




Universitetet  
i Stavanger

Faculty of Science and Technology

## MASTER`S THESIS

Study program/ Specialization:  Master Risk Management	Spring semester, 2011  Open
Writer: Lene Østrem	 (Writer's signature)
Faculty supervisor: Jan Erik Vinnem  External supervisor: Finn Roar Berg	
Title of thesis:  Evaluating Gassco`s barrier KPI model	
Credits (ECTS): 30	
Key words:  - Barriers - Indicators - Risk analysis - QRA analysis	Pages: 104  + enclosure: 40  Stavanger, 15.06/2011 Date/year

## Preface

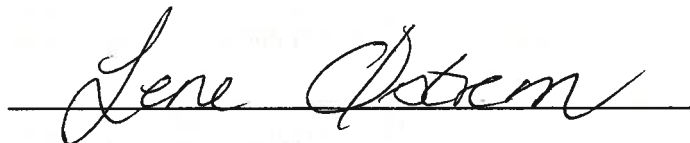
This master`s thesis is part of the Master`s degree education at the University of Stavanger. It is a time limited assignment and constitutes 30 credits in the field of risk management in the offshore industry. The aim is that the student shall develop an independent work, based on the multidisciplinary competence gained through the study.

Working with this assignment has been a very informative process. Since I have been working with implementation of Gasscos barrier KPI model the last year, it felt very natural to do an evaluation of the model and figure out room for further improvement. It has been very motivating to work with a barrier model already used by the industry. Knowing that the results in this report will be assessed in a work shop meeting at Gassco, as basis for further development of the model, also increases the motivation. The work has been challenging, due to a lot of discussion in the industry on how to monitor different barriers “the right way”. There are a lot of different opinions regarding the subject at hand. When I was writing this assignment, I needed to focus on how to get thing done, and how to get one step further in the development of the model. This report is a result from the experience gained with the model while implementing it, an extensive litterateur study, ideas gained through a lot of reading, and off course some pondering.

I want to give a huge thank you to Gassco and Alfred S. Hansen, for allowing me to take some time off from my regular work, and for allowing me to use the barrier KPI model as a case for the thesis. I also want to give a special thank you to my external supervisor Finn Roar Berg and Olav Rasmussen at Gassco for help and advices, good discussions and ideas.

I would also like to thank Professor Terje Aven, who recommended Professor Jan Erik Vinnem as my internal supervisor. And off course at last - but certainly not least, I would like to thank my internal supervisor Jan Erik Vinnem. Thank you for taking the time to meet with me, answer all my questions and for guiding my in how to structure and write this report, and for always giving me a quick response – I really appreciate it.

Stavanger 15<sup>th</sup> of June 2011



Lene Østrem

## Contents

Preface .....	2
Contents .....	3
Table-, formula and figure overview .....	5
Summary and conclusions .....	7
Chapter 1. Introduction .....	8
1.1 Background .....	8
1.2 Purpose .....	8
1.3 Problem description .....	9
1.4 Delimitations .....	9
1.5 Report structure .....	11
1.6 Terms and definitions .....	12
1.7 Shortenings .....	14
Chapter 2. Theory and regulation .....	15
2.1 Barriers .....	15
2.2 Performance indicators .....	17
2.4 Regulations .....	24
2.5 Risk analysis .....	24
Chapter 3. Gasscos's barrier KPI model .....	29
3.1 Description of Gassco AS and the barrier KPI project .....	29
3.2 Barrier KPI model .....	29
3.3 Reporting and follow up .....	31
Chapter 4. Does Gasscos's barrier KPI model reflect learning from recently major accident in the industry? .....	36
4.1 Longford 1998 .....	36
4.2 Texas City 2005 .....	41
4.3 Deep WaterHorizon 2010 .....	45
4.4 Gullfaks 2010 .....	48
4.5 Similarities – failure to learn .....	51
4.6 How to implement “lesson learned” in Gassco's barrier KPI model .....	54
4.7 Human factors in the nuclear industry .....	63
Chapter 5. Do changes in the barrier KPI model equal changes in the risk level? .....	66
5.1 QRA analysis .....	67
5.2 Sensitivity at installation level in the barrier KPI model .....	73

5.3 How to monitor the risk level more frequently? .....	76
5.4 Moving average and status/trend description .....	80
Chapter 6. Discussion .....	87
6.1 Discussion .....	87
6.2 Suggestions for further work .....	95
Chapter 7. Conclusion .....	96
Chapter 8. References .....	98
Chapter 9. Appendices .....	105
A. Regulations .....	105
B. Indicators in Gassco`s barrier KPI model and aggregation rules .....	108
C. Major accidents .....	114
C.1 Humber oil refinery 2001 .....	114
C.2 Toulouse 2001 .....	116
C.3 Buncefield 2005 .....	117
D. Indicators human factors .....	120
E. Risk calculations .....	129
F. Calculations status .....	134
G. Calculations moving average .....	141

## Table-, formula and figure overview

### Table overview:

Table 1: Suggested indicators .....	60
Table 2: Representative leak rates for process events.....	67
Table 3: The most important contributions to FAR value from process event (all contributions > 1%).....	68
Table 4: Contribution to personnel risk.....	69
Table 5: Status as a result of reported data for installation X in January, February and March 2011.....	75

### Formula overview:

Formula 2.1: Expression for risk.....	26
Formula 2.2: Expression for risk.....	26
Formula 2.3: Expression for Potential Loss of Life.....	27
Formula 2.4: Expression for annual frequency of an accident scenario.....	27
Formula 2.5: Expression for Fatal Accident Rate.....	27
Formula 2.6: Expression for Average Individual Risk.....	27
Formula 2.7: Expression for Bayes formula.....	28
Formula 5.1: Expression for failure for ESD valve.....	69
Formula 5.2: Expression for annual frequency combined with expression of failure rate.....	70
Formula 5.3: Expression for failure rate.....	70
Formula 5.4: Expression for total failure probability for isolating failure.....	70
Formula 5.5: Expression for posterior distribution .....	81
Formula B.1: Expression for rating and aggregation.....	113

### Figure overview:

Figure 1: Chain of events leading to an accident <sup>[17]</sup> .....	15
Figure 2: Distinction between the safety approach and the probabilistic risk approach <sup>[30]</sup> .....	19
Figure 3: Retrospective investigation versus predictive assessment <sup>[29]</sup> .....	19
Figure 4: General measurement model <sup>[29]</sup> .....	20
Figure 5: Organisational model <sup>[33]</sup> .....	22
Figure 6: Overview of the quantification process in the project <sup>[33]</sup> .....	23
Figure 7: Framework for establishment of organisational risk indicators <sup>[33]</sup> .....	23
Figure 8: Model for representation of the process risk assessment <sup>[34]</sup> .....	25
Figure 9: Bow-tie loss of containment <sup>[8]</sup> .....	30
Figure 10: Illustration aggregation in Gassco's hierarchy <sup>[8]</sup> .....	32
Figure 11: System level.....	32
Figure 12: Illustration Corporate level .....	33
Figure 13: Reporting and follow-up work process <sup>[42]</sup> .....	34
Figure 14: Explanation level, trend and colour rating <sup>[42]</sup> .....	34
Figure 15: Overview bow tie model.....	51
Figure 16: Illustration Barrier KPI chart .....	56
Figure 17: Example management element list .....	57
Figure 18: Reported figures at installation X, March 2011.....	66
Figure 19: PLL and Fnj as a function of the failure rate .....	71
Figure 20: Event tree .....	72
Figure 21: Event tree 40 % increase failure rate .....	72
Figure 22: Illustration aggregation .....	74

Figure 23: Risk monitor applications - example of an on-line risk graph <sup>[70]</sup> .....	78
Figure 24: Suggestion process flow .....	79
Figure 25: Limits in the barrier KPI model .....	81
Figure 26: Moving average reported data .....	83
Figure 27: Moving average and aggregated data .....	84
Figure 28: Status Gas detection.....	84
Figure 29: Presentation moving average Gas detection .....	85
Figure 30: Status Gas detection.....	86
Figure 31: Presentation graph .....	86
Figure 32: Aggregation hierarchy <sup>[6]</sup> .....	113
Figure 33: Risk calculations .....	129
Figure 34: Calculations overall % risk change .....	130
Figure 35: Calculation overall % change in FAR .....	130
Figure 36: Formulas used in figure 27 .....	131
Figure 37: Formulas used in figure 28 .....	132
Figure 38: Formulas used in figure 29 .....	133
Figure 39: : Overall status when all other indicators are green.....	134
Figure 40: Overall status when all other indicators are green – continuing from figure 27 ..	135
Figure 41: Overall status when all other indicators are 50 % green and 50 % yellow.....	136
Figure 42: Overall status when all other indicators are 50 % green and 50 % yellow – continuing from figure 35 .....	137
Figure 43: Calculations installation combinations .....	138
Figure 44: Quality check - number of possible combinations .....	139
Figure 45: Formula used when calculating possible values .....	140
Figure 46: Calculations moving average and FF gas detection .....	141
Figure 47: Calculations moving average, aggregated and FF gas detection .....	142
Figure 48: Calculations different status/trend when using method suggested in chapter 5.4	143
Figure 49: Formulas used when calculating moving average and FF.....	143
Figure 50: Formulas used when calculating aggregated values and FF.....	144
Figure 51: Formulas used when calculating different status/trend using method suggested in chapter 5.4 .....	144

## Summary and conclusions

Gassco has developed a barrier KPI model. After some use, there was a need to evaluate the model. Delimitations have been made, and the aim with this report was to answer the following questions:

1. Does Gassco's barrier KPI reflect learning from recent major accidents, or should more indicators be included in the model?
2. Do changes in the barrier KPI model equal changes in the risk level?
3. Is the information regarding failure rate in the model presented in an adequate way?

The answers were mainly sought by studying a selection of previously major accidents, work done in other industries in regards to these subjects and performing sensitivity calculations in the model. The methods have limitations, but in a practical view they all seemed reasonable and they could all be performed within the given time period of this thesis.

Similarities in several major accidents that have occurred in the time period 1998 – 2010 are that the underlying causes can all be addressed as management elements. These elements should be presented better in the barrier KPI model. Since Gassco's management is located at Bygnes, the model should implement an indicator placing Bygnes at the barrier KPI chart. This indicator should represent several management elements dealt with by the management in Gassco, as well as the work done to prevent a major accident within Gassco's portfolio. Implementing an indicator is not enough if the aim is to learn from previous major accidents. More effort must be put in trying to manage human factors; to have a 'human factor manager', develop a data base with experience data regarding human failures and work towards implementing the key element of a high reliability organisation.

The barrier KPI model does not reflect changes in the risk level sufficient enough to be used as an indicator reflecting the risk level at a given installation. To improve the risk management in the organisation, the aim must be to have an updated risk overview at all times at a given installation. Work and effort in developing an experience database on human factors will give a huge benefit when developing a new QRA model, which take into account dependencies between barriers and changes in the failure rate. Also, the work done with the barrier KPI model will become useful. This should be the ultimate goal in the industry should be to have a more dynamic QRA model. A lot can be learned from the work done in the nuclear industry regarding human factors and in building a more dynamic QRA model. Such a model could give a risk indicator and a risk graph updated on a regular basis. This would give important information when trying to manage the risk within Gassco's portfolio.

As of today, the failure rate of safety critical equipment is displayed as a 12 month moving average in the model. To calculate the trend, prevailing reporting period is compared up against the previous, to determine whether or not the failure rate stays unchanged or decreased/increased. The requirement to the failure rate is based on a probability distribution, and a 12 month moving average does not contain enough data to give a "correct" picture of the failure rate. Changing the presentation of the failure rate to include all reported data in the model will give a more correct basis of comparison. One should use the Bayesian approach when aggregating the data, then it will make more sense to compare the failure rate to the requirement even if there are few reported data available. Presenting the trend as a

comparison between the failure rate reported the last 24 months and the aggregated value, will ensure sensitivity in the model.

## **Chapter 1. Introduction**

### **1.1 Background**

In 2002 the Norwegian government introduced a new set of laws through the management regulations. Among other things, Operators were demanded to keep an overview of established barriers and their function. A complete overview of all non function barriers or barriers with impairment should be kept. In 2011 these regulations were also introduced for facilities onshore.

Implementation of new regulations has contributed to innovative thinking in the oil and gas industry. Different projects intended to meet the new requirements have been carried out. Statoil started the project Teknisk Tilstand Sikkerhet – TTS (Technical Condition Safety) in the year 2000. This is a continuous process where all facilities are evaluated on a regular basis to ensure a high level of safety. The goals for TTS is to map conditions, build competence within technical safety, keep a focus on the risk for major accidents and follow the rules and legislations. ConocoPhillips has developed a comprehensive description of technical barriers through their barrier panel concept<sup>[1]</sup>. The barrier panel facilitates a performance measurement system for monitoring preventive maintenance activities and the barrier systems for all installations. The objective of the barrier panel is to establish an effective management system to secure control of barriers to prevent major accident. Other offshore companies have other initiatives, all with the same goal: to reduce the risk of major accidents.

In 2008 Gassco started to work with the development of a barrier KPI model. The goal was to get an overview and control of all safety critical barriers, including inspection, maintenance and testing of safety critical equipment at installations within Gassco's area of responsibility.

### **1.2 Purpose**

The purpose of this thesis is to evaluate the Gassco barrier KPI model. The model will be assessed against lessons learned from major accidents occurring the last decade. A selection of major accidents and their investigation reports and studies performed subsequently, are thoroughly examined to determine what went wrong. Similarities in the accident sequences are then mapped and evaluated against Gassco's barrier KPI model. The purpose is to locate any gaps between the model and lesson learned from previous major accident. If gaps are identified, suggestion on how to close them will be evaluated. The model should reflect lessons learned and ensure management focus on areas that are important to reduce the major accident potential.

Afterwards, it is of interest to evaluate the connection between the barrier KPI model and the risk level at a given installation. Do changes in the barrier KPI model equal changes in the risk level? It is also of interest to evaluate the reported data already present in the model. Are they presented in an adequate way?



Trying to answer these questions a literature study will be carried out. The aim is to figure out how other industries have approached equivalent challenges.

To summarise the purpose of this report: it is to evaluate the model and recommend how it could be further developed to reach its full potential.

### 1.3 Problem description

When evaluating Gassco's barrier KPI model the following will be assessed:

Does Gassco's barrier KPI reflect learning from recent major accidents, or should more indicators be included in the model?

Do changes in the barrier KPI model equal changes in the risk level?

Is the information regarding failure rate in the model presented in an adequate way?

These questions will be answered by studying what went wrong in a selection of major accidents which occurred in the last decade. The need for new indicators and development of the model will be assessed and discussed. Sensitivities in the barrier KPI model will be evaluated and dependencies between the barrier model and the quantitative risk analysis (QRA) for a given installation will be assessed. A literature study will be conducted to get ideas on how the barrier KPI model can be further developed. Based on the reported data in the pilot tests, the 12 month moving average used when presenting the results in the model will be assessed.

### 1.4 Delimitations

Delimitations are necessary in every project. Clear delimitations give a good foundation for achieving a good result. Some delimitations fall naturally, while others must be set prior to start up. When working and focusing on a problem, elements that are not relevant must be excluded. Other limiting aspects are available time and the level of knowledge of the person(s) working on the project.

Delimitations made in this report are:

- only a selection of major accidents is reviewed. Another selection could have resulted in another outcome/conclusion. The chosen accidents have been thoroughly investigated and are well known
- the sources related to an accident are often limited to one investigation report or one person's presentation/approach to the accident. There could be several aspects to the accidents that, for this reason, are not reflected in this report.
- only the causes and barrier breaches in the accidents are presented in this report. There is limited focus in regards to the consequences for the companies/local society etc. involved in the accidents.
- the description of the accidents varies due to the quality of the investigations performed
- there are several things to evaluate in the barrier KPI, but this report is limited to evaluate areas described in chapter 1.3
- reported data in the model will not be analysed, neither will the distribution of status/trend lights
- it is not just the offshore industry that fails to learn, probably other industries do too. This will not be assessed or discussed in this report

- whether or not indicators already implemented in the barrier KPI model are good indicators or not, will not be assessed. Neither will the uncertainty regarding choosing and labelling of safety critical equipment
- suggestions of new indicators are based on experiences of what went wrong in previous accidents. What could go wrong in the future independently of this is not evaluated
- only personnel risk is presented in this report (not environmental and assets risk)
- figures used are from an existing risk analysis, but the installation is mentioned as installation x due to anonymity
- all risk calculations in this report contain the same amount of uncertainties as the risk analysis itself. The uncertainties are not listed and evaluated in this report due to the time limitation. Reference is made to the risk analysis performed for installation X
- the risk calculations in this report are very simplified. The point is not the figures used, but the way they affect the result and the dependence
- when assessing the sensitivity to the barrier KPI model, a selection of 5 indicators is chosen. These are indicators that probably would contribute the most to increasing the risk level at an installation if they fail.
- when calculating status values, all indicators other than the ones evaluated, are given a value that equals a green status. This is done to see how much the overall status will be affected if only indicators that contribute most to a higher level of risk change. If the installation status changes when the majority of indicators are green, the model is sensitive enough to reflect changes in the risk level. If the changes are not reflected in the overall status, the model is probably not sensitive enough to reflect the changes in the risk level
- in the scenario where the distribution of all other indicators are set to 50% yellow and 50% green, the indicators with the highest weighting are given yellow value
- only one emergency shutdown indicator and one deluge indicator are chosen to limit possible combinations (the model separates between emergency shutdown valve and logic and deluge valve and nozzle)
- only one indicator with the weight 3 is chosen to limit the number of combinations. Only 4 of 18 indicators are weighted 3, so the delimitation seems reasonable
- assessment of the 12 month moving average is only done for indicators that have status based on test data. The 12 month moving average used on number of inspection findings is not assessed

## 1.5 Report structure

### **Chapter 1 - Introduction**

The introduction contains background, purpose, problem description, delimitations and report structure as topic headings.

### **Chapter 2 - Theory and regulation**

Chapter 2 explains terms such as barriers, indicators, risk and risk analysis. Prevailing regulations in the industry are also presented. The purpose with this chapter is to give the reader an introduction to the theory behind the subjects presented. Based on this chapter the reader should gain enough background information to understand the subsequent discussions in the following chapters.

### **Chapter 3 - Gassco's barrier KPI model**

Description of Gassco and the development of Gassco's barrier KPI model are presented.

### **Chapter 4 - Does the barrier KPI model reflect learning from recently major accidents in the industry?**

In this chapter recent major accidents are presented. The most important learning's from the investigation reports are emphasised. The aim is to see if the barrier KPI model reflects this knowledge. If not, in which areas could the model be further improved based on the learning from recent major accidents?

### **Chapter 5 - Do the changes in the barrier KPI model equal changes in the risk level?**

The aim of this chapter is to see if there is dependence between the status given in the barrier KPI model and the QRA model at a given installation. The sensitivity for a selection of indicators in the barrier KPI model is assessed. How will the failure rate affect the input data in the QRA model? Is it possible to make a more "dynamic" barrier KPI model? The 12 month moving average is also evaluated in this chapter.

### **Chapter 6 - Discussion**

Choices made in the report and results from previous chapters are discussed. The discussion is divided into parts and is then summarized into one overall discussion. The discussion gives the basis for the conclusion.

### **Chapter 7 - Conclusion**

The overall conclusion is made in this chapter.

### **Chapter 8 - References**

An overview of sources and references used when writing the report is presented. The references are presented chronological and are marked as following in the report: <sup>[1],[2],[3]...etc</sup>

### **Chapter 9 - Appendices**

The appendices contain information regarding regulations, the barrier KPI model, previous major accidents and research done in the industry regarding indicators. The appendices are needed to create an independent document.

## 1.6 Terms and definitions

Accident:	An unexpected and undesirable event resulting in damage or harm.
Barriers:	Physical and/or non-physical means planned to prevent, control, or mitigate undesired events or accidents <sup>[2]</sup> .
Cumulative risk:	Related risks that increase in effect with each added risk <sup>[3]</sup> .
Deterministic risk assessment	Risk evaluation involving the calculation and expression of risks as single numerical values or “single point” estimates of risk, with uncertainty and variability discussed qualitatively <sup>[4]</sup> .
Failure fraction (FF):	The number of failures (x) divided by the corresponding number of test (n) <sup>[5]</sup> .
Human factors:	Environmental, organisational and job factors, and human and individual characteristics, which influence behaviour at work in a way that can affect health and safety <sup>[6]</sup> .
Indicator:	Measurable variable used as a representation of an associated (but non-measured or non-measurable) factor or quantity <sup>[7]</sup> . In the KPI model, input data on the lowest level is denoted indicators.
Management elements:	A “lump category” for non physical barriers. Interact with both preventive and reactive barriers and can be looked upon as barriers to follow up the physical barriers <sup>[8]</sup>
Non-conformities:	Failure to comply with requirements <sup>[9]</sup> .
Preventive barriers/elements:	Measure to reduce the probability of a top-event to occur <sup>[8]</sup>
Proactive:	Acting in advance to deal with an expected difficulty <sup>[10]</sup>
Procedure:	A given method to perform an activity <sup>[11]</sup>
Probabilistic risk assessment	is a systematic and comprehensive methodology to evaluate risks associated with a complex engineered technological system. Risk is characterized by two quantities: the likelihood and the consequence <sup>[12]</sup> .
Reactive barrier/elements:	Measure to reduce the effect of a top event and to prevent escalation <sup>[8]</sup>

Risk:	Classification of the most probable consequences/losses and the most probable frequency of recurrence in connection with an undesirable event/condition <sup>[13]</sup> .
Risk analysis:	use of available information to identify hazards and to estimate the risk <sup>[14]</sup> .
Risk assessment:	Overall process of risk analysis and risk evaluation <sup>[14]</sup> .
Safety critical equipment:	Safety critical equipment refers to all equipment defines as safety barriers which reduces the probability of a situation of hazard and accident occurring, or which limit the consequences of an accident <sup>[5]</sup> .
Seveso installation:	The Seveso II Directive aims to ensure high levels of protection against accidents involving dangerous substances. Operators of establishments where certain quantities of dangerous substances are present (called Seveso plants or Seveso installations) are requested to notify the competent authorities and to establish and implement a major implement prevention policy <sup>[15]</sup> .
Undesirable events:	Event that has caused, or could have caused injury, work-related illness and/or damage to/loss of assets, or harm to the environment or to a third party. This includes accidents, hazardous conditions and near-miss incidents <sup>[13]</sup> .
Qualitative approach:	An approach that refers to situations where data are collected in an unstructured way. Often qualitative data will form the basis of a pilot study, where the aim is to get the best possible feel for the situation through broadly defined data <sup>[16]</sup> .
Quantitative approach:	An approach where relatively well-defined measurement tool is used <sup>[16]</sup> .

## 1.7 Shortenings

BOP	Blow Out Preventer
CBS	Chemical Safety Board
COMAH	Control Of Major Accident Hazard
ESD	Emergency Shout Down
ETA	Event Tree Analysis
FTA	Fault Tree Analysis
HRA	Human Reliability Analysis
HSE	Health and Safety Executive
INERIS	Institut National de l'Environnement Industriel et des Risques (French National Institute for Industrial Environment and Risks)
KPI	Key Performance Indicator
PMG	Performance Management in Gasso
PSA	Petroleum Safety Authority
RNNP	Risikonivå norsk petroleumsvirksomhet (Risk level Norwegian Petroleum Industry)
TNT	Trinitrotoluene, an explosive
QRA	Quantitative Risk Assessment

## Chapter 2. Theory and regulation

This chapter present relevant theory and regulation prevailing for the subjects discussed in this report.

Theory regarding barrier approach and performance indicators is relevant for assessing lessons learned by the offshore industry. To give a basis for understanding the discussion concerning the barrier KPI model, extract from the most relevant theory regarding these subjects are presented in this chapter. Relevant regulations are presented briefly in this chapter. They are also presented fully in appendix A.

Theory concerning risk, risk analysis and QRA models are presented briefly to give a basis for understanding the discussion regarding whether or not the barrier KPI model could be linked to a installations risk assessment and risk level. Assessing the data reported in the Gassco's barrier KPI model is done based on a Bayesian framework. The Bayesian methodology is therefore also presented in this chapter.

The driving force behind the barrier KPI model is the continuous work on reducing the major accident potential. The desire is to be able to foresee a major accident and prevent it from happening by the help of indicators. A lot of work has been carried out, in the industry, on this highly complex problem, trying to develop a methodology for developing suitable indicators.

### 2.1 Barriers

When reading this report it is crucial to understand what is meant by barriers, and their significance in a chain of events leading towards an accident. There are also other terms following the barrier expression that needs to be emphasised, such as undesirable event and accident. These terms are explained in chapter 1.6 and they can be placed in a chain of event leading towards an accident, as illustrated in figure 1:

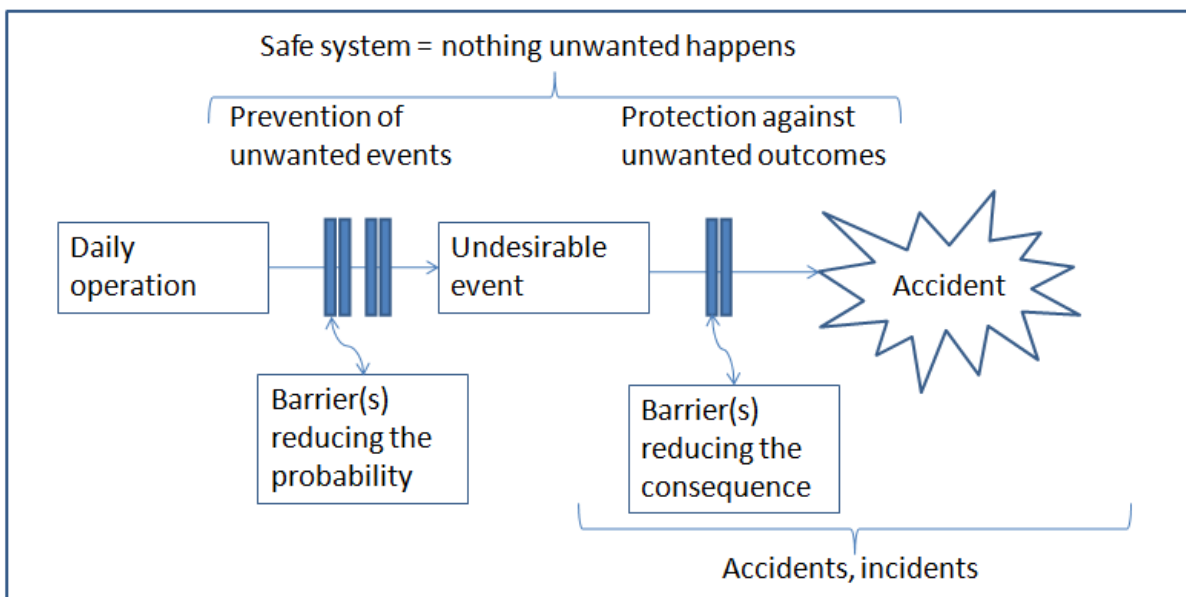


Figure 1: Chain of events leading to an accident <sup>[17]</sup>

To prevent an accident the chain of events must be broken. This could be done by implementing a barrier that reduces the likelihood for an undesirable event or reduces the consequences of the undesirable event. Implementation of actions/initiatives will affect the chain of events, either by reducing the development or the consequence of an undesirable event. The actions/initiatives could be obstructions, fences or blockade (barriers). The main principle is that obstructions which are difficult or impossible to get past are established. For the undesired event to happen, these obstructions must be breached.

According to Hollnagel there are four types of barrier systems <sup>[17]</sup>:

- physical or material barrier systems; prevent an event from taking place or mitigate the effects of an unexpected event by blocking the transportation of mass, energy or information from one place to another. Examples: building, containers etc.
- functional barrier system; create one or more pre-conditions that have to be met before an action can be carried out. Examples: automatic or human obstruction of events)
- symbolic barrier systems; work indirectly through their meaning. Requires an act of interpretation of someone. Examples: signs and signals
- incorporeal barrier system; largely synonymous with the so-called organisational barriers, i.e., rules for actions that are imposed by the organisation.

Whereas the barrier system seem consist of just four types, barrier functions are not as easily categorised. One possibility is to distinguish whether the barrier function is active or passive, i.e. whether it does something, such as sprinkler (functional barrier system) that extinguishes a fire, or whether it simply is, such as a wall (physical barrier system) which blocks the transportation of matter and energy. But the classification of barriers is unfortunately not always as simple as the previous example. How does one characterise a procedure? A procedure is an instruction on how to do an action and is therefore an example of facilitation rather than prevention. Procedures do, however, often include both cautions and conditional actions (if-then rules). The procedures also work by virtue of its contents or meaning rather than by virtue of its physical characteristics. For that reason, it is warranted to classify a procedure as a symbolic barrier system <sup>[17]</sup>.

#### Human, technology and organisation approach:

When investigating an accident, it is primarily to understand what went wrong and identify lessons to be learned. To prevent recurrence, indirect and underlying causes need to be identified and the chain of events needs to be analysed. The human, technology and organisation approach (HTO) is often used as the main tool in the offshore industry when investigating the cause of an accident. Using a tool, such as the human, technology and organisation method, helps map the course of events together with identifying non-conformities and barrier failures. Triggering and underlying causes are mapped and categorised. When investigating an undesired event, it is of interest to see if a barrier could have been implemented to prevent the event or a subsequent escalation of the event. When using the HTO approach during investigations the event is seen in relation to all human, technology and organisational aspects leading towards the event. Underlying causes accounted for, explaining the cause for actions, which could be mutually dependent on training, work routines, risk awareness, regulations, ergonomics and so on. All are important



barriers in preventing an event. Using this approach can also contribute with comparable data to use in statistics and trend analysis in the industry.

## 2.2 Performance indicators

Performance indicators provide the company's management with information used to monitor the status and development of one or a set of activities or conditions. In industry and business, quantitative indicators are used to monitor performance in areas such as finance, efficiency, customer satisfaction and safety. The term indicator may be used in several ways, which means that many definitions exist. A broad definition used in the offshore industry, that also covers several other definitions, are:

*“An indicator is a measurable/operational variable that can be used to describe the condition of a broader phenomenon or aspect of reality”*<sup>[18]</sup>

Well known indicators are called key performance indicators (KPIs). They are used for achieving different strategic purposes. Commonly used expressions are leading and lagging indicators. In the literature these expressions are defined in several ways in the offshore industry, and the precise definition of leading and lagging continues to be a source of discussion<sup>[20]</sup>. In this report, from a practical viewpoint, this is not given a lot of attention. Still, some of the discussion and different definition of leading and lagging will be presented in this chapter, so that the reader is aware of them. Organisations require indicators to monitor the results of failures (e.g. accidents, incidents) and indicators of precursors to these accidents and incidents, which might be used to prompt corrective action before these accidents are realized. The concept of leading and lagging indicators has been around for a long time in economic and financial performance<sup>[20]</sup>. The definition in the economic and financial performance is:

Lagging indicator: *“A measurable economic factor that changes after the economy has already begun to follow a particular pattern or trend”*<sup>[21]</sup>. Changes after the occurrence.

Leading indicator: *“A measurable economic factor that changes before the economy has begun to follow a particular pattern or trend”*<sup>[22]</sup>. Changes before the occurrence.

A leading safety performance indicator is, in this interpretation, an indicator that changes before the actual risk level has changed. This interpretation is consistent with the definition of leading indicators in economy but deviates from the interpretation discussed by Hopkins in the article “thinking about process safety indicators”<sup>[23]</sup>. In this article the HSE's guide definition of leading and lagging indicators are presented<sup>[23]</sup>:

*The leading indicator identifies failings or ‘holes’ in vital aspects of the risk control system discovered during routine checks on the operation of a critical activity within the risk control system. The lagging indicator reveals failings or ‘holes’ in that barrier discovered following an incident or adverse event. The incident does not necessarily have to result in injury or environmental damage and can be a near miss, precursor event or undesired outcome attributable to a failing in that risk control system.*

Hopkins concludes in his article <sup>[23]</sup> that in the quest for process safety, the important thing is to identify measures of how well the process safety controls are functioning. Whether they are called lead or lag indicators is a secondary matter.

According to Andrews Hale article <sup>[24]</sup> the HSE guidance document <sup>[25]</sup> fails to communicate a clear, explicit and well-articulated model forming the basis for defining and using indicators, and it is therefore confusing. The document uses the Reason model (1997, or more known as the swiss cheese model) <sup>[25]</sup>, but presents it with the idea that an indicator is leading or lagging in respect of the working of a barrier, rather than the much more commonly used definition that it leads or lags the occurrence of harm, or at least the loss of control in the scenario leading to harm. In the article it is also stated that Hopkins dismisses too lightly the distinction between leading and lagging indicators. To gain more information of the discussion concerning leading or lagging indicators references is made to Safety Science volume 47, 2009 <sup>[26]</sup>. A potentially useful distinction between types of indicators has emerged recently <sup>[51]</sup>; drive indicators (that represent input to the safety management process and correspond closely to leading or activity indicators), monitor indicators (that present the current level of safety in the organisation) and feedback indicators (that correspond closely to lagging or outcome indicators. These definitions also correspond to the use of indicators in economic, which in addition to leading and lagging indicators also have coincident indicators <sup>[27]</sup>. A coincident indicator changes at approximately the same time as the whole economy, thereby providing information about the current state of the economy.

Safety performance indicators are needed for three different uses <sup>[24]</sup>;

1. Monitoring the level of safety in a system (whether that is a department, a site, or an industry). This answers the question: is the level of safety OK as we are managing things, or should extra action be taken to improve it? This requires data which shows reliable and valid trends in safety. The indicators do not need to be causally linked to safety outcomes, as long as the correlation is and stays high and the numbers are big enough to show trends.
2. Deciding where and how to take action if the answer to question 1 is that action is needed. This requires indicators deeper in the system showing the state of those causal links to the harm which have been proven to exist (or at least are strongly believed).
3. Motivating those in position to take the necessary action to take it.

In the offshore industry today there are several common HSE indicators, such as gas leaks, critical incidents, personal injuries etc. However, these indicators do not help when trying to evaluate the performance of barriers meant to prevent a major accident. It is said that "*You can't manage what you can't measure,*" <sup>[28]</sup> and much work has been invested in trying to establish proactive indicators of safety performance.

One strategy to avoid accidents is to be continuously vigilant through the use of indicators <sup>[29]</sup>. Often, hindsight has shown that if signals or early warnings had been detected and managed in advanced, the unwanted event could have been prevented (e.g. Longford accident, chapter 4.1 and Texas City accident, chapter 4.4). Building Safety<sup>1</sup> is a research project which addresses safety opportunities and challenges in petroleum exploration and production in the northern regions, with emphasis on the Goliat field outside the northern coast of Norway. One

---

<sup>1</sup> <http://www.sintef.no/buildingsafety>

of the main research issues in Building Safety is to develop new models and methods for the establishment of indicators, which can unveil early warnings of major accidents <sup>[29]</sup>.

Development of early warning indicators to prevent major accidents can, from a theoretical foundation, be done from two different perspectives. There is a close connection between safety and risk, but it is important to distinguish between the concepts and their indicators, as shown in figure 2:

Organisational factors	Indicators	
I Qualitative treatment	II Safety indicators	Safety approach (proactive or retrospective)
III Quantitative treatment	IV Risk indicators	Probabilistic risk approach (predictive)

Figure 2: Distinction between the safety approach and the probabilistic risk approach<sup>[30]</sup>

However, the safety approach is not purely qualitative, and the risk approach is not purely quantitative. Safety indicators (second quadrant) are often quantitative, and the quantitative/probabilistic treatment of organisational factors (third quadrant) also include qualitative aspects <sup>[30]</sup>.

It makes a big difference whether trying to predict the possibility of having a major accident “tomorrow” or if “only” trying to establish the causes after the event (in retrospect). For the prediction of risk, as for accident investigation, it makes sense to talk about a development from technical, to human, and even to organisational causes. This does not imply that all features of risk assessment can be classified according to a technical-human and organisational “scheme”. There are features that cut across these aspects, such as dependent failure analysis and uncertainty analysis. However, some aspects can be attached to primarily one of the causal categories, for example, human reliability analysis (HRA) attached to the human causes of accidents. Based on the two presented perspectives; the technical-human-organisational, and the predictive-versus-retrospective, a conceptual model to structure and illustrate the previous is presented in the building safety project <sup>[29]</sup>:

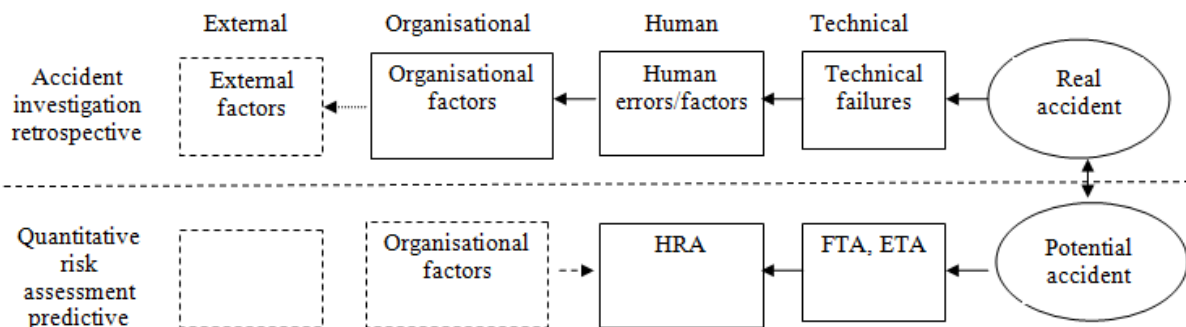


Figure 3: Retrospective investigation versus predictive assessment <sup>[29]</sup>

A risk influencing factor (RIF) is defined as “an aspect (event/condition) of a system or an activity that affects the risk level of this system or an activity” <sup>[29]</sup>. A given risk RIF (e.g., an

organisational factor) might not be directly measurable. Instead we need an operational definition of the RIF, that represents the theoretical variable, as illustrated in figure 4<sup>[29]</sup>:

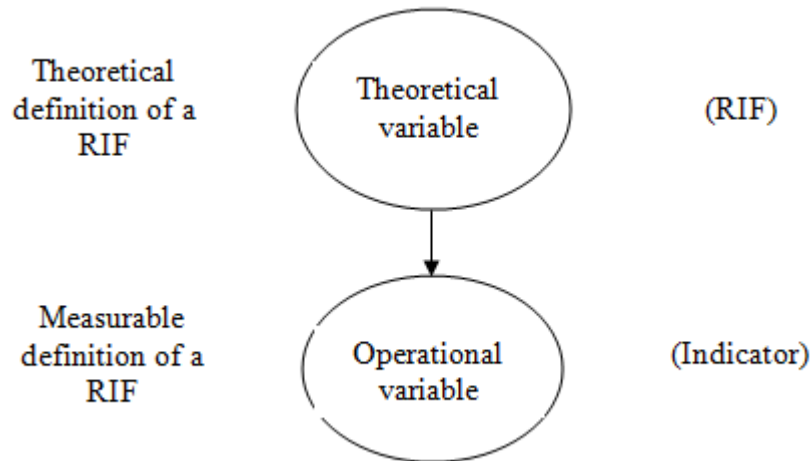


Figure 4: General measurement model <sup>[29]</sup>

The operational variable is an indicator. The indicator is not a RIF itself, just a measurable representation of the RIF. Measurement of one RIF may be performed by a set of indicators. Making a (theoretical) variable operational means giving instruction on how to measure the theoretically defined variable – this transformation is both controversial and a possible source of errors. It is stated that ‘the basic, inherent difficulty with indicators is that they are selective. They each represent one measure of one aspect of any situation <sup>[29]</sup>. This means that there is always room for discussion and even disagreement about whether they really represent what one wants to measure. Even though this may be of theoretical interest, it can be counterproductive in practice. Discussion and disagreement regarding indicators should not be allowed to impede the development of early warning indicators to help prevent a major accident.

