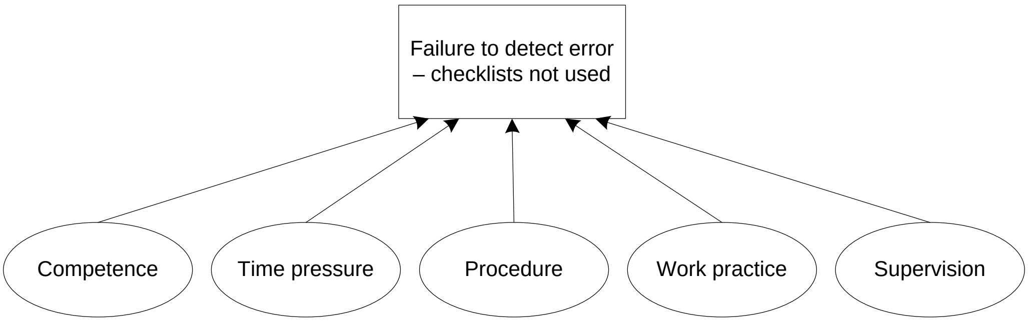


Figure 48 Influence diagram for barrier 2 – basic event 4.

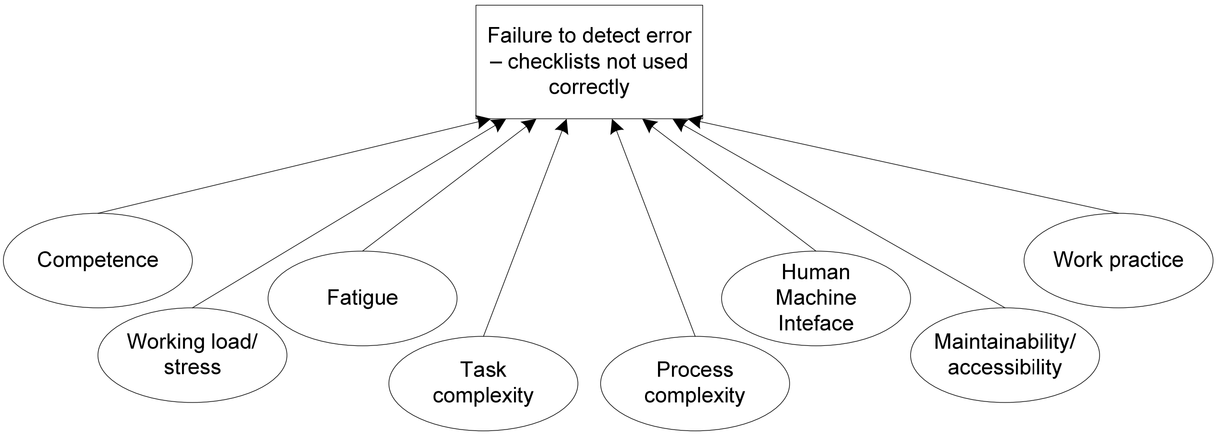


Figure 49 Influence diagram for barrier 2 – basic event 5.

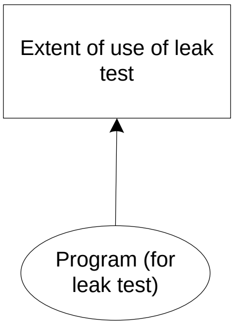


Figure 50 Influence diagram for barrier 3 – basic event 1.

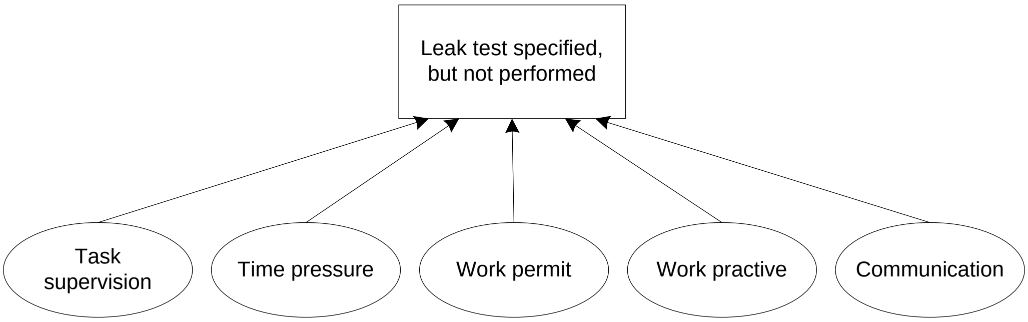


Figure 51 Influence diagram for barrier 3 – basic event 2.

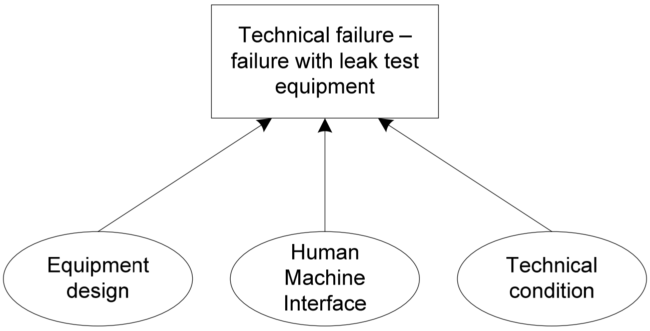


Figure 52 Influence diagram for barrier 3 – basic event 3.

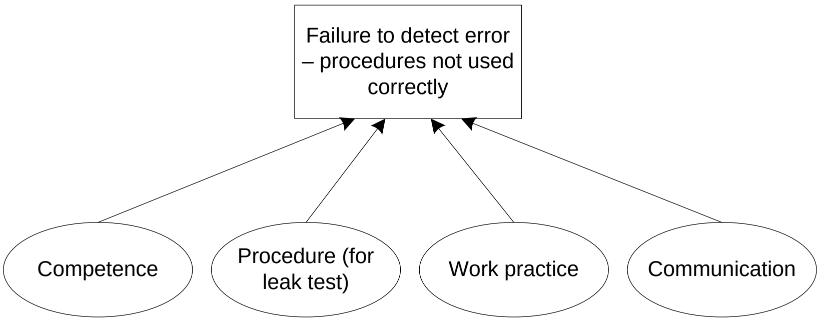


Figure 53 Influence diagram for barrier 3 – basic event 5.

1.7 Scenario B6 Release due to mal-operation of temporary hoses

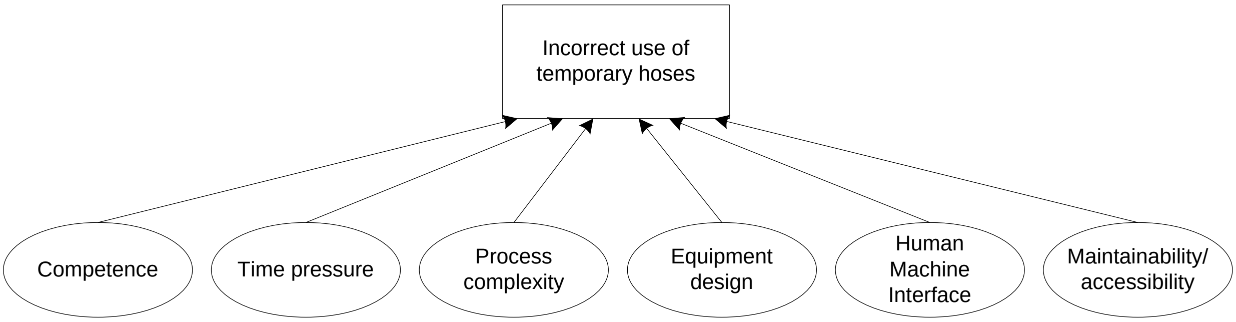


Figure 54 Influence diagram for the initiating event.

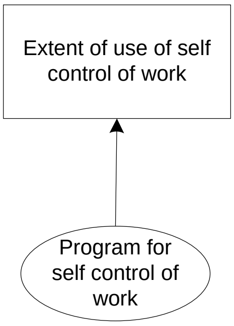


Figure 55 Influence diagram for barrier 1 – basic event 1.

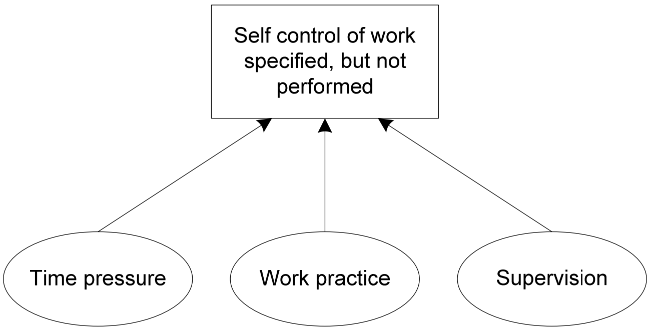


Figure 56 Influence diagram for barrier 1 – basic event 2.

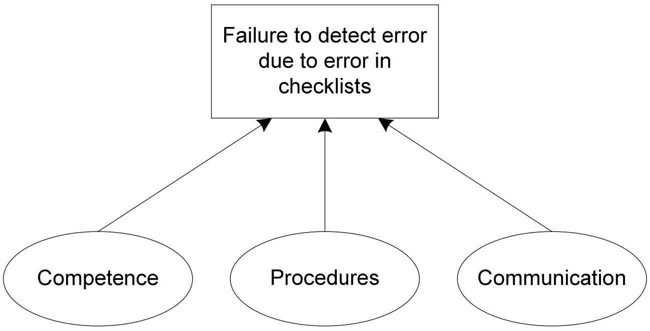


Figure 57 Influence diagram for barrier 1 – basic event 3.