The terms safety indicator and risk indicator are sometimes used interchangeably in the literature, but the difference between these two indicators are: if the RIFs are included in a risk model, such as a probabilistic risk assessment, then it is possible to determine the effect on risk because of a change in the indicator value of a given RIF. If we do not have such a risk model, we can still identify some of the same factors and also establish some of the same indicators. However, the effect on safety has to be related to some other measures than risk metrics, e.g. number of accident or purely qualitatively without quantifying safety. The indicators and the corresponding factors are then often selected, based on either an assumed effect on safety, or through correlation. These indicators should be denoted safety indicators <sup>[29]</sup>.

To summarize the above discussion; when developing indicators, different approaches for the development of indicators may be classified into <sup>[31]</sup>:

- safety performance-based indicators
- event indicators
- barrier indicators

- activity indicators
- programmatic<sup>2</sup> indicators
- risk-based indicators:
- technical indicators
- organisational indicators
- incident-based indicators
- resilience-based indicators

Research on indicators started with the need to measure safety or risk. The main function of a measure of safety/risk performance is to describe the safety/risk level within an organisation, establishment or work unit. An indicator is a measurable representation of an aspect of reality, e.g., safety or risk. Safety and risk indicators represent two different perspectives; one based on assumed relations, or the use of correlation, and the other on causal connection through a risk model. The major hazard industries can benefit substantially from increased utilisation of existing methods for the development of risk or safety indicators. However, there is no such thing as a universal model or method for the development of indicators<sup>[29]</sup>. A risk indicator is dependent on quality data, and criterion for assessment of major accident hazard risk indicators are<sup>[34]</sup>:

- observable and quantifiable
- sensitive to change
- transparent and easily understood
- robust against manipulation
- valid

The importance of management and organisational factors of the risk of major accidents in high-hazard industries has been demonstrated through accident investigations in the last couple of decades<sup>[33]</sup>. This will also be presented in chapter 4. But what about predicting the impact of organisational factors on risk in advance, and to use this insight proactively to avoid or reduce risk of new disasters?

In the oil and gas industry risk-based decision-making is used and performing risk analysis before carrying through an operation helps identify what might go wrong. 'QRA' is used as the abbreviation for 'Quantified Risk Analysis'. If one wants to predict the impact of organisational factors on risk in advance, this could be done as an extension of the QRA. It could be performed as a part of, or as add-on to the QRA. However, QRAs are updated rather infrequently, and in the meantime, parameters and assumptions in the QRA change, which means that the value of QRA as a risk control tool diminishes. It has been attempted to measure the safety performance of organisations qualitatively through so-called safety audit methods<sup>[33]</sup>, and quantitative tools have rarely been linked to a risk assessment. A framework for establishment of organisational risk indicators has been developed and was presented in Reliability engineering & system safety volume 74<sup>[33]</sup>. The framework was developed based on a review of existing organisational factor frameworks, research on safety performance indicators, and previous work on QRA-based indicators. No single field of research covers both the quantitative impact of organisational factors on risk and measuring of the quality of the organisational factors utilizing indicator measurements. It has been carried out as two separate research areas.

---

<sup>2</sup> Programmatic performance indicators (PPIs) are indicators that assist in assessing the quality and performance of various programs, functions, and activities relating to the safety of the plant.

When developing an organisational model, there are both theoretical and practical concerns regarding an adequate organisational model. On the theoretical side the model should preferably be <sup>[33]</sup>:

- theoretically founded, i.e. having a sound of basis from organisational theory, management theory, safety management theory, etc.
- structured, i.e consist of a network of relations, not just a classification of factors
- substantiated through incident and accident data. Alternatively, the factors/model may be validated based on comparison of high and low accident companies or based on studies of high reliability organizations.

On the practical side, the model must be comprehensible and usable both qualitatively and quantitatively. The qualitative organisational model, as shown in figure 5 (Bayesian network), was the basis for developing a quantitative model. In figure 6 the quantitative part in relation to the starting point for the development of organisational risk indicators is illustrated:

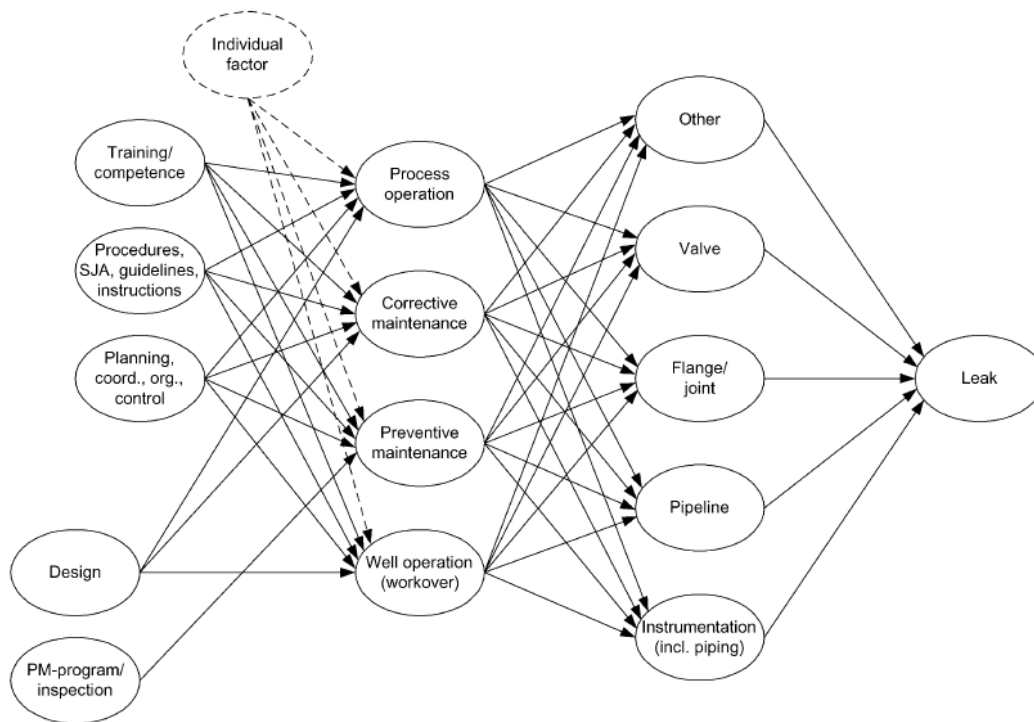


Figure 5: Organisational model <sup>[33]</sup>

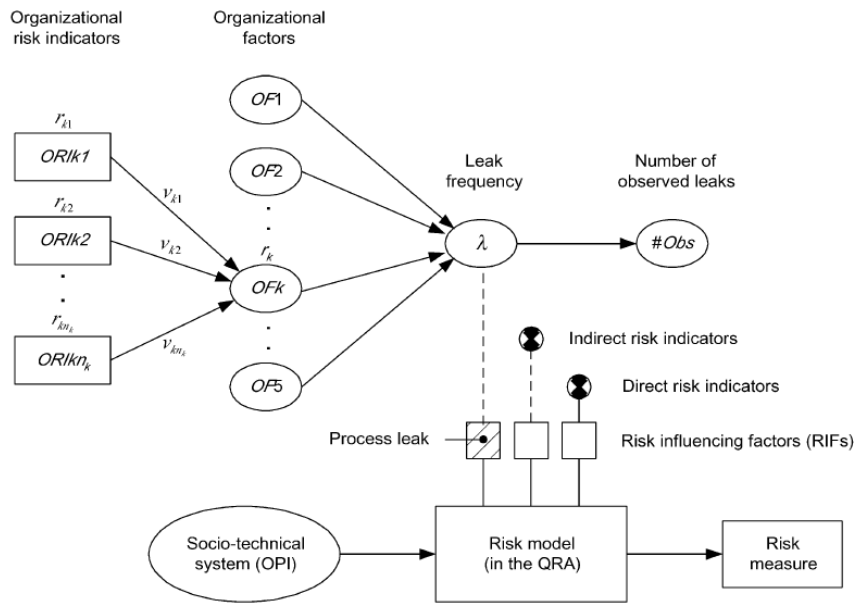


Figure 6: Overview of the quantification process in the project [33]

The overview of the outcome of work done to develop a framework for establishment of organisational risk indicators is shown in figure 7.

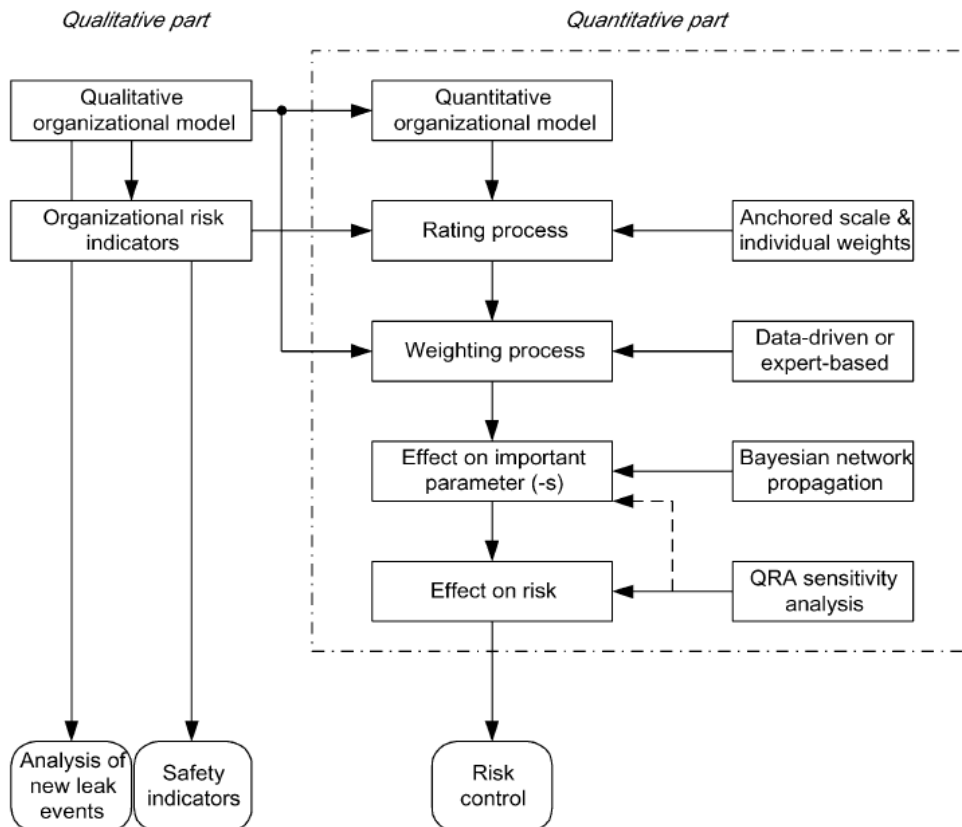


Figure 7: Framework for establishment of organisational risk indicators [33]

The model only cover one specific parameter; the leak frequency. If the aim is to capture the total effect on risk of one specific organisational factor explicitly, similar models as done for

the leak frequency for all parameters must be built. However, this model illustrates the relation between risk influence factors at a given installation and how they can be monitored by developing suitable indicators.

The framework described above is very similar to the methodology developed in the Barrier and Operational Risk analysis project (BORA). In the BORA project the aim was to model and analyse barriers, both physical, non – physical, threats and consequence barriers on offshore production installations. The project developed a methodology that has three main processes <sup>[34]</sup>:

- qualitative analysis of scenarios, basic causes and risk influencing factors
- quantification of average frequencies/probabilities
- quantification of installation specific frequencies/probabilities.

The purpose of developing a framework of organisational risk indicators is that the tool can be used to control the risk during operation. The risk indicators (direct, indirect and organisational) measure changes in important risk influencing factors. Based on this measurement, the relative change in risk can be estimated. However, the challenge is to develop indicators with the ability to predict future safety performance.

## 2.4 Regulations

The Petroleum Safety Authority (PSA) framework gives superior requirements that the industry has to correspond with. Section II in the Management regulation is called Risk Management and gives an account for regulation regarding risk reduction and barriers. Section V deals with analyses, such as risk and preparedness analyses. In appendix A the full contents of the sections are presented.

## 2.5 Risk analysis

A risk-based approach treats risk as a product of likelihood and consequence; the more likely the event is or more severe the possible consequence is, the greater the risk.

It is important to emphasize the signification of safety thinking and preventive safety work to avoid accidents. Performing a risk analysis before carrying through an operation helps identify what might go wrong and barriers and routines can be established to prevent occurrence of an undesired event.

A risk analysis is defined in the NORSOK standard <sup>[14]</sup> as:

*“An analysis which includes a systematic identification and description of risk to personnel, environment, and assets”*

A quantified risk analysis (QRA) has to be focused on <sup>[34]</sup>:

- identification of applicable hazards
- description (including quantification) of applicable risks to personnel, environment, and assets

The practical execution of a risk assessment is often described as <sup>[34]</sup>:

- identification of critical events



- coarse consequence analysis
- cause analysis (qualitative: intended to identify cause/conditions/combinations that may lead to the occurrence of initiating events and establish the basis for later quantitative analysis)
- quantitative cause analysis (intended to establish the probability of occurrence of initiating events)
- detailed consequence analysis
- risk calculations

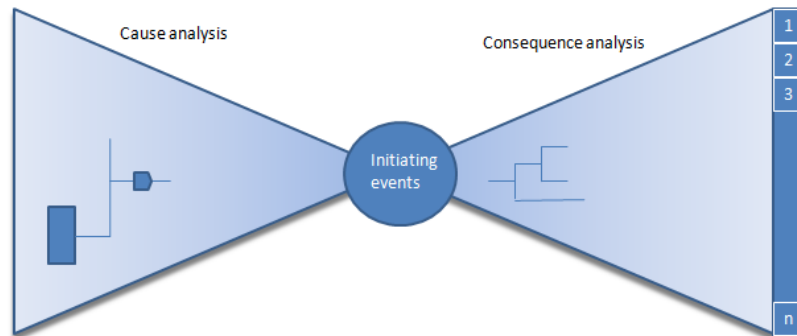


Figure 8: Model for representation of the process risk assessment <sup>[34]</sup>

Each of these steps may include extensive studies and modeling. Some examples on how to perform each step is presented here <sup>[34]</sup>:

- Identification of Initiating Event by using Hazard identification (HAZID):
  - o check list
  - o accident and failure statistics
  - o Hazard and Operability (HAZOP) studies
  - o comparison with detailed studies
  - o experience from previous similar projects, concepts, systems, equipment and operations.
- Cause analysis
  - o identification of the combination of causes that may lead to initiating events
  - o assessment of probability of initiating events
- Qualitative Cause Analysis Techniques
  - o Hazard and Operability analysis (HAZOP)
  - o Fault Tree Analysis (FTA)
  - o Preliminary Hazard Analysis (PHA)
  - o Failure Mode and Effect Analysis (FMEA)
  - o Human Error Analysis techniques, such as task analysis and error mode analysis
- Quantitative Cause Analysis Techniques
  - o Fault Tree Analysis (FTA)
  - o Event Tree Analysis (ETA)
  - o synthesis models
  - o Monte Carlo simulation
  - o human error quantification techniques

- calculation of frequency of initiating events from historical statistical data
- BORA methodology for analysis of hydrocarbon leaks and consequence barriers.
  
- Consequence Analysis
  - Event Tree Analysis (ETA)
  - cause consequence diagrams
  - influence diagrams
  - HTO analysis

Risk calculations are done with a basis in frequencies and consequences from the analysis.

The term 'risk' is according to international standard Risk Management – principle and guideline, defined as <sup>[35]</sup>:

*“the effect of uncertainty on objectives”*

The 2002 definition of risk *“combination of the probability or an event and its consequence”* is note to the definition given in ISO 31000 <sup>[36]</sup>.

Risk is often expressed in several ways, by probability distribution, expected values, single probabilities of specific consequence, etc. Most commonly used in the offshore industry is the expected value. An operational expression for practical calculation of risk is <sup>[34]</sup>:

$$R = \sum (p_i \times C_i) \quad \text{(Formula 2.1)}$$

where p equals the probability of an accident and C equals the consequence of the accident.

One important aspect though, which is not accounted for when expressing risk as mentioned above, is the uncertainties. When calculating risk a lot of assumptions are made and the probability calculation is a tool used to express this uncertainty. When expressing risk as a function of uncertainties and consequences another presentation of risk is the (A, C, U) perspective <sup>[37]</sup>:

$$R = (A, C, U) \quad \text{(Formula 2.2)}$$

where

A equals the event,

C equals the consequence of an event, and

U equals the uncertainty.

By risk is meant the two-dimensional combination of events A and the consequences of these events C, and the associated uncertainties U (will A occur and what value will C take)

Consequences may be related to personnel, to the environment, or to assets and production capacity. Personnel risk can be expressed as fatality risk.

Fatality risk:

Fatality risks have a number of expressions, such as individual risk, group risk and f-N curve. PLL value can, based on a QRA, be expressed <sup>[34]</sup>:

$$\text{PLL} = \sum_n \sum_j (f_{nj} \times C_{nj}) \quad \text{(Formula 2.3)}$$

where

- $f_{nj}$  = the annual frequency of accident scenario  $n$  with personnel consequence  $j$ .
- $C_{nj}$  = expected number of fatalities for accident scenario  $n$  with personnel consequence  $j$ .
- $N$  = total number of accident scenarios in all event trees
- $J$  = total number of personnel consequence types, usually immediate,

The annual frequency of an accidental scenario, related to hydrocarbon leakage and ignition,  $f_{nj}$ , may be expressed as follows, if it assumed that the factors are related <sup>[34]</sup>:

$$f_{nj} = f_{leka,n} \times P_{ign,n} \times P_{protfail,n} \times P_{escal,n} \times n_{nj} \quad \text{(Formula 2.4)}$$

where

- $f_{leka,n}$  = frequency of leak
- $P_{ign,n}$  = conditional probability of ignition, given leak
- $P_{protfail,n}$  = conditional probability of failure of the safety protective systems, such as ESD, blow down, deluge, passive fire protection, etc. given that ignition has occurred.
- $P_{escal,n}$  = conditional probability of escalation, given ignited leak and failure protective systems response.
- $n_{nj}$  = fatality contribution of the accident scenario (fraction of scenarios that result in fatalities).

Principally there are two options when expression individual risk; FAR (Fatal Accident Rate) and AIR (Average Individual Risk). Far value is the number of fatalities in a group per 100 million exposed hours, whereas AIR value is the average number of fatalities per exposed individual. Following equations define how the individual risk expressions are computed <sup>[34]</sup>:

$$\text{FAR} = \text{—————} \quad \text{(Formula 2.5)}$$

$$\text{AIR} = \text{—————} \quad \text{(Formula 2.6)}$$

Bayesian approach to risk:

The Bayesian thinking is not that different from the probability of frequency approach. The point is that the Bayesian approach, as presented in the literature <sup>[37]</sup>, allows for fictional parameters, based on thought experiments. These parameters are introduced and the uncertainty in them is assessed. Bayesians would not speak about true, objective risks and

probabilities. The predictive form is seen as the most important one. Risk analysis introduces two level of uncertainty: the value of observable quantities such as number of failures of a system, and the `correct` value of the risk. Both the analysis and the results of the analysis are considered uncertain <sup>[38]</sup>, which does not provide a good basis for communication and decision-making.

Bayes formula <sup>[39]</sup>:

$$\pi(\theta | x) = \frac{\pi(x | \theta)\pi(\theta)}{\pi(x)}$$

(Formula 2.7)

Where

$\pi(\theta|x)$  = posterior distribution

$\pi(x|\theta)$  = likelihood function

$\pi(x)$  = the probability distribution of x

$\pi(\theta)$  = prior distribution

The Bayes principle is to update a given probability distribution based on new knowledge/observed data. As can be seen from formula 2.7, there are some differences between classical and Bayesian statistics. First, the idea of prior information does not exist in classical statistics. All inferences in classical statistics are based on the sample data. In the Bayesian framework, prior information constitutes the basis of the theory. Another difference is in the overall approach of making inferences and their interpretation. For example, in Bayesian analysis the parameters of the distribution to be "fitted" are the random variables. In reality, there is no distribution fitted to the data in the Bayesian case. By applying formula 2.7, the posterior distribution of the shape parameter will be obtained. Thus, we end up with a distribution for the parameter rather than a estimate of the parameter, as in classical statistics.

## Chapter 3. Gassco's barrier KPI model

Gassco and the start up of the barrier KPI project, the development and the use of the model are described in this chapter.

### 3.1 Description of Gassco AS and the barrier KPI project

The creation of Gassco forms part of an extensive reorganization of the Norwegian oil and gas sector. Gassco was founded by the Ministry of Petroleum and Energy (MPE) on 14 May 2001, and took over the operatorship of all gas transport from the Norwegian continental shelf on 1 January 2002. The Gassco joint venture is the formal owner of the bulk of Norway's gas infrastructure. As Operator, Gassco is responsible for safe and efficient gas transport from the Norwegian continental shelf. Norway's gas pipelines have a total length of 7 975 kilometres. The gas flows from production installations to process plants, where natural gas liquid is separated out and exported by ship. The remaining dry gas is piped on to receiving terminals in continental Europe and the UK. In addition to pipelines, Gassco also have an operator responsibility for offshore installations, land based facilities and receiving terminals in the UK and at the continent.

Gassco operates the receiving terminals at the continent with own employees. At the receiving terminals in the UK, offshore installations and land based facilities daily operation are carried out by technical service providers (TSP's). A potential for major accidents clearly exists in Gassco's area of responsibility, and through its management systems the company must ensure that major accident potential is properly handled and minimised. Gassco have a well established set of KPIs for follow-up of HSE issues such as occupational injuries, frequency of critical incidents and gas leaks. However, these are lagging KPIs and do not give an overview of the potential for a major accident. Maintenance, testing, control etc. might be as important to the potential of major accidents as system design.

Gassco's management strategically focus in 2008 were among other things <sup>[40]</sup>:

- the highest priority shall be given to understanding, managing and reducing major risks on all facilities and during all operations
- overview and control of all safety critical barriers, including inspection, maintenance and testing of safety critical equipment is essential to manage risks

Furthermore, there is a requirement from the Petroleum Safety Authority in Norway to monitor the risk of major accidents <sup>[41]</sup>. Development of a new KPI system for safety critical barriers was one of the activities that was included in Gassco's research and development program in 2008. DNV was contracted by Gassco to develop a KPI model with the objective of establishing a framework, define parameters and requirements to reporting for follow-up of the most important safety critical barriers at Gassco's installations. The suggested indicators were to reflect the status and control of barriers intended to prevent major accidents <sup>[7]</sup>.

### 3.2 Barrier KPI model

When developing the model all relevant hazards subject to Gassco's installations were evaluated. Mitigating measures in terms of barrier was identified and visualised in a bow tie model, exemplified in figure 9 <sup>[8]</sup>.

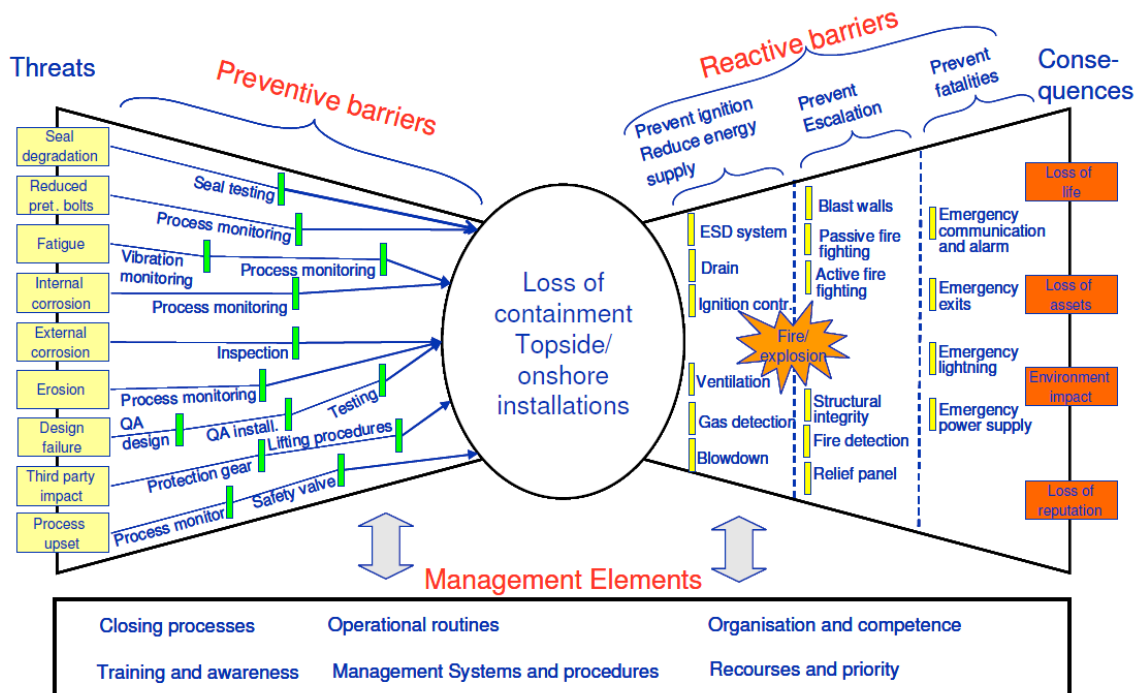


Figure 9: Bow-tie loss of containment [8].

The bow tie model forms the basis for the development of the barrier KPI model. Based on literature/industry review, workshops and discussions, a set of barriers were selected to be included in the model and sorted into three categories based on their functionality in line with the bow tie representation [8]:

- preventive barriers; mainly inspections activities
- reactive barriers; technical safety barriers
- management elements; non physical barriers such as closing processes, procedures and management systems.

Further the model had to adapt to the following objectives and requirements:

- ability to adapt to various types of installations (platforms, pipelines, processing facilities and receiving terminals)
- provide useful information both on a facility level and on an aggregated level
- allow for automatic transfer of information
- minimum need for manually generated data
- minimum need for collection of information not already being available in some form
- model to be implemented in Gassco's management tool – Performance Management Gassco, PMG.

Measuring parameters was identified and indicators to follow-up the selected barriers was derived. The input data to the model is reported on a system (barrier) level and the results aggregated up in Gassco's organisational hierarchy in PMG.

Limitations and assumptions for the model are as follows [8]:

- the model indicates how existing systems and function are followed up. Suitability of the safety systems in place or completely lack of safety system and/or preventive maintenance plans are not indicated in the model

- indicator rating indicates how the effort in prevention major accidents is carried out and how work develops over time, and is not directly correlated to the risk of major accidents at a certain installation
- the model assumes that a suitable preventive maintenance program is in place, including testing of safety barriers and inspection of pressurised equipment
- audit routines are assumed in place and audit outcomes are assumed to be documented properly.

Some important topics that are left out in the model and justification for doing that is <sup>[8]</sup>:

- competence and training: hard to establish suitable measuring parameter due to low degree of systematic competence mapping and requirements
- design and layout: handled by other means such as QRA on design, procedures and audits
- safety culture: no unambiguous definition, hard to establish suitable measuring parameter
- incidents: handled by other KPI's. Each incident handled separately
- management of change: hard to establish suitable measuring parameter, include several topics that may affect safety to smaller or larger extent.

It is well known that for some subjects it can be very difficult to establish suitable parameters, that also are effective. The justification for leaving several important topics out of the model is not good enough in the long run. But when the barrier KPI started, the aim was to get something done relative quickly without too much obstructions in the start. The aim with this report is to evaluate if it is possible to further develop the Barrier KPI model, including the topics mentioned above that were deliberately left out in the start of the project.

### **3.3 Reporting and follow up**

According to Gassco's procedure "Reporting and follow up of barrier indicators" <sup>[42]</sup> the HSEQ Manager is responsible for maintenance and further development of the Barrier KPI model. The Director for Technical Operation is responsible for implementation of the Barrier KPI model. The Director Gas Terminals, Director Transportation Network and Director Processing Facilities are responsible for reporting of data from all facilities as required, and that required improvement initiatives and actions are identified and implemented based on reported performance.

The input data to the model is reported on a barrier level and the results aggregated up in Gassco's organisational hierarchy as illustrated in the figure below <sup>[8]</sup>:

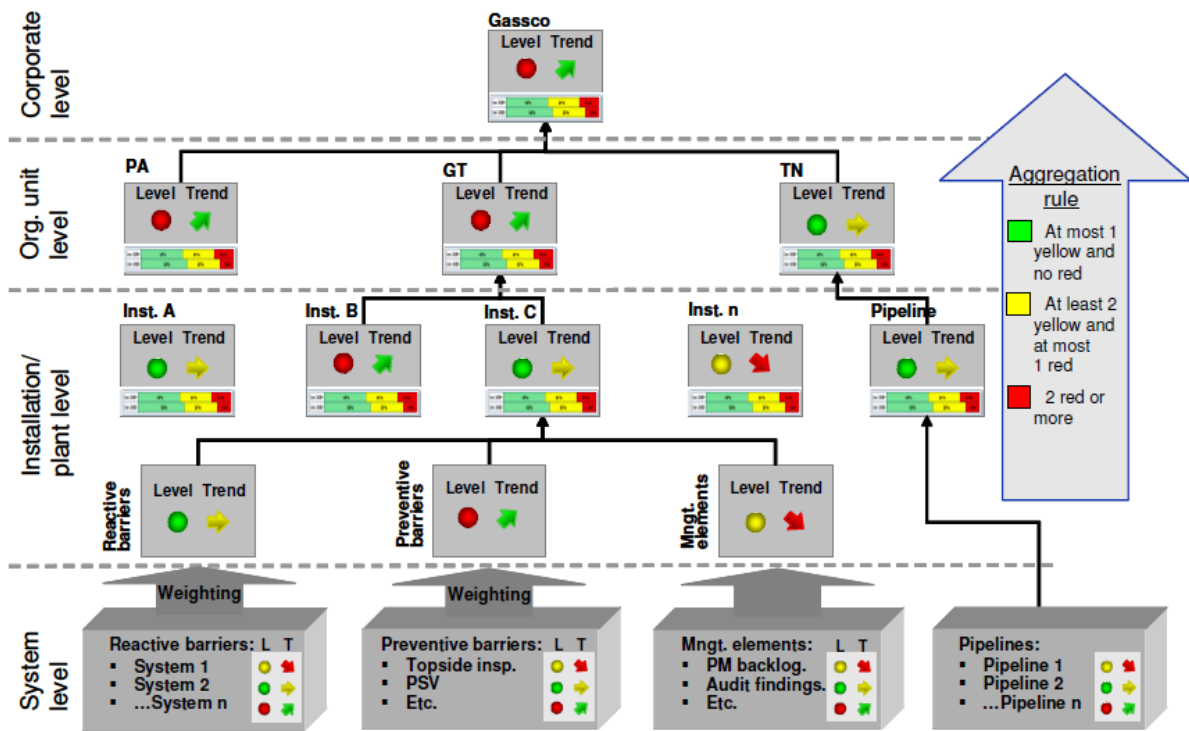


Figure 10: Illustration aggregation in Gassco's hierarchy [8]

Presentation of the Barrier KPI model on system level and corporate level in PMG are illustrated in the next two figures:

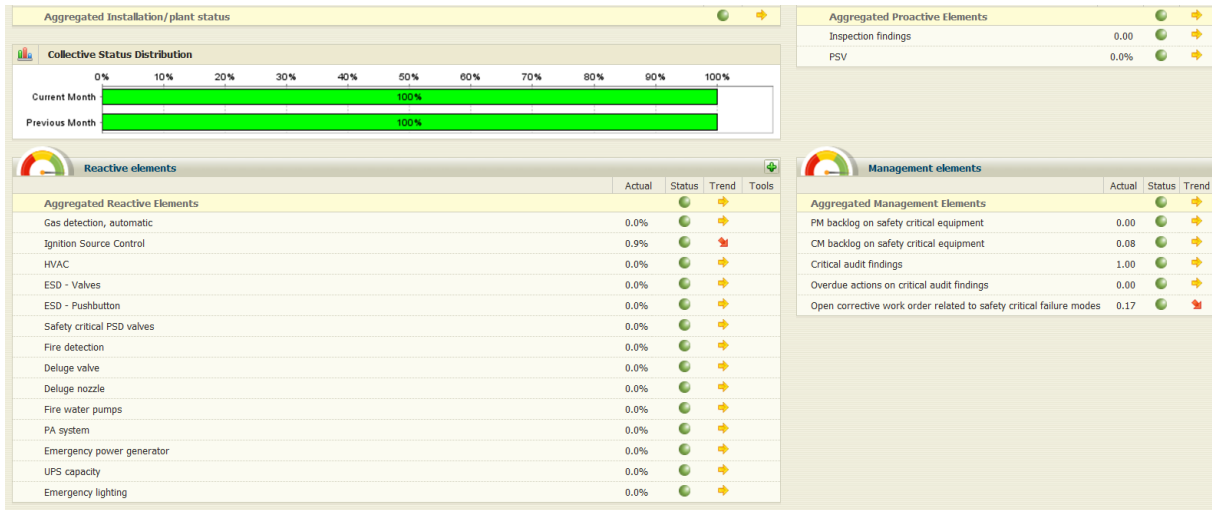


Figure 11: System level



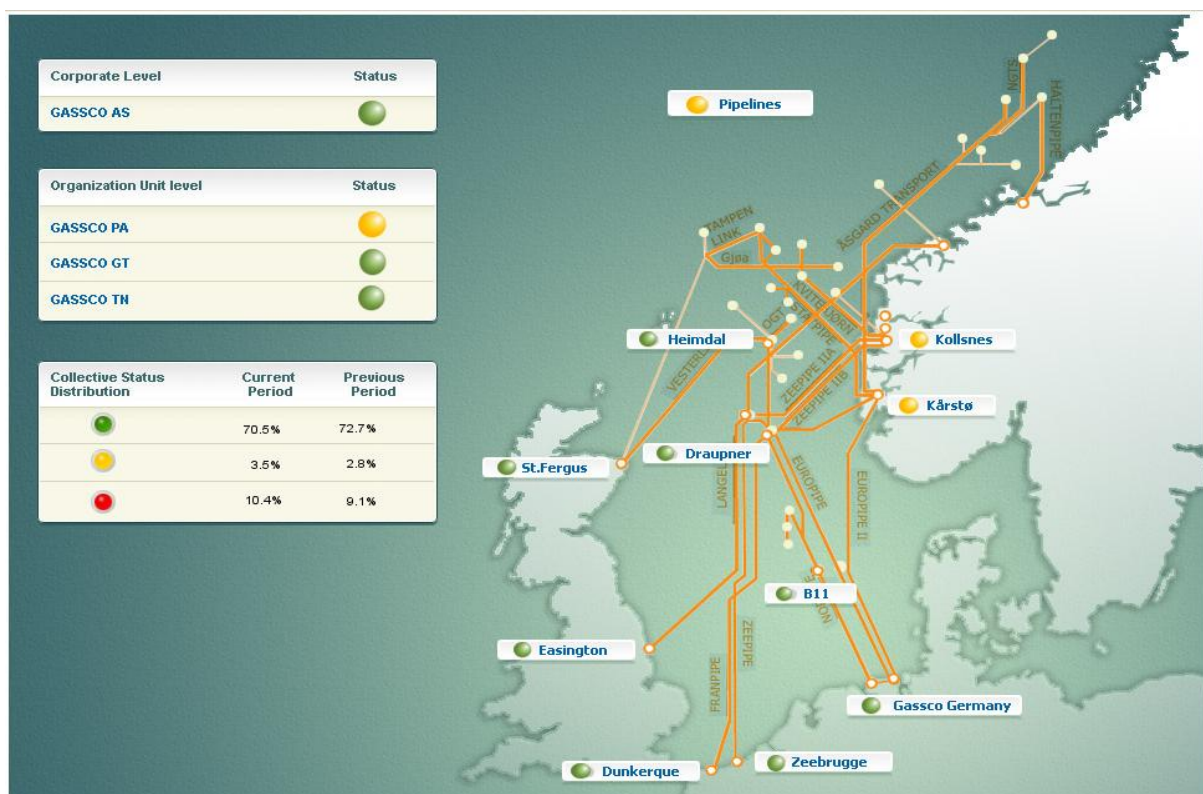


Figure 12: Illustration Corporate level

Full indicator list and aggregation rules are presented in appendix B.

One dedicated person in Gassco is responsible for the implementation and follow-up of the Barrier KPI model for each facility or plant. Typically the person in Technical Operation at Bygnes is responsible for daily follow-up of the respective asset. The asset responsible ensures that data is being reported regularly on a monthly basis. A schematic of the information flow and responsibility level is given in the following figure <sup>[42]</sup>:

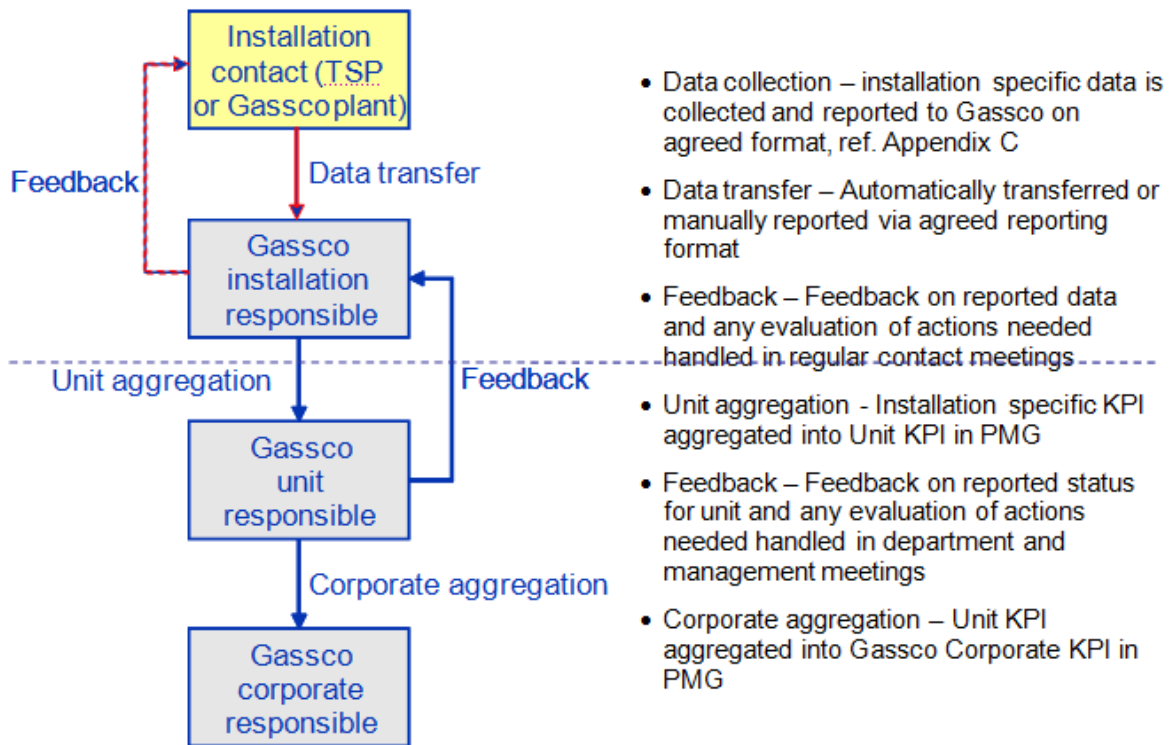
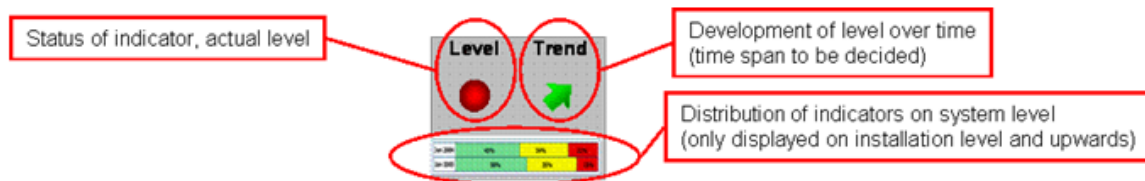


Figure 13: Reporting and follow-up work process [42]

Results in the Barrier KPI model are presented on indicator level and aggregated results for level and trend according to a traffic light system with the interpretation and accompanying actions as outlined in the following figure [42]:



**Interpretation of colour rating**

Colour Rating	Interpretation		Action (based on level rating)	
	Level	Trend	System level	Installation level
Green	Satisfying status	Improvement	No action required	No action required
Yellow	Improvement needed	Unchanged	Cause should be identified and trend monitored closely	Evaluate underlying KPIs to identify cause. Monitor trend closely.
Red <i>Note)</i>	Unsatisfying status	Deterioration	Immediate mitigating measures should be initiated	Evaluate the need for an overall risk assessment of the plant. Rank unsatisfying elements by risk and carry out mitigating actions according to rank.

Figure 14: Explanation level, trend and colour rating [42]

*Note: Unsatisfying status should be interpreted as an indication of elevated risk where action is needed. Unsatisfying status should however not be interpreted as unacceptable risk.*

If an indicator is yellow or red in PMG a comment explaining the cause is required from Gassco`s installation responsible.

Experience gained through the pilot test shows that by developing a barrier integrity indicator, the following experiences and conclusion have been made <sup>[43]</sup>:

- the "HTO" methodology gives a good foundation for the Barrier KPI.
- the Barrier KPI work has improved the focus and the understanding of barriers within the organisation
- "TTS" findings have been repaired and avoided as a consequence of this work
- as a result of the reporting, an annual verification of the A10 report is established
- an useful tool and a good indicator
- provides a good picture of the technical integrity on safety critical systems and covers up the organisations barriers well
- the greatest gain is that it puts the focus on barriers as a totality and development of good safety culture at the assets. Focus is put on the area with weakness and therefore also has the biggest improvement potential
- it is a good monitoring tool and it is useful when it comes to following up the daily work.

## Chapter 4. Does Gassco's barrier KPI model reflect learning from recently major accident in the industry?

The Petroleum Authority in Norway definition of a major accident is <sup>[44]</sup>:

*“ An acute incident, such as a major spill, fire or explosion, which immediately or later causes a number of serious personal injuries and/or loss of human life, serious harm to the environment and/or loss of large material assets. ”*

The history of major accidents goes way back <sup>[45]</sup>. Several accidents have resulted in new regulations and increased focus on barriers, such as the Seveso accident in 1976, which led to the Seveso directive (approved in European Union 1982). The Alexander Kielland accident in 1980 and the Piper Alpha accident in 1988 resulted in a change in the safety regime and new regulations in Norway and the UK.

Unfortunately, the history of the process industries shows that many accidents are repeated after a lap of few years. People move on and take their knowledge with them and the lessons are forgotten. Trevor Kletz, who has studied petrochemical industry disasters for many years, said that: *“ organisations have no memory, only individuals do ”* <sup>[46]</sup>.

In the following chapters, a selection of major accidents occurring in the period 1998 – 2010 will be studied. Triggering and underlying causes for the accidents will be compared against each other. The aim is to identify similarities. Does the industry learn from other major accidents? Are the learnings implemented in Gassco's barrier KPI model?

Description of the accident and what went wrong are in some chapters limited due to few public reports. The quality of the investigations report also vary, some are very thorough and look at several aspects in the human technology and organisation method, while others do not.

### 4.1 Longford 1998

Reference for the bulk of information in this chapter is made to the book “Lessons from Longford” by Hopkins <sup>[47]</sup>. Findings presented in the book are from the Royal Commission<sup>3</sup> and the book is written by an expert witness at the Commission hearings. When other sources are used beside this book, reference is made in the text.

In September 1998, a heat exchanger in the Esso (subsidiary of Exxon) gas plant in Longford, Victoria, Australia, fractured and released hydrocarbon vapors and liquids. An explosion and fire followed, killing two employees and injuring eight. It took more than 2 days before the fires were fully extinguished. Supplies of natural gas were interrupted throughout the state of Victoria and were not fully restored until October. Most of Melbourne's 3.2 million residents were affected in some way and many thousands of people were laid off because their

---

<sup>3</sup> Royal Commissions are called to look into matters of great importance and usually controversy. These can be matters such as government structure, the treatment of minorities, events of considerable public concern or economic questions.

employers relied on gas. Many industrial and domestic users were without fuel for all or part of the time the plant was shut down.

The direct cause was that a pump supplying heated oil to a heat exchanger stopped and was offline for several hours. No flow of warm oil through the heat exchanger, causing the temperature to drop to a value below normal operating temperature. The low temperature resulted in a formation of ice on the heat exchanger nozzle. When restarting the oil pump warm lean oil flowed into the exchanger, causing stress in the vessel (due to temperature differential) and fracture. A vapour cloud of 10 tones of hydrocarbons was released and ignited by heaters 170 meters away, leading to a series of explosions and vessel ruptures. Although the direct causes of the explosion were operational and engineering issues, the government Royal Commission blamed Esso and its management. The reason why will be explained in this chapter.

The operators and their supervisors made a critical error when deciding to reintroduce the warm oil into the heat exchanger after it had become super cold. Esso claimed that the operators had received adequate training and did know about the dangers of cold temperature embrittlement, and that they should have known better. They should have allowed the heat exchanger to thaw out before they began to re-establish the warm liquid flow. Still Esso was blamed and not the individual operators. The Royal Commission claimed that the accident could have been prevented.

Operators at Longford did make mistakes and Esso was to blame for faulty training. There were a number of root causes of the training failure<sup>[47]</sup>; 'Competence-based training': the operators were given written tests for which they were able to memories answers. Test results were used to determine job classification and pay level. This gives intensive to answer correctly. It was possible to answer all the questions correctly, but not understand the reason. The training did not test for understanding. An operator that was almost answered correctly was given coaching by the assessor. The person was then asked if the answer was understood – if they said 'yes' they passed. But did they really understand? One could assume that it took "gumption" to ask for a re- explanation. If they said that they didn't understand, it could implicate that the explanation given by the assessor was inadequate. And given the pay increase intensive, there was no guarantee that the operator really understood the question. One operator admitted that it was 'normal practice' for operators to give answers that they didn't understand. The view was that it is not generally required to get 100% correct answer to pass an exam.

Personnel should be provided with training in the limitation of plant equipment. One of the reasons of insufficient training is failure to identify the hazards. Longford gas plant changed over time, the plant grew and evolved. These changes invalidate prior risk assessments and created new risk that needed to be managed diligently. Significant changes in operating processes, staffing and procedures at Longford plant were carried out without thorough risk assessments. As plant 2 and 3 were added to the Longford site without any consideration of the risk of interconnectedness. Two other management of change failures were that changes in the process upset of gas plant 1 was done without proper assessment of the risks involved, and engineering staff was moved from the plant to the head office without assessing possible risks involved. Problems at Longford were too complex for operators and their supervisors to manage and there was no engineering staff on site on the day of the accident. Until 1991 engineers had been employed at Longford. They knew the plant and had worked with the

operators. Due to cost cutting, the engineers were moved from the plant. The relocation was implemented without performing any risk assessment and evaluation.

A Hazard and Operability study (HAZOP) which could have identified the potential hazards was not carried out. The Commission's view was that a HAZOP would have identified the need for written procedures for dealing with the loss of warm oil flow, as well as procedures for plant shutdown and restart (which occurred infrequently and may present special dangers not faced during normal operation).

When something was wrong at the plant an alarm would go off. In this case, the operator failed to respond to the alarm that went off, and subsequently failed to control the upset in the process and return the plant to normal. The result of these continuing abnormal conditions was an automatic shutdown of the warm oil pumps next morning. But why did the operator fail to react to the alarm? Variations in operating conditions might affect the quality of the gas produced, causing it to go 'off spec' and causing alarms. It was easier sometimes to maintain the quality of the outgoing gas by allowing processing to occur outside the specific limits, resulting in that the operators cancelled the audible alarm. When experiencing many alarms on a daily basis, humans often start ignoring alarms. The condensate transfer system which had been installed in gas plant 1 in 1992 required the system to operate outside its normal temperature limits when condensate transfer was occurring. This disturbed the whole system and meant that certain other alarms occurred routinely and had to be tolerated.

Also, lack of good communication between shifts was a problem at Longford. Problems were not passed up to the right person and critical information was unrecognized, ignored or buried until something occurred to resurrect it. This is a common problem in several other industries as well, such as the space travel industry. The failure to pass information up the line is exemplified in the Challenger disaster (1986, 7 people lost their lives). Information that earlier shuttle rockets had experienced technical problems was confined to one person at NASA and neutralized by a process of reinterpretation. Had the information passed upwards to the highest ranking, a different set of decisions would have been made<sup>[49]</sup>. At Longford there were two major reporting systems; the routine reporting system and incident or near miss reporting system.

The routine systems' reporting log was supposed to contain information about process upsets and significant alarms. In practice, very little of this information found its way into the log books. However, for all their defects, the logs did contain numerous entries- which should have alerted a careful reader. Unfortunately, management did not read these reports. Inadequate communications between the shifts resulted in the incoming shift not knowing about the alarms regarding the high level of condensate. The reporting system for non-routine incidents required all incidents, no matter how minor to be reported to a supervisor and recorded on a hard copy incident form. The definition of incidents was wide enough to encompass serious process upsets such as leaks and unexpectedly cold temperatures. But such matters almost never found their way into the reporting system and failed to trigger any investigations. Even process upsets, which was serious enough to lead to temporary shutdown of the plant, failed to enter the reporting system. Nor were any of the process upsets, which operators recorded in the control room logs, reported in this way. Management's view was that it was up to the operators to report matters if they thought they had an escalation potential.

Another major problem at Longford was corporate culture. The Royal Commission found that management at Esso had not demonstrated an uncompromising commitment to identify and control every hazard at Longford. The Longford accident was a deficiency in the safety culture of management. At Esso, the focus on lost time injuries and minor injuries lead the company to become complacent about their management of major hazards. Clearly, personnel safety and process safety is two very different things, and need to be handled accordingly. A good illustration of this is the airline industry. An airline would not make the mistake of measuring air safety by looking at the number of routine injuries occurring to staff. Moreover, the incident and near miss reporting systems operated in the industry are concerned with incidents which have the potential for multiple fatalities, no lost-time injuries.

Auditing at Longford also failed to uncover any significant problems and only provided good news. There had been plenty of auditing, but evidence was given at the Royal Commission that Esso's auditing process was not effective. An audit was held just six months prior to the explosion by a team from Esso's corporate owner Exxon. The audit had shown that the most elements of the safety management system were functioning at level three or better which basically said that everything was very good (level four was the highest assessment level). But as described earlier in this chapter, there were bad news in the company, which a good audit might have been expected to pick up. Accident investigators quickly highlighted that a HAZOP had not been carried out, the external audit failed to notice this. Also, it was no secret that operators had grown accustomed to managing the plant for long periods without responding to alarms triggered by abnormal situations. A thorough audit should have detected this. A thorough audit should also have picked up the fact that the near miss reporting system was not being used to report significant gas processing problems. The external assessment did not pick this up. Instead it concluded that *"there was a good understanding of and high discipline in safe work routines and procedures"*<sup>[47]</sup> and that *"near-miss reporting was actively encouraged by management and supported by Esso personnel"*<sup>[47]</sup>. The sum up from the audit stated that the company's safety management system was extensively utilized and well understood within Esso. The Commission found it otherwise and stated that the methodology employed by the assessment team was flawed.

Another issue at Longford was that the maintenance staff had been progressively reduced over the period from 1992 to 1998, as a cost-cutting measure. There was a backlog of work orders – items which had been reported and were waiting to be repaired. To deal with this Esso had introduced a system for deciding an order of priority. Matters in need for repair had to be assessed based on the urgency of the matters and a risk assessment number was assigned. Matters which workers assessed as safety-related were reviewed at a daily plant management meeting. The management could change the priority if they disagreed with the original assessment. The failure to effectively control the condensate level began the accident sequence at Longford. A valve known as TRC3B enabled some control to be exercised over the condensate level. Some weeks prior to the accident the valve was not functioning properly and operators had to manipulate a bypass valve manually to achieve an effect which would normally have been achieved automatically. A work order request was issued two weeks prior to the accident, but the valve was not regarded as a safety issue and was not prioritised. Still it was relevant to the accident. Since the valve was not working properly, operators had to make manual adjustments. As described earlier, a communication failure at the shift change before the accident resulted in the operator on the fatal shift not carrying out these adjustment in an appropriate way. This failure resulted in the spill-over of condensate into other parts of the

system which initiated the accident sequence. Had there been maintenance on the valve, the valve would have been operating automatically.

The emergency shutdown procedure did not effectively isolate gas plant 1 from gas plant 2 and 3. One of the obvious lessons from the Piper Alpha accident (1988, 167 men lost their lives) was the importance of being able to isolate a plant quickly and effectively.

When summarizing issues mentioned above, they can be categorised as followed:

Supervision and monitoring:

- culture of “causal compliance”, procedures were not followed – operating in alarm mode
- failed to respond to alarms
- insufficient auditing

Policies and procedures:

- procedures were repetitive, circular and contained unnecessary cross-referencing
- inadequate procedures and lack of procedures (operating procedures)
- deviation from procedures; it was easier at times to maintain the quality of the outgoing gas by allowing processing to occur outside the specific limits
- lack of management of change policy and procedures

Physical devices and instrumentation:

- ESD failed to isolate gas plant 1
- inadequately maintenance of equipment (indirect cause; valve)

Communication:

- insufficient communication between shifts
- problems were not passed up to the right person
- management failed to communicate the importance of process safety to the workforce

Training:

- lack of operator training for abnormal conditions
- lack of operator awareness of risk
- inadequate training

Several of the causes could be placed in more than one category, such as maintenance issues. However, it is chosen to categorise as above to easily compare and summarize the causes later in the report.

There were many lessons to learn from this accident and the most serious lessons were for management. As shown above there were several underlying causes regarding management and organisational elements leading to the Longford accident. When revealing these, it seems a little hasty to just make the Operators accountable for the accident.



## 4.2 Texas City 2005

Reference for the bulk of information in this is made to the book “Failure to learn” by Hopkins<sup>[50]</sup>. The book's basis is the investigation done by the US Chemical Safety and Hazard Investigation Board (CSB)<sup>[51]</sup>. Professor A. Hopkins is a world renowned safety culture expert and the book helps to give an understanding in why the explosion occurred based on insight in the safety culture at Texas City.

In 2005 there was an explosion at BP's Texas City Refinery, located on the outskirts of Houston. A total of 15 people died and nearly 200 were injured in the worst industrial disaster in the United States in more than a decade.

The accident sequence began when operators overfilled a 170-foot distillation column. As a result of this mistake, a mixture of liquid and gas flowed out of the gas line at the top of the column, travelled through emergency overflow piping and was discharged from a tall vent, which was located hundreds of feet away. No flare system resulted in that a vapor cloud accumulated and was ignited by a vehicle that had been left in the area. A number of mobile offices that had been located far too close to the plant were destroyed by the explosion, killing and injuring their occupants.

After this accident, the CSB for the first time conducted an examination of corporate safety culture. Therefore, this accident and the following investigation, is particularly of interest regarding this report and the chain of events leading to the accident will be described thoroughly.

The first step in the chain of events leading to the explosion at Texas City was a failure done by operators when the plant was being brought back into operation after a period of maintenance. Procedures specifying the required liquid level in the column had been totally ignored, the rate of heating was faster than specified in the startup procedures and pre-startup checks were not performed although employees had signed documents stating that they were. Also, the supervisor had absented himself for some hours during the startup. The question Andrew Hopkin asks is: *why did operators do as they did?*

Texas City had a culture of “casual compliance”. Management had developed a so-called “compliance delivery process” to confirm compliance. This involved processes of auditing and, if necessary, discipline. Unfortunately the site did not have the necessary supervisory resources to carry this through and there was no attempt by management to ensure compliance with startup procedures for the distillation column. In one way BP inadvertently encouraged an attitude of causal compliance. The startup procedures were not updated, even though the process had evolved. Various critical events were simply not covered by the procedures<sup>[50]</sup>. In short, the procedures were at times inappropriate and workers necessarily developed their own. When procedures are written with little consideration for those who must apply them, it is almost inevitable that they will be ignored or interpreted in ways that fail to take account of the hazards which they are intended to control. Despite inappropriate procedures, Texas City managers certified the procedures annually as up-to-date and complete. Prior to startup workers had also identified and reported various pieces of equipment on the column as malfunctioning<sup>[50]</sup>. Due to insufficient time available, these were not rectified prior to startup. Furthermore, the startup was to occur even though technicians had not the time to carry out checks on all of the instrumentation, as required by the procedures.

The preceding can explain why workers seemed relatively unconcerned about written procedures. But why did they depart from the procedures in the way that they did? Operators were aware of the negative consequences of underfilling the column, but they were quite unaware of the risk of overfilling the column. The operators had developed a practice that reflected their understanding of the risks involved. There are various ways BP could have discovered such significant and sustained non-compliance. Best practice is to define safe operating limits or critical operating parameters for all equipment. It also requires that equipment is installed to monitor compliance with these limits. Unfortunately BP's incident reporting system that would have highlighted these exceedences was not operational.

Next question is – how was it physically possible to make this mistake? Should there not be a cut-out device, preventing the operators from overfilling the column? The company view was that if operators followed procedures, there should not be a need for a backup safety mechanism. With this policy, BP was ignoring an abundance of evidence from other accident investigations that systematic deviation from stated procedures is the norm, rather than the expectation. Procedures are only effective if complied with. This requires supervisory resources. Had a cut-out device been in operation, the accident could not have happened.

Inadequate instrumentation contributed to the extent of the mistake – the operators were unaware of how full the distillation column was. Instruments on the column were designed to indicate where the liquid level was in the range from 4 to 9 feet. Once the level went above the upper level, there was no instrumentation to tell operators how full the column was. Also, a crucial instrument failure was the level measuring instrument showing that the level was slowly declining in the hours before the accident, from just under 9 feet to just under 8 feet. This very instrument was earlier reported as malfunctioning, but had not been fixed. There were two alarms designed to warn the operators and one of them was not working at the time. But since the operators were intending to fill the column above the level, whether or not it was functioning is beside the point. The liquid level in the column could be seen through glass. However, there was a build-up of residue on the glass and requests that the glass be cleaned during maintenance periods had gone unheeded.

Operation routines are important. Efficient and good communication among employees is crucial. Short and inadequate communication is one of the causes in this accident. At a management meeting held on the morning the startup was scheduled to take place, the decision was made not to proceed, precisely because the storage tanks that received the heavy liquid were full. Operators were not told of this decision and went ahead with the startup as originally planned. Further, the control room operator believed that he had been instructed to not open the heavy liquid outflow valve because the storage tanks where the liquid would be held were full. The startup also occurred over two shifts. At Texas City the operators' log book was brief and uninformative and there was no face-to-face communication between shifts. The incoming shift did not realise the extent to which the column and all of the associated pipework already "packed" with liquid, had he understood that the earlier operator had already completely filled the system to the required level in readiness for heating, he would probably have behaved differently and the accident would not have happened.

Another factor that contributed to this accident, was the lack of awareness by operators of the danger of overfilling the distillation column. This is in part due to the inadequacies in the training they had received. It did not provide in-depth understanding of the process, or what

might go wrong, or why certain alarms or procedures might be critical. Most importantly, there was no training on how to handle abnormal situations.

Questioning why the operators were not more alert to the warning signs, the answer could be that the problem-solving ability of the operators was degraded by fatigue. At the time of the accident, the day control room operator had been working 12-hour shifts, 7 days a week for 29 consecutive days. The control room operator reported that he routinely got only five or six hours of sleep per night. There is good experimental evidence that fatigue reduces performance, and good statistical evidence that fatigue causes accidents. For instance, there are data showing that accident rates increase markedly in the last 4 hours of a 12-hour shift [50].

There was also inadequate staffing of the control room. On several previous occasions internal analyses had drawn attention to the need for two operators when managing for instance a startup process and workers themselves had campaigned for improved staffing. There was a prolonged failure to upgrade the vent to a flare at Texas City. In the US the legislation is not explicitly based on any concept of risk reduction, it requires employers to provide a work place that is "free from recognized hazards that are causing or are likely to cause death or serious physical harm" [50]. There was no specific regulatory requirement that Texas City replace vents with flares, all that was required was that it manage the risk. Since process safety management was ultimately a matter of risk management rather than rule of compliance, Texas City was able to avoid the expense of implementing best practice.

Also, BP's budget priorities worked against risk reduction. Even though continuous risk reduction was a part of BP's stated philosophy, it had no place in BP's budget priorities, and risk-reduction proposals stood little chance of success in the cost cutting environment that BP had created at Texas City. This helps explain why BP failed to give priority to improving the instrumentation on the distillation column or even repairing defective instrumentation. All capital investment that affected the "license to operate" was regarded as essential, other spending was discretionary. It seems like repairing defective instrumentation was not prioritized because it didn't seem necessary to ensure the continuation of the license to operate, ensure reliability of production or to take advantage of new commercial opportunities. This insight in the safety culture is helpful when trying to understand why the operators did as they did. Their actions just reflected the overall management prioritizing of safety at the plant.

When the gas cloud ignited an explosion was inevitable. The source was a vehicle parked 25 feet away with its engine idling. BP's policy was that no vehicle could be left unattended with the motor operating. For maintenance shutdowns and capital projects a traffic control plan was required. Managers have freely admitted at interviews that there was no effective vehicle control policy at Texas City. This indicates a lack of awareness of the risks associated with refinery processing. Had no ignition source been present, the explosion would not have happened.

Another sign that indicates lack of awareness of the risk associated with refinery processing is the location of the trailers (mobile offices blocks). At the time of the accident there were 22 people gathered inside a trailer located 120 feet away from the vent. Two trailers located within 136 feet from the vent were demolished by the explosion. The trailers did not need to be located there, it was in principal for reasons of convenience [50]. Had they been located

further away, no one would have died. So why were they located there? Texas City had a management of change process, governing the location of trailers. If a trailer was to be located closer than 350 feet to a process unit, one had to proceed further in the workbook in order to perform risk calculations and evaluate the explosion risks. However, the people engaged in the risk assessment were not safety engineers and had no training in the use of the workbook<sup>[50]</sup>. They were unable to complete the required analysis and the management of change process was inadequate.

Summing up the factors that contributed to Texas City accident, they can be grouped into the following categories<sup>[50]</sup>:

Supervision and monitoring:

- Culture of “causal compliance” in which operators and supervisors treated procedures as guidelines that they were free to ignore rather than regulations
- BP did not audit operator compliance with start-up procedures
- BP failed to monitor and react to electronic data on previous start-ups.
- insufficient management of change

Policies and procedures:

- The procedures were incomplete and out of date
- Operators did reasonable belief that deviation from procedures was necessary to protect against level fluctuations
- Lack of fatigue management policy
- Lack of management of change policy/procedure

Physical devices and instrumentation:

- Lack of any physical cut-out device to prevent overfilling
- Instruments that only read liquid levels in the bottom of the column
- Inadequately maintained instruments
- Misleading instrument
- Lack of any display in the control room comparing inflow with outflow

Communication:

- Communication failure between shifts
- Management failed to communicate startup instructions
- Failed to communicate the importance of process safety to the workforce

Training:

- Lack of operator training for abnormal conditions
- Lack of operator awareness of risk (consequences of action, 350 feet rule, ignition control)

Most of the subjects mentioned above are management elements. The lack of preventing barriers such as instrumentation and cut of device was due to lack of focusing on maintenance and process safety from the management. The fact that the ignition source control at the site was insufficient (due to inadequate policy) reflects back on the prioritizing by the management.

### 4.3 Deep Water Horizon 2010

Reference to the information presented in this chapter is BPs' own investigation report <sup>[53]</sup> and the report made to the President <sup>[54]</sup>.

On April 20, 2010, an explosion and fire erupted on the drilling rig Deepwater Horizon in the Gulf of Mexico. Hydrocarbons escaped from the Macondo well onto Transocean's Deepwater Horizon, resulting in explosions and fire on the rig. Eleven people lost their lives, and seventeen others were injured. The fire, which was fed by hydrocarbons from the well, continued for 36 hours until the rig sank. The accident involved a well integrity failure, followed by a loss of hydrostatic control of the well. The causes of the accident were related to some key findings, each described thoroughly in this report. The rig was owned by Transocean and operated by BP.

The day before the accident cement had been pumped down to the wellbore annulus to prevent hydrocarbons from entering the wellbore from the reservoir. This annulus cement probably experienced nitrogen breakout and migration, allowing hydrocarbons to enter the wellbore annulus. BP's team had some concerns regarding Halliburton's cementing design, which led them to place a number of significant constraints. The first compromise in BP's plan was to limit the circulation of drilling mud through the wellbore before cementing. BP compromised again by deciding to pump cement down the well at the relatively low rate of 4 barrels or less per minute. Higher flow rates tend to increase the efficiency with which cement displaces mud from the annular space. But the increased pump pressure required to move the cement quickly would mean more pressure on the formation and an increased risk of lost returns. BP decided to reduce the risk of lost returns in exchange for a less-than-optimal rate of cement flow. BP made a third compromise by limiting the volume of cement that Halliburton would pump down the well. Pumping more cement is a standard industry practice to insure against uncertain cementing conditions. But more cement at Macondo would mean a higher cement column in the annulus, which in turn would exert more pressure on the fragile formation below. BP determined that the annular cement column should extend only 500 feet above the uppermost hydrocarbon-bearing zone (and 800 feet above the main hydrocarbon zones), and that this would be sufficient to fulfill regulations of "500 feet above the uppermost hydrocarbon-bearing zone." However, it did not satisfy BP's own internal guidelines, which specify that the top of the annular cement should be 1,000 feet above the uppermost hydrocarbon zone. As designed, BP would have Halliburton pump a total of approximately 60 barrels of cement down the well—a volume that its own engineers recognized would provide little margin for error. Finally, in close consultation with Halliburton, BP chose to use "nitrogen foam cement". This formula was chosen to lighten the resulting slurry and thereby reducing the pressure the cement would exert on the fragile formation. In theory, this would help to balance the pore pressure in the formation and clear the annular space of mud as the cement flowed upward. The investigation report concluded that there were weaknesses in cement design and testing, quality assurance and risk assessment.

It appears that Halliburton never reported the results of the February test to BP. Halliburton conducted another round of tests in mid-April, just before pumping the final cement job. By then, the BP team had given Halliburton more accurate information about the temperatures and pressures at the bottom of the Macondo well, and Halliburton had progressed further with its cementing plan. Using this information, the laboratory personnel conducted several tests,

including a foam stability test on April 13. The first test Halliburton conducted showed once again that the cement slurry would be unstable. The Commission does not believe that Halliburton ever reported this information to BP. Instead, it appears that Halliburton personnel subsequently ran a second foam stability test, this time doubling the pre-test `conditioning time` to three hours.

The shoe track barriers did not isolate the hydrocarbons. Both barriers in the shoe track must have failed to prevent hydrocarbon entry into the production casing. The first barrier was the cement in the shoe track, and the second was a device at the top of the shoe track designed to prevent fluid ingress into the casing. The investigation team identified potential failure modes that could explain how the shoe track cement and the float collar allowed hydrocarbon ingress into the production casing.

The negative-pressure test was accepted although well integrity had not been established. The test involved replacing heavy drilling mud with lighter seawater to place the well in a controlled underbalanced condition. In retrospect, pressure readings and volume bled at the time of the negative-pressure test were indications of flow-path communication with the reservoir, signifying that the integrity of these barriers had not been achieved. The Transocean rig crew and BP well site leaders reached the incorrect view that the test was successful and that well integrity had been established.

With the negative-pressure test having been accepted, the well was returned to an overbalanced condition, preventing further influx into the wellbore. Later, as a part of the normal operations, heavy drilling mud was again replaced with seawater, under balancing the well. This allowed hydrocarbons to flow up to the production casing and passed the blow down preventer (BOP). The rig crew did not recognize the influx and did not act to control the well until hydrocarbons had passed through the BOP and into the riser. The rig crew's first apparent well control actions occurred after hydrocarbons were rapidly flowing to the surface. Indications of influx with an increase in drill pipe pressure are discernable in real-time data from approximately 40 minutes before the rig crew to action to control the well.

The first well control actions were to close the BOP and diverter, routing the fluids exiting the riser to the mud gas separator. Nevertheless, the well control response actions failed to regain control of the well. Had the fluid been routed overboard instead, there may have been more time to respond, and the consequences of the accident may have been reduced. Once diverted to the mud gas separator, hydrocarbons were vented directly onto the rig, which increased the potential for the gas to reach an ignition source. Diversion to the mud gas separator resulted in gas venting onto the rig. The design of the mud gas separator allowed diversion of the riser contents to the mud gas separator vessel although the well was in a high flow condition.

The fire and gas system did not prevent hydrocarbon ignition. Hydrocarbon migrated beyond areas that were electrically classified to areas where the potential for ignition was higher. The heating, ventilation and air condition system probably transferred a gas-rich mixture into the engine rooms, causing at least one engine to overspeed, creating a potential source of ignition. The BOP emergency mode did not seal the well. Three methods for operating the BOP in the emergency mode were unsuccessful in sealing the well. Through a review of a rig audit findings and maintenance records, the investigation team found indications of potential weaknesses in the testing regime and maintenance management system for the BOP.

Most, if not all, of the failures at Macondo can be traced back to underlying failures of management and communication. Better management of decision making processes within BP and other companies, better communication within and between BP and its contractors, and effective training of key engineering and rig personnel would have prevented the Macondo incident.

Transocean failed to adequately communicate to its crew lessons learned from a similar near-miss on one of its rigs in the North Sea four months prior to the Macondo blowout. On December 23, 2009, gas entered the riser on that rig while the crew was displacing a well with seawater during a completion operation. As with Macondo, the rig's crew had already run a negative-pressure test on the lone physical barrier between the pay zone and the rig, and had declared the test a success. The tested barrier nevertheless failed during displacement, resulting in an influx of hydrocarbons. Mud spewed onto the rig floor—but fortunately the crew was able to shut in the well before a blowout occurred. The basic facts of both incidents are the same. Had the rig crew been adequately informed of the prior event and trained on its lessons, events at Macondo may have unfolded differently.

Decision-making processes at Macondo did not adequately ensure that personnel fully considered the risks created by time- and money-saving decisions. Many of the decisions that BP, Halliburton, and Transocean made that increased the risk of the Macondo blowout clearly saved significant time (and money). But in regard to BP's Macondo team, there appears to have been no formal system for ensuring that alternative procedures were in fact equally safe. None of BP's (or the other companies') decisions appear to have been subject to a comprehensive and systematic risk-analysis, peer-review, or management of change process.

A complex and interlinked series of mechanical failures, human judgments, engineering design, operational implementation and team interfaces came together and allowed the initiation and escalation of the accident. The causes can be categorized as followed:

Supervision and monitoring:

- Insufficient technical review of the cement slurry design
- Need for strengthening BP's rig audit process to improve the closure and verification of audit findings and actions across BP-owned and BP-contracted drillings rig

Policies and procedures:

- Insufficient guidelines for the negative-pressure test (a critical activity). No procedures containing detailed steps or minimum expectations for conducting a negative-pressure test
- Insufficient risk management and management of change
- Weaknesses in the testing regime and maintenance management system for BOP
- Cement slurry was not fully tested prior to execution
- Procedures stated that the well was to be monitored at all times, however the policy did not specify how to monitor the well during in-flow testing cleanup or other end-of-well activities
- Transocean's shut-in protocols did not fully address how to respond in high flow emergency situations after well controls have been lost.

Physical devices and instrumentation:

- The float collar failed to prevent hydrocarbons ingress
- The design of the mud gas separator allowed the riser fluids to be diverted to the mud gas separator vessel when the well was in high flow condition.
- Fire and gas system did not prevent ignition
- The BOP emergency mode did not seal the well

Communication:

- Interactions between BP and Halliburton in the planning, design, execution and conformation of the cement job
- The rig crew and well site leaders believed that the negative-pressure test was successful
- Transocean failed to communicate lesson learned from previously event in 2009

Training:

- Lack of awareness of risk (shortcomings in the planning/design and execution of the cement job, formal risk assessment of the annulus cement barriers were not conducted, personnel safety versus process safety)
- The rig crew and mudloggers did not observe or did not recognize indications of flow (from 20:58 until 21:38 – simultaneous operations occurred that may have affected the effectiveness)
- Rig crew was not sufficiently prepared to manage an escalating well control situation
- Lack of competency of personnel in key operational and leaderships positions

The well blew out because a number of separate risk factors, oversights and outright mistakes combined to overwhelmed the barriers meant to prevent such an event from happening. Most of the mistakes and oversights can be traced back to a single overarching failure - a failure of management. Better management by BP, Halliburton and Transocean would almost certainly have prevented the blowout by improving the ability of individuals involved to identify the risks they faced, and to properly evaluate, communicate and address them.

A question that has been asked following the Deep Waterhoriozon accident is; could it occur in the North Sea? This will not be discussed in this report, but it seems very relevant to present an event that occurred at a platform operated by Statoil in the North Sea, described in the next chapter. Perhaps the description of the event will help to answer the question.

## **4.4 Gullfaks 2010**

Reference regarding information in this chapter, is Statoils internal investigation report <sup>[55]</sup> and a letter from the Petroleum Safety Authority submitted to Statoil regarding the investigation report <sup>[56]</sup>.

On May 19 2010 Norway could have experienced a major accident at Gullfaks C. The Petroleum Safety Authority claim <sup>[57]</sup> that under slightly altered circumstances, a well control incident on the Statoil-operated Gullfaks C platform in the North Sea could have developed into a major accident.



During the final circulation and hole cleaning of the reservoir (well 34/10-C-06 AT5) a hole occurred in the 13 3/8" casing, with subsequent loss of drilling fluid (mud) to the formation. The hole in the casing implied loss of both well barriers. Loss of back pressure led to influx from the exposed reservoirs into the well, until solids or cuttings packed off the well by the 9 5/8" liner shoe. The pack-off limited further influx of hydrocarbons into the well. The crew on the platform and the onshore organisation struggled to understand and handle the complex situation during the first twenty-four hours. Well control operation continued for almost two months before the well barriers were reinstated.

The consequences of the event were implied gas release on the platform, compromised barriers and loss of reputation. The production on the platform was shut down for almost two months. So, what caused this event? Statoil's own investigation report has concluded that the casing had insufficient technical integrity and that there was a lack of monitoring and follow-up of the pressure in the C-annulus, causing the pressure to increase over weeks resulting in the leak. A cause contributing to the difficulties related to handling of the subsequent well control situation was that the managed pressure drilling operation was commenced and carried out with insufficient margin between the pore and fracture pressure.

An underlying cause is considered to be the risk assessment related to application of the 13 3/8" casing as a common well barrier element. The insufficient risk assessment was considered as the cause of using a casing with insufficient technical integrity and lack of follow-up and monitoring of pressure in the annulus outside the casing. The investigation team states that; the risk assessment performed in the planning phase was insufficient, the risk evaluation during execution of the managed pressure drilling operation was insufficient and the transfer of experience related to pressure control from the managed pressure drilling operation in well C-01 in 2009 was insufficient. Other causes are related to insufficient planning of the operation, knowledge to and compliance with requirements, management pressure drilling knowledge and involvement of the Company's technical expertise.

The Petroleum Safety Authority Norway (PSA) has closely followed up the loss of well control on Gullfaks C <sup>[59]</sup>, and pursued various activities aimed at clarifying the causes of the incident. The work has focused on how Statoil handled the event, on its planning and execution of the well and Statoil's efforts to re-establish safety barriers and secure the well, as well as its internal investigation of the incident.

The PSA regards the incident as very serious; it involved the lengthy loss of a barrier. Only chance averted a sub-surface blowout and/or explosion, and prevented the incident from developing into a major accident. This resulted in an audit carried out 8-15 October 2010. The PSA's finding is that the planning for the drilling and completion operation on well C-06A featured serious and general deficiencies. These concerned such key factors as risk management and change control, experience transfer and use of expertise, knowledge of and compliance with governing documents, and documentation of decisions. Viewed overall, the PSA has concluded that serious deficiencies have been identified in Statoil's planning and in management checks that the work was being done in an acceptable manner. The audit resulted in a notification with orders.

The PSA has assessed Statoil's own investigation of the incident, and has conveyed its comments, which among others were <sup>[56]</sup>:

- that underlying causes related to control, management and other organisational factors were not discussed, so that factors which could have been relevant, such as lack of resources, pressure of time, changes/reorganisations, major replacements of personnel and inadequate training, are not identified
- it is not considered in detail why risk assessments were not made and why no central specialist expertise was used. Further, why were not work processes familiar to personnel responsible for the activity and why did not internal control system, including responsible management, pick up the undesirable conditions
- PSA assessment is that measures directed at organisational factors which lie further back in the causal chain have not been adequately identified
- the estimated leak rates are based on important assumptions which have not been verified (uncertainty concerning ventilation conditions, for example), and are very uncertain. Nor is the ignition probability or consequences of a possible fire/explosion in the well area analysed or discussed
- the investigation team notes that risk assessments were deficient, but does not clarify whether this reflected inadequacies in methods used, content, execution, participation or other conditions. Nor are specific recommendations made for measures related to this
- similarities with the causes of events on other installations, such as the gas blowout on Snorre A, are not discussed
- Statoil's investigation report concludes that the possibility of sub-surface blowout was very low. PSA cannot see this conclusion is adequately supported

These are all very important comments. How can an organization learn from an undesirable event if they do not find the actual root cause in the organisation?

In an interview the PSA <sup>[58]</sup> criticises Statoil's own investigation, due to the insufficient mapping of underlying causes, which may contribute to the lack of important learning and improvement measurements.