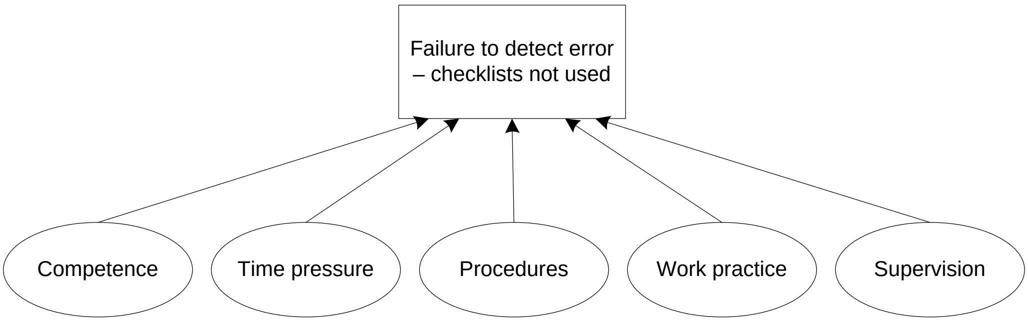


Figure 58 Influence diagram for barrier 1 – basic event 4.

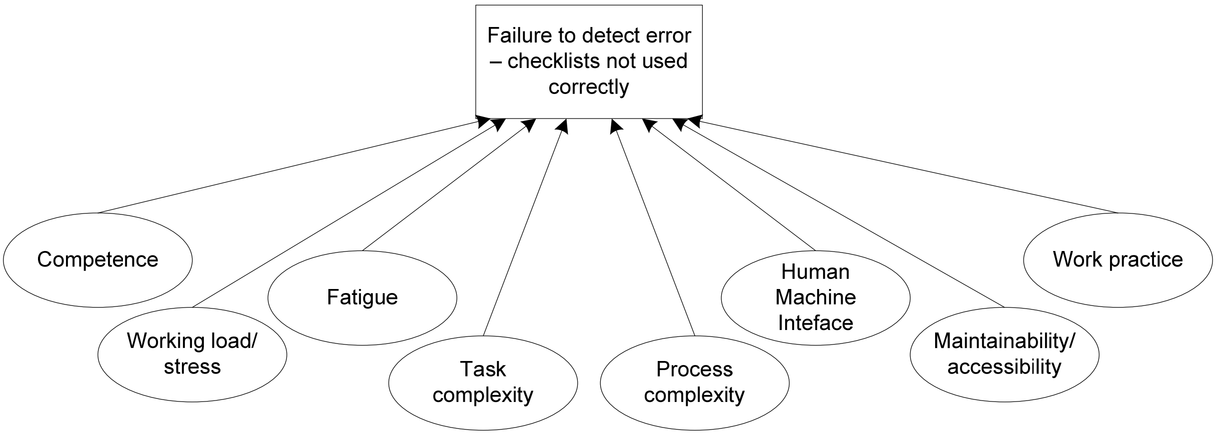


Figure 59 Influence diagram for barrier 1 – basic event 5.

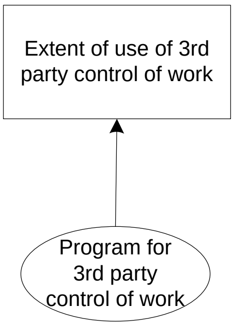


Figure 60 Influence diagram for barrier 2 – basic event 1.

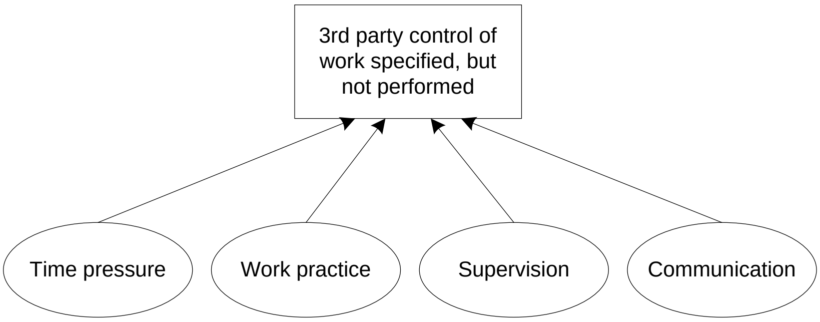


Figure 61 Influence diagram for barrier 2 – basic event 2.

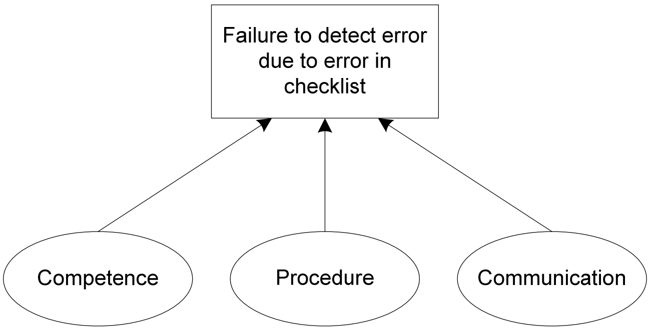


Figure 62 Influence diagram for barrier 2 – basic event 3.

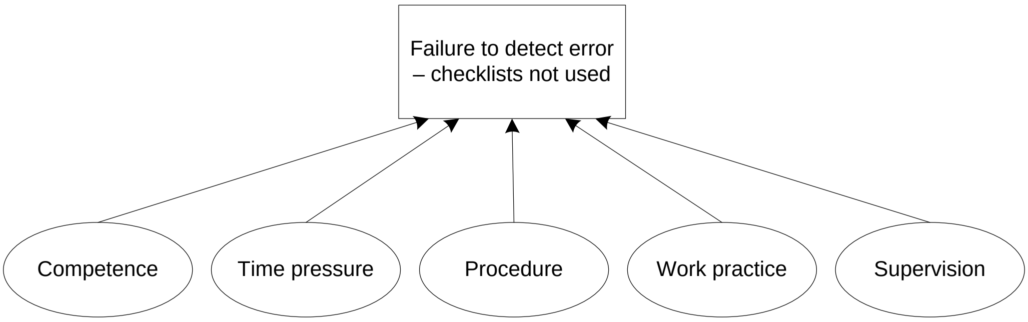


Figure 63 Influence diagram for barrier 2 – basic event 4.

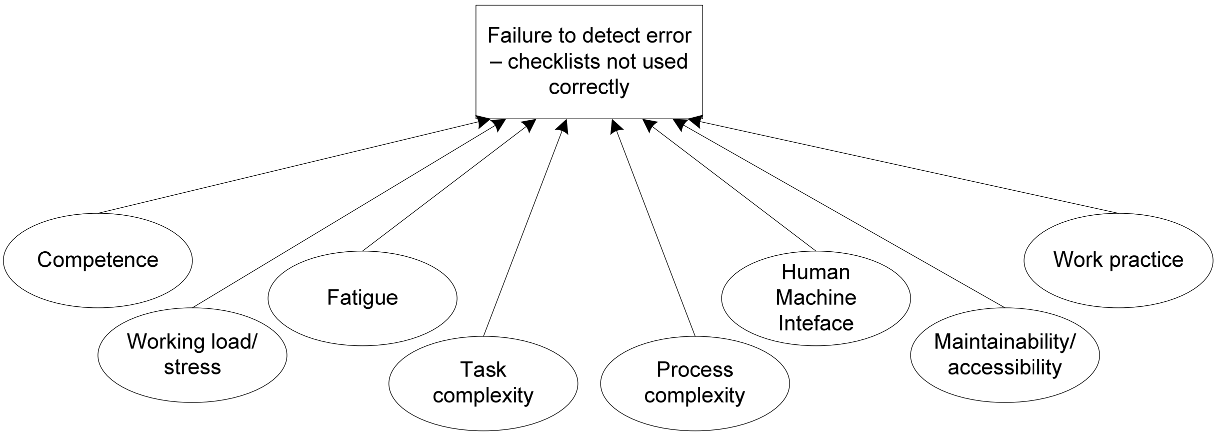


Figure 64 Influence diagram for barrier 2 – basic event 5.

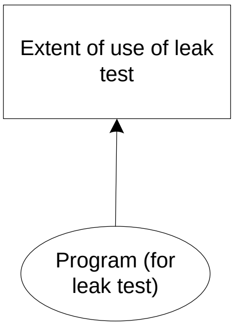


Figure 65 Influence diagram for barrier 3 – basic event 1.

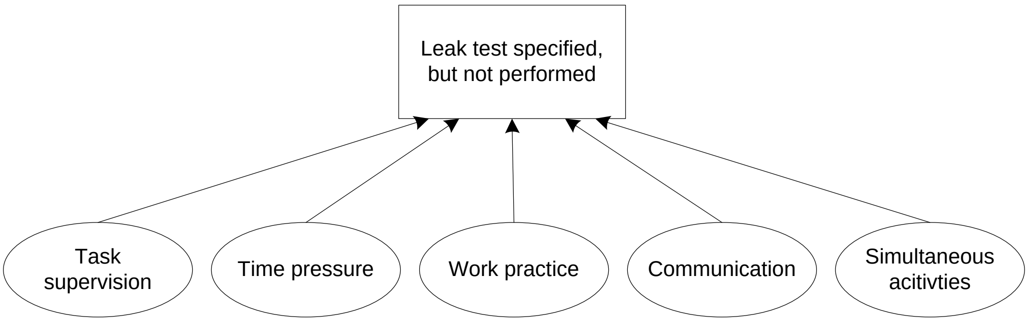


Figure 66 Influence diagram for barrier 3 – basic event 2.