On December 4 2010, there were a hydrocarbon leak on Gullfaks B<sup>[59]</sup>. The incident occurred during leak testing in connection with maintenance work with a choke valve on one of the wells, and the leak had a high initial rate of 1.3 kilograms per second and lasted for an hour. The PSA decided to investigate this event themselves and identified non-conformities were related to <sup>[60]</sup>:

- planning of the work – the isolating plan had deficiencies
- testing of barrier valve identified in the isolating plan
- planning, clearing and carrying through the reset including the leak testing
- identifying risk related to pressure build up between subsurface safety valve and hydraulic main valve
- maintenance of manual main valve
- emergency shutdown system – can unintentionally be set out of function
- securing adequate capacity and competence when planning and carrying through the reset work – lack of role clarification
- strategy for barriers and establishing performance requirements for barrier elements

- update of risk analysis – no documentation stating that the risk associated with explosions had been reduced as low as possible

Several things seem to repeat itself within the company; lack of risk understanding, insufficient planning and testing, insufficient barriers and lack of training/competence. If some circumstances were altered, a major accident could occurred in the North Sea in the year 2010.

#### 4.5 Similarities – failure to learn

More major accidents are presented in appendix C: Humber oil refinery in 2001, Toulouse in 2001 and Buncefield in 2005.

Going through the accidents described in previous chapters and in appendix C, it is quite striking how many similarities there actually are between these accidents, regardless of company or country involved. Summing up the main triggering categories and underlying, they can be placed as followed in the bow tie model:

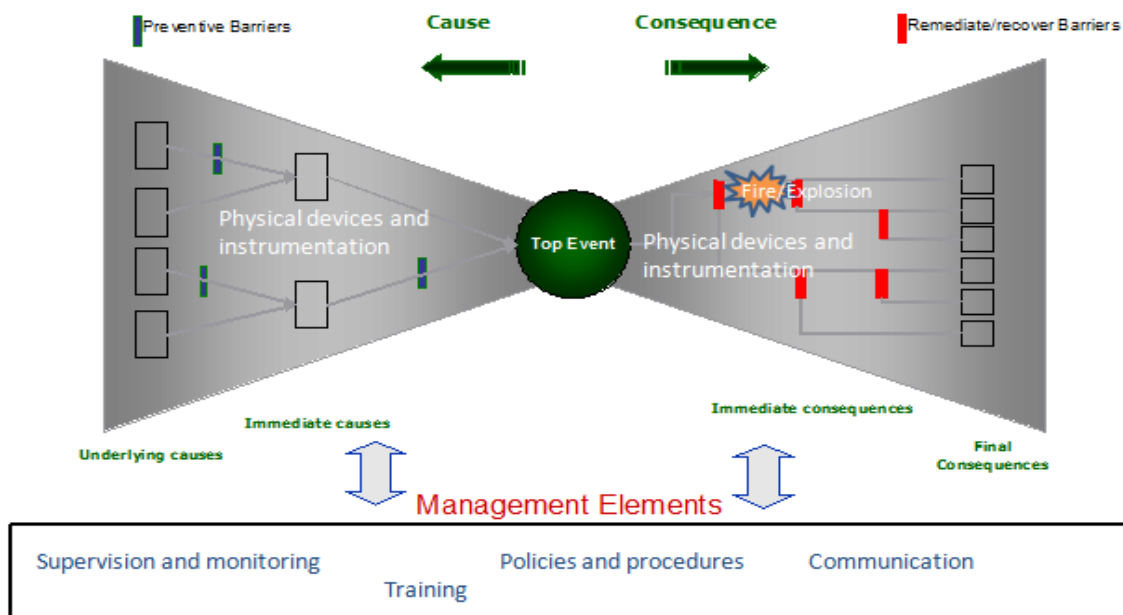


Figure 15: Overview bow tie model

As illustrated in figure 15 most of the underlying causes in the accidents described are management elements. The picture in figure 15 gives a simplified picture of a complex chain of events leading to an accident. But the essence is that most of the causes can be traced back to the management of the company.

The triggering cause is most likely to be an Operator error, often connected to a physical/instrumentation failure. As seen in the accidents described earlier in this report the technical causes vary from one accident to another, but the organisational failures seem remarkably similar, such as insufficient maintenance, lack of risk understanding, insufficient training and a lack of safety culture. Some of the investigation reports devote little attention to the organisational causes and the management systems. By looking at the triggering causes

and the initiatives from the investigation, it is clear that there are conditions that are censurable regarding the organisation. For example, Buncefield accident: safety critical valve fails and goes unnoticed by the monitoring system, Toulouse accident; large amount of ammonium nitrate stored without proper knowledge regarding the consequence. These examples indicate insufficient maintenance management and a lack of risk understanding in the organisation. Insufficient maintenance and risk understanding, followed by insufficient monitoring and lack of procedures seem to repeat itself in all organisations represented in this report.

In principle one could say that by getting the organisational factors right the technical causes of the accident will not come into play. For instance, if the instruments that read the liquid level at Texas City were maintained correctly and showed correct liquid level, the accident could have been avoided. Also, if the organisation had an understanding of the risk involved by overfilling the column, they might have installed a cut-out device to prevent overfilling.

In the oil and gas industry risk-based decision-making is commonly used, and in the industry there will always be a level of risk, that is inevitable. The question is how much risk is acceptable? Another approach to risk is a consequence-based, which takes no account of the likelihood. The philosophy is that if the consequences are severe, people must be protected of them no matter how unlikely they may be. This principle cannot be universally applied and it is not possible to protect people from all risk. But, as illustrated in the Texas City accident, the risk to trailer occupants could have been eliminated. It was not an issue of cost, it was a question of convenience. Had the management understood the risk involved, the trailers would most likely be placed somewhere else.

Most of the accidents described in this report had an ignition source which caused a fire/explosion. One could say that if the ignition source had not been present, none of the accidents would have occurred. But there are many potential ignition sources at a petrochemical plant and efforts must be focused on ensuring that flammable materials do not escape. In contrast, flammable gas is an ever-present problem and ignition control is therefore a vital safeguard against explosion. Barriers connected to ignition source control and loss of containment (inspections) must be focused on.

One of the central conclusions of most disaster inquiries was that the auditing of safety management system was defective. Theoretically, the aim of safety auditing is not to identify uncontrolled or inadequately controlled hazards – it is to identify strengths and weaknesses in safety management systems. One finding, which emerged from every disaster inquiry, was that the company auditing provided only good news and failed to identify problems, which became very obvious after the event. Also, an effective management of change system, which consider both plant and process modifications, is essential to prevent major accidents. Especially care is needed to ensure that “quick fix” modifications, during the commissioning and early operation phases of new plan, are covered. Again, just as quality in audit process, this is an organisational issue.

Communication and training are also frequently repeated as an underlying cause. Effective communication is an important element of any safety management system. Another organisational issue which is hard to measure, safety culture, is also implicated in every disaster. Why is it that the organisational elements seem to repeat itself? Organisations change

and people move on, taking their knowledge with them. Aiming for the optimal organisation bring along several organisational changes that could result in draught of people in key roles.

The industry is aiming for being capable of measuring management issues. When summing all up it seems very natural that this is the way to go, but as of today, this is not especially implemented in the industry. It has failed to implement "lesson learned" regarding management elements.

All accidents presented in the previous chapters are well known. One might say that by choosing other accidents the conclusion could be altered. It is not a given that these similarities are present in Gassco's organisation. It is therefore chosen to evaluate the underlying causes of two randomly selected undesirable HSE events classified with a high degree of seriousness in Gassco's portfolio in the period 2009 – 2010.

In 2009 Gassco experienced a gas leak with a major accident potential at one of the land based facilities. The leak rate was 22 kg/sec and total amount of gas leaked were estimated to 1200 kg. There were no injuries, but the leak resulted in 2.5 days with production stop. The triggering cause was insufficient stud pulling. The investigation report revealed that the underlying causes were<sup>[61]</sup>:

- insufficient management of change
- procedures were not followed, insufficient implementation of work process requirements
- lack of competence and training among installer (probably)

All the underlying causes mentioned above have been repeated several times in this report already. In 2010 Gassco experienced another incident at a land based facility that demonstrates insufficient safety culture. A contractor drives with high speed into a curve and the car tips over (the road was slippery). Fortunately there were no injuries/damages to personnel or equipment. The investigation report revealed that the underlying causes were<sup>[62]</sup>:

- lack of risk understanding
- insufficient HSE culture and lack of HSE competence
- procedures and regulations were not followed

The underlying causes in the events described above are the same as mentioned for all other accidents in this report, and they can be categorised as management elements in figure 15. Several other events within Gassco's portfolio could have been presented, but by presenting these two the point seems to be underlined: the similarities between the accidents are also reflected in Gassco's organisation.

What is the industry doing wrong, since the accidents seem to repeat themselves? How should one learn? Another industry that has to perform flawlessly under each operation is the U.S. Navy aircraft. This is a large and formal organisation that perform complex, inherently hazardous, and highly technical tasks under conditions of tight coupling and severe time pressure. If they fail, there will be human and social costs of great severity. And it is all done by people who are on average 20 years old, and average experience is 2- 3 years<sup>[63]</sup>. So, how do they do it? And why can the oil and gas industry not do the same? The key to the Navy's success is that there is no hierarchy during operations. Everyone has a duty to interrupt if they have a concern. Training is constant and relentless. There is a healthy challenge to constantly

improve, resulting in an active learning society. Communication throughout the team is far in excess of the norm. Turnover of people helps operations becoming stale<sup>[63]</sup>.

The U.S navy is a high reliability organisation (HRO). To become a high reliability organisation there are five key concepts, which are essential for any improvement initiative to succeed<sup>[64]</sup>:

- Sensitivity to operations: Preserving constant awareness by leaders and staff of the state of the systems and processes. This awareness is key to no risks and to prevent them.
- Reluctance to simplify: Simple processes are good, but simplistic explanations for why things work or fail are risky. Avoiding overly simple explanations of failure (unqualified staff, inadequate training, communication failure, etc.) is essential in order to understand the true reasons for risk.
- Preoccupation with failure: When near-misses occur, these are viewed as evidence of systems that should be improved to reduce potential harm. Rather than viewing near-misses as proof that the system has effective safeguards, they are viewed as symptomatic of areas in need of more attention.
- Deference to expertise: If leaders and supervisors are not willing to listen and respond to the insights of staff who know how processes really work and the risks one really face, you will not have a culture in which high reliability is possible.
- Resilience: Leaders and staff need to be trained and prepared to know how to respond when system failures do occur.

High reliability organisations will be further discussed in chapter 6.

#### **4.6 How to implement “lesson learned” in Gassco's barrier KPI model**

As shown in figure 15 and described in the preceding chapters there are a lot of similarities in the causes leading to the major accidents. The majority is categorised as management elements.

Gassco's barrier model has several indicators on reactive and proactive barriers such as technical equipment, these will not be discussed further in this chapter. The reason for this is the fact that the area of physical and instrumental causes for an accident seems to be covered in a good way by monitoring defined safety critical equipment in the model. The elements that need to be further assessed in the model are proactive elements other than technical and management indicators. For a complete list of indicators see appendix B. Proactive and management elements indicators used in the model are<sup>[8]</sup>:

- Inspection finding (measurement: number of findings)
- PSV (pressure shutdown valve, measurement: # of failures/ # of test)
- Preventive backlog on safety critical equipment (measurement: # of works orders in backlog)
- Corrective backlog on safety critical equipment (measurement: # of works orders in backlog)
- Critical audit findings ( measurement: # of critical open findings)
- Overdue actions on critical audit findings (measurement: # of overdue actions)
- Override indicator (measurement: # of critical safety barriers overridden a specific time)

- Open corrective work order related to safety critical failure modes (measurement: # of open orders)

The indicators mentioned above show that Gassco understands the importance of management elements in preventing a major accident. Inspection findings, critical audit findings, PM and CM backlog (maintenance) and overrides are all getting focus from the management in Gassco. But the quality of the inspections and audits are not reflected in the barrier KPI model. There are no indicators regarding competence and training, design and layout, safety culture, incidents and management of change. Incidents at Gassco are handled by other KPI's (each incident handled separately) and design and layout are handled by other means such as QRA on design, procedures and audits. However, competence and training, safety culture and management of change are left out due to the fact that it is hard to establish suitable measuring parameters. The importance of policies and procedures are not reflected in the model. Is it possible to implement indicators that give an overview and management focus on these barriers?

Human factors are important in the barrier thinking and the Health and Safety Executive (HSE) states that <sup>[65]</sup>:

*“Human factors is a professional discipline concerned with improving the integration of human issues into the analysis, design, development, implementation, and the operational use of work systems.”*

A research report from the HSE regarding human factors <sup>[65]</sup> states that for systems to operate safely and effectively, they must be designed to support the people who operate them. It is increasingly recognised that human factors issues must be considered as a central part of development thinking. Experience shows that it is ineffective to address them as an afterthought. The risks associated with poor human factors can best be avoided by starting human factors activities as early as possible in the design process and continuing them throughout. The report indicates the scope of human factors and addresses both the technical and human parts of the system. Good management is needed to address human factors comprehensively. Human factors is a barrier that should be monitored and focused on by the management at all times.

Another research report from the HSE regarding humans factors performance indicators for the energy and related process industries <sup>[6]</sup> present the human factors key topics and gives suggestion on how to select an appropriate set of indicators. The human factors key topics are summarised to be:

- Managing human failures
- Procedures
- Training and competence
- Staffing
- Organisational change
- Safety critical communications
- Human factors in design
- Fatigue and shift work
- Organisational culture
- Maintenance, inspection and testing

Suggested indicators for these topics are presented in appendix D.

Gassco has already implemented some of the indicators suggested in appendix D regarding maintenance, inspections and testing, and also some of the indicators suggested for staffing. When the aim is to learn from previous major accidents, the model could be used to include indicators that reflect the status of human factors regarding training, competence, organisational change and culture, communication and procedures. One way of doing this is sketched in the following section.

Gassco's management is located in the head offices at Bygnes. As of today there is no indicator in the model presenting Gassco's main office, due to no technical barriers etc. operated at this location. Learning from previous major accidents shows that management system and management focus are crucial when managing the major accident potential. The work by the management is crucial prevent a major accident. This is evident by going through the major accident history. To highlight this, Gassco should consider to implement an indicator prevailing for management elements at the offices at Bygnes. This indicator could reflect the status of some of the management elements prevailing at Bygnes. If the selection and implementation of management indicators are useful and successful, Gassco should insist implementation of several management indicators at installations within their area of responsibility.

The management indicator aim must be to represent many of the already ongoing initiatives at Bygnes in the work done to prevent a major accident, for example information gained from the new Management of Change and audit tool Smart (implemented 2010), audits, Gassled top 10 action plan etc. Gathering all systems and presenting them as a barrier to prevent a major accident will enhance the message, and contribute in building a good safety culture. The indicator will be visible to all employees in Gassco. The barrier model itself is an important contribution to the safety culture, and is guiding the management in keeping the right focus.

The indicator should be presented at the barrier chart as several management indicators aggregated into one overall status at Gassco Bygnes, as illustrated in figure 16:

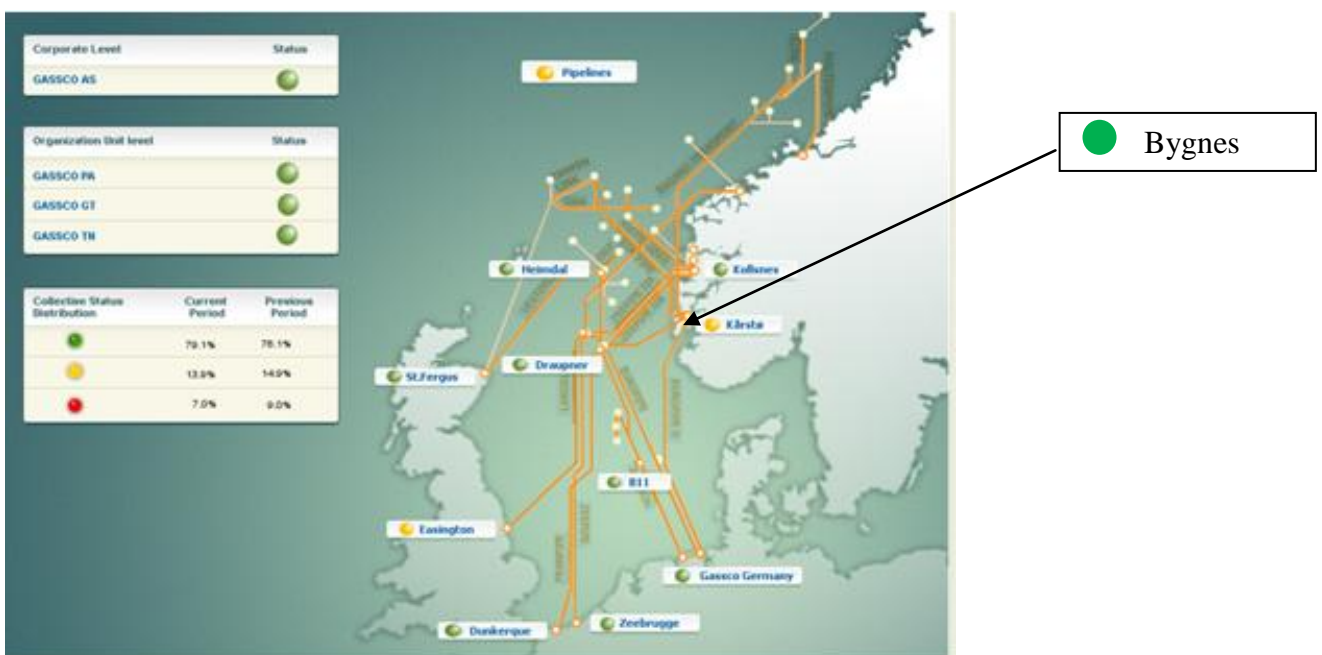
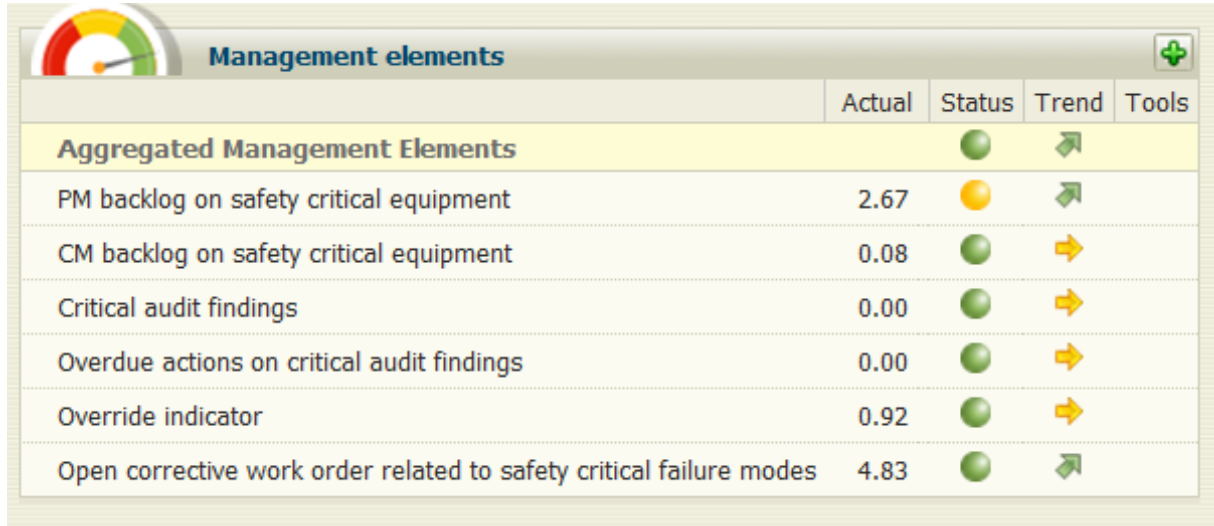


Figure 16: Illustration Barrier KPI chart



When “clicking” on the Bygnes indicator a list with status on all the selected management element indicators could occur as exemplified in figure 17. The management elements displayed in figure 17 are the ones that are already implemented in the model. The list connected to the indicator at Bygnes should contain a different selection of indicators, as discussed in the next section.



	Actual	Status	Trend	Tools
<b>Aggregated Management Elements</b>		●	↗	
PM backlog on safety critical equipment	2.67	●	↗	
CM backlog on safety critical equipment	0.08	●	→	
Critical audit findings	0.00	●	→	
Overdue actions on critical audit findings	0.00	●	→	
Override indicator	0.92	●	→	
Open corrective work order related to safety critical failure modes	4.83	●	↗	

Figure 17: Example management element list

Some indicators chosen from the research report from HSE 60<sup>[6]</sup> (listed in appendix D), assessed as underlying indicators in the management element indicator representing Gassco Bygnes, are presented in the subsequent sections. The main reason for choosing these is the gap between lesson learned from previous major accidents. Other indicators than the one represented in this chapter could also be of interest, but the one chosen for discussion are the ones most suitable for Gassco's organisation at Bygnes.

Human failures are very often the triggering causes of a major accident (ref. chapter 4). Before it is possible to implement a leading indicator on human failures, a system for registering risk assessment/HAZOPs including human failure must be developed in Gassco. Human failures are limited to only discussing the probability of Operator failure in risk assessments. In HAZOP's it is very rare to include assessments of human factors. This area must be further developed before implementing an indicator saying something regarding risk assessment/HAZOP's. Since the office at Bygnes does not perform work at the different plants directly and on a daily basis, one indicator that could be implemented and which do not require a lot of work to carry out, is to measure “*Number or percentage of plants/sites in the organisation that have designated champion to help manage human performance risk*”. When it comes to managing human errors, the number of installations that have a designated champion is not seen as the ultimate way of handling this subject. The reason for this is that the installations can then choose whether or not to have a dedicated responsible person. It is also easy to report a name, without having a decent work program. Gassco's management should decide whether or not it should be a requirement to have one champion to help manage human risk at each plant, which specialises in managing human error. If it becomes a requirement, and a part of someone's work instruction, there is no need for an indicator. Alternatively, one person in the Gassco organisation could be responsible for this subject. So when it comes to managing human errors, the recommendation is that there should be a requirement in the organisation demanding that a ‘human factors manager’ in an operation/project should be appointed rather than just implementing an indicator. This is seen

in connection with the discussion in chapter 6 regarding communication and safety culture. A requirement of a dedicated person to work with these issues seems to be far more sufficient than an indicator.

Also, inadequate procedures are often one of the root causes to a major accident (ref. chapter 4). The leading indicator most fitted for the organisation at Bygnes regarding procedures is *“Number or percentage of procedures documented /up-to-date/within scheduled review date, or compared with total number of procedures”*, *“Number or percentage of procedures meeting quality criteria/number of errors found in procedures (based on procedural ‘walkthroughs’ undertaken by managers and operators to confirm appropriateness)”* or *“Number or percentage of safety critical tasks for which appropriate (scope, critical tasks, emergency actions) procedures are in place”*. As a minimum, there should be an overview of number/percentage of procedures documented up-to-date within schedule. But this indicator does not say anything about the quality of the update and the procedure. There should be a quality criteria, such as number of errors found based on procedural ‘walkthroughs’. Doing this for all procedures requires a lot of work, and all procedures are not as important. A suggestion could be to have an indicator that measures the number/percentage of safety critical tasks for which appropriate (scope, critical tasks, emergency actions) procedures are in place. It is a requirement for Gassco that procedures are updated every third year and it is expected that a proper job is done. Every procedure has an owner. So if it is not updated according to the requirements, there is an employee that has not done the required job. Arguments for not implementing an indicator regarding procedures is that this job is a part of someone's job description and should be an issue between the leader and the employee. An indicator on this subject could easily just become a number which does not provide meaningful information for decisions on a high level.

Training and competence also seem to be a repeated underlying cause of major accidents (ref. chapter 4). There are several indicators that could be relevant to implement as an underlying indicator for Gassco Bygnes. An indicator measuring *“Number or percentage of employees trained per period as compared with schedule”* could be seen together with the new e-learning system implemented and emergency preparedness exercises, and will in some degree reflect the organisations focus on training and learning. Gassco Bygnes has already developed an e-learning system and performs emergency preparedness exercises regularly. The emergency exercises and the new e-learning system are required. So an indicator saying something regarding this will probably nearly always be green. It could be evaluated whether or not the indicator *“Frequency with which supervisors actively check staff competence (based on audit interviews with supervisors)” based on spot check audits”* is suitable. The indicator will increase management focus on competence and will help unveil and keep an overview of lack of qualifications among personnel – with the aim to improve their qualifications. Gassco Bygnes is not directly involved in the daily work at the installations. Because it is more or less the same personnel year after year at Gassco Bygnes and each position has requirements that need to be fulfilled in order to get hired, an indicator checking the staff competence does not seem to be adequate for the organisation. When it comes to training, Operators in Gassco's portfolio should be trained in handling abnormal situations by using a simulator. An indicator saying something regarding the performance in the simulator training could give useful information. But as of today it is not common to perform regular simulator training.

Maintenance backlog on safety critical equipment is already included in the” Barrier KPI model at installation level. For the management at the top level it could be of interest to have

an overall critical maintenance backlog for Gassco`s portfolio. After all, they are responsible for getting the job done, and it is important for everyone in the management to know the extent of the critical maintenance backlog. For the organisation at Bygnes, an appropriate indicator could be *CM backlog on safety critical equipment aggregated*. The major accident history shows that the quality of supervision is very important (ref. chapter 4). *“Number or percentage of audits that are undertaken for contractor activities, versus targets”* is an indicator that could be seen in connection with the indicator *“critical audit findings”* and *“overdue actions on critical audit findings”* already implemented at installation specific level. But these numbers does not say anything about the quality of the audit performed. No critical findings do not mean that they do not exist – it might just be that they have not been discovered. Further numbers of audits undertaken are included in the organisations work program, and will be displayed if all initiatives done to prevent a major accident becomes an indicator. This is already a part of the Gassled top 10 action plan. These initiatives should be visible in the barrier KPI model.

Insufficient Management of Change is repeated very often as an underlying cause in the major accident history (ref. chapter 4). Gassco has developed a new system (in 2010) called SMART to register audits and management of change processes. This should simplify the implementation of an indicator regarding organisational change. An indicator on organisational change, which measures *“number/percentage of MoC requests closed out or signed off versus number remaining alive for a given period”*, should due to the new system, be easily implemented without requiring a lot of work. But this is just a number saying something about the changes that are under control, and has management focus as a result of the new SMART system. But the management should be aware of and keep a close attention to, which is not highlighted in the SMART system, the number of exceptions/aberrations from the regulations regarding safety equipment within Gassco`s portfolio. How many high classified (for example rated red according to the TTS scale) exemptions are present in a given time period?

Regarding human factors in design and fatigue in shift work, *“Number/percentage of alarms that the operators fail to acknowledge per shift”* could be a human factor indicator at the control room at Bygnes. This is probably a very difficult indicator to measure. How should one register them and how should one set limits? It is also important to not mix what is important regarding a major accident potential and regular operation. An indicator showing the *“average number of hours worked for the shift personnel”* at Bygnes could be implemented. A trend towards more overtime might suggest increased potential for reduced alertness. In several major accidents the personnel involved have been working over a long period of time (ref. chapter 4). On the other hand, Gassco`s TCC is 3<sup>rd</sup> line in the emergency preparedness organisation and such an indicator would probably be of more interest on installation level.

Organisational safety is a very important factor. In several major accidents there has been a poorly safety culture (ref. chapter 4). Gassco`s management is not present at the plants on a daily basis, therefore it is very important to have a good safety culture in the company. There are 3 indicators that should be fairly easy to implement at Gassco Bygnes:

- *“Measure of visibility of senior executives in the workplace (number of site visits, etc.)”*,
- *“Number or percentage of reported events that are process safety related versus behavioural safety related”*

- *“Results from HSE safety climate surveys (or other safety culture/climate surveys or external audits), undertaken every 12 or 18 months, involving questionnaires, team interviews and individual interviews. Provide a snapshot of the organisation`s culture (compare results against industry benchmark/changes over time”.*

Out of these three indicators, it is probably the results from a HSE safety climate survey that would give the most valuable information. The other two could easily just become one number, expressing what has been done but not anything about what should be done. The PSA regular conducts a survey to map the risk level in the petroleum activity (RNNP) <sup>[66]</sup>. Gassco could benefit from this survey and use some of the answers in an indicator on safety culture at each installation. For the terminals abroad, a similar survey could be developed. A survey made especially for Gassco`s organisation could also be made from scratch (probably the best solution). Either way, a HSE safety climate survey should once a year be performed to provide a snapshot of the organisation`s HSE culture.

Number/percentage of reported events that are process safety related could easily be implemented and helps to sort out and focus on incidents with a major accident potential. An indicator stating how many events/accidents that are repeated could help measure whether or not the organisation is learning. This is a lagging indicator, but it is useful in determining whether or not lessons are learned. An option could be to have an indicator measuring percentage/number of implemented initiatives following lessons learned from other major accidents in the industry.

It is important to keep in mind that the first step in the process to get good non technical measurements, is to find some useful indicators that are meaningful for the management and that are efficient. Implementing too many indicators at once could work the opposite way and give little motivation for doing so, especially if the indicators are not very good. Several of the indicators mentioned in the sections above give us some numbers. But what purpose do the numbers have other than getting the management focus? For example: implementing an indicator that shows number of employees that have conducted the new e-learning system will probably always be green, due to the fact that it is a requirement to undergo the courses. Will such an indicator be efficient? Probably not. It is also a requirement that all procedures shall be kept up to date. It is probably more efficient to perform good quality audits to state that requirements are fulfilled, rather than having indicators on the subject. The discussion of why several indicators are left out deliberately will continue in chapter 6.

Underlying indicators to the management element indicator, placing the Bygnes offices at the barrier KPI chart, are suggested in table 1. These indicators are the ones left after evaluating the efficiency and meaning of each indicator. It is also taken into consideration that there should not be too many new indicators introduced in the beginning. The model needs to build trust among the employees and gain a good reputation. If it does not do so, the effect of it could be ruined.

**Table 1: Suggested indicators**

<b>Suggested indicators:</b>	<b>Advantage:</b>	<b>Disadvantage:</b>	<b>Unit:</b>
Ongoing initiatives to reduce the major	Already present in the top 10 action plan: managing major	The limits can be experienced somewhat	% fulfilled

Suggested indicators:	Advantage:	Disadvantage:	Unit:
accident potential	<p>accident hazard potential.</p> <p>Highlights the work done at Bygnes when trying to prevent a major accident. Makes it easy to present to others what the management focuses on.</p> <p>Audits/verifications are included in this indicator.</p> <p>Motivates the employees to get the work done, especially when the work is set in perspective and linked up against a major accident.</p>	<p>unfair since people work in different ways. But they should be decided in the same way as the top 10 action plan and HSE&amp;Q program.</p>	<p>up against the target.</p>
CM backlog on safety critical equipment aggregated	<p>Tells something about Gassco`s capability of handling the maintenance work.</p> <p>Insufficient maintenance management is one underlying cause of several major accidents, ref. chapter 4. Gassco need to show that they take this very serious, and that focuse is kept on this subject at all times.</p> <p>Maintenance is often affected when trying to save costs. Having focus on it will make the consequences more visible. Gives the opportunity to follow the trend development.</p> <p>On installation level it is only possible to see the development at one installation at a time. Aggregating it shows Gassco`s backlog portoflio and the development of it.</p> <p>Information already available in PMG – one only needs to aggregate values from the installations.</p>	<p>Could be hard to establish suitable limits, but it is important that the management decides what it is acceptable backlog on safety critical equipment.</p>	<p>Number of orders</p>

Suggested indicators:	Advantage:	Disadvantage:	Unit:
HSE safety climate surveys.	<p>Provides a snapshot of the organisations safety culture – at all levels and at all installations.</p> <p>Makes it possible to monitor the trend in safety culture development.</p> <p>Experiences from RNNP could be used in the development.</p> <p>The survey should be modelled in a way that employees with safety critical tasks are supplemented with more work related questions.</p> <p>Already present in Statoil (GPS).</p> <p>Several surveys already developed and on the marked.</p>	<p>Manual reporting</p> <p>Surveys must be developed.</p>	<p>Depends on how the survey is developed</p>
Exception on safety critical equipment	<p>It is the management responsibility to know what is not in accordance with prevailing regulations and the reasons why.</p> <p>Insufficient management of change is one underlying cause of several major accidents, ref. chapter 4. The new system SMART makes it possible to register and get information regarding this subject.</p> <p>Number and type of exception tell us something regarding the state of the installations.</p> <p>The management is responsible for the budget. It is important that safety matters of great importance are lifted up in the hierarchy to the one responsible for the allocation of resources .</p>	<p>Difficult to set limits on what is acceptable.</p> <p>Mapping all the exception must probably be done manually for each installation.</p>	<p>Numbers</p>

The aim with the indicators suggested in table 1 is to focus on areas that have proven to be very significant in previous major accidents in the industry. The indicators must also give meaning and give the management in Gassco important information which can be used when determining new initiatives and making decisions. There are also other indicators/measures that are suitable for Gassco as an organisation than the ones mentioned in table 1. But there is a balance in introducing new elements and trying to keep it simple to make the idea sellable. After all, this is a subject that has been discussed quite a while in the industry.

#### 4.7 Human factors in the nuclear industry

To learn and find good solutions on how to deal with human and organisational mistakes, it is important to seek information from other industries with the same challenges. In a complex industrial facility such as a nuclear power plant, the majority of the tasks are performed by machines. But man is involved to a great extent in their design, testing, maintenance and operation – just as in the process industry. The performance of a person working within a complex mechanical system depends on that person's capabilities, limitations and attitudes, as well as on the quality of instructions and training provided.

Human error can occur at every stage in the life of a nuclear facility and a variety of methods must be used to detect and prevent this. In the nuclear industry following aspects are, regarding human errors, focused on <sup>[67]</sup>:

- **Task analysis:** A task analysis can determine what kind of personnel are needed, how its members should be selected, what should be included in training programs, and other technical issues. In some countries, a specific data base to analyse operator tasks has been developed to assist management in selecting, testing and training personnel, and in evaluating control room instrumentation and procedures.
- **Personnel hiring and organisation:** A person's skills, personality and experience must be carefully reviewed during the hiring process to determine which candidates are best suited to operate and maintain a nuclear facility. Quality management of plant staff is also highly important, due to the way in which the work is organised, staffed, manned, supervised, evaluated and rewarded will determine the effectiveness, productivity and safety of the facility.
- **Operator training and testing:** Lack of proper training, as well as operational procedures, has been a major cause of human error in the nuclear industry. Great emphasis is being placed on training issues as the use of simulators, case studies, computer-assisted training, team training techniques and better evaluation of training programmes. Examinations based on a task analysis can help ensure that all requisite skills and knowledge are included.
- **Procedures:** Procedures for normal and emergency operations must be technically accurate, well-defined and entirely comprehensible. The presentation of procedures for routine maintenance, calibration and testing of equipment differs from operating procedures. For example, while maintaining clarity and conciseness, more detail should be included, especially if the task is not often repeated.
- **Control room design and layout:** Errors by control room personnel have often been caused by designs that did not take human limitations into account. Improvements in control room design, layout, and work environment can lead to the prevention of accidents or better management of accidents if they occur.

- **Reporting:** It is important to compile statistical data on the number and kind of human errors that occur in nuclear power plants through the proper use of a well-designed reporting system. Each time an event out of the ordinary occurs, a form is completed describing the event, the probable cause and other pertinent information. If human error data is correctly entered on this form, it can help to assess the likelihood of accidents and to evaluate changes in control room procedures and training programmes.
- **Equipment design, maintenance and testing** Human errors occur when machines are improperly designed or built or when they are poorly maintained. Errors in system design can only be eliminated by a thorough evaluation or testing prior to operation. Human error during test and calibration activities has also been attributed to inadequate organisation of these activities, design of the equipment or limitations of the maintenance personnel.

Overall system reliability in a nuclear power plant is more often dependent on individuals than on the equipment. For human reliability assessment, there are no equivalent methods for identifying significant potential human failures on a purely logical basis. It is difficult to evaluate human performance qualitatively because a decision can be affected by many psychological factors. For example, individuals may vary in their performance of well-defined tasks, depending on their familiarity with the task, their state of fatigue, what other tasks have to be performed, a changing physical environment at work or a tense psychological environment at home, and many other factors. Member countries in the Nuclear Energy Agency (NEA) <sup>[67]</sup> have recognised the need for a classification system to identify and define human errors, and in 1983, the Group of Experts on human error data and assessment suggested the principal elements of such a system. A three-level model of human thought processes was developed, and different types of mental errors were identified for each level: errors in trained skills, such as clumsiness; errors in learned rules, such as forgetfulness; and errors in creative thinking, such as incorrect interpretation of an event. All of these can cause critical mistakes in operating a nuclear power plant.

A probabilistic safety/risk assessment is the method used by the nuclear industry to calculate and compare different accident scenarios. A method has been developed by the nuclear industry to help estimate the probable occurrence of procedural errors, based on an extensive task analysis of each human action evaluated. This method concentrates on mechanical tasks, with little analysis of the thinking behind human actions. For example, it identifies errors in reading and implementing emergency operating procedures but not errors caused by faulty knowledge or reasoning during an event. Under accident conditions, an operator must first diagnose the nature of the accident before selecting the appropriate procedures and recovery action. Errors of diagnosis are more frequent than procedural errors or those which result from misread instruments. When an accident sequence occurs, operators may <sup>[67]</sup>:

- fail to realise that an event has occurred,
- fail to diagnose the event correctly and identify proper responses to it, or
- fail to take timely or proper corrective actions.

Designing systems so that they increase the time available for operators to respond to abnormal conditions can help resolve these problems <sup>[67]</sup>. When they realise that the plant is not responding as expected, they will have time to analyse the situation and implement the proper corrective actions. It is hard to assess these errors by the data bank approach used for procedural errors because of the difficulty of observing diagnostic and other hidden thought



processes. The alternative is to use the judgement of individuals who have experienced these errors in plant or simulator situations, or who have other appropriate knowledge. This can help assess the likelihood of human failure. Such individuals may be plant designers, operators, trainers, human factor specialists, risk analysts, or others who have expertise in the area and who are experienced in quantitative thinking. The need for qualitative information to support conventional statistical error analysis has been demonstrated. There are at least three ways to collect such information: by in-depth event reports submitted by plant personnel; by on-site investigation of significant abnormal events carried out by experienced human factor experts; and by the use of simulators.

A NEA group of experts recommended a system of collecting information based on the use of detailed reports on the circumstances leading up to the incident, to be submitted by plant personnel, and the use of teams of specialists to analyse selected important events in greater detail. Among the categories of information recommended for inclusion in incident reports were <sup>[67]</sup>:

- the exact nature of the error (e.g., omission of task or action, wrong action, wrong piece of equipment);
- factors relating to the general work situation (was the task routine or unfamiliar, performed under difficult physical working conditions, on night-shift, etc.);
- which mental function failed (wrong decision made, wrong action taken);
- why it failed (the person was distracted, had the wrong information, was ill); and
- how it failed (describes the psychological mechanism involved, such as absentmindedness).