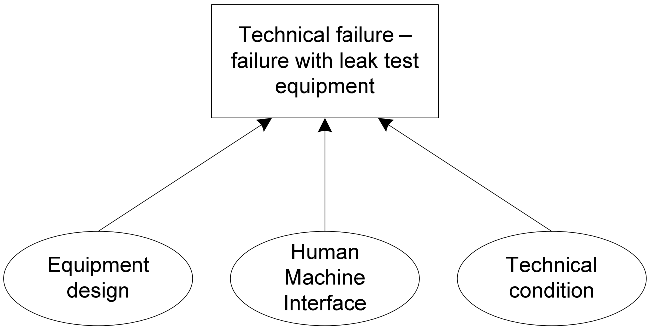


Figure 67 Influence diagram for barrier 3 – basic event 3.

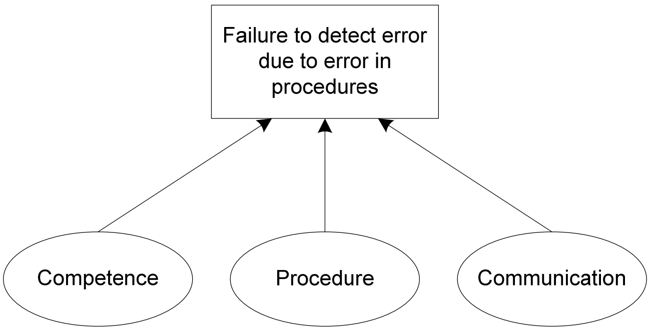


Figure 68 Influence diagram for barrier 3 – basic event 4.

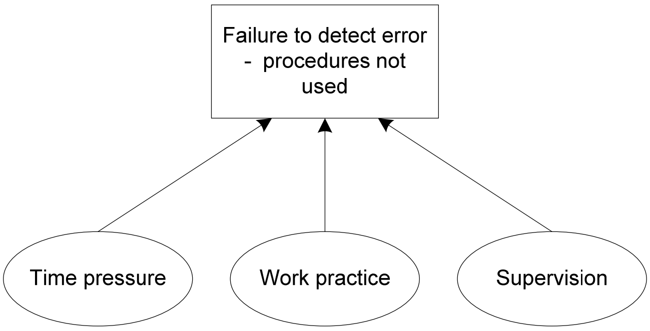


Figure 69 Influence diagram for barrier 3 – basic event 5.

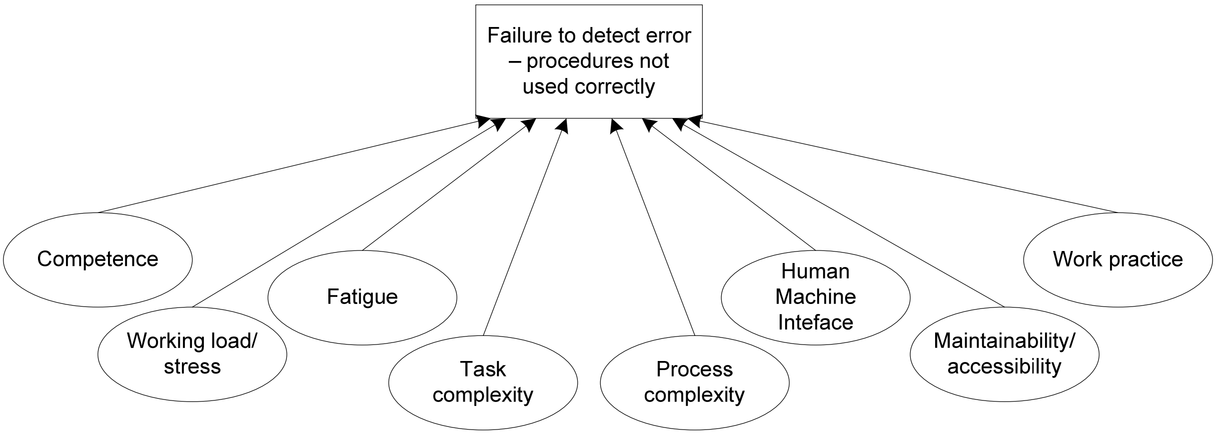


Figure 70 Influence diagram for barrier 3 – basic event 6.

1.8 Scenario C1 Release due to break-down of isolation system

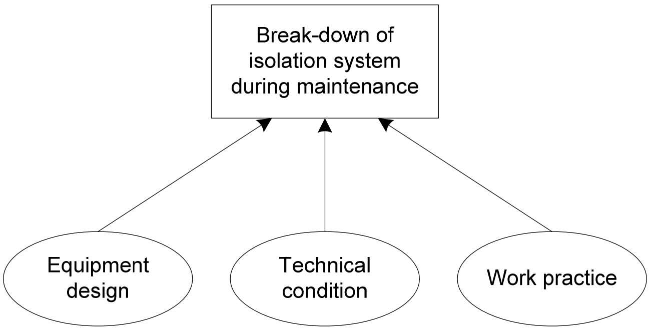


Figure 71 Influence diagram for the initiating event.

1.9 Scenario C2 Release due to mal-operation of valve(s) during manual operation

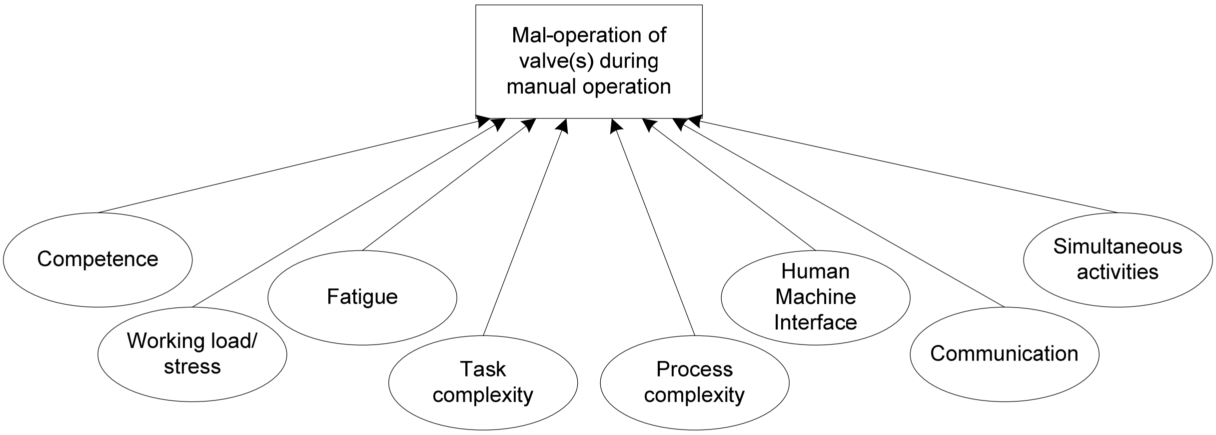


Figure 72 Influence diagram for the initiating event.

1.10 Scenario C3 Release due to work on wrong equipment

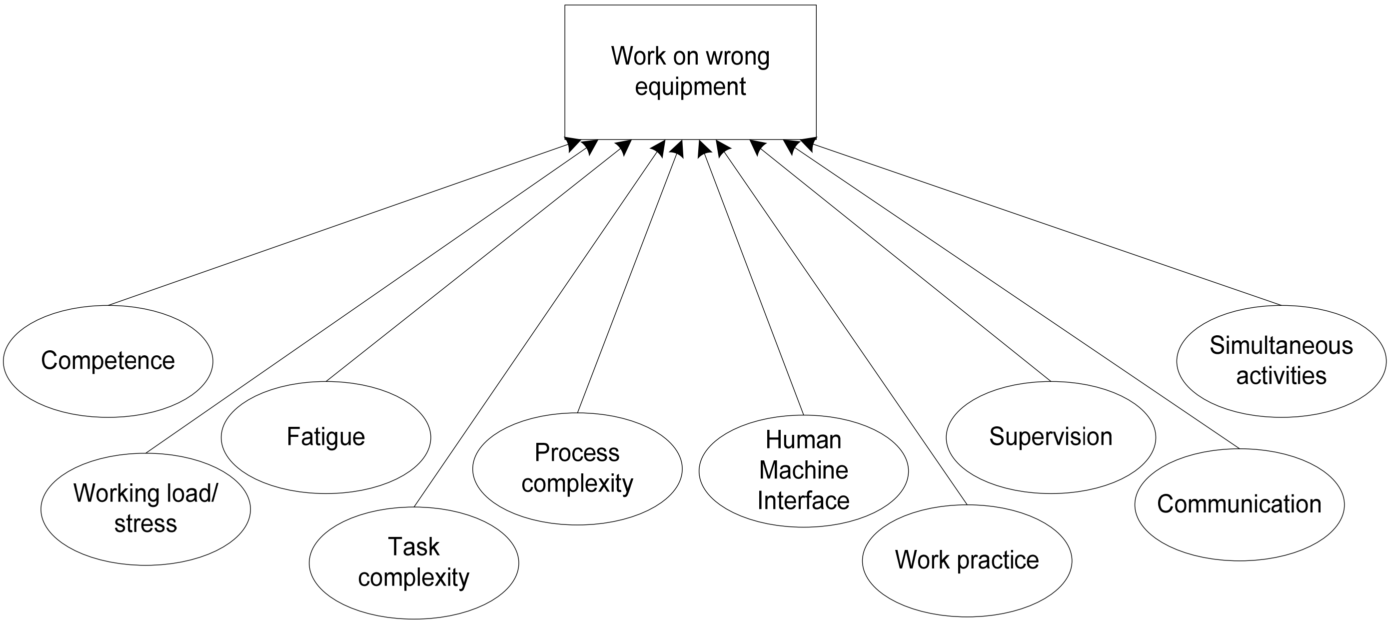


Figure 73 Influence diagram for the initiating event.

BORA

Barriere- &

operasjonell risikoanalyse

Operational Risk Analysis – Total Analysis of Physical and Non-physical Barriers

H3.1 Generalisation Report
Appendix 2
Human Error Probability Statistics

29 January 2007

1. Introduction

1.1 General

Risk influence diagrams are used to illustrate the RIFs influencing the different initiating events or basic events. Risk influence diagrams for different scenarios were developed during the case studies and are presented in this appendix.