The NEA Working Group studied the methods used in Member countries to analyse events in nuclear power plants involving human error. The results showed<sup>[67]</sup> that some countries have set up a specific system for analysing these incidents, and that site visits are the most effective way to gather information and identify root causes. Written reports seldom contain enough information for the purpose. In some countries, a human performance evaluation specialist is responsible for the analysis of unplanned reactor events, and for making recommendations to correct the root causes of human performance problems. Simulators are also used to accumulate human error data in the performance of individual tasks during abnormal events. In the nuclear industry human factor studies are advancing rapidly in many countries. Greater attention is being paid to human needs in designing equipment, and efforts are being made to learn from experience in order to correct past errors. Current NEA work in the human factor area is focussed on <sup>[67]</sup>: the need for operators to be better trained to understand what happens during plant emergencies, including the use of simulators, analysis of the misinterpretation of plant status by operators, and evaluating the use of digital computers in the control room. Using defined criteria, the United States Nuclear Regulatory Commission (NRC) sorts the descriptions of human performance issues into the following eight categories and codes them <sup>[68]</sup>:

1. Training
2. Procedures and Reference Documents
3. Fitness for Duty
4. Oversight
5. Problem Identification & Resolution
6. Communication
7. Human-System Interface and Environment
8. Work Planning and Practices

Each category is further divided into areas, and each area contains a series of details that describe the human performance issue.

By describing the work done in the nuclear industry to prevent human mistakes, it makes it conspicuous that lesson from previous major accident can not only be learned by implementing some new indicators in Gassco barrier KPI. It contributes to a better safety culture and awareness of influencing factors, but more work is required. This will be further discussed in chapter 6.

## Chapter 5. Do changes in the barrier KPI model equal changes in the risk level?

In this chapter it is of interest to evaluate how much the reliability of the barriers affect the risk level at a given installation. One goal is to figure out whether or not the barrier model can be used to state an increase in the risk level.

Barrier function is defined as a function to prevent, control, or mitigate undesired events or accidents <sup>[32]</sup> Keeping this definition in mind, five technical barrier functions to prevent major accidents can be identified:

- prevent leaks
- prevent ignition
- limit energy supply
- limiting escalation of fire/explosion
- secure personnel if major accidents occur

Aggregation rules used in the barrier KPI model is thoroughly described in appendix B.

Combining the QRA model at a given installation with the theory presented in chapter 2, can identify how the failure rate of selected barriers from the KPI model affects the risk level at a given installation.

Aggregated Reactive Elements	Actual	Status	Trend	Tools
Gas detection, automatic	0.1%	●	→	
HVAC	0.0%	●	→	
ESD - Valves	8.7%	●	↗	
ESD - Pushbutton	0.0%	●	→	
Blowdown	0.0%	●	→	
Fire detection	0.1%	●	→	
Deluge valve	5.6%	●	→	
Deluge nozzle	17.9%	●	→	
Fire water pumps	3.1%	●	↗	
PA system	1.4%	●	↗	
Emergency power generator	3.2%	●	↗	
UPS capacity	0.0%	●	→	
Emergency lighting	5.8%	●	↘	

Figure 18: Reported figures at installation X, March 2011

## 5.1 QRA analysis

Figures and risk values used in this report are from a performed QRA analysis at installation X<sup>[69]</sup> in Gassco's portfolio. The software OHRAT is used in the QRA, and details regarding the software is given as an appendix in the performed risk analysis<sup>[69]</sup>. The program performs all consequence modelling and gives the risk results directly. In the risk analysis only scenarios that can result in a major accident are evaluated. When a risk analysis is performed, a lot of assumptions are made and the results will always have some degree of uncertainty.

Looking closer at the calculations performed in this risk analysis, only risk values from the process and storage area are assessed. Also, only estimated individual risk for 1. person (FAR-value) are assessed (not society risk, material damage and environmental risk).

### Leak frequencies:

The Hydrocarbon process at the installation is divided in 75 ESD (Emergency Shut-Down) segments in total. Each segment is defined with help from ESD valves and blow down valves. In the QRA model frequencies calculations are performed using the programs LEAK version 1.2 and VEREDA version 1.1 (Veritas recommended Data). For each representative event, three different leak rates have been modelled, as shown in table 1.

**Table 2: Representative leak rates for process events**

Leak size	Representative initial leak rate (kg/sec)	Represented categories (kg/sec)	
		Gas	Fluid
Small	0,5	0,1 - 2	0,1 - 1,2
Medium	5	2 - 15	1,2 - 25
Large	50	> 15	> 25

The different leak rates are modelled differently regarding the escalation potential. Based on experiences, 13 leaks are estimated on the given installation per year in the QRA model. Estimated frequencies at the installation give a distribution between large, medium and small leaks in the ratio 1:6:12. A large leak covers more ignition sources than a small leak. A subsequent fire will then affect a much larger area than a subsequent fire following a small leak.

### Probability for ignition:

Whether or not a gas leak ignites is crucial regarding the risk. Large leaks have a higher probability for igniting than medium and small leaks. In areas where large leaks reach the surrounding roads, the probability of ignition is dominated by passing cars. The probability of ignition in these areas is between 4% and 19%. All other areas the probability of ignition for larger leaks is around 1-2%.

Typical ignition probability for small leaks is around  $3 \cdot 10^{-4}$  and for medium leaks between  $10^{-3}$  -  $10^{-2}$ .

### Fire frequencies:

Estimated fire frequencies in the QRA shows that a medium leak will only contribute to fatality risk in a few areas. This is mainly due to the high probability for ignition of large leaks. Summarised the fire frequency is calculated to 0,05 per year – one fire every 20<sup>th</sup> year.

Escalation probability:

A total, average escalation probability is calculated to 30 % in the QRA. Escalation means that the initial fire escalates to other equipment, followed by subsequent larger fire. However, this will take time (10-15 min.), and in many cases it will not contribute to an increase in the consequences regarding fatality risk. This is because evacuation occurs before escalation.

Risk result in the QRA:

When combining fire frequencies and expected number of people killed in each scenario, an estimated number of yearly fatalities are calculated (Potential Loss of Life). The acceptance criterion is often given in Fatal Accident Rate (Far-value), and relates to PLL as shown in formula 2.5 in chapter 2. Total number of working hour at the installation in the QRA is 1.150.000.

In total a FAR value due to an accident in the process area is estimated to be around 2,0. The largest contributing factors are listed in table 3:

**Table 3: The most important contributions to FAR value from process event (all contributions > 1%)**

Scenario number	Size and area	Contribution to FAR value from process events	
		Value	% of total
1	Large leak, Train 100, south	0,51	25
2	Large leak, Train 100, north	0,38	18
3	Large leak, Train 300, south	0,35	17
4	Large leak at the quay	0,19	9
5	Large leak, Train 200, south	0,09	4
6	Large leak at the metering station	0,08	4
7	Medium leak at the metering station	0,06	3
8	Large leak at the gas metering station	0,05	3
9	Medium leak, Train 100, south	0,05	2
10	Medium leak, Train 200, south	0,05	2
11	Large leak, Train 200, north	0,05	2
<b>Sum 11 most important event (in total 45 modelled)</b>		<b>1,84</b>	<b>89</b>

Large leaks dominate the risk picture. Some important weaknesses must be emphasized in this risk presentation. In the calculation of FAR the risk from the process area is divided on all employees. This does not relate to how the risk, in reality, is divided. The risk from a process leak will only affect the people in the process area, which is about 350.000 work hours. The actual FAR- value is then 6,7. For employees, who spend a lot of time in the administration

building, the FAR contributions from process events equals close to 0. It is also worth mentioning that all values in the QRA have a certain amount of uncertainty. All frequencies and probabilities are based on experience and statistics. They say something about to history. None knows if history is telling us something about what is laying ahead. This illustrates the difference in the definition of risk given in equation 2.1 and 2.2 in chapter 2. This will not be further discussed in this report, since it is the barrier KPI model that is under evaluation and not the risk analysis.

As shown in table 4 process risk is the largest contribution to the overall FAR value at the installation in the QRA.

**Table 4: Contribution to personnel risk**

Event:	FAR-value	% of total
Fire and explosion in process and storage area	2,0	65
Occupational accident	0,6-1,0	32
BLEVE, tank fracture and explosion inside buildings	$4,5 \cdot 10^{-2}$	1,5
Quay operations (risk only related to vessels)	$4 \cdot 10^{-2}$	< 1
Propane filling station	$2 \cdot 10^{-4}$	< 1
<b>Total</b>	<b>2,7 - 3,1</b>	<b>100</b>

So, how will changes in the reliability to the chosen indicators influence the risk calculations? Fatality risk presented as PLL is calculated as in equation 2.3, and is the product of annual frequency of the event and number of fatalities. Further on, the frequency is calculated as in equation 2.4; the product of frequency of leak, probability of ignition, probability of failure of the safety protective system, probability of escalation and fatality contribution of the accident scenario.

The gas detection system affects the consequence and fatality contribution of the accident scenario; people get the chance to evacuate. Ignition source control reduces the probability of ignition and thereby also effects the consequences. Safety critical PSD valves, ESD and deluge reduces the consequences and escalation potential and is regarded as a safety systems, mentioned as “ $P_{\text{profail}}$ ” in equation 2.4 in chapter 2. There are a lot of dependences in equation 2.4. Several of the chosen barriers will affect several of the input data, such as the gas detection system, which will affect the consequence and the fatality contribution. The gas detection system will also affect the liability to the ESD system. For example, if a node in the QRA is stated as `closure of ESD valves`, it will include implicitly: ESD valves, ESD logic, auto gas detection and manual gas detection sub-functions. The probability of failure to shut the ESD valves can be calculated for this node in the following manner <sup>[34]</sup>:

$$P_{\text{TOT}} = P_{\text{ESDv}} + P_{\text{ESDI}} + (P_{\text{gasdet}} * P_{\text{mandet}}) \tag{Formula 5.1}$$

where

- $P_{\text{TOT}}$  = probability of failure to shut the ESD valve
- $P_{\text{ESDv}}$  = probability of failure of the actual ESD valve itself

$P_{ESDI}$  = probability of failure of the ESD logic  
 $P_{gasdet}$  = probability of failure of gas detection  
 $P_{mandet}$  = probability of failure of manual gas detection

By combining equation 5.1 with equation 2.4 the expression for the annual frequency of an accidental scenario were the ESD valve fails will become:

$$f_{nj} = f_{leka,n} \times P_{ign,n} \times (P_{ESDv} + P_{ESDI} + (P_{gasdet} * P_{mandet})) \times P_{escal,n} \times n_{nj} \quad (\text{Formula 5.2})$$

where

$f_{leka,n}$  = frequency of leak  
 $P_{ign,n}$  = conditional probability of ignition, given leak  
 $P_{escal,n}$  = conditional probability of escalation, given ignited leak and failure protective systems response.  
 $n_{nj}$  = fatality contribution of the accident scenario (fraction of scenarios that result in fatalities).  
 $P_{ESDv}$  = probability of failure of the actual ESD valve itself  
 $P_{ESDI}$  = probability of failure of the ESD logic  
 $P_{gasdet}$  = probability of failure of gas detection  
 $P_{mandet}$  = probability of failure of manual gas detection

In the QRA analysis the failure rate is calculated as followed:

$$P2 = P_{isol.fail.} = 1 - (1 - P_{proc})(1 - P_{human})(1 - P_{esd}) \quad (\text{Formula 5.3})$$

Total failure probability for isolating failure given manually initiation is described as:

$$P_{esd} = 1 - (1 - 5.5 * 10^{-6} * \tau_{esd})^{N_{esd}} * 0.9997 \quad (\text{Formula 5.4})$$

where

$P_{esd}$  =  $f(N_{esd}, \tau_{esd})$   
 $N_{esd}$  = Number ESD valve to isolate the actual segment  
 $\tau_{esd}$  = test interval for valve (2190 hour)

The failure rate for one ESD valve to close given a leak is set to be 0,062 in the QRA [69]. Reported failure rate for ESD valve in March for the same installation is given in figure 18 and is 0,087. How will changes in the failure rate affect the risk level at the installation expressed in FAR?

As illustrated in figure 19, the annual frequency of an accidental scenario and the PLL value is proportional with the failure rate. For the PLL value the consequences are the proportionality coefficient. For the annual frequency there are several terms that determine the gradient, as shown in equation 2.4

Calculations are shown in appendix E. Most of the figures are from the QRA analysis. Figures stating the fatality contribution of the accident scenario and the consequences used when calculating the PLL were not available in the QRA document. Figures for these factors have been randomly selected, due to the fact that they will not affect the conclusion, which is that the frequency of an accidental scenario and the PLL value are proportional with the failure rate.

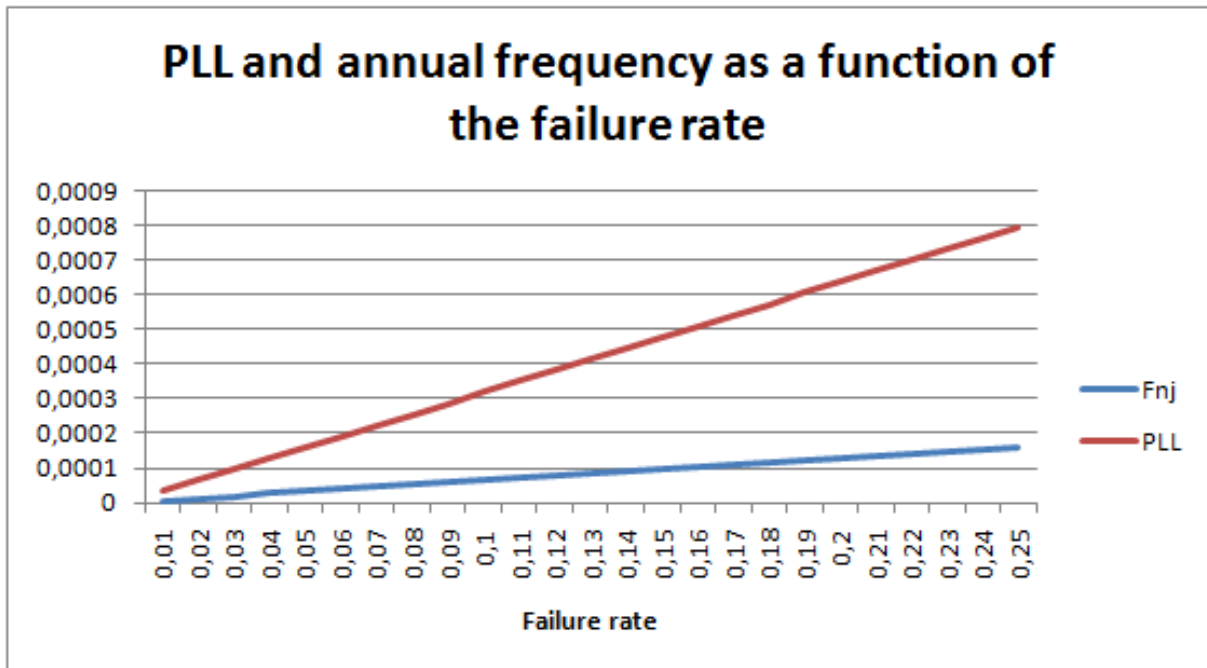


Figure 19: PLL and Fnj as a function of the failure rate

The FAR value is, as shown in equation 2.5, proportional with the PLL value.

In figure 19 the PLL value for one possible outcome of a given scenario is proportional with the failure rate. But, as shown in equation 2.3, the PLL value for one scenario is the sum of all possible outcomes. Therefore the PLL value for one scenario with all possible outcomes is not proportional with the failure rate. This is illustrated in the event tree in figure 20 and figure 21.

In figure 20 the event tree given a medium gas leak, is sketched. In figure 21 the event tree of the same event is sketched, but with an increase in the failure rate.

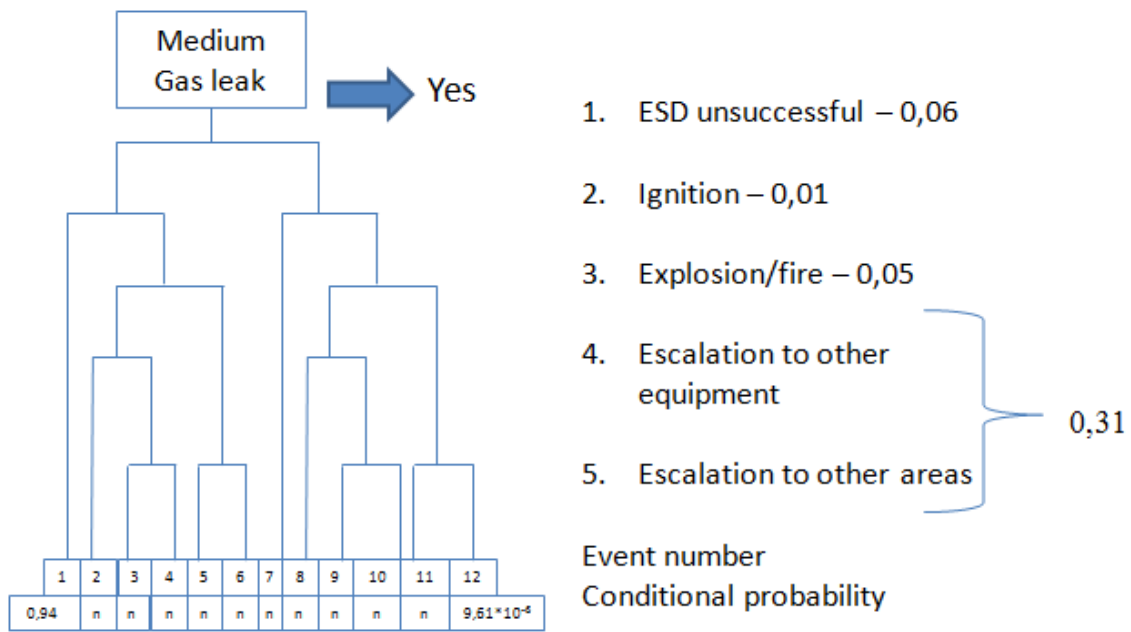


Figure 20: Event tree

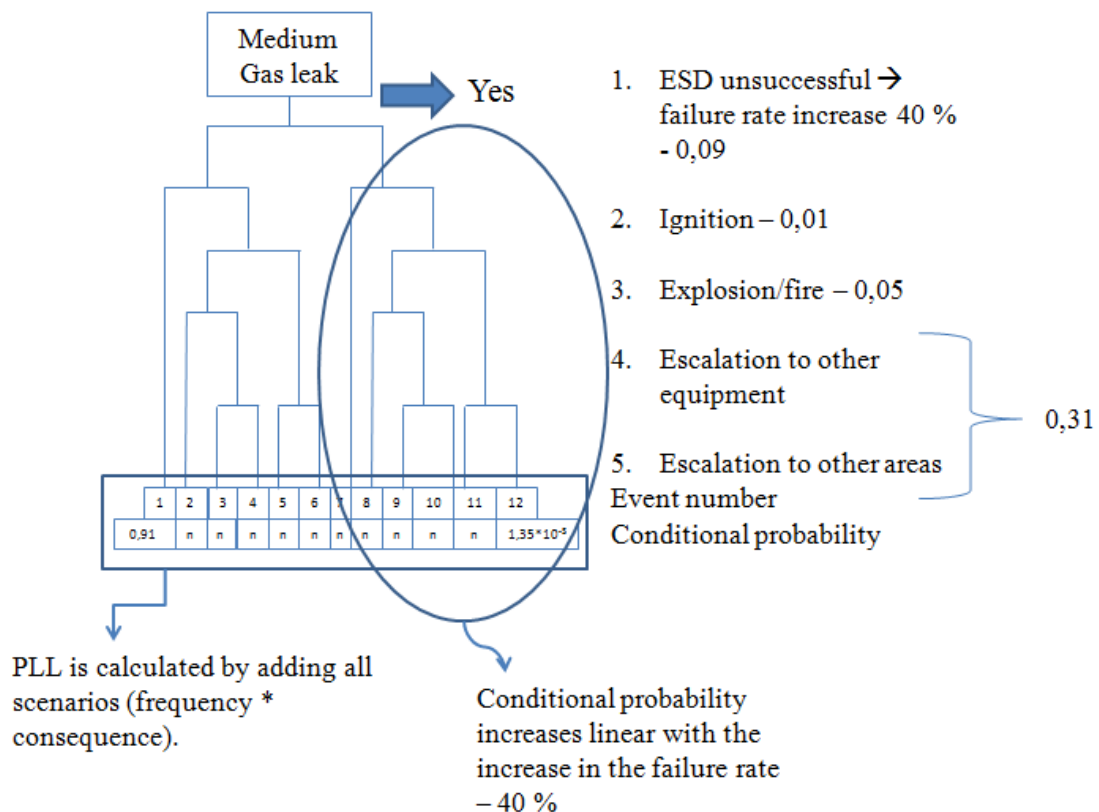


Figure 21: Event tree 40 % increase failure rate

An increase in the failure rate in this example will only affect 50 % of the possible outcomes. The result of an approximately 40% increase in the failure rate (from 0,062 to 0,087) will in this example result in a 20 % increase in the PLL value. This is still a significant number. But as shown in table 3, this scenario constitutes 3 % of the total FAR contribution from gas leaks.



As shown in table 4 the FAR contribution from gas leaks constitute 65 % of the total FAR value for the installation. So a 20 % increase in the scenario 7 would only affect the total FAR value 0,74 %. But, a higher failure rate in the ESD valve would affect more scenarios than just scenario 7 in table 3. An 20% increase in the PLL value for all scenarios listed in table 3, would result in an almost 15 % increase in the total FAR value at the installation (from 2,7 – 3,1 to 3,1 – 3,5). The failure rate of a barrier early in the chain of event would affect many scenarios in the QRA analysis.

The calculations in this report are very simplified (appendix E). There are many dependencies related to barriers. As mentioned earlier in this report, the human and organisational risk also play very significant roles in the risk level at an installation. This is however very difficult to quantify. The calculations show that the failure rate affects the risk level at an installation. The more dependencies between the barrier and different scenarios – the greater the impact from the failure rate on the total FAR value. If the barrier affects only a couple outcomes of a scenario it will hardly be reflected in the FAR value at all. This brings up some questions regarding the QRA analysis. A QRA analysis is presented as a document stating the risk level at a given installation. The documents are update in interval, usually a couple of years. Detailed modelling regarding barriers are not performed. By evaluating the calculations performed in this report, barriers such as for example ESD valves, HIPPS and ignition source control will contribute in the overall FAR value, due to dependencies and the fact that they will be present in several scenarios. In a QRA the failure rate is calculated by using equation 5.2 and 5.3. In the barrier KPI model all failure rates are reported number of test divided on reported number of tests. The reported number will change as a result of amount of reported data. As shown from the calculations done above, the failure rates of barriers early in the chain of event does affect the risk level to some degree. If the QRA analysis is updated once in every second or third year, the changes in the risk level as a result of the condition to the safety critical equipment will not be visible.

There must be a way to combine all information regarding the risk level and present it in a informative and logical way. It seems reasonable to “connect” the barrier KPI model and the QRA analysis, thus both providing important information regarding the risk level. This could result in a more “dynamic QRA model”, which could further perhaps be presented as a risk indicator? This will be further assessed in chapter 5.3. First, there is a need to evaluate whether or not the barrier KPI model reflects the risk level. This will be done in the following chapter.

## 5.2 Sensitivity at installation level in the barrier KPI model

As shown in previous chapter, an increase in the failure rate of for example ESD valve will in some degree affect the risk level. But how will an increase in the failure rate of important reactive barriers in the KPI model be reflected? Will the overall status on reactive barriers become red when important barriers that affect the risk level have a red status (see figure 14 for colour interpretation)?

Following indicators and their sensitivity in the model will be assessed in this chapter:

- Gas detection (detect leaks)
- Ignition source (prevent ignition)
- Safety critical PSD valve (limit energy supply/escalation)
- ESD valve (limit energy supply/escalation)

- Deluge valve (limit escalation)

These five technical barrier functions cover the functions: to prevent, to control, or to mitigate an undesired event or accident. Logically, failure of these barriers will affect the risk level at the installation. But is the model sensitive enough to intercept changes in the risk level at the installation? Sensitivity analysis is particularly important if the data basis has an insufficient number of occurrences.

Delimitations when calculating the status sensitivity at installation level are listed in chapter 1.4.

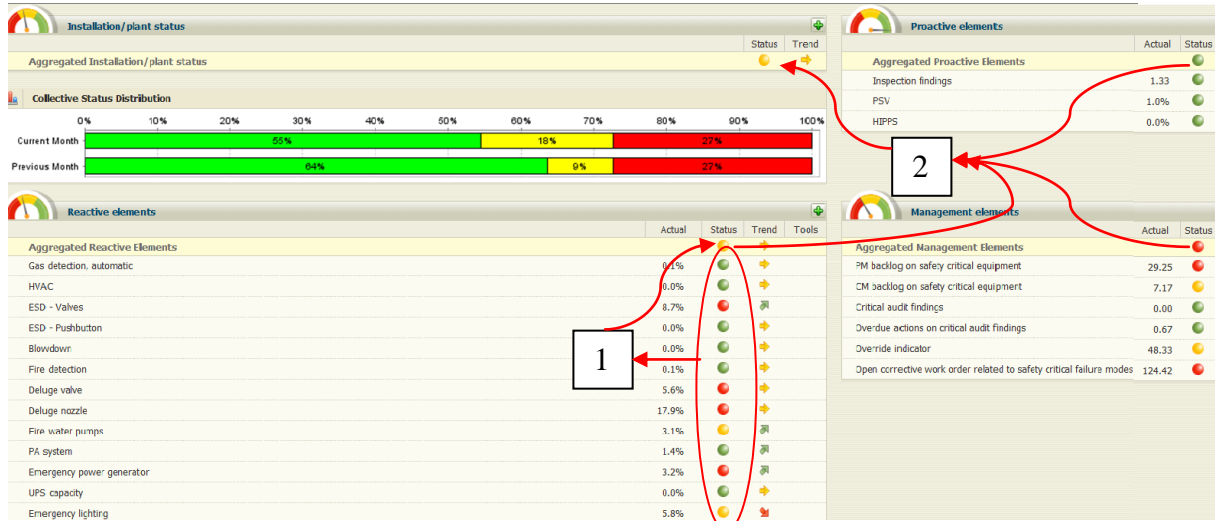


Figure 22: Illustration aggregation

Figure 22 illustrates the calculation scenarios assessed in this chapter. At first all reactive elements are aggregated into one overall status for reactive elements. Second, the overall status for reactive elements, proactive elements and management elements are aggregated into one installation status.

Calculations are presented in appendix F and aggregation rules are presented in appendix B.

Changing the status for the five selected indicators and giving all other reactive indicators to green status, results in that of 240 possible scenarios none of them will give an overall red status for the reactive elements (0%). 43 scenarios will give an overall yellow status for reactive elements (17,34%) and 205 will give an overall green status for all reactive indicators (82,66%). Even if all chosen indicators (gas detection, ignition source, safety critical PSD valve and ESD valve) have a higher failure rate than acceptable, the aggregated status on all reactive elements will be yellow. To get a red overall status for reactive indicators, all the five selected indicators must be red and at least 50% of the other indicators must be yellow (50% yellow and 50% green). Of 240 possible scenarios, one will give an overall red status (0,40%), 177 will give an overall yellow status (71,37%) and 70 will give an overall green status for all reactive indicators (28,23%).

Reactive indicators, proactive indicators and management indicators are all aggregated up to one installation status. So, even if the status on reactive elements is red, the overall installation status will only be red in 2 of 8 possible scenarios (25%). So the possibility of getting a red installation status, given the scenario that first give a red status on reactive elements (all five selected indicators are red, distribution other indicators: 50 % yellow and 50% green) is only approximately 0,1%.

Table 5: Status as a result of reported data for installation X in January, February and March 2011.

Reactive indicator	Weight	January	February	March
Gas detection	2	Green	Green	Green
Ignition source control	2	No data input	No data input	No data input
HVAC	1	Green	Green	Green
ESD valve	3	Red	Red	Red
ESD pushbutton	3	Green	Green	Green
Safety critical PSD valve	2	ESD valve also have PSD function	ESD valve also have PSD function	ESD valve also have PSD function
Blowdown	3	Green	Green	Green
Fire detection	2	Green	Green	Green
Deluge valve	2	Red	Red	Red
Deluge nozzle	2	Red	Red	Red
Fire water pumps	2	Red	Yellow	Yellow
PA system	1	Yellow	Green	Green
Emergency power generator	2	Red	Red	Red
UPC capacity	2	Green	Green	Green
Emergency lighting	1	Green	Green	Yellow
<b>Overall status reactive indicators</b>		Yellow	Yellow	Yellow

The installation status was yellow in January, February and March. In the same time period the failure rate for the ESD valve was higher than acceptable. This is shown as red in the model and requires imitate actions. As shown in previous chapter, the failure rate did affect the risk level. But in the barrier KPI model, the aggregated status for reactive elements is yellow. Yellow on installation level requires evaluating the underlying KPIs to identify cause. Trend should be monitored closely. When the status on installation level is red, the need for an overall risk assessment is required. So, based on this, it is reasonable to assume that when the overall installation status is red, there has been an increase in the risk level at the installation. The risk level will increase before the overall status is red, but the model is not sensitive enough to capture all risk changes. The model could be more sensitive if barriers that affect the risk level, were given a higher weight.

The QRA lacks a detailed model for barriers and dependences. Some barriers early in the chain of event, which affects leak, ignition and escalations probabilities will be evaluated in the QRA and affect the risk level. A red status on some of these barriers in the barrier KPI model will probably not give an red overall status on installation level, which would result in a new overall risk assessment. The conclusion is that the barrier KPI model is not sensitive enough to capture an increase in the overall risk level at an installation when the indicators are aggregated to an overall status. Due to this, the barriers that have the most effect on the risk level is not weighted enough in the aggregation. But still, by evaluating each indicator at system level as required by the installation responsible, the status gives very important information regarding the risk at the installation. This helps in getting important barriers repaired faster, and decreasing the risk level.

### 5.3 How to monitor the risk level more frequently?

Being able to monitor the risk level at all times must be the ultimate goal. Previous chapters showed that neither the QRA model nor the barrier KPI model have this function as of today. The barrier KPI model gives useful information when it comes to identifying weak barriers in operation and it helps getting them repaired faster if they fail due to the management focus. The QRA analysis gives the overall risk picture at the installations at a given time. But the risk level is not constant. It changes as a function of several aspects, amongst the failure rate of safety critical equipment. A solution could be to combine the information gained by these two models. A way this could be done is suggested in this chapter, after presenting what is already been done on this subject in the nuclear industry.

It is common to perform extensive event tree and fault tree analysis for QRA studies in the nuclear industry<sup>[34]</sup>. The analysis is performed to an extent where dependencies can be analyzed in detail. The most common used tool is RiskSpectrum (Relcon, 2006), which has event trees and fault trees in a common manner, but also is able to transform event trees to fault trees, so that all fault trees for barriers may be integrated into a huge common fault tree. Advantages gained by using the RiskSpectrum analysis tool are;

- dependencies may be identified, together with common mode failures
- importance measures may be calculated for components, systems and failures
- the analysis may be used to identify requirements for barriers to be effective
- the analysis may be used in order to identify what compensating measures are required if barrier systems are unavailable.

A study aimed for mapping what could be learnt from nuclear industry regarding process safety has been performed by Scandpower<sup>[70]</sup>. Reference for the information presented regarding the nuclear industry in the following sections is made to the article Process safety, instrumented safety barriers – what can we learn from the nuclear industry?<sup>[70]</sup>

A major difference between the nuclear and oil and gas industries regarding basic design principles, is that in the oil and gas industry, the operator may play a more active role as a "barrier" in the early stages of an accident, e.g. in some cases it may be up to operators to initiate depressurisation of a plant within 5 minutes after the onset of the hazardous situation. Still, both industries need to control risks in processes that involve high pressures and temperature. Loss of confinement may lead to severe consequences related to health and environment. This has resulted in a high focus on safety in both industries, on strict requirements for the implementation and follow-up of safety, on safety during all life cycle phases, on defence in depth and barrier integrity, etc.

In the nuclear industry a safety analysis is based both on deterministic safety analysis (DSA) and human factor analysis. The DSA analyses the evolvement of postulated incidents or accidents, including design accidents. Barriers are analysed one by one. Probabilistic safety analysis (PSA), or QRA as they are usually called in the oil and gas industry, are performed in order to systematically identify, model and evaluate scenarios that might potentially lead to unwanted consequences, e.g., core damage or an unacceptable release of radioactive material. The analysis explicitly models all safety systems, including both the frontline part (pumping water, shutting down, etc.) and all support functions (electrical power supply, activation signals, interaction with cooling system, etc.). The analysis also identifies and considers the impact from human error. The actual model consists of an extensive and complex structure of linked fault trees and event trees – as mentioned earlier in this chapter. Boolean logic (a logical calculus of truth values) is used in the evaluation and quantification of the model. Quantitative data is included on initiating event frequencies, component failure data, test and maintenance data and human error probabilities. An important part of PSA activities is what is called “living PSA”, i.e., activities aimed at keeping the plant PSA model continuously updated with regard to plant changes, changes in failure data and initiating event frequencies. In order to fulfil the requirements of living PSA, nuclear utilities in Sweden now updates PSA on a yearly basis.

Human factor analyses aim at analysing the importance of personnel and of work organisation on plant safety. The analysis may be both qualitative and quantitative. Quantitative analysis is performed to support PSA, and are called human reliability analysis (HRA). An HRA aims at quantifying operator actions and maintenance activities. This is done for three types of human error; errors before an incident, errors that initiate an incident and errors during the handling of an incident. The general methodology involves detailed scenario analysis that are performed together with plant personnel, and that are quantified using a set of performance shaping factors (PFS), which may include, e.g., the complexity of a task, the stress level, the competence level of the operator, and the time available.

Performing the safety analysis in this way makes it possible to assess quantitatively the overall safety of the installation. Also, a risk profile, i.e., what types of incidents and accidents dominate the risk, what maintenance activities are most important, what safety systems, components and human actions are most important to plant safety, is also possible to assess when performing the safety analysis in such a way. The safety analysis can then be used for various kinds of risk informed applications, including identification of plant vulnerabilities, evaluation of design alternatives for plant upgrades and modifications, planning of major maintenance activities, including complete planning of the yearly refuelling outage, risk-based definition of pipe inspection and testing activities, risk follow-up and detailed evaluation of incidents, etc.

PSA models are beginning to be integrated into so-called risk monitors in the nuclear industry. A risk monitor is a tool that is used by plant personnel, including but not limited to control room personnel, maintenance planning personnel, and personnel at the safety department. Thus, a risk monitor is an on-line tool, where information about the current status of plant systems and components, including both planned tests and outages and failures detected, is fed into the PSA model to provide a risk profile. The input can be based both on on-line data transmission and on manual input. In the nuclear industry risk monitors are typically used for: risk optimisation, risk follow-up, risk monitoring and risk planning.

A risk graph from the PSA is shown in figure 23:

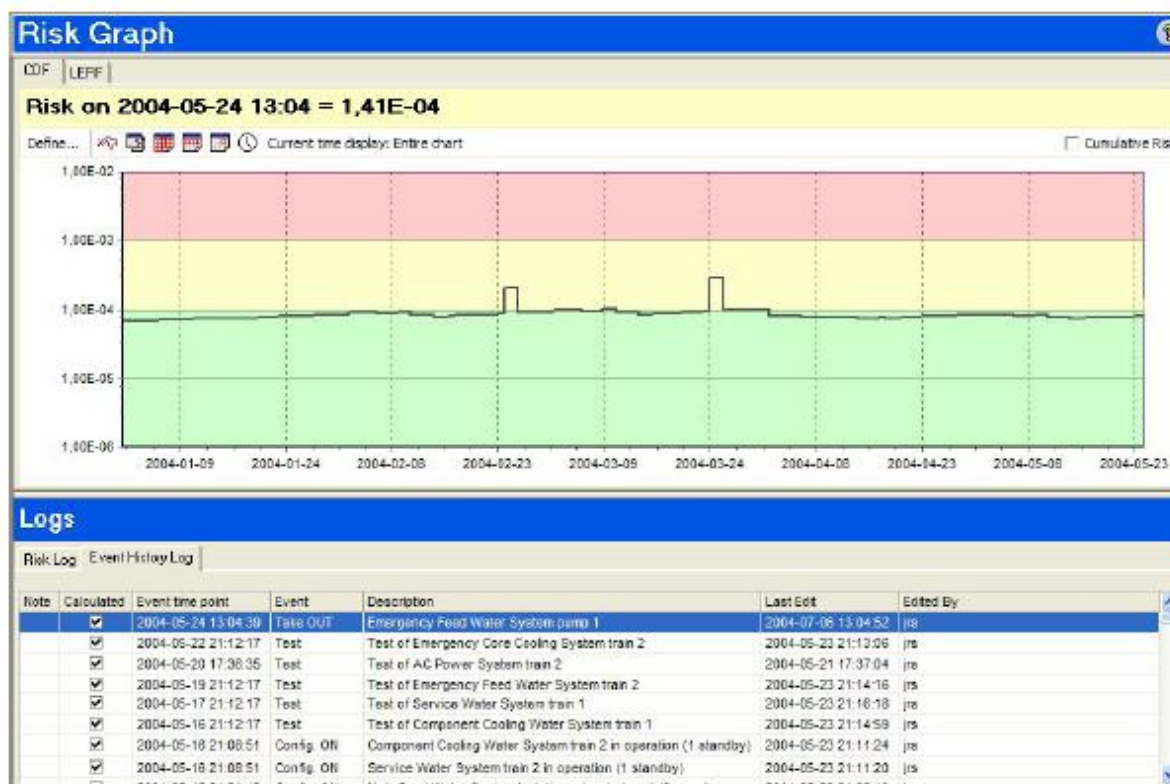


Figure 23: Risk monitor applications - example of an on-line risk graph <sup>[70]</sup>

The graph includes both current and past information. The colour areas indicate relation to predefined acceptance levels, which can be associated with an ALARP approach (as low as reasonably practicable), with green indicating a broadly acceptable risk level and red an unacceptable level. The yellow region in-between is the ALARP region, which is basically acceptable, but where reasonable measures are required to be taken to try to reduce the risk level into the green area. An on-line use is mainly for plant operators, and allows them to input information about present and planned status. This allows both qualitative and quantitative monitoring of risk levels. Users involved in over-all safety assessment and in planning and follow-up of maintenance are mainly using the risk monitor off-line. This allows planning of coming outages, long-term follow up of the plant risk profile including analysis of cumulative risk during the operating year, evaluation of disturbances and failures as well as experience feedback.

It seems there is a more active approach within the nuclear industry, and the differences from the oil and gas industry are <sup>[70]</sup>:

- Quantitative and qualitative analysis of human factors. This is becoming more and more focused in the oil and gas industry, and there should be a lot to learn from the nuclear industry in this context.
- Defence against dependencies both in design, maintenance and analysis. The methods applied in the nuclear industry are highly developed within this area. As the oil and gas industry becomes increasingly dependent on instrumented safety systems there should be significant benefits to learn from other industries within this area.

- Extensive usage of risk informed applications in the nuclear industry to supervise, plan and follow up safety. Done by using on-line risk monitors.
- Dynamic PSA used in the nuclear industry, i.e., activities aimed at keeping the plant PSA model continuously updated with regard to plant changes, changes in failure data and in initiating event frequencies.