1.2 Data Sources

Human error probability (HEP) data has been excerpted from the following sources:

- Swain and Guttman [1]
- Reason [2]
- Blackman and Gertman [3]
- Kirwan I [4]
- Kirwan II [5]

Each data source is described further below.

Swain, A.D and Guttmann H.E., Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, U.S. Nuclear regulatory commission report NUREG/CR-1278, SAND80-020, August 1983
The NUREG report presents methods, models and estimates human error probabilities to enable qualified analysts to make quantitative or qualitative assessments of occurrences of human errors that may affect the availability or operational reliability of engineered safe features and components in nuclear power plants

The handbook was started as a research in September 1976. The first draft came in 1980 where users provided comments and suggestions for improvement

The report provides the methodology to identify and quantify the potential for human error in nuclear power plant tasks. Most of the material in the handbook is also applicable to human reliability in other large process plants e.g. offshore oil production, oil refineries, chemical plants etc.

Limitations
- Limitation in the coverage and accuracy of human performance estimates.
- Human performance is difficult to predict because of its variability. This leads to uncertainties in human performance estimates. The uncertainty will be smallest when prediction behavior is made in performance of routine tasks such as test, maintenance, calibration, and normal control room operations and will be largest for prediction of behavior in response to an abnormal event.
- Models and estimated HEPs have not been developed for all NPP tasks.
- The handbook does not provide estimated HEPs related to the use of new display and control technology that is computer-based.
- It does not provide HEPs for corrective maintenance such as repairing a pump
- Scarcity of objective and quantitative data on human performance in NPPs
- Does not deal with/consider malevolent behavior

Reason, J., Managing the Risks of Organizational Accidents, 1997.
The aim of this textbook is to identify general principles and tools that are applicable to all organizations facing dangers of one sort or another. It includes banks and insurance companies just as much as nuclear power plants, oil exploration and production etc.

Limitation;
The generalization of dangers in different organizations may lead to a greater uncertainty in data.

Blackman, H. S. and Gertman, D. I., Human Reliability & Safety Analysis Data Handbook, 1994.
The book presents a summary of different methods and techniques, data and concepts as they are applied in the practice of HRA. The book first present probabilistic data that was available at time of print. These data are gathered from system engineer, risk analyst, behavioral scientist, human factors engineering, human reliability analyst, or other interested parties. Secondly it is tried to place the use of these data in context by providing a brief review of HRA methods and a few outstanding HRA issues. The intention is to provide effort to develop tools to help society cope and coexist in a safe and peaceful manner with the high risk industries.

Kirwan, B., A Guide to Practical Human Reliability Assessment, 1994.
The book is concerned with practical approaches to HRA, set in the framework of the HRA process, backed up by a number of appendices containing both relevant data and real case studies

Tables presented show data available drawn from Kirwan (1982), Kirwan et al (1990), and the database used in the Kirwan (1988) validation experiment

The report presents generic data, typical judgment-derived kinds of data that nevertheless provide acceptable guidelines for HRAs. Further it is presented data from operational plants, data from ergonomics studies and data from simulator studies.

The data presented are not intended to be used directly but rather to give the practitioner a feel for error rates.

Kirwan, B., Human Factors & Human Reliability in Offshore Systems, Course for SINTEF, Trondheim, May 11-13, 1998
This report was presented during a course in May 1998. The course concerns the discipline of Human Factors and its sub-discipline of Human Reliability Assessment. It also presents some tools available for the determination of the human's limitations and the improvement of system performance.

The focus of the course was on practical assistance in analyzing and enhancing offshore operations' safety and efficiency. It outlined the data types and sources, and available tools consider human error in systems. The course was based on Kirwan's experience in the offshore arena, and in other contemporary areas (nuclear power, chemical, transport)

2. Data Tables for Initiating Events

The following sections present HEP data related to initiating events, excerpted from the data sources listed in Section 1.2. The column “Data Source” refers to the references presented in Section 4. Occasionally, the data sources refer further to other data references. These references are quoted in the “Description” column, but it is referred to the main data sources for the full reference.

2.1 B1: Incorrect blinding/isolation

The data which are used as background values when assigning human error probability related to the event “incorrect blinding/isolation” are shown in Table 1.

Table 1 HEP Data Reviewed in Connection with the Event ”Incorrect Blinding/Isolation”

Event: Incorrect Blinding/Isolation						
Probability of Failure					**Data Source**	**Description**
		Percentiles				
Average	**EF**	**5 %**	**50 %**	**95 %**		
						Estimated probabilities of errors of omission per item of instruction when use of written procedures with checkoff provisions are correctly used:
$1.00 \cdot 10^{-3}$	3				1	Short list, ≤ 10 items
$3.00 \cdot 10^{-3}$	3				1	Long list, > 10 items
						Estimated probabilities of errors of omission per item of instruction when use of written procedures is specified, but not used or incorrectly used
$3.00 \cdot 10^{-3}$	3				1	Short list, ≤ 10 items
$1.00 \cdot 10^{-2}$	3				1	Long list, > 10 items
$5.00 \cdot 10^{-2}$	5				1	Estimated probabilities of errors of omission per item of instruction when written procedures are available and should be used but are not used.
						Estimated HEPs related to failure of administrative control:
$1.00 \cdot 10^{-3}$	3				1	Initiate a scheduled shiftly checking or inspection function
$1.00 \cdot 10^{-2}$	5				1	Carry out a plant policy or scheduled tasks such as periodic tests or maintenance performed weekly, monthly, or at longer intervals
$5.00 \cdot 10^{-2}$	5				1	Use of written test or calibration procedures
$5.00 \cdot 10^{-2}$	5				1	Use written maintenance procedures
$5.00 \cdot 10^{-1}$	5					Use a checklist properly
		$8.00 \cdot 10^{-4}$	$3.00 \cdot 10^{-3}$	$7.00 \cdot 10^{-3}$	2	Restore or shift system to original or new state following procedures with some checking Generic task and associated probabilities (Williams)
$1.50 \cdot 10^{-1}$					3	Vigilance task. Data on human failure rates for general tasks (Lanzetta et al.)

Event: Incorrect Blinding/Isolation						
Probability of Failure					**Data Source**	**Description**
		Percentiles				
Average	**EF**	**5 %**	**50 %**	**95 %**		
		$2.00 \cdot 10^{-2}$	$7.00 \cdot 10^{-2}$	$1.70 \cdot 10^{-2}$	3	Detect deviation from standard. Data on human failure rate for general tasks (Williams 1989)
		$4.00 \cdot 10^{-4}$	$1.00 \cdot 10^{-3}$	$3.00 \cdot 10^{-3}$	3	Control/demand. Data on human failure rates for general tasks (Williams 1989)
	12	$5.50 \cdot 10^{-4}$		$8.30 \cdot 10^{-2}$	3	Violate procedure and reconfigure equipment. (Gertman et al. 1992)
	10	$1.20 \cdot 10^{-3}$		$1.20 \cdot 10^{-1}$	3	Checker performing quality assurance tolerate a discrepancy. (Gertman et al. 1992)
	7	$4.60 \cdot 10^{-3}$		$2.00 \cdot 10^{-1}$	3	Common mode: failures due to poor safety culture (Gertman et al. 1992)
	8	$3.90 \cdot 10^{-3}$		$2.20 \cdot 10^{-1}$	3	Right diagnosis, wrong response; capture sequence based on response set; right conclusions bur wrong action pathway selected (Gertman et al. 1992)
						Comparison of Error Probabilities on Maintenance Tasks for Pumps and Valves (Stewart 1981):
$4.00 \cdot 10^{-2}$					3	Couplings: alignment or clearance in valves
$6.00 \cdot 10^{-2}$					3	Couplings: alignment or clearance in pumps
$6.00 \cdot 10^{-2}$					3	Poor fitting or coupling joints in valves
$1.60 \cdot 10^{-1}$					3	Poor fitting or coupling joints in pumps
		$1.00 \cdot 10^{-3}$		$1.00 \cdot 10^{-2}$	4	Failure to start procedure when procedure used. (Task analysis: initiation of flow via stand-by train, Webley & Acroyd, 1988)
$1.00 \cdot 10^{-2}$					4	General error of omission
$3.00 \cdot 10^{-3}$					4	Error of omission of an act embedded in a procedure
$3.00 \cdot 10^{-3}$					4	General error rate for an act performed incorrectly
$1.00 \cdot 10^{-4}$					4	Human performance limit: single operator
$2.00 \cdot 10^{-4}$					4	Incorrect setting (this HEP was derived from a number of NPP simulator scenarios, and based on unrecovered errors.)
		$8.00 \cdot 10^{-4}$	$3.00 \cdot 10^{-3}$	$9.00 \cdot 10^{-3}$	5	Restore or shift system to original or new state following procedures with some checking (generic classification HEART)

2.2 B2: Incorrect Fitting of Flanges and Bolts

The data which are used as background values when assigning human error probability related to the event “incorrect fitting of flanges and bolts” are shown in Table 2.

Table 2 HEP Data Reviewed in Connection with the Event ”Incorrect Fitting of Flanges and Bolts”

Event: Incorrect Fitting of Flanges and Bolts						
Probability of Failure					**Data Source**	**Description**
		Percentiles				
Average	**EF**	**5 %**	**50 %**	**95 %**		
						Estimated probabilities of errors of omission per item of instruction when use of written procedures with checkoff provisions are correctly used:
$1.00 \cdot 10^{-3}$	3				1	Short list, ≤ 10 items
$3.00 \cdot 10^{-3}$	3				1	Long list, > 10 items
						Estimated probabilities of errors of omission per item of instruction when use of written procedures is specified, but not used or incorrectly used:
$3.00 \cdot 10^{-3}$	3				1	Short list, ≤ 10 items
$1.00 \cdot 10^{-2}$	3				1	Long list, > 10 items
$5.00 \cdot 10^{-2}$	5				1	Estimated probabilities of errors of omission per item of instruction when written procedures are available and should be used but are not used.
						Estimated HEPs related to failure of administrative control:
$1.00 \cdot 10^{-2}$	5				1	Carry out a plant policy or scheduled tasks such as periodic tests or maintenance performed weekly, monthly, or at longer intervals
$5.00 \cdot 10^{-2}$	5				1	Use of written test or calibration procedures
$5.00 \cdot 10^{-2}$	5				1	Use written maintenance procedures
		$8.00 \cdot 10^{-4}$	$3.00 \cdot 10^{-3}$	$7.00 \cdot 10^{-3}$	2	Restore or shift system to original or new state following procedures with some checking
$7.00 \cdot 10^{-2}$					3	Meter reading. Data on human failure rates for general tasks (Horst et al.)
		$2.00 \cdot 10^{-2}$	$7.00 \cdot 10^{-2}$	$1.70 \cdot 10^{-2}$	3	Detect deviation from standard. Data on human failure rate for general tasks (Williams 1989)
		$4.00 \cdot 10^{-4}$	$1.00 \cdot 10^{-3}$	$3.00 \cdot 10^{-3}$	3	Control/demand. Data on human failure rates for general tasks (Williams 1989)
		$3.00 \cdot 10^{-5}$	$7.00 \cdot 10^{-5}$	$4.00 \cdot 10^{-3}$	3	Assembly task element. Data on human failure rates for general tasks (Williams 1989).
	12	$5.50 \cdot 10^{-4}$		$8.30 \cdot 10^{-2}$	3	Violate procedure and reconfigure equipment. (Gertman et al. 1992)
	10	$1.20 \cdot 10^{-3}$		$1.20 \cdot 10^{-1}$	3	Checker performing quality assurance tolerates a discrepancy. (Gertman et al. 1992)

Event: Incorrect Fitting of Flanges and Bolts						
Probability of Failure						
		Percentiles				
Average	**EF**	**5 %**	**50 %**	**95 %**	**Data Source**	**Description**
	7	$4.60 \cdot 10^{-3}$		$2.00 \cdot 10^{-1}$	3	Common mode: failures due to poor safety culture (Gertman et al. 1992)
	8	$3.90 \cdot 10^{-3}$		$2.20 \cdot 10^{-1}$	3	Right diagnosis, wrong response; capture sequence based on response set; right conclusions bur wrong action pathway selected (Gertman et al. 1992)
$4.00 \cdot 10^{-3}$					3	Tighten nuts, bolts, and plugs. Task element reliabilities from data store (Irwin et al. 1964)
$2.00 \cdot 10^{-3}$					3	Install nuts, plugs, and bolts. Task element reliabilities from data store (Irwin et al. 1964)
$1.90 \cdot 10^{-3}$					3	Remove nuts, plugs, and bolts. Task element reliabilities from data store (Irwin et al. 1964)
$1.90 \cdot 10^{-3}$					3	Install torque wrench adapter. Task element reliabilities from data store (Irwin et al. 1964)
$9.00 \cdot 10^{-4}$					3	Remove torque wrench adapter. Task element reliabilities from data store (Irwin et al. 1964)
						Comparison of Error Probabilities on Maintenance Tasks for Pumps and Valves (Stewart 1981):
$1.00 \cdot 10^{-2}$					3	Bolts; length and type for pumps
$1.00 \cdot 10^{-2}$					3	Bolts; Torque for pumps
$1.00 \cdot 10^{-2}$					3	Bolts; Damaged for pumps
$6.00 \cdot 10^{-2}$					3	Bolts; length and type for valves
$1.00 \cdot 10^{-1}$					3	Bolts; Torque for valves
$6.00 \cdot 10^{-2}$					3	Bolts; Damaged for valves
		$1.00 \cdot 10^{-3}$		$1.00 \cdot 10^{-2}$	4	Failure to start procedure when procedure used. (Task analysis: initiation of flow via stand-by train, Webley & Acroyd, 1988)
		$1.00 \cdot 10^{-2}$		$5.00 \cdot 10^{-2}$	4	Failure to start procedure when procedure is not used. (Task analysis: initiation of flow via stand-by train, Webley & Acroyd, 1988)
$1.00 \cdot 10^{-2}$					4	General error of omission
$1.00 \cdot 10^{-2}$					4	Error in a routine operation where care is required
$3.00 \cdot 10^{-3}$					4	Error of omission of an act embedded in a procedure
$3.00 \cdot 10^{-3}$					4	General error rate for an act performed incorrectly
$1.00 \cdot 10^{-4}$					4	Human-performance limit: single operator
$1.00 \cdot 10^{-3}$					4	Valve mis-set during calibration task 3)
$2.00 \cdot 10^{-4}$					4	Incorrect setting (this HEP was derived from a number of NPP simulator scenarios, and based on unrecovered errors.)
		$8.00 \cdot 10^{-4}$	$3.00 \cdot 10^{-3}$	$9.00 \cdot 10^{-3}$	5	Restore or shift system to original or new state following procedures with some checking (generic classification HEART)

2.3 B3: Valve(s) in Incorrect Position after Maintenance

The data which are used as background values when assigning human error probability related to the event “valve(s) in incorrect position after maintenance” are shown in Table 3.

Table 3 HEP Data Reviewed in Connection with the Event ”Valve(s) in Incorrect Position after Maintenance”

Event: Valve(s) in Incorrect Position after Maintenance						
Probability of Failure					**Data Source**	**Description**
		Percentiles				
Average	**EF**	**5 %**	**50 %**	**95 %**		
						Estimated HEPs for selection errors for locally operated valves. Making an error of selection in changing or restoring a locally operated valve when the valve to be manipulated is;
$1.00 \cdot 10^{-3}$	3				1	Clearly and unambiguously labeled, set apart from valves that are similar in all of the following: size and shape, state, and presence of tags1)
$3.00 \cdot 10^{-3}$	3				1	Clearly and unambiguously labeled, part of a group of two or more valves that are similar in one of the following: size and shape, state, or presence of tags1)
$5.00 \cdot 10^{-3}$	3				1	Unclearly or ambiguously labeled, set apart from valves that are similar in all of the following: size and shape, state, and presence of tags1)
$8.00 \cdot 10^{-3}$	3				1	Unclearly or ambiguously labeled, part of a group of two or more valves that are similar in one of the following: size and shape, state, or presence of tags1)
$1.00 \cdot 10^{-2}$	3				1	Unclearly or ambiguously labeled, part of a group of two or more valves that are similar in all of the following: size and shape, state, and presence of tags1)
						Estimated HEPs in detecting stuck locally operated valves. Given that a locally operated valve sticks as it is being changed or restored, the operator fails to notice the sticking valve when it has (prob. Valve sticking 0.001 per manipulation, EF=10):
$1.00 \cdot 10^{-3}$	3				1	A position indicator only (incorporates a scale that indicates the position of the valve relative to a fully opened or fully closed position).
$2.00 \cdot 10^{-3}$	3				1	A position indicator and a rising steam (does not have a scale in difference to position indicator)
$5.00 \cdot 10^{-3}$	3				1	A rising stem but no position indicator
$1.00 \cdot 10^{-2}$	3				1	Neither rising stem nor position indicator
						Estimated probabilities of errors of omission per item of instruction when use of written procedures with checkoff provisions are correctly used:
$1.00 \cdot 10^{-3}$	3				1	Short list, ≤ 10 items
$3.00 \cdot 10^{-3}$	3				1	Long list, > 10 items

Event: Valve(s) in Incorrect Position after Maintenance						
Probability of Failure					**Data Source**	**Description**
		Percentiles				
Average	**EF**	**5 %**	**50 %**	**95 %**		
						Estimated probabilities of errors of omission per item of instruction when use of written procedures is specified, but not used or incorrectly used
$3.00 \cdot 10^{-3}$	3				1	Short list, ≤ 10 items
$1.00 \cdot 10^{-2}$	3				1	Long list, > 10 items
$5.00 \cdot 10^{-2}$	5				1	Estimated probabilities of errors of omission per item of instruction when written procedures are available and should be used but are not used.
						Estimated HEPs related to failure of administrative control:
$1.00 \cdot 10^{-2}$	5				1	Carry out a plant policy or scheduled tasks such as periodic tests or maintenance performed weekly, monthly, or at longer intervals
$1.00 \cdot 10^{-2}$	3				1	Use a valve change or restoration list
$5.00 \cdot 10^{-2}$	5				1	Use of written test or calibration procedures
$5.00 \cdot 10^{-2}$	5				1	Use written maintenance procedures
		$8.00 \cdot 10^{-4}$	$3.00 \cdot 10^{-3}$	$7.00 \cdot 10^{-3}$	2	Restore or shift system to original or new state following procedures with some checking Generic task and associated probabilities (Williams)
		$3.30 \cdot 10^{-2}$	$1.30 \cdot 10^{-1}$	$3.00 \cdot 10^{-1}$	3	Error of omission by auxiliary operator (opens/closes valve) (Gilbert et al. 1990)
		$5.50 \cdot 10^{-4}$	$2.80 \cdot 10^{-3}$	$1.40 \cdot 10^{-2}$	3	Error of commission by auxiliary operator (opens/closes valve) (Gilbert et al. 1990)
$1.80 \cdot 10^{-3}$					3	Close valve. Data on human failure rates (adapted from Williams 1989, data source Peters)
$1.50 \cdot 10^{-3}$					3	Align manual valve. Data on human failure rates (adapted from Williams 1989, data source Lukas and Hall)
$4.00 \cdot 10^{-4}$					3	Operate remote valve. Data on human failure rates (adapted from Williams 1989, data source Lukas and Hall)
		$2.00 \cdot 10^{-2}$	$7.00 \cdot 10^{-2}$	$1.70 \cdot 10^{-2}$	3	Detect deviation from standard Data on human failure rates for general tasks (Williams 1989)
		$4.00 \cdot 10^{-4}$	$1.00 \cdot 10^{-3}$	$3.00 \cdot 10^{-3}$	3	Control/demand. Data on human failure rates for general tasks (Williams 1989)
	12	$5.50 \cdot 10^{-4}$		$8.30 \cdot 10^{-2}$	3	Violate procedure and reconfigure equipment. (Gertman et al. 1992)
	10	$1.20 \cdot 10^{-3}$		$1.20 \cdot 10^{-1}$	3	Checker performing quality assurance tolerate a discrepancy. (Gertman et al. 1992)
	7	$4.60 \cdot 10^{-3}$		$2.00 \cdot 10^{-1}$	3	Common mode: failures due to poor safety culture (Gertman et al. 1992)
	8	$3.90 \cdot 10^{-3}$		$2.20 \cdot 10^{-1}$	3	Right diagnosis, wrong response; capture sequence based on response set; right conclusions bur wrong action pathway selected (Gertman et al. 1992)