In the oil and gas industry online risk monitors and living PSAs are hardly used today. The QRAs should be further developed by use of tools and methods from the nuclear industry. This could open the possibility for a more active use of risk modelling in the operational phases of the installation. Risk based inspection (RBI) and Reliability Centred Maintenance (RCM) are being applied to some extent in the oil and gas industry today, and this is considered to be a growing field.

In general, the study performed by Scandpower concludes that <sup>[70]</sup>: even if there are considerable differences between the two industries, many of the basic challenges to safety are the same. There are several areas of interest where the oil and gas industry could benefit from the experience gained within the nuclear industry when it comes to instrumented safety system.

Gassco can benefit from the experience gained in the nuclear industry. Reported figures to the barrier KPI could be used in a more “dynamic QRA model”, more similar to the one used in the nuclear industry. Suggested process flow is illustrated in figure 24:

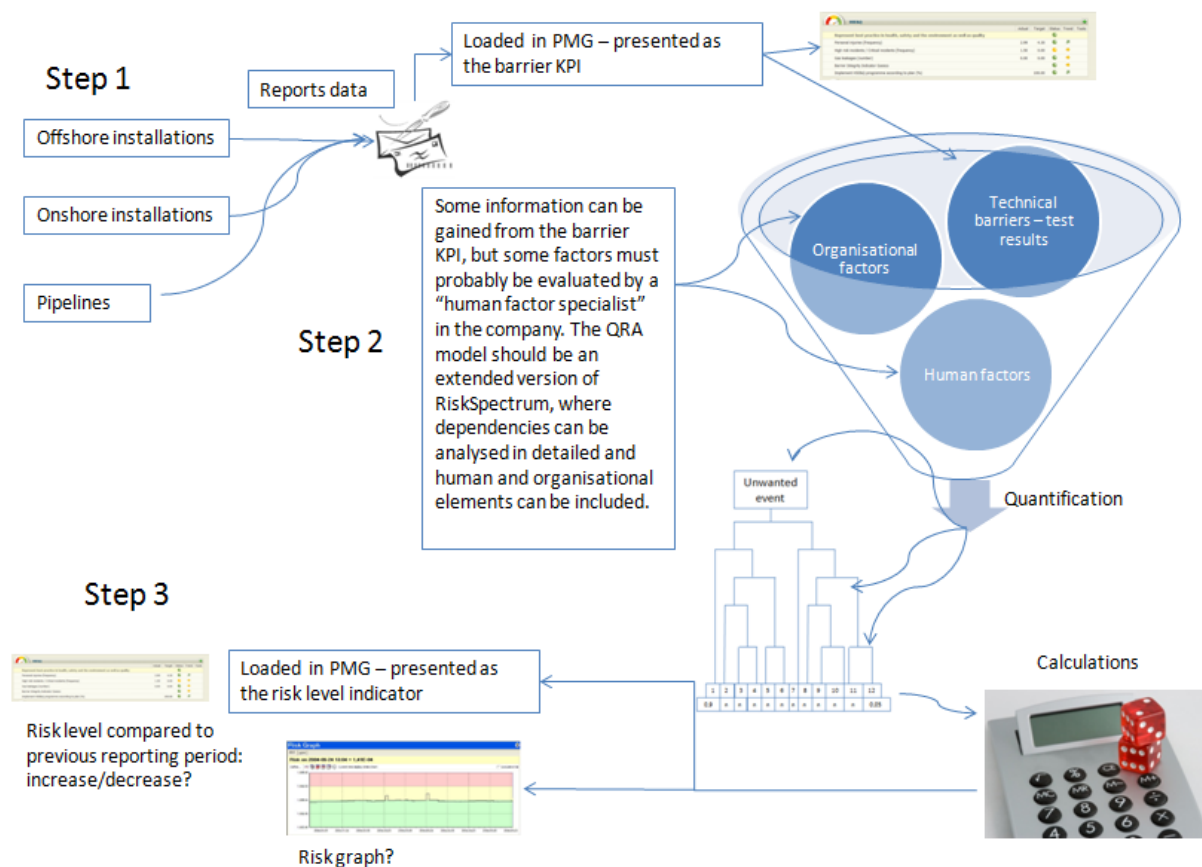


Figure 24: Suggestion process flow

1. Step 1: test data reported from different installations: already implemented at Gassco.
2. Step 2: development of new "dynamic QRA model"- the big challenge, a new model must be developed.
3. Step 3: presentation of the risk level – presentation tool should be PMG which is already implemented and used as the management tool in Gassco. A potential risk graph could also be displayed in PMG.

The big challenge is to build a more "dynamic QRA model". But by using experiences made in the nuclear industry, this should be a practicable assignment. Building the model illustrated in figure 24 will make Gassco able to manage and control risk in several ways:

1. A risk indicator showing whether the risk level in Gassco portfolio increases or decreases. The indicator should be built in the same way as the barrier KPI (as regards aggregation rules etc.)
2. A barrier KPI model which shows the status on important safety critical barriers and management elements that are effecting the risk level. If the risk level increases, the barrier KPI will show where the effort must be laid down to decrease the risk.
3. The live QRA model allows for planning of coming outages, long-term follow up of the installations risk profile including analysis of cumulative risk during the operating year, evaluation of disturbances and failures as well as experience feedback.

The risk indicator, the barrier KPI and the dynamic QRA model can be used separately and combined. The risk indicator is one possible way to present the dynamic QRA model to the Gassco management and to the board. The barrier KPI model will be the supporting management tool to the risk indicator, stating where effort must be laid down to reduce risk. The dynamic QRA model will be an update of the QRA as we know it in the oil and gas industry as of today, and gradually replace the old version of QRA.

Gassco has already several distributors that speak for developing such a model. It is a relative young company (10 years) that slowly has grown and gained more responsibility. In the barrier KPI model the work has started with gathering test data. If Gassco follow in the steps of the nuclear industry and starts gathering data regarding human factors, this could be used when trying to quantify human barriers in a new and more dynamic version of the QRA model. This will be further discussed in chapter 6.

## **5.4 Moving average and status/trend description**

In Gassco's barrier KPI model all indicators, except the status on critical audit findings, are shown as a 12 month moving average. The status indicates the actual level of the indicator and the trend shows development over time. The colours; red, yellow or green state if the status is unsatisfying, improvement needed or satisfying. Regarding the trend the colour interpretation equals deterioration, unchanged or improvement.



Gassco's procedure "Safety critical failures" [5] states quantitative requirements for safety critical failures in terms of "acceptable failure fractions". The failure fraction is defined as the ration between the number of safety critical failures and the corresponding number of tests performed. In the event of a significant deviation in the performance of the safety critical equipment, when compared to the acceptance criteria, the results must be reviewed assessing issues like the test intervals, inspection and maintenance activities and the conditions of the components used. As a guide to decide what is "significantly different", the procedure refers to use the following Bayesian approach:

The maximum allowed failure fraction is denoted  $FF_{max}$ . The prior distribution is a gamma-distribution based on one failure in  $1/FF_{max}$  tests, which means that one starts by assuming that the component is as good as it should be. The idea behind this is to make the approach less sensitive during the first few tests. The expectation in the posterior distribution  $E(FF)$  is calculated by the equation:

$$E(FF) = \frac{x+1}{n+1/FF_{max}} \quad \text{(Formula 5.5)}$$

where

x = number of failures

n = number of tests

If the posterior expectation  $E(FF)$  is larger than  $2FF_{max}$  or smaller than  $2FF_{max}/2$ , it is "significantly different" from the requirement.

If reported failure rate differs significantly from the acceptance criteria, a change in the test intervals should be evaluated as a measure together with an assessment of other relevant actions:

Limits in the model for reactive elements are decided as illustrated in 25:

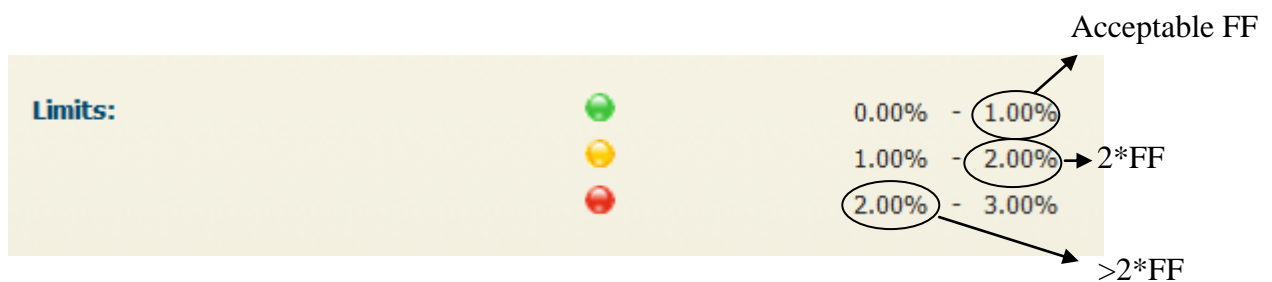


Figure 25: Limits in the barrier KPI model

An indicator shows green if the failure rate is within the acceptable failure rate given by the procedure Safety critical failure [5]. If the failure rate is in the area between the acceptable failure rate and 2 times the failure rate the status is yellow, stating that improvement is needed. If the failure rate is larger than "significant different" the status becomes red. As of today the failure rate is calculated as a 12 month moving average. This brings along some issues:

- few test data gives a high failure rate when the equipment fails – render the yellow area. For example if the equipment is tested twice a year and one fails,

this will give a failure rate 50%. If the limit is 1 %, this is a very significant difference. But it will take 50 years to gather 100 tests, and if this was the only failure in 50 years, the failure rate is acceptable and within the requirements

- for some safety critical equipment test are performed weekly or monthly, while for others they are performed once a year
- the failure rate could increase/decrease without any test performed as a result of the moving average
- for some equipment the test interval is every 12 months, but in practice the tests are performed once a year. If the tests are performed in February one year and November the next, it will not be reflected in the 12 month moving average
- the performance “history” to the equipment is lost if only the 12 month moving average is presented.

Acceptable failure rate in the procedure is equivalent to recommended minimum Safety Integrity Levels within industry standards and guidelines. Safety Integrity Level (SIL) is defined as a relative level of risk-reduction provided by a safety function, or to specify a target level of risk reduction<sup>[71]</sup>. SIL represents the expected failure rate of a safety function provided by a safety function. The higher the Safety Integrity Level of the safety-related systems, the lower the probability that they will perform the requested safety function. The given SIL requirements are based on experience, with a design practice that has resulted in a safety level considered adequate<sup>[72]</sup>. Gassco's quantitative requirements are formulated as requirements to the failure fraction<sup>[5]</sup>. The failure rate function can be interpreted as the probability (risk) of failure in an infinitesimal unit interval of time<sup>[73]</sup>. The increasing failure rate of an object is an indication of its deterioration or ageing. A constant failure rate is usually an indication of a non-ageing property, whereas a decreasing failure rate can describe, e.g., a period of “infant mortality” when early failures, bugs, etc., are eliminated or corrected.

The definition of the failure rate in Gassco's procedure is; the ration between the number of safety critical failures and the corresponding number of tests performed. Meaning that if a very large amount of tests are performed ( $n \rightarrow \infty$ ) the failure rate should not exceed a given % value (based on SIL requirement). The % value is the limit value based on infinite amount of data. Using this requirement when only a small amount of tests are performed each year will give some issues with high failure rates if the safety equipment fails. This will not provide “the correct picture”. If all reported data are aggregated instead of using a 12 month average, eventually there will be a much better data foundation to compare with the requirements. But the catch is that a large amount of data will not be very sensitive to changes. For example, if the equipment starts to get an increase in the failure fraction, this would not be very visible if the average is calculated over a 10 years` time of data gathering.

For one of the tests pilot installation data has been gathered over a time period of 3 years. One indicator – the gas detection system has in this time period a failure rate apparently higher than acceptable. Taking a closer look at the reported data and actions taken could help to identify a better way of presenting the reported data.

Figure 26 shows 12 months, 24 months and 36 months moving average and the red and yellow limit for the failure rate. As shown, the failure rate has been higher than acceptable since the start of the data reporting. This has resulted in several corrective actions in accordance to Gassco's safety critical procedure such as; increased inspection frequency from

6 months to 4 months and a long term mitigation: replacement of gas detection system in 2011 – 2012. This is a positive result from the barrier KPI.

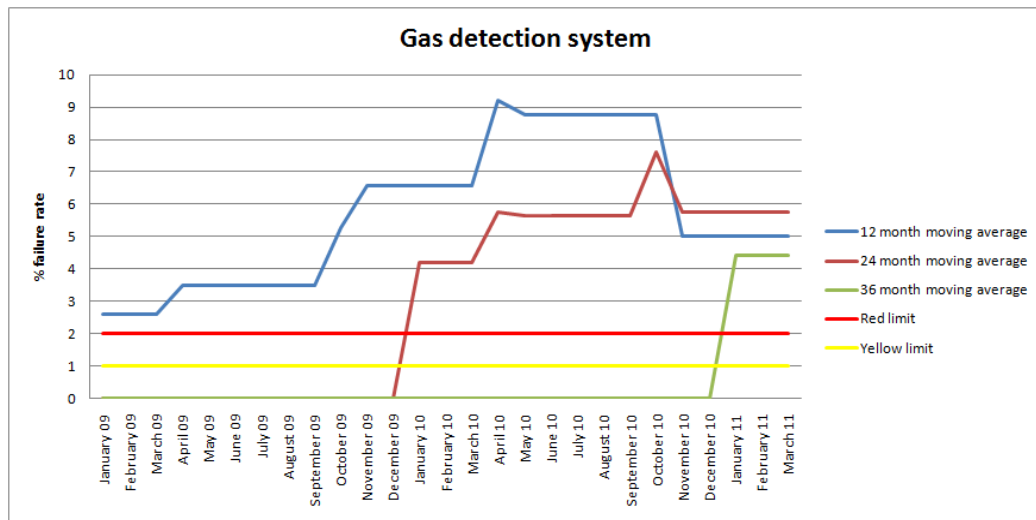


Figure 26: Moving average reported data

Calculating E(FF) for March 2011 for the 12 months, 24 months and 36 months moving average gives 0,028, 0,039 and 0,035. These values are all greater than  $2 FF_{max}$  (which is 0,02) and the moving average is significantly different from the requirement. From the E (FF) values we can see that the actions taken have a positive effect on E(FF) which decreases (from 0,035 to 0,028) as a result of shorter test intervals. Meaning that the 12 months moving average is “less” different than the 36 months moving average. This tells us that the 36 months moving average also is very sensitive for changes, due to a small amount of data input.

When trying to determine how a large amount of aggregated data will affect the moving average, some fictitious data are added to the average calculations. The same amount of tests performed in 2008 are assumed performed each year in the period 2001 – 2008. No failures are assumed in the period 2001 – 2008. This is probably not realistic, but the number of failures in the period 2001-2008 will only affect the % failure rate and not the shape and the gradient of the curve. In this connexion it is the shape and the gradient which is of interest. In figure 27 the graph with aggregated data is shown together with the moving averages. Calculation E (FF) for March 2011 for the aggregated graph gives 0,011 which is between  $0,5 FF_{max}$  and  $2FF_{max}$  (0,05 and 0,02) and the average is not significantly different from the requirement.

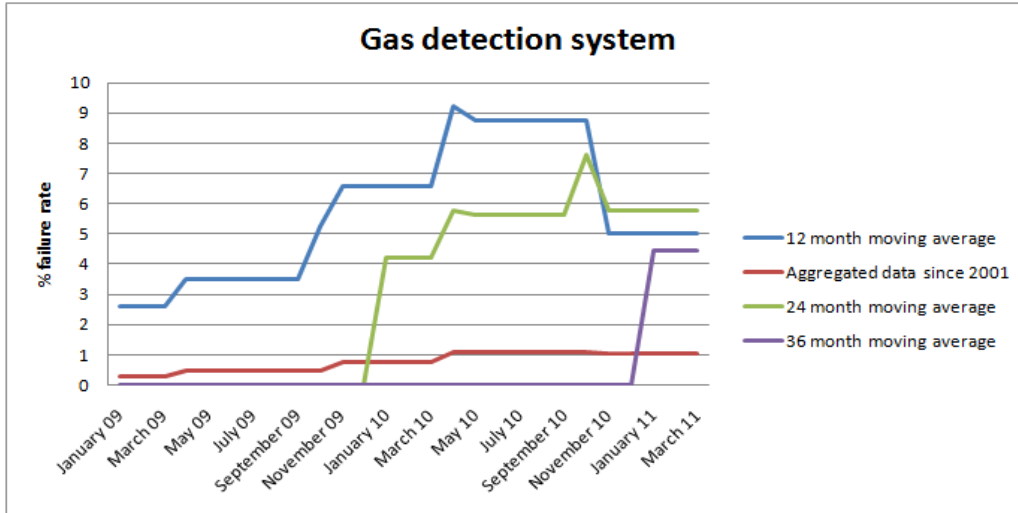


Figure 27: Moving average and aggregated data

When aggregating a lot of data the failure rate will not be very sensitive. As shown in figure 27, an increase in the failure rate, which is very visible in the 12 and 24 months moving average curve, is barely visible in the aggregated curve.

As of today, data in the barrier KPI model is presented as shown in figure 28 and 29. The status red, yellow or green, are calculated from the 12 months moving average. The trend shows whether or not the 12 months moving average increases/decreases or is unchanged compared to previous reporting period.

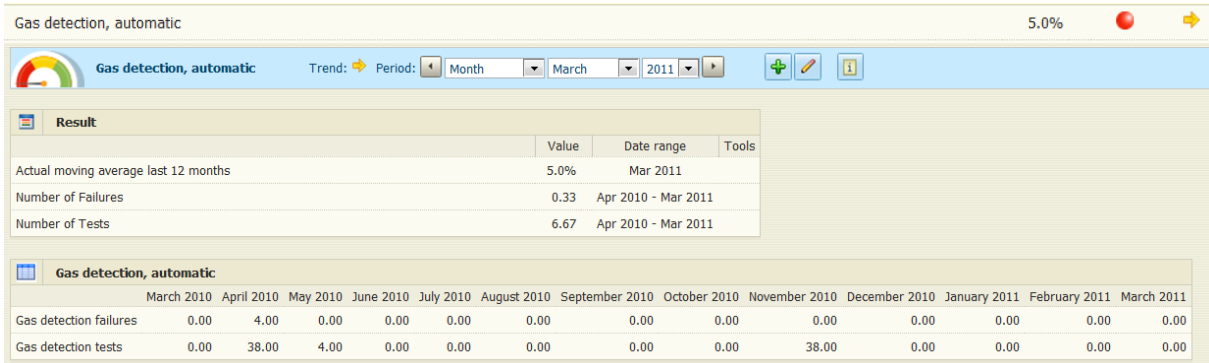


Figure 28: Status Gas detection

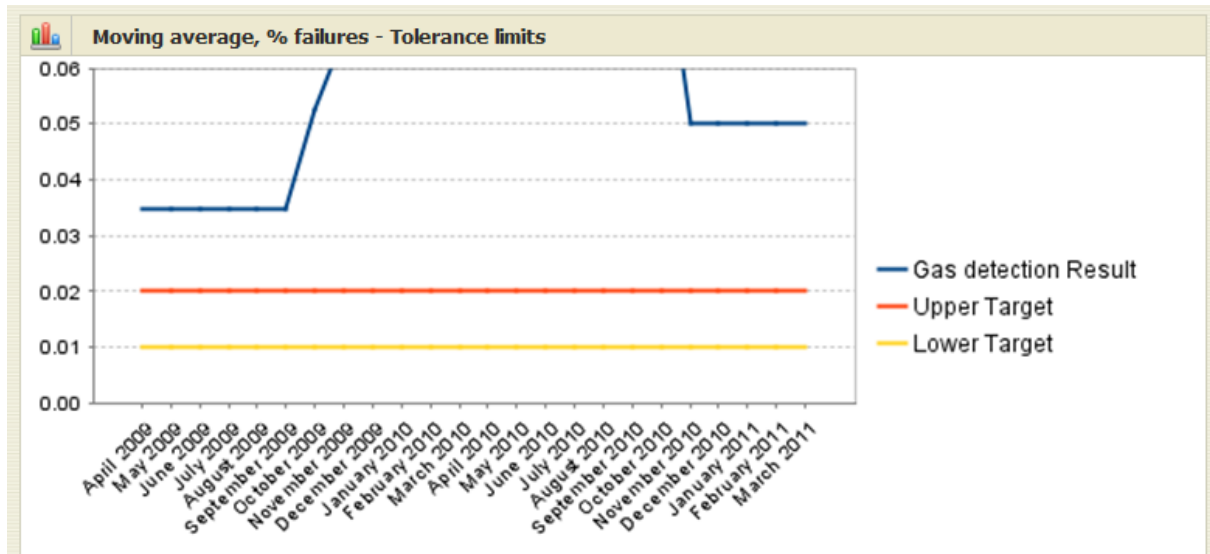


Figure 29: Presentation moving average Gas detection

The model is implemented and people have gained training in how to use and interpret the results. When making suggestion on changes in the model, these should be well argued for and not deviate significantly from signs and symbols already used.

Aggregation of the reported results in the model will after a while rule out issues such as few test giving a high failure rate, data being lost as a result of the moving average and historical data being lost. Further on, the requirements regarding reactive elements in the model are based on “an infinitive amount of tests”, and therefore it is more adequate to aggregate the data reported in the model. But it also becomes less sensitive for changes. Also, if only a few tests are performed each year, it will take some time to collect data even if they are aggregated. From a practical point of view, it is important for the management to be aware of an increase in the failure rate over a short time period. This challenge can be solved by using the trend more effectively. If the status value for one indicator is calculated from the aggregated data reported, the trend could show the relation between the aggregated failure rate value and the moving average failure rate for a shorter time period. Using the trend interpretation as it is today in the model this will mean:

- if the moving average over a time period, for example 12 or 24 months, is 10 % higher than the aggregated failure rate the trend arrow is red, meaning that the failure rate is increasing
- if the moving average over a time period is 10 % lower than the aggregated failure rate the trend arrow is green, meaning that the failure rate is decreasing
- if the moving average over a time period is between 90% and 110 % of the aggregated failure rate, the trend is yellow and unchanged.

Then, the next question will be: how short should the time period be? If using the 12 months moving average, some data included in the test year may be lost due to irregularity in the test period. In practice some test are performed once a year, meaning that they one year can be performed in January, but next year they could be performed in August due to for example a planned shutdown. If the time period is set to 24 months moving average, all test data for the last year will be included. Also, having a table as presented in figure 28 presenting the test performed the last 12 months, will give additional useful information regarding tests performed recently.

To deal with safety critical equipment where only a few tests are performed yearly, formula 5.5 should be used. By using the Bayesian approach and assuming that the equipment performs as expected (e.g. 2% failure rate), one could “build in” some history in the model.

Using the rules suggested above, the results for March 2011 will be presented as a yellow status light and a red trend. Meaning that the failure rate is above the requirement (calculated as 1,1), but not significantly different. The trend shows that failure rate has increased the last 24 months compared to the historical values (calculated as 444% higher). This has been calculated for several time periods and all result are meaningful according to the graph presented in figure 27. Calculations are presented in appendix G.

When presenting the reported data in the barrier KPI model it should be as following:

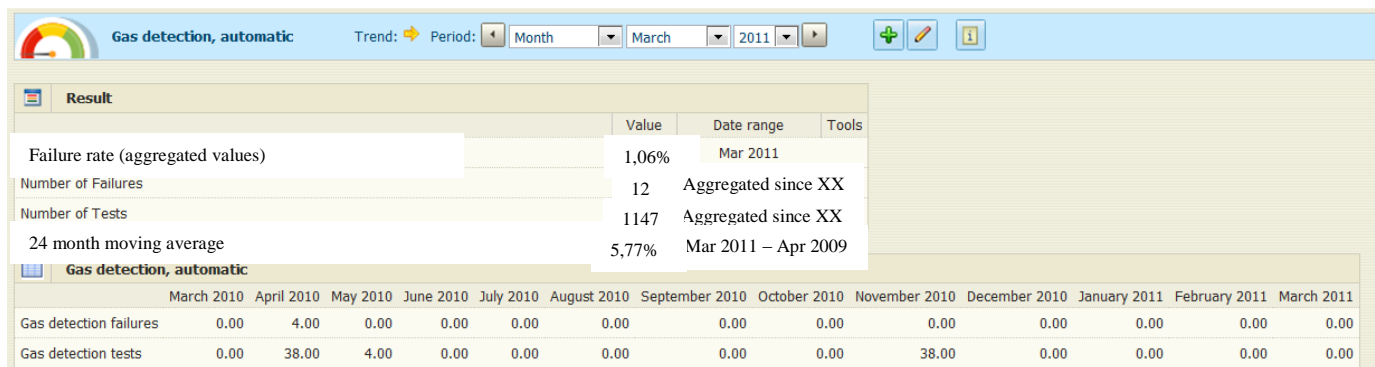


Figure 30: Status Gas detection

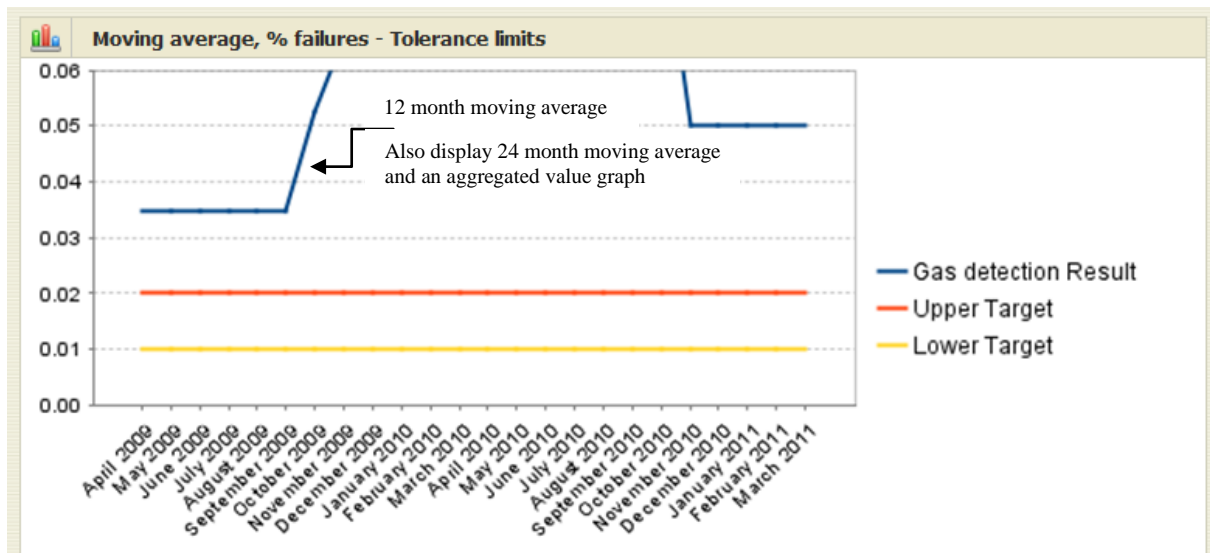


Figure 31: Presentation graph

This is one way to present the reported data that gives a more “correct” comparison with the requirement, and also allows for revealing a negative trend in the last reporting period. The interpretation of status and trend are not altered, which is a good thing since the model is already implemented. It is important that there is a certain continuity in the interpretation through the model (reactive barriers compared with proactive and management elements). Several other ways to present the data were evaluated, but overall, the method suggested in this chapter is recommended. The reason for this is given in chapter 6.

## Chapter 6. Discussion

### 6.1 Discussion

Discussing indicators in the abstract is not necessarily productive. When representing the theory there was a lot of discussion regarding barriers and indicators, whether or not they are leading/lagging indicators or what to call a barrier, reactive or proactive? The differences between safety and risk indicators were also discussed. There is no such thing as a universal model or method for the development of indicators. Perhaps the use of several methods will provide the best result – the most appropriate set of indicators, mixing barrier indicators, safety indicators and risk influencing factors. To quote Benjamin Franklin <sup>[20]</sup>:

*“For the want of a nail, the shoe was lost; for the want of a shoe the horse was lost; and for the want of a horse the rider was lost, being overtaken and slain by the enemy, all for the want of care about a horseshoe nail.”*

This saying should be kept in mind. Not everything is straight forward, but the aim must be to get something done, learn and then make improvements. This has been the main strategy when writing this report; to make improvements and get one step further. But it is important to keep in mind that the road is long and that afterwards, there will be several steps to walk. It is better to try and fail, rather than not try at all. As a company, Gassco needs a full overview of the barrier function within their area of responsibility. They developed a model with the aim to fulfill their needs. It can be discussed if the barriers are put in the right category, and whether or not is it right to call it a barrier KPI model when it displays both barriers, risk influence factors and safety indicators. Gassco decided to act instead of using an amount of time discussing what is theoretically right to call an indicator. The practical results have been good according to persons who are using it in their daily work. Now that some experience has been gained with the model it is easier to see where improvements could be needed.

It is important to emphasize that indicators used only in terms of the data gathered and put on display boards and presented in management briefings, do not represent any meaningful use of indicators.

Going through several accidents that occurred in the period 1998 – 2010, it is inevitable to ask why the industry does not learn from previous major accident. Clearly they do not. If they had, the signs of equality would not have been so distinctive. One might say that choosing other major accidents in the period, such as Ghislenghin 2004 (explosion in gas pipeline, 24 killed and 122 injured) or Mexico 2010 (explosion oil pipeline, 27 killed and more than 50 injured), could have given other lessons to learn. But due to available time when writing this assignment a selection had to be done. If 7 major accidents, all have several of the same root causes, one could assume that there is a pattern in the challenges in the industry. Accidents chosen are from the western part of the world, due to the fact that they have several similarities in the legislation, economic situation, security and the safety work. But these parameters will also vary between the different countries in the western world, and they will in some degree affect the safety level at a given installation. Also the leadership culture plays a role in the safety work. As of today the leadership style in Norway is to have a high focus on safety issues. As shown in several of the accident mentioned in this report, some leadership styles were undermining the knowledge and advices from the staff regarding maintenance

issues (Longford). This leader mindset contributes to a very dangerous leadership style, and it should not be present in an organisation dealing with transportation of hydrocarbons. If the key element deference to expertise had been present at Longford, maintenance on the valve had been prioritized. So leadership style and culture within each country are also important parameters that increase/decrease the risk of having a major accident.

Lesson learned from the Longford accident, which have been published and also have circulated around the oil and gas industry via email, is<sup>[50]</sup>:

- reliance on lost-time injury data in major hazard industries is itself a major hazard
- systematic hazard identifications are vital for accident prevention
- corporate headquarters should maintain safety departments which can exercise effective control over the management of major hazards
- frontline operators must be provided with appropriate supervision and backup from technical experts
- routine reporting system must highlight safety-critical information
- maintenance cutbacks foreshadow trouble
- companies should apply the lessons from other disasters.

These are some of the lessons that BP needed to learn to avoid the Texas City accident. Excerpts from lessons from Longford circulated within BP and specifically at Texas City on various occasions <sup>[50]</sup> still they failed to learn the lesson. An organisation has no memory, and the persons within it failed to learn.

When evaluating Gassco`s barrier KPI model, there was a gap between the lessons learned from previous major accidents and the indicators already implemented in the model. One might say that what has occurred in the past, does not necessarily say something about what might be expected to occur in the future. But going through the major accidents, history shows that some issues are repeated. Still, there could be problem areas that have not been pointed out by going through the history. In this report, the focus area has been to try to learn from previous major accidents, and no effort have been put in trying to predict what might go wrong in the future. Technical causes vary from one accident to another, but the organisational failures are often the same. These organisational failures need to somehow get the attention from the management. To decrease the gap, some indicators are suggested implemented in chapter 4.6. A way to achieve management focus in the Gassco organisation, is a new indicator at the barrier KPI chart, that reflects the status of management elements at Gassco Bygnes. This indicator does not cover all areas that need management focus. In appendix D a long list of indicators suggested by the HSE in the UK is presented. Only four indicators are suggested implemented in the barrier KPI, but the list represented in appendix D contains several more. The reason for leaving most of them out, is that the indicators implemented in the barrier KPI should give meaning and be useful for the management when making important decisions. It is better to start with implementing some few indicators and gain some good experiences with them, rather than implementing a lot of indicators which does not necessarily give meaningful and crucial information to the management. Several of the suggested indicators in the appendix are already implemented in Gassco as a requirement. An audit should be performed to secure compliance with the requirements rather than implementing an indicator which will be green most of the time (due to the requirement). Also, if there are too many underlying indicators, an aggregation in the model could result in that important information is not highlighted enough. The outcome of the indicator must give



meaning. A number saying that all procedures are up to date (100%) does not give anything except perhaps a "false" safety feeling, thinking that everything is okay regarding this subject. But the indicator does not say anything about the quality and whether or not the employees act in accordance to the procedures. So a green indicator on the subject procedures might result in that the management relaxes while believing that everyone in the organisation acts in compliances with prevailing procedures. In the same way that an indicator stating the number of audits performed up against target, or number of audits performed with a good score, does not say anything about the quality of the audit. To quote E. Deming "you can expect what you inspect" [28].

The first step taken in the barrier KPI regarding management elements at Bygnes, is to have some indicators saying something about the safety culture, ongoing initiatives, maintenance management and exceptions on safety critical equipment. These are proposed because they will give the management useful information as soon as one start to report on them. The result can be used when making decisions regarding budget cost and whether or not a upgrading project is needed. Several of Gassco's installations are old and ageing is a challenge. There are without doubt several other indicators that also could be implemented, but it is not desirable to implement to many indicators all at once. If experience shows that the indicators implemented are useful, it is easier to get the approval for implementing several indicators. If they are not useful, the need for several indicators might not be present. The suggested indicators require that actions are taken to get good measurements (develop a good survey, list exceptions', make limits etc.). This is also one reason to start with a few indicators - it makes the job manageable. All indicators suggested will provide useful information to the management when trying to decide on further initiatives/projects and budget cost. A good experience with these indicators can motivate the management to implement several indicators as the next step.

Areas such as supervision/monitoring, policies and procedures, communication and training are not covered by implementing the indicators suggested in chapter 4.6. Implementing an indicator to help focus on management elements at a high level in the Gassco organisation, is not enough to learn the lesson from other major accidents. Data provided by indicators itself does not provide improvements in safety. It is the quality of the management system that is important. Earlier in this report it was mentioned that "*You can't manage what you can't measure,*" [28]. It is said that this is an incorrectly quotation of William E. Demning [28]. In fact, Demning stated that one of the seven deadly diseases of management is running a company on visible figures alone. Many people in the oil and gas industry believes that you cannot manage what you cannot measure. Demning was an American statistician, professor, author, lecturer and consultant. Demning realized that not everything of importance to management can be measured [28]. But one still has to manage those important things. What is the benefit of spending \$20,000 in training 10 people in a special skill? Probably one will never know this accurate, because one will never be able to measure it precisely. But it is done because it is believed that it will pay off some day. Among other things, Demning said that "*The worker is not the problem. The problem is at the top! Management!*" [74]. It is the management's job to direct the efforts of all components toward the aim of the organisation. The first step is clarification: everyone in the organisation must understand the aim, and how to direct his efforts toward it.

It requires a motivation and an understanding for the organisation to be seeking opportunities for improvements. More work than just implementing a new indicator is needed to ensure that

the lessons from previous major accidents are learned. Working towards being a high reliability organisation will improve the focus regarding management elements and organisational issues. The nuclear industry works with human factors differently than done by the oil and gas industry today, as described in chapter 4.7. Human error can occur at every stage in the life of an installation, and a variety of methods must be used to detect and prevent it. Some arguments for why the oil and gas industry should rethink their approach to human factors are presented in the following sections.

The characteristic of a high reliability organisation are that it is sensitive to operations, reluctant to simplify, preoccupied with failure and deference to expertise and resilience. In the oil and gas industry some of these elements are present, such as preoccupation with failure, but other areas such as reluctance to simplify, is one area where the industry seems to fail. In investigation reports the underlying causes are often set to be unqualified staff, inadequate training or communication failure, without asking the question why the staff is unqualified or why the communication fails. Leaders and staff in the oil and gas industry must have constant awareness of that system and process risks can be prevented. To gain reliability, leaders need to listen to the advices given from the employees that are experts on the process equipment. Knowledge in the company must not be restricted due to the hierarchy. Training leaders and employees so that they know how to act in abnormal situations, is crucial. Lessons must be frequently repeated. If the oil and gas industry had worked consistent as an high reliability organisation, some of the underlying causes in the accident described in this report would not be present. As an example; if the management at Longford had shown deference to expertise a critical valve would have been maintained and could have been operated automatically. Further, if the management at Texas City had asked why the operators at Longford lacked training and why they did not understand the risk involved with the process, they could have trained their own employees better. This could probably have changed the outcome of the event at Texas City 2005.

When discussing high reliability organisations after going through the accidents described in this report, one question that reveals itself is: what about organisational redundancy? Is it possible to build an organisation with established interactions, which makes the organisation capable to perform tasks more reliable than one single person could? In the oil and gas industry organisational redundancy is created when employees consult, check and correct each other. As of today there is no good method to evaluate to which extend people could function like an independent. For example could strong dependencies come into being, if several operators share the same incorrect mental model of a system, or if a technical barrier and an operator make use of the same incorrect information. In high reliability organisations they are aiming for an overlap with personnel. Personnel have the same competence and work tasks. The overlap is due to the believe that humans will fail eventually. An overlap increases the probability that the failure will be discovered and corrected before an accident occurs. To gain such organisational redundancy, both structural and cultural conditions in the organisation must be open for mutual correction of error.

The Management regulation states that there should be independency between barriers. In the industry the term barrier is traditionally used of technical barriers. But with basis in the description of previous major accidents, one could argue for that employees in practice often function as barriers. As a result, human factors play a significant role in supporting installation safety and providing defence in depth (several layers of barriers). Permit to work and safe job analysis are good initiatives that contribute to an increase in the safety level. But

the need for a safe job analysis could be restrained due to work pressure. The work with human factors requires continuous focus from the management. The most important factor is to build a good safety culture within the organisation.

Communication failures are implicated in every disaster. There is always information somewhere in the system, which, if responded to appropriately, would have averted the disaster. Effective communication is an important element of any safety management system. Another organisational issue which is hard to measure, safety culture, is also implicated in every disaster. If culture, understood as mindset, is to be the key to preventing major accidents, it is management culture rather than the culture of the workforce in general which is most relevant. The management mindset must be that every major hazard should be identified and controlled, and management should be committed to make available whatever resources necessary to ensure that the workplace is safe. Safety culture must be built from the top of the organisation and downwards. The major accident history shows that the industry fails to learn how to ensure good communication and to build a good safety culture. Perhaps the keyword here is learning. It seems like it is taken for granted that everyone knows how to communicate and how to behave to ensure a good safety culture. Especially the management, which is well educated and are intellectual people. One might think: of course they know how to communicate and how to behave. But how can people know something that they have not learned? It is written several books on communication in practice<sup>[75][76]</sup> and culture knowledge in organisations<sup>[77][78][79]</sup>, but these books are commonly used in educations other than engineering, such as for instance social workers, teachers, psychologists and sociologists. Looking at a plant as a society the employees have to communicate clearly and directly (like social workers), the engineer has to teach, both expressed orally and in writing (like teachers) and the management must keep the organisation on the right track, and understand the risks and build a good and safe culture (like a psychologist "programs" people and helps in building a new way of life). All should learn how to fulfill their tasks the best way possible. Professor Andrew Hopkins, which has an undergraduate Science Degree and a Masters in Sociology<sup>[80]</sup>, has written some very thorough books about the Longford and Texas City accident regarding human and management failures. For Hopkins, it is evident what causes the accidents because he has been educated in understanding humans and organisations. The oil and gas industry is a highly developed technological industry. But perhaps it lacks knowledge in how to effectively communicate in writing and oral, how to make people behave in a safe manner and how to build a good safety culture? Engineers are not educated in these things.