Event: Valve(s) in Incorrect Position after Maintenance						
Probability of Failure					**Data Source**	**Description**
		Percentiles				
Average	**EF**	**5 %**	**50 %**	**95 %**		
		$1.00 \cdot 10^{-3}$		$1.00 \cdot 10^{-2}$	4	Failure to start procedure when procedure used. (Task analysis: initiation of flow via stand-by train, Webley & Acroyd, 1988)
		$1.00 \cdot 10^{-2}$		$5.00 \cdot 10^{-2}$	4	Failure to start procedure when procedure is not used. (Task analysis: initiation of flow via stand-by train, Webley & Acroyd, 1988)
$1.00 \cdot 10^{-3}$						Roving operators opens correct valve, error of omission - verbal order (Task analysis: initiation of flow via stand-by train, Webley & Acroyd, 1988)
		$1.00 \cdot 10^{-3}$		$1.00 \cdot 10^{-2}$		Roving operators opens correct valve, error of commission - selecting incorrect valve (Task analysis: initiation of flow via stand-by train, Webley & Acroyd, 1988)
$1.00 \cdot 10^{-2}$					4	Failure to return the manually operated test valve to the correct configuration after maintenance.
$1.00 \cdot 10^{-2}$					4	General error of omission
$3.00 \cdot 10^{-3}$					4	Error of omission of an act embedded in a procedure
$3.00 \cdot 10^{-3}$					4	General error rate for an act performed incorrectly
$1.00 \cdot 10^{-3}$					4	Error in simple routine operation
$1.00 \cdot 10^{-4}$					4	human performance limit: single operator
$1.00 \cdot 10^{-3}$					4	Valve mis-set during calibration task 3)
$2.00 \cdot 10^{-4}$					4	Incorrect setting (this HEP was derived from a number of NPP simulator scenarios, and based on unrecovered errors.)
$2.00 \cdot 10^{-4}$					4	Equipment turned in wrong direction (this HEP was derived from a number of NPP simulator scenarios, and based on unrecovered errors.)
		$8.00 \cdot 10^{-4}$	$3.00 \cdot 10^{-3}$	$9.00 \cdot 10^{-3}$	5	Restore or shift system to original or new state following procedures with some checking (generic classification HEART)

2.4 B4: Erroneous Choice/Installation of Sealing Device

The data which are used as background values when assigning human error probability related to the event “erroneous choice/installation of sealing device” are shown in Table 4.

Table 4 HEP Data Reviewed in Connection with the Event ”Erroneous Choice/Installation of Sealing Device”

Event: Erroneous Choice/Installation of Sealing Device						
Probability of Failure						
		Percentiles				
Average	**EF**	**5 %**	**50 %**	**95 %**	**Data Source**	**Description**
						Estimated probabilities of errors of omission per item of instruction when use of written procedures with checkoff provisions are correctly used:
$1.00 \cdot 10^{-3}$	3				1	Short list, ≤ 10 items
$3.00 \cdot 10^{-3}$	3				1	Long list, > 10 items
						Estimated probabilities of errors of omission per item of instruction when use of written procedures is specified, but not used or incorrectly used
$3.00 \cdot 10^{-3}$	3				1	Short list, ≤ 10 items
$1.00 \cdot 10^{-2}$	3				1	Long list, > 10 items
$5.00 \cdot 10^{-2}$	5				1	Estimated probabilities of errors of omission per item of instruction when written procedures are available and should be used but are not used.
						Estimated HEPs related to failure of administrative control
$1.00 \cdot 10^{-3}$	3				1	Initiate a scheduled shiftly checking or inspection function
$1.00 \cdot 10^{-2}$	5				1	Carry out a plant policy or scheduled tasks such as periodic tests or maintenance performed weekly, monthly, or at longer intervals
$5.00 \cdot 10^{-2}$	5				1	Use of written test or calibration procedures
$5.00 \cdot 10^{-2}$	5				1	Use written maintenance procedures
		$8.00 \cdot 10^{-4}$	$3.00 \cdot 10^{-3}$	$7.00 \cdot 10^{-3}$	2	Restore or shift system to original or new state following procedures with some checking Generic task and associated probabilities (Williams)
		$2.00 \cdot 10^{-2}$	$7.00 \cdot 10^{-2}$	$1.70 \cdot 10^{-2}$	3	Detect deviation from standard. Data on human failure rate for general tasks (Williams 1989)
		$4.00 \cdot 10^{-4}$	$1.00 \cdot 10^{-3}$	$3.00 \cdot 10^{-3}$	3	Control/demand. Data on human failure rates for general tasks (Williams 1989)
	12	$5.50 \cdot 10^{-4}$		$8.30 \cdot 10^{-2}$	3	Violate procedure and reconfigure equipment. (Gertman et al. 1992)
	10	$1.20 \cdot 10^{-3}$		$1.20 \cdot 10^{-1}$	3	Checker performing quality assurance tolerate a discrepancy. (Gertman et al. 1992)
	7	$4.60 \cdot 10^{-3}$		$2.00 \cdot 10^{-1}$	3	Common mode: failures due to poor safety culture (Gertman et al. 1992)

Event: Erroneous Choice/Installation of Sealing Device						
Probability of Failure					**Data Source**	**Description**
		Percentiles				
Average	**EF**	**5 %**	**50 %**	**95 %**		
	8	$3.90 \cdot 10^{-3}$		$2.20 \cdot 10^{-1}$	3	Right diagnosis, wrong response; capture sequence based on response set; right conclusions bur wrong action pathway selected (Gertman et al. 1992)
$2.90 \cdot 10^{-3}$					3	Install O-ring. Task element reliabilities from data store (Irwin et al. 1964)
$2.20 \cdot 10^{-3}$					3	Install gasket. Task element reliabilities from data store (Irwin et al. 1964)
						Comparison of Error Probabilities on Maintenance Tasks for Pumps and Valves (Stewart 1981):
$9.00 \cdot 10^{-2}$					3	Position or seating of gasket in valves
$1.00 \cdot 10^{-1}$					3	Position or seating of gasket in pumps
$4.00 \cdot 10^{-2}$					3	Improper size of gasket in in valves
$1.00 \cdot 10^{-2}$					3	Improper size of gasket in in pumps
$4.00 \cdot 10^{-2}$					3	Wrong material, gasket in valves
$1.40 \cdot 10^{-1}$					3	Wrong material, gasket in pumps
$7.00 \cdot 10^{-2}$					3	Poorly cut gasket in valves
$9.00 \cdot 10^{-2}$					3	Poorly cut gasket in pumps
		$1.00 \cdot 10^{-3}$		$1.00 \cdot 10^{-2}$	4	Failure to start procedure when procedure used. (Task analysis: initiation of flow via stand-by train, Webley & Acroyd, 1988)
		$1.00 \cdot 10^{-2}$		$5.00 \cdot 10^{-2}$	4	Failure to start procedure when procedure is not used. (Task analysis: initiation of flow via stand-by train, Webley & Acroyd, 1988)
$1.00 \cdot 10^{-2}$					4	General error of omission
$3.00 \cdot 10^{-3}$					4	Error of omission of an act embedded in a procedure
$3.00 \cdot 10^{-3}$					4	General error rate for an act performed incorrectly
$1.00 \cdot 10^{-3}$					4	Error in simple routine operation
$1.00 \cdot 10^{-4}$					4	Human performance limit: single operator
$2.00 \cdot 10^{-4}$					4	Incorrect setting (this HEP was derived from a number of NPP simulator scenarios, and based on unrecovered errors.)
		$8.00 \cdot 10^{-4}$	$3.00 \cdot 10^{-3}$	$9.00 \cdot 10^{-3}$	5	Restore or shift system to original or new state following procedures with some checking (generic classification HEART)

2.5 B5, C2: Maloperation of Valve(s) During Manual Operation

The data which are used as background values when assigning human error probability related to the event "maloperation of valve(s) during manual operation" are shown in Table 5.

Table 5 HEP Data Reviewed in Connection with the Event " Maloperation of Valve(s) During Manual Operation"

Event: Maloperation of Valve(s) During Manual Operation						
Probability of Failure					**Data Source**	**Description**
		Percentiles				
Average	**EF**	**5 %**	**50 %**	**95 %**		
						Estimated HEPs for selection errors for locally operated valves. Making an error of selection in changing or restoring a locally operated valve when the valve to be manipulated is;
$1.00 \cdot 10^{-3}$	3				1	Clearly and unambiguously labeled, set apart from valves that are similar in all of the following: size and shape, state, and presence of tags 1)
$3.00 \cdot 10^{-3}$	3				1	Clearly and unambiguously labeled, part of a group of two or more valves that are similar in one of the following: size and shape, state, or presence of tags1)
$5.00 \cdot 10^{-3}$	3				1	Unclearly or ambiguously labeled, set apart from valves that are similar in all of the following: size and shape, state, and presence of tags1)
$8.00 \cdot 10^{-3}$	3				1	unclear or ambiguously labeled, part of a group of two or more valves that are similar in one of the following: size and shape, state, or presence of tags1)
$1.00 \cdot 10^{-2}$	3				1	Unclearly or ambiguously labeled, part of a group of two or more valves that are similar in all of the following: size and shape, state, and presence of tags1)
						Estimated HEPs in detecting stuck locally operated valves. Given that a locally operated valve sticks as it is being changed or restored, the operator fails to notice the sticking valve when it has (prob. Valve sticking 0.001 per manipulation, error factor 10):
$1.00 \cdot 10^{-3}$	3				1	A position indicator only (incorporates a scale that indicates the position of the valve relative to a fully opened or fully closed position).
$2.00 \cdot 10^{-3}$	3				1	A position indicator and a rising stem (does not have a scale in difference to position indicator)
$5.00 \cdot 10^{-3}$	3				1	A rising stem but no position indicator
$1.00 \cdot 10^{-2}$	3				1	Neither rising stem nor position indicator

Event: Maloperation of Valve(s) During Manual Operation						
Probability of Failure					**Data Source**	**Description**
		Percentiles				
Average	**EF**	**5 %**	**50 %**	**95 %**		
						Estimated probabilities of errors of omission per item of instruction when use of written procedures with checkoff provisions are correctly used:
$1.00 \cdot 10^{-3}$	3				1	Short list, ≤ 10 items
$3.00 \cdot 10^{-3}$	3				1	Long list, > 10 items
						Estimated probabilities of errors of omission per item of instruction when use of written procedures is specified, but not used or incorrectly used
$3.00 \cdot 10^{-3}$	3				1	Short list, ≤ 10 items
$1.00 \cdot 10^{-2}$	3				1	Long list, > 10 items
$5.00 \cdot 10^{-2}$	5				1	Estimated probabilities of errors of omission per item of instruction when written procedures are available and should be used but are not used.
						Estimated HEPs related to failure of administrative control
$1.00 \cdot 10^{-2}$	5				1	Carry out a plant policy or scheduled tasks such as periodic tests or maintenance performed weekly, monthly, or at longer intervals
$1.00 \cdot 10^{-2}$	3				1	Use a valve change or restoration list
$5.00 \cdot 10^{-2}$	5				1	Use of written test or calibration procedures
$5.00 \cdot 10^{-2}$	5				1	Use written maintenance procedures
		$8.00 \cdot 10^{-4}$	$3.00 \cdot 10^{-3}$	$7.00 \cdot 10^{-3}$	2	Restore or shift system to original or new state following procedures with some checking Generic task and associated probabilities (Williams)
		$3.30 \cdot 10^{-2}$	$1.30 \cdot 10^{-1}$	$3.00 \cdot 10^{-1}$	3	Error of omission by auxiliary operator (opens/closes valve) (Gilbert et al. 1990)
		$5.50 \cdot 10^{-4}$	$2.80 \cdot 10^{-3}$	$1.40 \cdot 10^{-2}$	3	Error of commission by auxiliary operator (opens/closes valve) (Gilbert et al. 1990)
$1.80 \cdot 10^{-3}$					3	Close valve. Data on human failure rates (adapted from Williams 1989, data source Peters)
$1.50 \cdot 10^{-3}$					3	Align manual valve. Data on human failure rates (adapted from Williams 1989, data source Lukas and Hall)
		$2.00 \cdot 10^{-2}$	$7.00 \cdot 10^{-2}$	$1.70 \cdot 10^{-2}$	3	Detect deviation from standard Data on human failure rates for general tasks (Williams 1989)
		$4.00 \cdot 10^{-4}$	$1.00 \cdot 10^{-3}$	$3.00 \cdot 10^{-3}$	3	Control/demand. Data on human failure rates for general tasks (Williams 1989)
	12	$5.50 \cdot 10^{-4}$		$8.30 \cdot 10^{-2}$	3	Violate procedure and reconfigure equipment. (Gertman et al. 1992)
	10	$1.20 \cdot 10^{-3}$		$1.20 \cdot 10^{-1}$	3	Checker performing quality assurance tolerate a discrepancy. (Gertman et al. 1992)
	7	$4.60 \cdot 10^{-3}$		$2.00 \cdot 10^{-1}$	3	Common mode: failures due to poor safety culture (Gertman et al. 1992)

Event: Maloperation of Valve(s) During Manual Operation						
Probability of Failure						
		Percentiles				
Average	**EF**	**5 %**	**50 %**	**95 %**	**Data Source**	**Description**
	8	$3.90 \cdot 10^{-3}$		$2.20 \cdot 10^{-1}$	3	Right diagnosis, wrong response; capture sequence based on response set; right conclusions bur wrong action pathway selected (Gertman et al. 1992)
		$1.00 \cdot 10^{-3}$		$1.00 \cdot 10^{-2}$	4	Failure to start procedure when procedure used. (Task analysis: initiation of flow via stand-by train, Webley & Acroyd, 1988)
		$1.00 \cdot 10^{-2}$		$5.00 \cdot 10^{-2}$	4	Failure to start procedure when procedure is not used. (Task analysis: initiation of flow via stand-by train, Webley & Acroyd, 1988)
$1.00 \cdot 10^{-3}$					4	Roving operators opens correct valve, error of omission - verbal order (Task analysis: initiation of flow via stand-by train, Webley & Acroyd, 1988)
		$1.00 \cdot 10^{-3}$		$1.00 \cdot 10^{-2}$	4	Roving operators opens correct valve, error of commission - selecting incorrect valve (Task analysis: initiation of flow via stand-by train, Webley & Acroyd, 1988)
$1.00 \cdot 10^{-2}$					4	Failure to return the manually operated test valve to the correct configuration after maintenance.
$1.00 \cdot 10^{-2}$					4	General error of omission
$3.00 \cdot 10^{-3}$					4	Error of omission of an act embedded in a procedure
$3.00 \cdot 10^{-3}$					4	General error rate for an act performed incorrectly
$1.00 \cdot 10^{-3}$					4	Error in simple routine operation
$1.00 \cdot 10^{-4}$					4	Human performance limit: single operator
$1.00 \cdot 10^{-3}$					4	Valve mis-set during calibration task **
$2.00 \cdot 10^{-4}$					4	Incorrect setting (this HEP was derived from a number of NPP simulator scenarios, and based on unrecovered errors.)
$2.00 \cdot 10^{-4}$					4	Equipment turned in wrong direction (this HEP was derived from a number of NPP simulator scenarios, and based on unrecovered errors.)
		$8.00 \cdot 10^{-4}$	$3.00 \cdot 10^{-3}$	$9.00 \cdot 10^{-3}$	5	Restore or shift system to original or new state following procedures with some checking (generic classification HEART)

2.6 B6: Maloperation of Temporary Hoses

The data which are used as background values when assigning human error probability related to the event “maloperation of temporary hoses” are shown in Table 6.

Table 6 HEP Data Reviewed in Connection with the Event ” Maloperation of Temporary Hoses”

Event: Maloperation of Temporary Hoses						
Probability of Failure					**Data Source**	**Description**
		Percentiles				
Average	**EF**	**5 %**	**50 %**	**95 %**		
						Estimated probabilities of errors of omission per item of instruction when use of written procedures with checkoff provisions are correctly used:
$1.00 \cdot 10^{-3}$	3				1	Short list, ≤ 10 items
$3.00 \cdot 10^{-3}$	3				1	Long list, > 10 items
						Estimated probabilities of errors of omission per item of instruction when use of written procedures is specified, but not used or incorrectly used
$3.00 \cdot 10^{-3}$	3				1	Short list, ≤ 10 items
$1.00 \cdot 10^{-2}$	3				1	Long list, > 10 items
$5.00 \cdot 10^{-2}$	5				1	Estimated probabilities of errors of omission per item of instruction when written procedures are available and should be used but are not used.
						Estimated HEPs related to failure of administrative control:
$1.00 \cdot 10^{-2}$	5				1	Carry out a plant policy or scheduled tasks such as periodic tests or maintenance performed weekly, monthly, or at longer intervals
$5.00 \cdot 10^{-2}$	5				1	Use of written test or calibration procedures
$5.00 \cdot 10^{-2}$	5				1	Use written maintenance procedures
		$8.00 \cdot 10^{-4}$	$3.00 \cdot 10^{-3}$	$7.00 \cdot 10^{-3}$	2	Restore or shift system to original or new state following procedures with some checking
		$2.00 \cdot 10^{-2}$	$7.00 \cdot 10^{-2}$	$1.70 \cdot 10^{-2}$	3	Detect deviation from standard. Data on human failure rate for general tasks (Williams 1989)
		$4.00 \cdot 10^{-4}$	$1.00 \cdot 10^{-3}$	$3.00 \cdot 10^{-3}$	3	Control/demand. Data on human failure rates for general tasks (Williams 1989)
	12	$5.50 \cdot 10^{-4}$		$8.30 \cdot 10^{-2}$	3	Violate procedure and reconfigure equipment. (Gertman et al. 1992)
	10	$1.20 \cdot 10^{-3}$		$1.20 \cdot 10^{-1}$	3	Checker performing quality assurance tolerate a discrepancy. (Gertman et al. 1992)
	7	$4.60 \cdot 10^{-3}$		$2.00 \cdot 10^{-1}$	3	Common mode: failures due to poor safety culture (Gertman et al. 1992)
	8	$3.90 \cdot 10^{-3}$		$2.20 \cdot 10^{-1}$	3	Right diagnosis, wrong response; capture sequence based on response set; right conclusions bur wrong action pathway selected (Gertman et al. 1992)