When evaluating suggested indicators from the report published by HSE<sup>[6]</sup>, the need for a designated champion to help manage human performance risk, are underlined (ref. chapter 4.6). The suggestion is that each plant/project should have a 'human factors manager' rather than just implementing an indicator. This person should provide expertise in oral and written communication and teach engineers and managers the importance of getting this part of the job right. The nuclear industry has already started implementing a 'human factor specialist'. In some countries, a human performance evaluation specialist is responsible for the analysis of unplanned reactor events, and for making recommendations to correct the root causes of human performance problems.

The triggering cause in a major accident is most likely to be an Operator error, often connected to a physical/instrumentation failure. In the nuclear industry, more and better training of abnormal situations for the Operators in simulators is recommended. Also, a better

analyse of selected important events in the incidents report, is recommended. The conclusion is that this will help to prevent human errors repeating themselves. This should also be done in the process industry. Better training is also one of the key elements in a high reliability organisation. Implementing required simulator training would help preventing human error in repeating themselves. If an abnormal situation occurred in the process, the Operators would be trained and better prepared to handle the situation. Also, it would be easier for the Operators to discover signs of something wrong if they have been trained in the importance of awareness.

Audits were carried out prior to the accidents mentioned in this report. But usually there were no serious findings. Is a large scale audit which fails to uncover problems a credible audit? No, and a lot of effort must be put into training personnel and to choose the right persons to perform an audit. Perhaps there should be a qualification requirement for the audit personnel regarding the subject they are going to verify? This could increase the quality of the audit performed, which is a very important tool in the work done to prevent major accidents. There should at least be a quality check of the audits performed, for example spot checks.

The barrier KPI model is a tool to help the management with the motivation and the understanding of the importance of barriers. And what is good about the barrier KPI model is that it involves several people in Gassco's organisation. The employees that follow up the daily work at the different installations are made accountable for the status at the installation. Further the different directors are made responsible for the installations within their portfolio. Making employees accountable and combine it with management focus, makes things happen and hopefully ensures a good quality in the reporting. The barrier KPI helps manage important safety critical barriers. If the indicators suggested in this report regarding management elements are implemented, the gap between lessons learned from previous major accidents will decrease. But there will still be a gap. The need for more focus on human factors and the safety culture in the oil and gas industry are also needed. Trying to measure human and organisational factors creates many discussions. Some believe it can be done, while others do not believe that it is possible to measure human and organisational elements, and that relying on KPI's could be dangerous. One thing everyone agrees upon is that a good safety culture is important to maintain a high level of safety. Initiatives that can contribute to increase the safety culture will also increase the reliability of human and organisational barriers. A good safety culture is crucial in a high reliability organisation. The barrier KPI model contributes to a better safety culture within the organisation, due to increased focus on important barriers.

A lot can be learned from the way the nuclear industry handles this issue. When investigating an incident, more effort should be put in mapping out the human failures. By having a person in the organisation dedicated to work with human failure and safety culture, it would also be easier to quantify the possibility of human failure in a more dynamic version of the QRA model. A register of human failure and the cause of them should be developed within Gassco's portfolio. This has already been done in the nuclear industry.

For the barrier KPI tool to be useful in the organisation, Gassco should also work constantly with the high reliability organisation principles; sensitivity to operations, reluctance to simplify, preoccupation with failure, deference to expertise and resilience. To achieve more focus on human factors Gassco should learn by the nuclear industry and start to work more goal-oriented with this subject. A way to start is to dedicate the work to someone how could

be a 'human factor manager' in the company. This is a way to start a more goal-oriented, efficient and structured work with human and organisational barriers. Experience data regarding human factors and failures should be registered, and the use of human factor analysis in project and operation should be used more consistent. Making one person responsible for human and organisational elements in the company would be one initiative that shows that the learning's regarding management elements are taken serious, and that time and resources are set ensure implementation of it.

Another question is whether or not the barrier KPI model can further on be developed to say something about the risk in Gassco's portefolio. Neither the barrier KPI model or the way QRA analysis are performed as of today gives a "dynamic picture" of the risk level at a given installation. But both the barrier model and the QRA analysis provide useful information regarding the risk at a given installation. The barrier KPI model could be made more sensitive to reflect the risk level by giving important barriers a higher weight, or the influence on the risk level could be highlighted in some other way. But the barrier KPI does not show dependencies, and at some installations, reported data on important barriers, such as ignition source control, are missing due to insufficient labeling of equipment. Even though there is no input data on a barrier, it could be a very important barrier. If it is not present in the barrier KPI model their impact on the risk level would not be reflected. Also, for example the blowdown system could be rated high due to the fact that it could prevent escalation. But if the gas detection alarms functions, people inside the installation have evacuated, reducing the fatality consequences. The barrier KPI model also has its limitations due to the program used to present it. As learnt from the nuclear industry the risk level could be monitored more actively than done today in the oil and gas industry. Gassco is already one step closer to a more dynamic QRA model due to the barrier KPI model. Due to several aspects mentioned, it seems more adequate to develop a new model aiming for representing the risk picture at any time at an installation.

A solution could be to combine the information gained in the barrier KPI model with the QRA analysis already present and develop a new more "dynamic" QRA model as suggested in chapter 5.3. This will give several more benefits for Gassco: allow for planning of coming outages, long-term follow up of risk profile and evaluation of disturbances and failures as well as experienced feedback. Results from this model could easily be used to develop a risk indicator based on the same principle used in the barrier KPI. The risk indicator could show % increase/decrease in the risk level compared with the previous period, and whether or not the level is acceptable. This will give the management and board a fairly representation of risk within Gasscos portefolio. The risk indicator and the barrier KPI will become very dependent of each other. If the risk level increases this will be reflected in the barrier KPI model – a lot of barriers will become red. By continuous work with maintaining the barriers, the risk indicator will be at an acceptable level. It is important to be aware of that if important safety critical barriers are not included in the barrier KPI indicator, failure and the effect on the risk level will be harder to reveal. Yet an argument for getting all installations to implement all indicators. Some of Gassco's installations have not implemented the ignition source indicator due to inadequate labeling of equipment, which make it hard to figure out the failure rate based on performed tests. But as shown in previous chapter, ignition source control is an important barrier and plays a significant role in the risk level at a given installation. Based on this, effort should be made to implement this indicator at all Gassco's installations. Reasons for why indicators are not implemented should be argued for and documented. Perhaps emphasising at each installation which important barrier indicators that are "missing" would

motivate the management to get the indicator implemented. But experiences have shown that it is not always very easy to get the right data input into the model. It is important that the data reported into the model is good and in accordance with the specification, or else the model will lose its credibility. This is also one reason why it is not desirable to implement many new indicators regarding management elements all at one.

The new QRA model must take into account dependencies and changes in failure rate regarding barriers and human/organisational values. By implementing several management elements in the barrier KPI model, a lot of information could be gained directly from here. By having a person responsible for the human and organisational factors in the organisation, this person will gradually gain experience and could evaluate the input data to the dynamic QRA model. Also, developing a database with experience data on human factors would simplify this work. The largest challenge will be to build the new "dynamic QRA" model. But it is possible and a lot can be learned from the nuclear industry. By starting to develop this model Gassco will add another aspect to risk management in the oil and gas industry and utilize the barrier KPI model for all it is worth. Since Gassco is a relatively young company and their responsibility increases gradually, it would be very useful to start working on a human factor database and a new dynamic QRA model as early as possible in Gassco's operating time. One motivation for starting to work on a more dynamic QRA model is that PSA has requested the industry to conduct risk analysis and use the results more efficiently<sup>[81]</sup>. This request makes development of a new QRA model and a risk indicator a natural step for the barrier KPI indicator. The way QRA's are used in the industry as of today simply is not sufficient enough compared with the potential of a QRA. And if it has been done in the nuclear industry, there is no reason for why it should not be done in the oil and gas industry. After all, a lot of money is spent on performing QRA's, but the benefit is small compared to the potential. There are several reasons for starting this work, but two arguments that should be heavily weighted are: It will be a natural step to further improve the risk management and risk communication in Gassco, and the Authorities have requested a more efficient use of the QRA<sup>[81]</sup>.

Data reported into the model needs to be presented in a suitable way. As of today the reactive elements in the model are presented as a 12 months moving average. This solution brings some challenges such as; few test data gives a high failure rate when the equipment fails, equipment history is lost and the fact that the calculated failure rate could actually be acceptable if seen over a long time period. There are several ways to present the data; increase time period for the calculated average, display time period between each failure, display failure reported last test month etc. It is important that the data presented in the Barrier KPI model gives the "right" picture of the condition of the safety critical equipment. The suggested method in chapter 5.3 (aggregate the reported data), makes the failure rate more comparable with the requirement than the 12 months moving average. Using the Bayesian approach and formula 5.5, helps present the failure rate more correctly when few tests are performed yearly (by assuming that the equipment is performing as anticipated, history is built in to the model). By using the trend description to show how the failure rate has developed the last 24 months, ensures the sensitivity in the model. When the results for the last 12 months are presented as well, it is easy to find out when the failure(s) occurred. Using the same trend description as earlier (10% increase/decrease), it will be easy for the users to adjust to the changes. The suggested changes seem to be an improvement of the model without large changes in the model setup or presentation. It is of importance that the ones making decision based on the reported failure rate get the right impressions regarding the safety critical equipment conditions.

The other limits in the model are presented as a 12 months moving average (proactive and management elements), and are not evaluated in this report. The reason for this is that they are presented as a number and the requirements are not connected to a probability distribution. So whether or not they are presented as a 12 months moving average or a monthly value, is more or less a question of what is desirable.

Summing up the discussion, it is clear that more work regarding the management elements is needed in Gassco, but it does not seem like this could be achieved only by implementing some new indicators in the barrier KPI model. The model can be used to increase the focus, and management elements at Gassco Bygnes should be represented in the model due to the fact that the work done by the management is crucial in the work done to prevent major accidents. Other areas also need to be further developed when it comes to human factors and the way QRA's are used as of today. A lot can be learned from the nuclear industry regarding this. Also, implementing the five key elements of a high reliability organisation will increase the level of safety within Gassco's organisation. Some changes in the way the failure rate in the model is presented must be done to give a more fair comparison to the requirements. Suggestions for further work, not only for the barrier KPI model, but how to ensure learning from previous major accidents, are suggested in the next chapter.

## 6.2 Suggestions for further work

Suggestion on how to further develop the barrier KPI model and also how to ensure learning from previous major accidents:

- develop an HSE climate survey which is suitable for all employees in Gassco's organisation. The survey should be developed in such a manner that if a person is responsible for safety critical equipment/tasks, additional questions could be added
- implement a new overall indicator for Gassco Bygnes, representing several management elements that seems to be repeated in the major accident history, suggestions are made in chapter 4.6. All indicators should be discussed in a work shop held in Gassco
- if the indicators implemented in the overall indicator for Bygnes give valuable information after some experience has been made, effort should be made to implement several of the indicators at installation level. New indicators in the Gassco Bygnes indicator should also be assessed
- decide on a `human factor manager` in the organisation/at the installations/in projects, which is given the opportunity to learn and become an expert on human errors, oral and written communication and the function of organisations
- develop an overview of human failures in Gassco's portofolio. Reference is made to the database developed by NRC: Human Factors Information System (HFIS). This is a database which stores information about human performance issues
- establish a project and start trying to develop a more "dynamic QRA" model, or join other research studies which are working on a more dynamic QRA model.

Suggestions mentioned above are based on the evaluations and work done in this report.

## Chapter 7. Conclusion

This report is the result of the evaluation of Gassco's barrier KPI model. When evaluating the model, the aim was to answer three questions:

1. Does Gassco's barrier KPI reflect learning from recent major accidents, or should more indicators be included in the model?
2. Do changes in the barrier KPI model equal changes in the risk level?
3. Is the information regarding failure rate in the model presented in an adequate way?

By studying several major accidents that occurred recently, some gaps between lessons learned and indicators that are implemented in the barrier KPI model as of today, are exposed. Since the management in Gassco is located at Bygnes, a new indicator containing management elements at Bygnes, is suggested implemented in the barrier KPI model. Gathering all initiatives done to prevent a major accident could result in better motivation for "getting the job done". The indicator will visualise the importance of the management elements and the work done at Bygnes to prevent major accidents. If the experiences made with the new indicators are good, Gassco should aim for implementing several of them at installation specific level. Some indicators are suggested in chapter 4.6 to reduce the gap, but the solution is not only to implement some new indicators. More work has to be done. Summing up, it is all about improving the safety culture in the organisation. People are affected by culture. One person should be dedicated the role as "human factor manager" or something more suitable, and continuously work with this subject. Also an experience database regarding human factors should be built. References are made to the way the nuclear industry is handling organisational and human factors, presented in chapter 4.7. Gassco should work continuous with the five key elements of a high reliability organisation, and a lot of learning could be achieved by studying what has been done in the nuclear industry through the years.

The barrier KPI model should be kept as an indicator of the state of the barriers within Gassco's portfolio. To achieve a more "dynamic" status on the risk level, the QRA model should be further developed to become a more "dynamic QRA model". References are also here made to the nuclear industry, chapter 5.3. This model would benefit from the effort put down when developing a database regarding human factors and the barrier KPI model. When the model has been built, a natural step further would be to develop a risk indicator. This indicator will become closely linked to the barrier KPI indicator, and together they will provide very useful information to the management and board when trying to manage risk. A risk graph to use in daily operation and projects could be one outcome from the new QRA model. Suggestion to such a process is illustrated in chapter 5.3. There are several reasons for starting this work. One is that it will be a natural step further to improve the risk management in Gassco. The fact that the Authorities has requested a more efficient use of the QRA is also a weighty argument.

If the data in the barrier KPI model shall be used further for analysis, it is important that the failure rate is presented fairly compared to the requirements. The 12 months moving average used when representing status on reactive elements as of today, is not suitable. One fair way to present the data, due to the fact that the requirements are set based on an infinitive amount of tests, is to aggregate all reported figures and use the Bayesian approach. To maintain the sensitivity in the model, the trend arrow could be used to measure the failure rate the last 24



months up against the aggregated value. This would reveal if the failure rate in the last time period is worse, more or less the same or better than the aggregated value.

Some of these conclusions can be handled short term, such as changing the presentation of the failure rate and start the work with developing and implementing new indicators. The benefit of having a `human factor manager` and the effort put down in developing a new QRA model and a risk indicator must be seen in the long term. Management elements, including human factors, are very important areas when working with the prevention of major accidents, and effort must be put in handling this subject efficiently. Lessons from other industries shows that this could be done through continuous and hard work, combining knowledge from several aspects, both regarding technical and non technical issues. It is also important with innovative work, and the time has come to further develop the existing QRA model in the oil and gas industry. By doing this, risk management in the industry will improve.

## Chapter 8. References

1. CONOCOPHILLIPS 2009. Krav til tekniske vedlikehold av utvalgte sentrale barrieresystem. Stavanger: ConocoPhillips.
2. SKLET, S. 2006. Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries*, 19, 494-506.
3. 2011. *Cumulative risk* [Online]. Available: [http://wiki.answers.com/Q/What\\_the\\_definition\\_of\\_cumulative\\_risk](http://wiki.answers.com/Q/What_the_definition_of_cumulative_risk) [Accessed 2011.05.21].
4. 2011. *Deterministic risk assessment* [Online]. National agricultural library. Available: <http://agclass.nal.usda.gov/mtwdk.exe?k=default&l=60&w=137442&n=1&s=5&t=2> [Accessed 2011.05.21].
5. RASMUSSEN, O. 2011. Safety critical failures. Bygnes,: Gassco AS.
6. ENERGY, I. 2010. Human factors performance indicators for the energy and related process industries. ISBN 9780852935873. 1 ed. London,: Energy institute.
7. 2011. *Indicators* [Online]. Available: <http://www.businessdictionary.com/definition/indicator.html> [Accessed 2011.05.21].
8. STOKKE, A. & ENEGEBRETHSEN, E. 2009. Barrier indicators. 1 ed. Høvik: Det Norske Veritas AS.
9. 2011. *Non conformity* [Online]. Praxicom. Available: <http://www.praxiom.com/iso-definition.htm#Nonconformity> [Accessed 2011.05.21].
10. 2011. *Proactive* [Online]. Farlex. Available: <http://www.thefreedictionary.com/proactive> [Accessed 2011.05.21].
11. 1991. *Kvalitetssystemer: NS-ISO 9000 serien*, [Oslo], Forbundet.
12. 2011. *Probabilistic risk assessment* [Online]. Wikipedia. Available: [http://en.wikipedia.org/wiki/Probabilistic\\_risk\\_assessment](http://en.wikipedia.org/wiki/Probabilistic_risk_assessment) [Accessed 2011.05.21].
13. NORSOK, S. 2002. *Health, Safety and Environment (HSE) in construction-related activities S-012*, Lysaker, Standard Norge.
14. NORSOK, S. 2010. *Risk and emergency preparedness assessment*, Lysaker, Standard Norge.
15. 2011. *Seveso plant* [Online]. European environment agency. Available: [http://glossary.eea.europa.eu/EEAGlossary/S/Seveso\\_plant](http://glossary.eea.europa.eu/EEAGlossary/S/Seveso_plant) [Accessed 2011.05.22].

16. 2011. Qualitative and qualitative thinking [Online]. Monash university. Available: <http://www.csse.monash.edu.au/~smarkham/resources/qual>. [Accessed 2011.05.22]
17. HOLLNAGEL, E. 2008. Risk + barriers = safety? *Safety Science*, 46, 221-229.
18. ØIEN, K., UTNE, I. B. & HERRERA, I. A. 2011a. Building Safety indicators: Part 1 - Theoretical foundation. *Safety Science*, 49, 148-161.
19. KJELLÉN, U. 2009. The safety measurement problem revisited. *Safety Science*, 47, 486-489.
20. WREATHALL, J. 2009. Leading? Lagging? Whatever! *Safety Science*, 47, 493-494.
21. 2011. *Lagging indicator* [Online]. Investopedia ULC. Available: <http://www.investopedia.com/terms/l/laggingindicator.asp> [Accessed 2011.05.22].
22. 2011. *Leading indicator* [Online]. Investopedia ULC. Available: <http://www.investopedia.com/terms/l/leadingindicator.asp> [Accessed 2011.05.22 ].
23. HOPKINS, A. 2007. Thinking about process safety indicators. Australia: National research center for OHS regulation, Australian National University.
24. HALE, A. 2009. Why safety performance indicators? *Safety Science*, 47, 479-480.
25. HSE 2006. Developing process safety indicators: a step by step guide for chemical and major accident industries. London: UK Health and Safety Executive, HSE.
26. HALE, A. 2009. Special Issue on Process Safety Indicators. *Safety Science*, 47, 459-459.
27. 2011, *Leading, lagging and coincident indicators* [Online]. Investopedia ULC. Available: <http://www.investopedia.com/ask/answers/177.asp> [Accessed 2011.05.22].
28. 2011, *Deming, Edward* [Online]. Wikipedia. Available: [http://en.wikipedia.org/wiki/Edward\\_Deming](http://en.wikipedia.org/wiki/Edward_Deming) [Accessed 2011.05.22].
29. ØIEN, K., UTNE, I. B. & HERRERA, I. A. 2011. Building Safety indicators: Part 1 - Theoretical foundation. *Safety Science*, 49, 148-161.
30. ØIEN, K., UTNE, I. B., TINMANN SVIK, R. K. & MASSAIU, S. 2011b. Building Safety indicators: Part 2 - Application, practices and results. *Safety Science*, 49, 162-171.
31. ØIEN, K., UTNE, I. B., TINMANN SVIK, R. K. & MASSAIU, S. 2011b. Building Safety indicators: Part 2 - Application, practices and results. *Safety Science*, 49, 162-171.
32. VINNEM, J. E. 2010. Risk indicators for major hazards on offshore installations. *Safety Science*, 48, 770-787.

33. ØIEN, K. 2001. A framework for the establishment of organizational risk indicators. *Reliability Engineering & System Safety*, 74, 147-167.
34. VINNEM, J. E. 2007. *Offshore Risk Assessment: Principles, Modelling and Applications of QRA Studies*, London, Springer-Verlag London Limited.
35. 2010, *Risikostyring, terminologi*, Lysaker, Standard Norge.
36. 2010, *Risikostyring: prinsipper og retningslinjer*, Lysaker, Standard Norge.
37. AVEN, T. 2010. *Misconceptions of risk*, Chichester, Wiley.
38. AVEN, T. 2006. *Pålitelighets- og risikoanalyse*, Oslo, Universitetsforl.
39. MOSTAD, P. 2005. *Bayesiansk statistikk* [Online]. Oslo: Oslo University. Available: [http://docs.google.com/viewer?a=v&q=cache:1-BHJOFU0OAJ:www.uio.no/studier/emner/medisin/helseadm/HSTAT1101/h05/undervisningsmateriale/Forelesning9.ppt+petter+mostad+bayesiansk+statistikk&hl=en&pid=bl&srcid=ADGEESiGBpu90rZTzqU2rrw\\_Arx4b3WgWW\\_Z\\_iGJgJ5XYdP\\_IUhO\\_gF6tc4I3xeZH5F1\\_Mmk3aLl-U2wpvKGw9vomlMhfGULjyQVRPk5qRsSU3iUWtbp7Fw-tCddvY-\\_iCYkYrVBMP7A&sig=AHIEtbSj763ZGhxeWUHjwzSmcPQXfGeLKg](http://docs.google.com/viewer?a=v&q=cache:1-BHJOFU0OAJ:www.uio.no/studier/emner/medisin/helseadm/HSTAT1101/h05/undervisningsmateriale/Forelesning9.ppt+petter+mostad+bayesiansk+statistikk&hl=en&pid=bl&srcid=ADGEESiGBpu90rZTzqU2rrw_Arx4b3WgWW_Z_iGJgJ5XYdP_IUhO_gF6tc4I3xeZH5F1_Mmk3aLl-U2wpvKGw9vomlMhfGULjyQVRPk5qRsSU3iUWtbp7Fw-tCddvY-_iCYkYrVBMP7A&sig=AHIEtbSj763ZGhxeWUHjwzSmcPQXfGeLKg) [Accessed 2011.05.25].
40. RASMUSSEN, O. 2008. HSE&Q strategic focus. Bygnes: Gassco AS.
41. 2011. *Regulations Petroleum Safety Authority* [Online]. Stavanger: Petroleum Safety Authority. Available: <http://www.ptil.no/lover/category213.html> [Accessed 2011.05.22].
42. ØSTREM, L. 2009. Reporting and follow-up of barrier indicators. Bygnes: Gassco AS.
43. STATOILHYDRO 2009. Experiences pilottest Kollsnes - Barrier Kpi. Kollsnes: StatoilHydro.
44. 2011. *Definition major accident* [Online]. Stavanger: Petroleum Safety Authority. Available: <http://www.ptil.no/major-accidents/major-accident-risk-article4172-144.html> [Accessed 2011.05.22].
45. LEES, F. P. 1996. *Loss prevention in the process industries: hazard identification, assessment, and control*, Boston, Butterworth-Heinemann.
46. KLETZ, T. A. 2009. *What went wrong? case histories of process plant disasters and how they could have been avoided*, Burlington, MA, Gulf Professional Pub.
47. HOPKINS, A. 2000. *Lessons from Longford: the Esso gas plant explosion*, Sydney, CCH Australia Ltd.

48. BARNETT, R. 2006. The Esso gas plant explosion: lessons for forms management. Available: [http://www.conyte.cl/archivos/LONGFORD\\_BFMA\\_2006b.pdf](http://www.conyte.cl/archivos/LONGFORD_BFMA_2006b.pdf) [Accessed 2011.05.22].
49. NASA. 2003. Columbia accident investigation board. Available: <http://caib.nasa.gov/> [Accessed 2011.05.22].
50. HOPKINS, A. 2009. *Failure to learn: the BP Texas City refinery disaster*, Sydney, N.S.W., CCH Australia.
51. BOARD, C. S. 2007. Investigation report refinery explosion and fire. Available: <http://www.csb.gov/assets/documnet/CSBFinalReportBP.pdf> [Accessed 2011.05.22].
52. 2011. *US regulations* [Online]. U.S. government's official web portal. Available: [http://www.usa.gov/Topics/Reference\\_Shelf/Laws.shtml](http://www.usa.gov/Topics/Reference_Shelf/Laws.shtml) [Accessed 2011.05.22].
53. 2010. BP Deepwater Horizon accident investigation report. Available: [http://www.bp.com/liveassets/bp\\_internet/globalbp/globalbp\\_uk\\_english/incident\\_response/STAGING/local\\_assets/downloads\\_pdfs/Deepwater\\_Horizon\\_Accident\\_Investigation\\_Report.pdf](http://www.bp.com/liveassets/bp_internet/globalbp/globalbp_uk_english/incident_response/STAGING/local_assets/downloads_pdfs/Deepwater_Horizon_Accident_Investigation_Report.pdf) [Accessed 2011.05.22].
54. 2011. Deepwater, the Gulf oil disaster and the future of offshore drilling. Report to the president. Available: <http://www.oilspillcommission.gov/final-report> [Accessed 2011.05.22].
55. STATOIL. 2010, Brønnhendelse på Gullfaks C. Available: [http://www.statoil.com/en/NewsAndMedia/News/2010/Downloads/5Nov\\_2010\\_%20Rapport\\_broennhendelse\\_Gullfaks%20C.pdf](http://www.statoil.com/en/NewsAndMedia/News/2010/Downloads/5Nov_2010_%20Rapport_broennhendelse_Gullfaks%20C.pdf) [Accessed 2011.05.22].
56. ETTERLID, H. 2010. Oversender rapport etter tilsynsaktivitet med Statoils planlegging av brønn 34/10-C-06A - aktivitet 001050012 – med varsel om pålegg. Available: [http://www.ptil.no/getfile.php/Tilsyn%20p%C3%A5%20nettet/P%C3%A5legg\\_varsel%20om%20p%C3%A5legg/2009\\_1626\\_Brev%20til%20Statoil%20med%20varsel%20om%20p%C3%A5legg%20-%20planlegging%20av%20br%C3%B8nn%20C-06A%20-%20Gullfaks%20C.pdf](http://www.ptil.no/getfile.php/Tilsyn%20p%C3%A5%20nettet/P%C3%A5legg_varsel%20om%20p%C3%A5legg/2009_1626_Brev%20til%20Statoil%20med%20varsel%20om%20p%C3%A5legg%20-%20planlegging%20av%20br%C3%B8nn%20C-06A%20-%20Gullfaks%20C.pdf) [Accessed 2011.05.22].
57. ANDA, I. 2011.02.10. *Nære på for Gullfaks C* [Online]. Stavanger: Petroleum Safety Authority. Available: <http://www.ptil.no/nyheter/naere-paa-for-gullfaks-c-article7606-24.html> [Accessed 2011.05.22].
58. STANGELAND, G. 2010.11.19. *Ptil refser Statoils egen Gullfaks-granskning* [Online]. Stavanger: Offshore.no. Available: [http://www.offshore.no/sak/Ptil\\_refser\\_Statoils\\_egen\\_Gullfaks-granskning](http://www.offshore.no/sak/Ptil_refser_Statoils_egen_Gullfaks-granskning) [Accessed 2011.05.22].

59. ANDA, I. 2011.03.24. *Petroleumstilsynet (Ptil) ber Statoil om redegjørelse etter granskning på gasslekkasje på Gullfaks B* [Online]. Stavanger: Petroleum Safety Authority. Available: <http://www.ptil.no/nyheter/petroleumstilsynet-ptil-ber-statoil-om-redegjoerelse-etter-gransking-av-gasslekkasje-paa-gullfaks-b-article7729-24.html> [Accessed 2011.05.28]
60. ETTERLID, H. 2011. Gasslekkasje på Gullfaks B 4.12.2010. Available: <http://www.ptil.no/getfile.php/PDF/Ptil%20granskingsrapport-gullfaksB-gasslekkasje.pdf> [Accessed 2011.05.22].
61. PSA. 2009. Kondensatlekkasje på Kollsnes 19.5.2009. Available: <http://www.ptil.no/nyheter/granskingsrapport-etter-kondensatlekkasje-paa-kollsnes-article5814-24.html> [Accessed 2011.05.25].
62. STATOIL 2010. Granskningsrapport - Uønsket hendelse med tjenestebil. Bygnes: Gassco AS.
63. *What is a high reliability organisation?* [Online]. BP. Available: <http://www.sirfrt.com.au/Meetings/IMRt/NSW/IMRT%20NSW%2005%20Jun%200809/050608%20NSW%20IMRt%20HRO%20at%20BP%20Bulwer%20Island.pdf> [Accessed 2011.05.22].
64. 2008. *Becoming a high reliability organization* [Online]. U.S. Department of Health & Human Services. Available: <http://www.ahrq.gov/qual/hroadvice/hroadviceexecsum.htm> [Accessed 2011.05.22].
65. HSE. 2002. Human factors integration: Implementation in the onshore and offshore industries. Available: <http://www.hse.gov.uk/research/rrpdf/rr001.pdf> [Accessed 2011.05.22].
66. 2010, Rapporten fra Risikonivå i norsk petroleumsvirksomhet (RNNP) - 2009. Available: <http://www.ptil.no/nyheter/rapporter-fra-risikonivaa-i-norsk-petroleumsvirksomhet-rnnp-2009-article6812-24.html> [Accessed 2011.05.22].
67. NEA. 1988. *The human factor in nuclear power plant operation* [Online]. Nuclear energy agency. Available: <http://www.oecd-nea.org/brief/brief-02.html> [Accessed 2011.05.22].
68. U.S.NRC. 2011. *Human Factors* [Online]. United States nuclear regulatory commission. Available: <http://www.nrc.gov/reactors/operating/ops-experience/human-factors.html> [Accessed 2011.05.22].
69. CAPPELEN, P. 2008. XXXX Total risikoanalyse - fase 2. Høvik: Det norske veritas.
70. KNOCHENHAUER, M., BAKKEN, B. I. & BAAS L, T. *Process safety, instrumented safety barriers - what can we learn from the nuclear industry?*, Kjeller, Scandpower AS.

71. 2011. *Safety integrity level* [Online]. Wikipedia. Available: [http://en.wikipedia.org/wiki/Safety\\_Integrity\\_Level#SIL\\_in\\_Safety\\_Standards](http://en.wikipedia.org/wiki/Safety_Integrity_Level#SIL_in_Safety_Standards) [Accessed 2011.05.22].
72. OLF. 2001. Application of IEC 61508 and IEC 61511 in the Norwegian petroleum industry. 70. Available: <http://www.olf.no/PageFiles/1213/070%20-%20Application%20of%20IEC%2061508%20and%20IEC%2061511.pdf?epslanguage=no> [Accessed 2011.05.22].
73. FINKELSTEIN, M. 2008. *Failure Rate Modelling for Reliability and Risk*, London, Springer London.
74. DEMNING, E. 1982. *Out of the crisis*, Cambridge, Massachusetts Institute of Technology.
75. KARLSEN, T. 2005. *Kommunikasjon: målstyrt samarbeid og informasjon*, Oslo, Gyldendal undervisning.
76. EIDE, T. & EIDE, H. 2004. *Kommunikasjon i praksis: relasjoner, samspill og etikk i sosialfaglig arbeid*, Oslo, Gyldendal akademisk.
77. BROOKS, I. 2009. *Organisational behaviour: individuals, groups and organisation*, Harlow, Prentice Hall.
78. SACKMANN, S. A. 1991. *Cultural knowledge in organizations: exploring the collective mind*, Newbury Park, Calif., Sage.
79. CRAY, D. & MALLORY, G. 1998. *Making sense of managing culture*, London, International Thomson Business Press.
80. 2011. *Professor Andrew Hopkins* [Online]. Available: <http://www.professorandrewhopkins.com/biography> [Accessed 2011.05.22].
81. PSA. 2011. RNNP 2010: Store utfordringer på viktige områder. Available: [http://www.ptil.no/getfile.php/PDF/RNNP%202010/Pressebrief%2027.4.11\\_.pdf](http://www.ptil.no/getfile.php/PDF/RNNP%202010/Pressebrief%2027.4.11_.pdf) [Accessed 2011.05.22].
82. PSA. 2011. Forskrifter. Available: <http://www.ptil.no/forskrifter/category215.html> [Accessed 2011.06.04].
83. 1999. *Petroleums og naturgassindustri: kontroll og reduksjon av brann og eksplosjoner på produksjonsinstallasjoner til havs : krav og retningslinjer*, Oslo, Norges standardiseringsforbund.
84. 2000. *Guidelines on the application of IEC 61508-2 and IEC 61508-3*, Geneva, International Electrotechnical Commission.

85. HSE. 2005. Public report of the fire and explosion at the Conocophillips Humber refinery on 16 April 2001. Available:  
<http://www.hse.gov.uk/comah/conocophillips.pdf> [Accessed 2011.05.22].
86. DECHY, N., BOURDEAUX, T., AYRAULT, N., LE COSE, J. C. & KORDEK, M.-A. 2004. *First lessons of the Toulouse ammonium nitrate disaster 21st September 2001, AZF plant, France*, Park Alata, INERIS, France.
87. KLETZ, T. 1991. *Plant design for safety: a user-friendly approach*, New York, Hemisphere Publ.
88. 2008. The final report of the Major Incident Investigation Board. 1. Available:  
<http://www.buncefieldinvestigation.gov.uk/reports/volume1.pdf> [Accessed 2011.05.22].
89. 2010. *Buncefield Investigation Homepage* [Online]. Available:  
<http://www.buncefieldinvestigation.gov.uk/index.htm> [Accessed 2011.05.22].



## Chapter 9. Appendices

### A. Regulations

The Petroleum Safety Authority in Norway is the regulatory authority for technical and operational safety, including emergency preparedness, and for the working environment in the offshore industry. There are five regulations which control safety of design and operation of offshore and land based installation<sup>[82]</sup>. There are several sections in the Management regulations that are important, with respect to analysis of risk and barriers. The sections relevant for this report are given in full below:

#### Section 4

##### *Risk reduction*

*In reducing risk as mentioned in 11 of the Framework Regulations, the responsible party shall select technical, operational and organisational solutions that reduce the probability that harm, errors and hazard and accident situations occur.*

*Furthermore, barriers as mentioned in 5 shall be established.*

*The solutions and barriers that have the greatest risk-reducing effect shall be chosen based on an individual as well as an overall evaluation. Collective protective measures shall be preferred over protective measures aimed at individuals.*

#### Section 5

##### *Barriers*

*Barriers shall be established that:*

- a) reduce the probability of failures and hazard and accident situations developing,*
- b) limit possible harm and disadvantages.*

*Where more than one barrier is necessary, there shall be sufficient independence between barriers.*

*The operator or the party responsible for operation of an offshore or onshore facility, shall stipulate the strategies and principles that form the basis for design, use and maintenance of barriers, so that the barriers' function is safeguarded throughout the offshore or onshore facility's life.*

*Personnel shall be aware of what barriers have been established and which function they are intended to fulfil, as well as what performance requirements have been defined in respect of the technical, operational or organisational elements necessary for the individual barrier to be effective. Personnel shall be aware of which barriers are not functioning or have been impaired. The responsible party shall implement the necessary measures to remedy or compensate for missing or impaired barriers.*

The guidelines to the regulations state that barriers as mentioned in the first sub, can consist of either physical or non-physical measures, or a combination. The requirement for independence as mentioned in the second sub, means that it should not be possible for multiple important barriers to be impaired or malfunction simultaneously, e.g. as a result of a single fault or a single incident.

*The NS-EN ISO 13702<sup>[83]</sup> standard should be used for development and stipulation of strategies for risk-reducing measures and functions. IEC 6150884<sup>[84]</sup> should be used for safety systems. In addition, OLF's Guideline 070<sup>[72]</sup> should be used as a basis for offshore petroleum activity.*

Section 6

*Management of health, safety and the environment*

*The responsible party shall ensure that the management of health, safety and the environment comprises the activities, resources, processes and organisation necessary to ensure prudent activities and continuous improvement, cf. 17 of the Framework Regulations.*

*Responsibility and authority shall be unambiguously defined and coordinated at all times. The necessary governing documents shall be prepared, and the necessary reporting lines shall be established.*

Section V in the Management regulation is about analyses and states among other things that:

Section 16

*General requirements for analyses*

*The responsible party shall ensure that analyses are carried out that provide the necessary basis for making decisions to safeguard health, safety and the environment. Recognised and suitable models, methods and data shall be used when conducting and updating the analyses.*

*The purpose of each risk analysis shall be clear, as well as the conditions, premises and limitations that form its basis.*

*The individual analysis shall be presented such that the target groups receive a balanced and comprehensive presentation of the analysis and the results.*

*Criteria shall be set for carrying out new analyses and/or updating existing analyses as regards changes in conditions, assumptions, knowledge and definitions that, individually or collectively, influence the risk associated with the activities.*

*The operator or the party responsible for operating an offshore or onshore facility shall maintain a comprehensive overview of the analyses that have been carried out and are underway. Necessary consistency shall be ensured between analyses that complement or expand upon each other.*

## Section 17

### Risk analyses and emergency preparedness assessments

The responsible party shall carry out risk analyses that provide a balanced and most comprehensive possible picture of the risk associated with the activities. The analyses shall be appropriate as regards providing support for decisions related to the upcoming operation or phase. Risk analyses shall be carried out to identify and assess contributions to major accident and environmental risk, as well as ascertain the effects various operations and modifications will have on major accident and environmental risk.