Event: Maloperation of Temporary Hoses						
Probability of Failure					**Data Source**	**Description**
		Percentiles				
Average	**EF**	**5 %**	**50 %**	**95 %**		
						Comparison of Error Probabilities on Maintenance Tasks for Pumps and Valves (Stewart 1981):
$4.00 \cdot 10^{-2}$					3	Couplings: alignment or clearance in valves
$6.00 \cdot 10^{-2}$					3	Couplings: alignment or clearance in pumps
$6.00 \cdot 10^{-2}$					3	Poor fitting or coupling joints in valves
$1.60 \cdot 10^{-1}$					3	Poor fitting or coupling joints in pumps
		$1.00 \cdot 10^{-3}$		$1.00 \cdot 10^{-2}$	4	Failure to start procedure when procedure used. (Task analysis: initiation of flow via stand-by train, Webley & Acroyd, 1988)
$1.00 \cdot 10^{-2}$					4	General error of omission
						Error in a routine operation where care is required:
$3.00 \cdot 10^{-3}$					4	Error of omission of an act embedded in a procedure
$3.00 \cdot 10^{-3}$					4	General error rate for an act performed incorrectly
$1.00 \cdot 10^{-4}$					4	Human performance limit: single operator
$2.00 \cdot 10^{-4}$					4	Incorrect setting (this HEP was derived from a number of NPP simulator scenarios, and based on unrecovered errors.)
		$8.00 \cdot 10^{-4}$	$3.00 \cdot 10^{-3}$	$9.00 \cdot 10^{-3}$	5	Restore or shift system to original or new state following procedures with some checking (generic classification HEART)

3. Data Tables for Fault Tree Data

The following sections present HEP data related to barrier fault trees, excerpted from the data sources listed in Section 1.2. The column "Data Source" refers to the references presented in Section 4. Occasionally, the data sources refer further to other data references. These references are quoted in the "Description" column, but it is referred to the main data sources for the full reference.

Although a large number of barriers with corresponding fault trees is defined, the actual events to which HEP values are to be assigned can be grouped into the following three cases:

- Manuals, procedures, datasheets etc. are not used
- Manuals, procedures, datasheets etc. are not used correctly
- Checklists are not used
- Checklists are not used correctly
- Failure to detect leak manually

3.1 Manuals, Procedures, Datasheets etc. not Used

The data which are used as background values when assigning human error probability related to the event "manuals, procedures, datasheets etc. not used" are shown in Table 7.

Table 7 HEP Data Reviewed in Connection with the Event "Manuals, Procedures, Datasheets etc. not Used"

Event: Manuals, Procedures, Datasheets etc. Not Used						
Probability of Failure						
		Percentiles			**Data**	
Average	**EF**	**5 %**	**50 %**	**95 %**	**Source**	**Description**
$5.00 \cdot 10^{-2}$	5				1	When written procedures are available and should be used but are not used
$1.00 \cdot 10^{-3}$	3				1	Estimated HEPs related to failure of administrative control. Initiate a scheduled shiftly checking or inspection function
$1.00 \cdot 10^{-2}$	5				1	Estimated HEPs related to failure of administrative control. Carry out a plant policy or scheduled tasks such as periodic tests or maintenance performed weekly, monthly, or at longer intervals
		$2.00 \cdot 10^{-2}$	$7.00 \cdot 10^{-2}$	$1.70 \cdot 10^{-1}$	3	Data on Human failure rates for general tasks Detect deviation from standard (Williams 1989)
$3.00 \cdot 10^{-3}$					4	Error of omission of an act embedded in a procedure
$1.00 \cdot 10^{-4}$					4	Human performance limit: single operator
$1.00 \cdot 10^{-5}$					4	Human performance limit: team of operators performing a well designed task, very good PSFs, etc

3.2 Manuals, Procedures, Datasheets etc. not Used Correctly

The data which are used as background values when assigning human error probability related to the event "manuals, procedures, datasheets etc. not used correctly" are shown in Table 8.

Table 8 HEP Data Reviewed in Connection with the Event "Manuals, Procedures, Datasheets etc. not Used Correctly"

Event: Manuals, Procedures, Datasheets etc. not Used Correctly						
Probability of Failure					**Data Source**	**Description**
		Percentiles				
Average	**EF**	**5 %**	**50 %**	**95 %**		
						Estimated probabilities of errors of omission per item of instruction when use of written procedures is specified, and incorrectly used:
$3.00 \cdot 10^{-3}$	3				1	Short list, ≤ 10 items
$1.00 \cdot 10^{-2}$	3				1	Long list, > 10 items
$1.00 \cdot 10^{-2}$	5				1	Estimated HEPs related to failure of administrative control. Carry out a plant policy or scheduled tasks such as periodic tests or maintenance performed weekly, monthly, or at longer intervals
		$2.00 \cdot 10^{-2}$	$7.00 \cdot 10^{-2}$	$1.70 \cdot 10^{-1}$	3	Data on Human failure rates for general tasks (Williams 1989) Detect deviation from standard
$3.00 \cdot 10^{-3}$					4	Error of omission of an act embedded in a procedure
$3.00 \cdot 10^{-3}$					4	General error rate for an act performed incorrectly
$1.00 \cdot 10^{-4}$					4	Human performance limit: single operator
$1.00 \cdot 10^{-5}$					4	Human performance limit: team of operators performing a well designed task, very good PSFs, etc
$1.60 \cdot 10^{-1}$					4	Faul diagnosis using rules

3.3 Checklists not Used

The HEP values for the event "checklist not used" is based on the same data as the event "manuals, procedures, datasheets etc. are used". It is referred to Section 3.1.

3.4 Checklists not Used Correctly

The HEP values for the event "checklist not used correctly" is based on the same data as the event "manuals, procedures, datasheets etc. are used correctly". It is referred to Section 3.2.

The HEP assignments listed in the main report reflect the assumption that checklist based operations are carried out with less degree of attention as compared with procedure based operations, hence the HEP assignments are adjusted somewhat upwards.

3.5 Failure to Detect Leak Manually

The data which are used as background values when assigning human error probability related to the event “failure to detect leak manually” are shown in Table 9.

Table 9 HEP Data Reviewed in Connection with the Event ” Failure to Detect Leak Manually”

Event: Failure to Detect Leak Manually						
Probability of Failure						
		Percentiles				
Average	**EF**	**5 %**	**50 %**	**95 %**	**Data Source**	**Description**
						Failure to perform rule-based actions correctly when written procedures are available and used
$5.00 \cdot 10^{-2}$	10				1	Error per critical step without recovery factors
$2.50 \cdot 10^{-2}$	10				1	Error per critical step with recovery factors
						When procedures with checkoff provisions are correctly used (assumed for items in which written entries such as numerical values are required of the user)
$1.00 \cdot 10^{-3}$	3				1	Short list, ≤ 10 items
$3.00 \cdot 10^{-3}$	3				1	Long list, > 10 items
						When procedures without checkoff provisions are used, or when checkoff provisions are incorrect used (If the task is judged to be second nature, use a lower uncertainty bound use 0.01 EF=5)
$3.00 \cdot 10^{-3}$	3				1	Short list, ≤ 10 items
$1.00 \cdot 10^{-2}$	3				1	Long list, > 10 items
$5.00 \cdot 10^{-2}$	5				1	When written procedures are available and should be used but are not used
$1.00 \cdot 10^{-2}$	5	-	-	-	1	Estimated HEPs related to failure of administrative control. Carry out a plant policy or scheduled tasks such as periodic tests or maintenance performed weekly, monthly, or at longer intervals
$1.00 \cdot 10^{-3}$	3				1	Estimated HEPs related to failure of administrative control. Initiate a scheduled shiftly checking or inspection function
		$2.00 \cdot 10^{-2}$	$7.00 \cdot 10^{-2}$	$1.70 \cdot 10^{-1}$	3	Data on Human failure rates for general tasks (Williams 1989) Detect deviation from standard

Event: Failure to Detect Leak Manually						
Probability of Failure						
		Percentiles				
Average	**EF**	**5 %**	**50 %**	**95 %**	**Data Source**	**Description**
						Data on Human failure rates for general tasks (Williams 1989):
$1.00 \cdot 10^{-2}$		-	-	-	4	General error of omission
$3.00 \cdot 10^{-3}$		-	-	-	4	Error of omission of an act embedded in a procedure
$3.00 \cdot 10^{-3}$					4	General error rate for an act performed incorrectly
$1.00 \cdot 10^{-4}$					4	Human performance limit: single operator
$1.00 \cdot 10^{-5}$					4	Human performance limit: team of operators performing a well designed task, very good PSFs, etc
$1.60 \cdot 10^{-1}$					4	Faul diagnosis using rules
$2.00 \cdot 10^{-4}$					4	Selection of wrong control (functionally grouped) HEPs are based on a number of NPP simulator scenarios. 20 incorrect from out of a total of 11490 opportunities for control selection.

4. References

1 Swain, AD and Guttmann HE: *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications,* U.S. Nuclear regulatory commission report NUREG/CR-1278, SAND80-020, August 1983

2 Reason, J: *Managing the Risks of Organizational Accidents,* Ashgate Publishing Company, Burlington, 1997.

3 Blackman, HS and Gertman, DI: *Human Reliability and Safety Analysis Data Handbook,* John Wiley & Sons, 1994.

4 Kirwan, B: *A Guide to Practical Human Reliability Assessment,* Taylor & Francis Ltd., 1994.

5 Kirwan, B: *Human Factors & Human Reliability in Offshore Systems,* Course arranged at SINTEF, Trondheim, May 11-13 1998.