*Necessary assessments shall be carried out of sensitivity and uncertainty.*

*The risk analyses shall*

- a) identify hazard and accident situations,*
- b) identify initiating incidents and ascertain the causes of such incidents,*
- c) analyse accident sequences and potential consequences, and*
- d) identify and analyse risk-reducing measures.*

*Risk analyses shall be carried out and form part of the basis for making decisions when e.g.:*

- a) classifying areas, systems and equipment,*
- b) demonstrating that the main safety functions are safeguarded,*
- c) identifying and stipulating design accidental loads,*
- d) establishing requirements for barriers,*
- e) stipulating operational conditions and restrictions,*
- f) selecting defined hazard and accident situations.*

*Emergency preparedness analyses shall be carried out and be part of the basis for making decisions when e.g.*

- a) defining hazard and accident situations,*
- b) stipulating performance requirements for the emergency preparedness,*
- c) selecting and dimensioning emergency preparedness measures.*

**B. Indicators in Gassco`s barrier KPI model and aggregation rules**

Category	Indicator	Mathematical description	Comment/failure mode	Tolerance limits		Weight	Data sources
				Lower	Upper		
Preventive barriers	Inspections - Onshore/offshore installations	# of critical obs in period (period = reporting period, normally 30 days)	<p>Critical observation if corrective action is required within 30 days</p> <p>Examples of critical findings:</p> <ul style="list-style-type: none"> <li>- Wall thickness less than code minimum thickness (e.g. ANSI B 31G)</li> <li>- Significant cracks</li> <li>- Loose bolts</li> <li>- Deformations</li> </ul> <p>Several findings on one tag is regarded one finding</p>	Installation specific	Installation specific	NA	SH: RIS/ SAP CP: SAP Gassco: Spreadsheets Total: SAP Centrica: Maximo
	Visual inspection - onshore pipeline	# of critical obs in period (period=reporting period, 30 days)	Overall pipeline condition from Orbit.	Given by Orbit	Given by Orbit	NA	SH: Orbit CP: Orbit Gassco: Orbit Total: NA Centrica: NA
	ROV inspection	# of critical obs in period (period=reporting period, 30 days)		Given by Orbit	Given by Orbit	NA	
	Intelligent pigging (ILI)	# of critical obs in period (period=reporting period, 30 days)		Given by Orbit	Given by Orbit	NA	
Reactive barriers	Gas detection, automatic	# of failures / # of tests	F&G logic does not receive a signal from the detector when tested	1.0 %	2.0 %	2	SH: A10 report/SAP CP: Barrier panel/SAP Gassco: Spreadsheets Total: SAP Centrica: Maximo

## Evaluating Gassco`s barrier KPI model

Ignition Source Control	# of failures / # of tests	1. Switch/ignition source not disconnected 2. Fuel valve for rotating equipment not closed NB! Does not include hot work, car driving and ex equipment.	1.0 % <sup>4</sup>	2.0 %	2	SH: Vary across installations CP: Barrier panel/SAP Gassco: Vary, not tested in Zeebrügge Total: Not reg. tested Centrica: As Total
HVAC	# of failures / # of tests	Damper does not close tight on demand	2.0 %	4.0 %	1	SH: A10 report/SAP CP: Barrier panel/SAP Gassco: Spreadsheets Total: Not regularly tested Centrica: Not regularly tested
ESD - Valves	# of failures / # of tests	The valve does not close on signal within specified time or has a higher internal leakage rate than specified criterion	1.0 %	2.0 %	3	SH: A10 report/SAP CP: Barrier panel/SAP Gassco: Reports Total: SAP Centrica: Maximo
ESD - Pushbutton	# of failures / # of tests	The ESD logic does not receive a signal from the pushbutton when activated	0.5 %	1.0 %	3	SH: A10 report/SAP CP: Barrier panel/SAP Gassco: Reports Total: SAP Centrica: Maximo
Safety critical PSD valves	# of failures / # of tests	The valves do not close on demand in time	2.0 %	4.0 %	2	SH: A10 report/SAP CP: Barrier panel/SAP Gassco: Spreadsheets Total: SAP Centrica: Maximo
PSV	# of failures / # of tests	The valve does not open at 120 % of set point or at a pressure 50 bar above set point if this is lower	4.0 %	8.0 %	3	SH: A10 report/SAP CP: Barrier panel/SAP Gassco: Spreadsheets Total: SAP Centrica: Maximo

<sup>4</sup> Limits for Ignition source control is not given in ref. GL0114, but assumed equal to gas detection which initially trigger the deactivation of ignition sources.

## Evaluating Gassco`s barrier KPI model

	HIPPS	# of failures / # of tests	HIPPS valve does not open/close on signal within specified time.	0.1 % <sup>5</sup>	0.2 %	2	SH: A10 report/SAP CP: Barrier panel/SAP Gassco: Spreadsheets Total: SAP Centrica: Maximo
	PPS	# of failures / # of tests	Same function as the HIPPS system.	0.1 %	0.2 %	2	Only applicable for SH
	Blowdown	# of failures / # of tested valves	1. The pushbutton does not send a signal when activated 2. The valve does not open on signal within specified time	0.5 %	1.0 %	3	SH: A10 report/SAP CP: Barrier panel/SAP Gassco: Spreadsheets Total: SAP Centrica: Maximo
	Fire detection	# of failures / # of tested detectors	F&G logic does not receive a signal from the detector when tested Include heat-, smoke- and flame detectors	1.0 %	2.0 %	2	SH: A10 report/SAP CP: Barrier panel/SAP Gassco: Spreadsheets Total: SAP Centrica: Maximo
	Deluge valve	# of failures / # of tests	Deluge valve does not open	1.0 %	2.0 %	2	SH: A10 report/SAP CP: Barrier panel/SAP Gassco: Spreadsheets Total: SAP Centrica: Maximo
	Deluge nozzle	# of failures / # of tests	Nozzle does not distribute water with the expected amount and release pattern.	3.0 %	6.0 %	2	SH: A10 report/SAP CP: Barrier panel/SAP Gassco: Spreadsheets Total: SAP Centrica: Maximo
	Fire water pumps	# of failures / # of tests	1. The pump fails to start 2. The pump capacity is reduced with more than 10 %	2.0 %	4.0 %	2	SH: A10 report/SAP CP: Barrier panel/SAP Gassco: Spreadsheets Total: SAP Centrica: Maximo

<sup>5</sup> Limit not given in ref.GL0114, SIL 3 requirement used as basis for lower limit.

## Evaluating Gassco`s barrier KPI model

	PA system	# of speakers failed / # tested	Too low battery capacity UHF radios)	2.0 %	4.0 %	1	SH: A10 report/SAP CP: Barrier panel/SAP Gassco: Spreadsheets Total: SAP Centrica: Maximo
	Emergency power generator	# of failures / # of tests	The generator does not start or does not supply specified voltage	0.5 %	1.0 %	2	SH: A10 report/SAP CP: Barrier panel/SAP Gassco: Spreadsheets Total: SAP Centrica: Maximo
	UPS capacity	# of failures / # of tests	The UPS does not have the capacity to supply the required emergency power for a period of 30 minutes	0.5 %	1.0 %	2	SH: A10 report/SAP CP: Barrier panel/SAP Gassco: Spreadsheets Total: SAP Centrica: Maximo
	Emergency lightning	# of failures / # of tests	Emergency lighting does not remain lit, using emergency power supply, for a period of 30 minutes	5.0 %	10.0 %	1	SH: A10 report/SAP CP: Barrier panel/SAP Gassco: Spreadsheets Total: SAP Centrica: Maximo
Management elements	PM backlog on safety critical equipment	# of work orders in backlog related to inspection and tests	Backlog according to company specific definition SH: Backlog if >30 days over due	Installation specific	Installation specific	1	SH: Currently not available CP: Barrier panel, PM backlog Gassco: SAP, PM backlog Total: Backlog not defined (?) Centrica: Maximo
	CM backlog on safety critical equipment	# of work orders in backlog related to CM on safety critical equipment	Backlog according to company specific definition (see example in figure below)	Installation specific	Installation specific	3	SH: MIS-CMR CP: Barrier panel ZB, PM backlog Gassco: SAP Total: SAP Centrica: Own KPI

## Evaluating Gassco`s barrier KPI model

	Critical audit findings	# of critical open findings	Criticality dependent on audit system. Example is findings rated yellow or red (or 1 in new rating scale) in SH system	Installation specific	Installation specific	2	SH: SAMS CP: Impact Gassco: Synergi Total: Stream (?) Centrica: CATS
	Overdue actions on critical audit findings	# of overdue actions	Overdue time bound actions initiated by critical audit findings. Action should be a concrete improvement measure.	Installation specific	Installation specific	3	SH: SAMS CP: Impact Gassco: Total: Centrica:
	Override indicator	# Of critical safety barriers overridden a specific time (e.g. first Friday in reporting period at 08:00 - the time can be chosen by reporting person, but should be the same for each period).	Disconnection or by-pass of a technical safety barrier e.g.: <ul style="list-style-type: none"> <li>- Override onscreen using switch on control panel, with or without a key</li> <li>- Physical by-passes or disconnections in equipment lockers or terminal blocks</li> <li>- Override of safety functions in electrical systems</li> </ul>	Installation specific	Installation specific	2	SH: Monitored in control room CP: Control room Gassco: Control room Total: Centrica: Separate risk assessment
	Open corrective work order related to safety critical failure modes	# of outstanding work orders on safety critical equipment	Example: <ul style="list-style-type: none"> <li>- ESD valve with to high leak rate</li> <li>- Non functional gas detector</li> </ul>	Installation specific	Installation specific	2	SH: MIS-CMR CP: Available in other format Gassco: Not registered Total: Centrica:



### Aggregation rules and colour interpretation

Each indicator is summarized and an overall status for reactive elements, preventive elements and management elements are calculated by using equation B.1. Reactive and preventive elements are given weight based on where the barriers are located in the chain of events. Some systems though, are regarded exceptions to this rule of thumb. Here, a weight is allocated to each barrier applying a combination of the weights used in the TTS project (ref chapter 1.1) and expert judgments [6].

An aggregate parameter P is calculated as the weighted average of the score allocated to each indicator according to colour using the weights described in the table in chapter iii. Red rating is given extra attention and is allocated an additional "criticality" score point [7]:

$$P = [\lambda_1 \times R_1 + \lambda_2 \times R_2 + \dots + \lambda_n \times R_n] \times \text{---} \quad \text{(Formula B.1)}$$

$\lambda_i$ : weight factor for system i

$R_i$ : rating according to colour on system level (green = 1, yellow = 2, red = 4)

Applying formula B.1, a rating of yellow for all system level indicators would give a P value of 2. Upper and lower tolerance level is calculated by respectively adding and subtracting 16,67 % of the value corresponding to all yellow, giving following limits [7]:

Green value:  $1 \leq x < 1.67$

Yellow value:  $1.67 \leq x < 2.33$

Red value:  $2.33 \leq x < 4$

Further, on installation, organisational unit- and corporate level the aggregation rules indicated in the figure below is applied, and summarized to one status for Gassco, as illustrated in figure 25 [6].

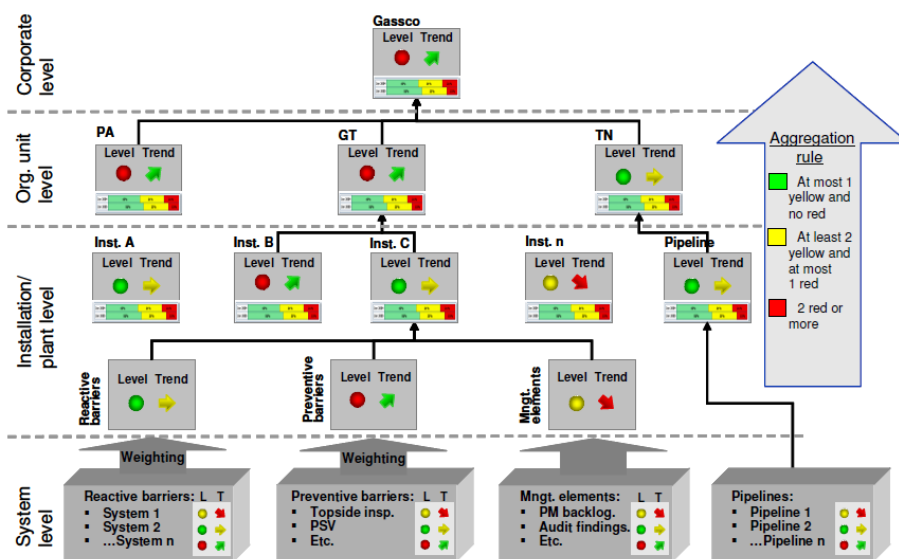


Figure 32: Aggregation hierarchy [6]

## C. Major accidents

In this chapter some more major accidents are presented which are referred to in the report.

### C.1 Humber oil refinery 2001

Reference for information in this is made to the HSE public investigation report <sup>[85]</sup>.

In April 2001, on Easter Monday at approximately 2:20 p.m, a large explosion occurred on the Humber oil refinery in UK. There were no fatalities, but two people were injured. The explosion caused widespread damage to houses and businesses within a 1 kilometer radius of the plant. In total 180 metric tons of flammable liquids and gases were released during the incident along with just over half a tone of the toxic gas hydrogen sulphide. ConocoPhillips, owner of the refinery, was investigated and subsequently fined and ordered to pay £218,854 costs by the Health and Safety Executive for failing to effectively monitor the degradation of the refineries' pipework. The company pleaded guilty to these charges in court and has since implemented a Risk Based Inspection program.

The primary cause of the explosion was the erosion/corrosion of the 6" diameter pipe, known as P4363. Examination showed that the elbow had failed owing to an erosion-corrosion damage mechanism which, over time, had reduced the wall thickness at the outside of the elbow to such an extent that the wall could no longer withstand the internal pressure within. The pattern of thinning appeared to be directly associated with the water injection position and the downstream flow path of the water from the injection point and around the outside of the elbow. Following its installation the use of P4363 water injection was not well documented. There is evidence that from early 1980s water injection through this pipe was continuous, until 1995 when the decision was taken that it would only be used intermittently as required (or not at all). The change to intermittent use was not progressed through a Management of change procedure and therefore there was no evaluation of the effects this might have on corrosion potential. Sometime during 2000 or early 2001 the water injection was put back into continuous use.

The design and installation of the water injection point in P4363 was not subject to any management of change assessment. Had such an assessment been carried out the corrosion risk that the injection point introduced for the downstream pipework could have been identified. Similarly no assessment was made of the changes in the use of the water injection point, between continuous and intermittent, over the lifetime of the plant.

ConocoPhillips corrosion management was not sufficiently thorough or systematic to prevent the failure of P4363. Positive actions, such as a full time Corrosion Engineer for the Refinery, were allowed to lapse with the result that there was both insufficient data on, and inadequate resource or focus applied to, corrosion as a potential major accident initiator. Systematic and thorough arrangements are necessary for the effective management of corrosion on major hazard installations. Adequate resource, including relevant expertise, should be applied to ensure that adequate standards are achieved and maintained.

Two significant communication failings contributed to the incident. The various changes to the frequency of use of the P4363 water injection were not communicated outside plant operation personnel. As a result there was a belief elsewhere that it was in occasional use only and did not constitute a corrosion risk. Secondly information from the P4363 injection point inspection, which was carried out in 1994, was not adequately recorded or communicated with the result that the recommended further inspections of the pipe were never carried out.

Communication systems should aim to actively involve the workforce. This was also pointed out in a detailed inspection of human factors issues at the Refinery. Safety communication were found to be largely instructions related to personal safety issues, rather than seeking to involve the workforce in prevention of major accidents. The inspection identified that there were insufficient attention on the Refinery to the management of process safety.

ConocoPhillips failed to implement an effective system for the inspection of pipework. The system used fell far below recognized industry good practice at the time. In addition they failed to use knowledge and experience from others of the plant that should have identified the need for more inspection of the SGP pipework. Over time pipework condition data should have been obtained, and entered onto an inspection database, to verify the believed integrity and inform assessments of future inspection requirements. Summing up the factors that contributed to Humber refinery accident can be grouped into the following categories:

Supervision and monitoring:

- management of pipework inspection – failed to implement a effective system for the inspection of pipework, there should have been an inspection database

Policies and procedures:

- lack of management of change policy and procedure

Physical devices and instrumentation:

- inadequately maintenance of equipment (corrosion)

Communication:

- various changes to the frequency of use of the P4363 water injection were not communicated outside plant operations personnel
- information from the point inspection in 1994 was not adequately recorded or communicated – the recommended further inspection were never carried out
- safety communication were found to be largely ‘top down’ instructions on personal safety, rather than seeking to involve the workforce in preventing a major accident.

Training:

- lack of awareness off present risks

When summing up the underlying causes that contributed to the Humber oil refinery accident, it is evidently that there were several weaknesses in the management system. There were lack of management of pipework inspections, management of change policy and procedures and insufficient maintenance management.

## C.2 Toulouse 2001

The official investigation report of the Toulouse accident in 2001 is in French language and is not translated into English. Reference to information regarding this accident is made to an article published by Safety Science<sup>[86]</sup>; First lessons of the Toulouse ammonium nitrate disaster, 21st September 2001, AZF plant, France. This article summaries conclusions made for several investigation carried out subsequently following the accident.

21<sup>st</sup> September 2001 an explosion occurred in a downgraded ammonium nitrate store in Toulouse, France. The accident resulted in 30 fatalities and approximately 10 000 injuries. The plant belonged to Grande Paroisse Company, TotalFinaElf Group. The explosion occurred in a downgraded ammonium nitrates store, which was authorised for 500 tons and contained approximately 400 tons of product on the day of the explosion. The chemical was stored flat and separated by partitions. It is not known what caused the explosion. The TNT equivalent mass of the explosion was estimated by INERIS to be in the range of 20 to 40 tons of TNT.

There is still a controversy on the direct causes of the explosion. The key element is to find the ignition source of the ammonium nitrate stored. The Justice's main assumption is a chemical reaction (trichloramine  $NCl_3$ ), which is very unstable and able to explode. The TotalFinaElf companies focusing mostly on a huge underground electric arc between a transformer on SNPE's plant (owned by the French State) and EDF's electric line. Other assumptions are terrorism act or malicious intent. Neither has appeared relevant so far.

Several investigations of the accident gave lots of analysis and propositions that help the French Environment Ministry to implement a new law. The new law focuses on several points that complete the Seveso II Directive. Some lessons have also been implemented at a EU level (White book, ammonium nitrate changes in Seveso II Directive). For example, as recommended by several investigations, the Environment Ministry made compulsory in its new law in 2003 to involve more widely the employees and also to integrate the subcontractors in the risk management process. Also, the new laws aims at monitoring the use of subcontracting on Seveso installations.

On the plant there were 25 subcontracting companies that worked continuously and 3 different subcontracting companies worked in the warehouse (the ammonium nitrate was picked up, unloaded and removed by them) and the maintenance of the warehouse was carried out by another contractor. An organisational investigation carried out after the accident considered that the subcontracting was a "determining factor". One consequence of the operational subcontracting was a disengagement of AZF employees for its operational management, and AZF lost the control of some activities carried out by the subcontractors.

By the various investigations no specific analysis of the safety management system of the company and the way it worked has been performed. Neither has an investigation at a higher level of the organisation in the company been carried out. This seems to be a weak point in the investigations carried out after the Toulouse accident

A few days after the accident the European Parliament (EP) stated that they regretted that they didn't provide sufficient numbers of competent and specialised inspectors and calls. Staff were recruited and suitably trained, and minimum qualification criteria for inspectors were updated.

1570 firemen and militaries and 950 policemen were involved in the emergency response and housing monitoring. A problem was that they arrived without any plan and any discussion by

phone as the classical phone lines were partly destroyed and the mobile phone network was saturated. The internal and external emergency plan were not prepared to this scenario and its gravity and the first firemen were not protected with adequate equipment for any toxic cloud and with devices to detect those toxic gases. The French Environment Ministry gave additional funds to INERIS to increase the research on chemicals properties, on learning from experience, on safety studies and on emergency preparedness.

After the accident it was pointed out the need for introducing uncertainties of the accidental scenarios as probabilities in the risk assessment like in the UK. The new law therefore asks to take into account probability and the kinetic of scenarios in the new safety studies. However, they pointed the need to keep on assessing scenarios with a consideration of a possible failure of the safety barriers designed and implemented (deterministic approach).

Information in this will not be divided into categories due to insufficient information regarding the accident sequence and root causes. But from lessons learned as described above, it seems that most off the contributing factors were organisational and management elements, such as lack of risk understanding, lack of knowledge and lack of training. This accident clearly shows the importance of understanding the characteristics of chemical substances and the safety design principle given by Kletz<sup>[87]</sup>, intensification, attenuation, substitution and simplification.

### **C.3 Buncefield 2005**

Reference to the information in this chapter is made to the investigation report from the Major investigation board<sup>[88]</sup>, formally established by the Health and Safety Executive. The Buncefield Investigation Board publishes its Final Report and announces the end of its work 11. December 2008<sup>[89]</sup>. The Final Report captures all of the work over nearly three years in a single publication. Its aim was to identify the immediate causes of the explosion, rather than consider who was to blame for any deficiencies, so as not to prejudice further legal proceedings. The chain of events and direct and underlying causes to the accident is not described in the report. A picture of what went wrong is therefore established by evaluating the recommendations given in the report.

Sunday 11 December 2005 a series of explosions and subsequent fire destroyed large parts of the Buncefield oil storage and transfer depot, Hemel Hempstead, England. There were no fatalities, but 43 persons were injured. Fortunately, no one was seriously hurt. There was significant damage to both commercial and residential properties near the plant and about 2000 people had to be evacuated from their homes. The fire burned for five days, destroying most of the plant and emitting a large plume of smoke into the atmosphere that dispersed over southern England and beyond. The plant owners were Total UK limited (60%) and Texaco (40%).

The petrochemical storage tank overflow valve failed whilst fuel was being pumped into the tank causing a large quantity of that highly inflammable substance to seep out of the tank. There was evidence suggesting that a high-level switch, which should have detected that the tank was full and shut off the supply, failed to operate. The switch failure should have triggered an alarm, but it too appears to have failed. This was a safety critical event which went unnoticed by technicians and their monitoring systems. Consequently, a dangerous vapour cloud spread, quietly and ultimately disastrously, across the plant. A spark from either

the site's fire prevention system or a nearby generator at the Northgate building was enough to cause that fuel vapour cloud to ignite with destructive force.

The Board's recommendations (summed up) consist that the measures for controlling major incidents risk must integrate:

- integrity levels at major hazards sites in relation to containment of dangerous substances and process safety;
- mitigation against the effect of a major accident on off-site populations and buildings;
- preparedness for emergency response to limit the escalation of potential major accidents;
- land use planning and the control of societal risk; and
- the regulatory system for inspection and enforcement at major hazard industrial sites

Regarding design and operation at fuel storage sites there are recommendations given by the Board which emphasised the need to increase the protection provided by primary containment systems to reduce the likelihood of failure. The Buncefield incident highlighted the need

for high integrity systems and that there remains a need for an effective means of preventing environmental pollution in the event of a failure of primary containment. Therefore there are also recommendations given dealing with secondary and tertiary containment if an accident should occur.

Further, there are recommendations given on how to deal with technological matters and their management. It's also noted that human and organisational factors are important and there are given recommendations on how to deal with this matter. There are also recommendations on how to deal with a broader strategic objectives relating to sector leadership and culture. It is stated that to achieve the full benefit from the technological improvements to process safety and environmental protection depends on human and organisational factors such as the roles of supervisors, the way work is organised and the robustness of communications on critical tasks.

At the time of writing of the Boards investigation report there was also an investigation ongoing on the Texas City disaster (described in the preceding chapter). Both incidents occurred due to loss of primary containment by overfilling of a vessel resulting in the formation of large flammable vapour cloud that subsequently ignited. The Boards investigation report states that their report is equally strong on the importance on human factors in the overall program as the report after the Texas City accident <sup>[51]</sup>. Also, it is emphasized that process safety protection systems should not rely on operator response to alarms and that overfill protection must be independent of normal operational monitoring, just as in the reports after the Texas City disaster <sup>[51]</sup>. The Boards report states that there are a lot of similarities between the recommendation given after the Texas City explosion and their recommendations regarding high reliability organisations and the need for a better safety culture and adoption of better measures of performance that are more useful to major hazards sectors than injury rates and other measures (that are primarily occupational safety-related).

The Buncefield incident was a major test for contingency planning. The impressive emergency response to Buncefield effectively relied on initiative and good working relations of the responders in dealing with an incident that had been unforeseen and therefore not planned for. The recommendations in the report from the Board address the need to improve emergency arrangements at local, regional and national levels. The recommendations given

can mainly be divided into the following: assessing the potential for a major incident, managing a major incident on site, warning and informing the public, preparing for and responding to a major incident off sit, review of off-site emergency plans, responding and recovering to a major incident. There are also given recommendations on the design and operation of fuel storage.

The third of the main areas of concern, stated in the report<sup>[88]</sup> is the system for land use planning and the control of societal risk around major hazard plant. The first recommendations called for a wide-ranging review of the system for land use planning around major hazard sites to begin without delay and include the incorporation of societal risk into land use planning decision making. The following recommendations asks for the economic case for land use planning and control of societal risk to be clarified, and for the workings of the planning system to be set out in clear guidance for the general public. There are also recommendations given that calls for a simplified, generic approach to risk assessment used around flammable storage to be replaced by a site-specific assessment of risks, using QRA methods. Further recommendations calls for an alignment in the risk assessment approach in the COMAH safety report system with land use planning, and in setting priorities on the management of sites to ensure continuing integrity of the control measures incorporated in the planning decisions. At the end the recommendations are that the key stakeholders demystify the concept of societal risk and envisage a future system where they support the planning authority in coming to transparent decision on what level of societal risk that can be accepted. Planning authorities also need to be suitable resourced to develop the expertise and procedures necessary for their role.

Looking at the recommendations given by the Board it seems like most of the causes can be categorised into the same group as mentioned earlier in previous chapters; supervision/monitoring, policies and procedures, physical devices and instrumentation and communication. Also risk in design and planning and emergency preparedness are areas that need to be focused on.

## D. Indicators human factors

In this appendix the suggestions of human factors indicators from HSE's research report from Energy institute are presented <sup>[6]</sup>. The indicators suggested are meant to be assessed in the risk assessment. In this appendix some of the indicators are suggested implemented in the barrier KPI model, based on the experiences gained from previous major accidents. The indicators must be suitable to the organisation at Bygnes. As a starter, the aim of the barrier KPI model is to have a chance in revealing a growing major accident potential. Therefore it is of interest to try and implement mostly leading indicators. The suggested lagging indicators have not been evaluated.

The suggested indicators below are human factors performance indicators. The indicators are important risk influencing factors, and as illustrated previously in this report, play a role in the chain of event leading towards a major accident. It is important to have a way of "reading" signs of bad development in the organisation.

### Managing human failures:

<i>Potential lagging indicators</i>	<i>Potential leading indicators</i>
Number or percentage of incidents, accidents or root cause investigations in which human failures identified as being contributed or causal factor	Number or percentage of risk assessments/HAZOPs that include assessment of potential human failure.
Total number per year of recommendations made in response to identified human factors related failures	Number or percentage of risk assessments/HAZOPs/HAZIDs with defined team competencies including human factors specialist competence/capability.
Number or percentage of API RP <sup>6</sup> 754 loss of containment incidents in the industry at each level with associated human factors root causes.	Number or percentage of plants/sites in the organisation that have designated champion to help manage human performance risk.
Number or percentage of incidents involving human failures in which potential for failure was previously identified via risk assessment, hazard identification study (HAZID) or HAZOP process but not sufficiently mitigated.	Number of or percentage of projects in the organization for which a 'human factors manager' has been appointed.  Number or percentage of safety critical task assessments (human reliability assessment, human error analysis) completed vs. number planned.

<sup>6</sup> American Petroleum Institute Recommended Practice



**Procedures:**

<i>Potential lagging indicators</i>	<i>Potential leading indicators</i>
Number or percentage of incidents, accidents or root cause investigations in which inadequate procedures identified as being a causal factor.	Number or percentage of safety critical tasks for which procedures are in place.
Number or percentage of incidents related to failure to follow procedures.	Number or percentage of procedures documented/up-to-date/within scheduled review date, or compared with total number of procedures.
Number or percentage of non-compliances/violations in following procedures.	Number or percentage of procedures meeting quality criteria/number of errors found in procedures (based on procedural 'walkthroughs' undertaken by managers and operators to confirm appropriateness).
	Number or percentage of errors found in procedures.
	Number or percentage of safety critical tasks for which appropriate (scope, critical tasks, emergency actions) procedures are in place.
	Number or percentage of PTWs <sup>7</sup> reviewed and considered fit-for-purpose.

**Training and competence:**

<i>Potential lagging indicators</i>	<i>Potential leading indicators</i>
Number or percentage of incidents, accidents or root cause investigations in which lack of competence identified as being a causal factor.	Number or percentage of employees trained per period as compared with schedule <sup>8</sup> .
	Number or percentage of training records complete/up-to-date.
Feedback on staff competence from third party body (based on annual audit).	Number or percentage of staff satisfactorily completing refresher training as compared with schedule <sup>9</sup> .
	Number or percentage of safety critical roles filled versus unfilled. <sup>10</sup>
	Frequency with which supervisors actively

<sup>7</sup> Permit to work

<sup>8</sup> Indicators can be developed if necessary for % of employees successfully completing: general safety awareness training, emergency response training/drill, technical training, etc.

<sup>9</sup> NB: this is not the same as competence. Also, the number of non-attendees may indicate staffing pressures.

<sup>10</sup> Requires that safety critical roles to be defined, so likely to be used for mature and more mature organisations.

check staff competence (based on audit interviews with supervisors).
Number or percentage of staff acting up <sup>6</sup> (temporarily filling more senior roles), based on spot check audits.
Number or percentage of training not given on request.
Number or percentage of technical specialists available versus required number (ref. Longford).

**Staffing (staffing levels and workload, supervision, contractors):**

<i>Potential lagging indicators</i>	<i>Potential leading indicators<sup>11</sup></i>
	<b>Staffing levels and workload</b>
Number or percentage of incidents, accidents or root cause investigations in which workload/staff shortages identified as being causal factor.	Staff workload assessment <sup>12</sup>
	Maintenance backlog.
	Percentage of optimum staffing level achieved, or degree to which required percentage staffing levels are being met (e.g. for emergency requirements).
Average hours worked/overtime worked (taken from timesheet analysis).	Team availability (number or percentage of personnel available on each shift who are fully trained).
Number or percentage of times work stopped because of lack of personnel.	Number or percentage of tasks carried over to next shift and/or that exceed programmed time.
Number or percentage of staff off work because of stress.	Number or percentage of people available/trained to cover required signing authority roles versus target (PTW issuer, receiver).
Number or percentage of identified skills shortages.	
Staff turnover.	
	<b>Supervision</b>
Number or percentage of accidents, incidents or root cause investigations in which lack of or poor supervision identified as being a causal factor.	Ratio of supervisors to staff reporting to them.
	Supervisor time on plant against time in office versus target (hours) <sup>13</sup> .

<sup>11</sup> Measures can be indicative of resource/workload problems, but careful interpretation of the data is required.

<sup>12</sup> Workload assessment is particularly important for safety critical tasks

<sup>13</sup> Can be useful, but depends on site context

	Number or percentage use of upward appraisal and 360 degree feedback.
	Contractors
Number or percentage of incidents, accidents or root cause investigations in which poor management of contractors identified as being a causal factor.	Number or percentage of risk assessments relating to contractor activities that involve contractor personnel.
	Number or percentage of audits that are undertaken for contractor activities, versus targets.

**Organisational change:**

<i>Potential lagging indicators</i>	<i>Potential leading indicators<sup>14</sup></i>
Number or percentage of incidents, accidents or root cause investigations in which failures in the MoC process identified as a causal factor.	Number or percentage of engineering and organisational, changes that are risk assessed as part of MoC process.
Number or percentage of issues arising from failure in MoC process (e.g. delays, impact on operations etc.)	Number or percentage of MoC requests closed out or signed off versus number remaining live (for period/against targets).
	Number or percentage adherence to MoC procedures, based on spot check audits.

**Safety critical communications (including permits and shift handover):**

<i>Potential lagging indicators</i>	<i>Potential leading indicators<sup>15</sup></i>
	Communication
Number or percentage of incidents, accidents or root cause investigations in which failures in communication identified as a causal factor.	Number or percentage compliance with communication protocols (based on spot check/sampling audits).
	Correct use of communications proformas (identify number or percentage non-compliance via sampling).
	Permits
Number or percentage of incidents, accidents or root cause investigations in which failures in permits identified as a causal factor.	Number or percentage adherence to correct permit process (quality checks based on sample auditing).
	Competence of permit issuers/receivers
	Shift handover

<sup>14</sup> Measures can be indicative of resource/workload problems, but careful interpretation of the data is required.

<sup>15</sup> Measures can be indicative of resource/workload problems, but careful interpretation of the data is required.

Number or percentage of incidents, accidents or root cause investigations in which failures in shift handover process identified as a causal factor.	Number or percentage of shift handovers meeting required criteria <sup>16</sup> /number or percentage of errors found in handover process (quality checks based on sample auditing of handover process and review of logs).
Number or percentage of reported end-of-tour or shift handover problems.	

**Human factors in design (control rooms; human/computer interfaces (HCI); alarm management; lighting, thermal comfort, noise and vibration):**

<i>Potential lagging indicators</i>	<i>Potential leading indicators<sup>17</sup></i>
<b>Human factors in design</b>	
Number or percentage of incidents, accidents or root cause investigations in which human factors design failings identified as a causal factor.	Compliance with human factors integration plan, based on review of site activities, interviews, documentation.
Number or percentage of items not accessible for maintenance (ergonomic considerations for accessibility have not been addressed).	Number or percentage of ergonomic walkabout reviews/audits.
Number or percentage of installations requiring re-work (revealed by commissioning/decommissioning).	Number or percentage of items of equipment non-compliant with ergonomic standards (based on spot check sampling audits/review of ergonomic assurance evidence).
	Number or percentage of design reviews with defined team competencies including human factors/ergonomics specialist knowledge.
	Number or percentage of workarounds found related to design problems (based on audit sampling).
	Subjective operator views on equipment usability, obtained via interviews/sampling audit.
	Compliance of workplaces with ergonomic environmental design requirements (lighting, noise, etc.) based on sample audits.
<b>Control room and interface design</b>	
Number or percentage of incidents, accidents or root cause investigations in which design factors/ergonomics failures identified as a	Compliance of equipment/workplace with requirements of ergonomic standards, based on sample audits.

<sup>16</sup> Checks to include correct completion of handover documentation , quality of spoken handover, and acceptance of handover by incoming team.

<sup>17</sup> Measures can be indicative of resource/workload problems, but careful interpretation of the data is required.

causal factor.

Number or percentage of repeat incidents associated with specific equipment (NB: repeated problems may be indicative of a problem in the design).

Number or percentage of design issues raised on Issues Register.

**Alarm systems**

Number or percentage of incidents in which alarms issues/failures identified as a causal factor.

Number or percentage of alarms that operators fail to acknowledge per shift.

Compliance with EEMUA guidance on human/machine interfaces and alarm handling. Possible indicators include counts of overall alarm frequency, number or percentage of standing alarms, number or percentage of alarms failing to initiate, number or percentage of false alarms etc.

Evaluation of alarm follow-up actions (e.g. accepted/disabled) and standing alarm reviews, based on sampling.

What could be of interest for the offices at Bygnes is control room and interface design: "Compliance of equipment/workplace with requirements of ergonomic standards, based on sample audits". Further also "Number or percentage of alarms that operators fail to acknowledge per shift" is a potential indicator. Based on the accidents studied, only alarm management was mentioned as an issue that contributed to an accident, for example the Longford accident.

**Fatigue and shiftwork:**

<i>Potential lagging indicators</i>	<i>Potential leading indicators</i>
Number or percentage of incidents, accidents or root cause investigations in which fatigue issues or shift scheduling identified as a causal factor.	Average number of hours worked (or percentage overtime worked) from timesheet analysis.
Number or percentage of near misses arising from shift work/fatigue issues.	Number or percentage of open shifts.
Levels of sickness absence <sup>18</sup> .	Number or percentage of consecutive shifts worked by individuals.
Reported and observed cases of fatigue.	Number or percentage work breaks missed (sampling/interview).

<sup>18</sup> May be indicative of fatigue issues if sickness absence is a means to avoid working a shift. Care is required in interpretation.

<p>Number or percentage of non-compliances with documented shift pattern.</p> <p>Number or percentage of exceptions (breaches of company policy), including staff working non-compliant working hours.</p> <p>Scheduled versus actual hours worked.</p>
---

**Organisational culture (leadership, behavioral safety, learning organisations):**

<i>Potential lagging indicators</i>	<i>Potential leading indicators</i>
<p><u>Reporting and incident investigation:</u> Number or percentage of reported near-misses (should not be zero).</p> <p>Number or percentage of incidents, accidents or root cause investigations in which organisational culture/safety culture identified as being causal factor.</p> <p><u>Continuous improvement:</u> Number or percentage of incidents/accidents that are repeat incidents/accidents (measure of how well the organization is learning from incident investigations).</p> <p><u>Safety climate and culture:</u> Breaches of company policy.</p>	<p><u>Leadership:</u> Measure of visibility of senior executives in the workplace (number of site visits, etc.)</p> <p>Number or percentage of safety tours undertaken by managers and middle managers.</p> <p>Number or percentage of task observations undertaken by leaders (behavioral safety measure).</p> <p>Outcomes of upward/360 appraisals.</p> <p><u>Provision of resources:</u> Number or percentage of items of equipment requested but not provided.</p> <p><u>Communication and risk awareness:</u> Feedback on adequacy of regular toolbox talks.</p> <p>Number or percentage of working groups (including employee representation).</p> <p><u>Reporting and incident investigation:</u> Number or percentage of incidents reported upwards through the reporting chain.</p> <p>Effectiveness of incident investigation process, including:</p> <ul style="list-style-type: none"> <li>- Circulation of incident investigation reports;</li> <li>- Adherence to planned timeframes for incident</li> </ul>

- investigation;
- Effectiveness of interventions, and
- Adherence to timescales for remedial actions (number or percentage of actions closed out by target dates).

Continuous improvement:

Number or percentage of issues reported in timely fashion by workforce. NB: non-reporting or delay in reporting might be indicative of undesirable cultural issues.

Safety climate and culture:

Results from HSE safety climate surveys (or other safety culture/climate surveys or external audits), undertaken every 12 or 18 months, involving questionnaires, team interviews and individual interviews. Provide a snapshot of the organization`s culture (compare results against industry benchmark/changes over time).

Employee attitude and perception survey (including management, supervisors and workforce), results benchmarked against industry.

Number or percentage of actions identified from previous safety culture/climate audits that have been closed, against prioritized targets.

Evaluation of working culture: completeness and adequacy of work undertaken versus `tick-box` mentality (determined via spot check audits).

Major accident hazards/behavioral safety focus:

Number or percentage of reported events that are process safety related versus behavioral safety related.

**Maintenance, inspection and testing (maintenance error, intelligent customers):**

***Potential lagging indicators***

***Potential leading indicators***

Number or percentage of incidents, accidents

Relative number or percentage of reactive

<p>or root cause investigations in which human failures in maintenance, inspection or testing identified as being a causal factor, including maintenance-induced latent failures.</p>	<p>(corrective) versus proactive (planned) maintenance.</p>
<p>Number or percentage of loss control reports/reported failures, including key component failures, attributable to lack of maintenance.</p>	<p>Maintenance backlog (number or percentage of equipment not maintained against prioritized targets).</p>
<p>Number or percentage of reported maintenance errors/number of tasks requiring rework.</p>	<p>Number or percentage of equipment inspections/test undertaken against target scheduled.</p>
<p>Number or percentage of times issues reported with equipment that has been maintained or repaired (i.e. maintenance incorrectly performed leading to latent defects/maintenance induced failure).</p>	<p>Completeness and accuracy of maintenance records (based on sampling review).</p>
	<p>Timescale for closure of work orders, against targets.</p>
	<p>Availability of critical spares.</p>
	<p>Number or percentage of workarounds (temporary modifications) in place because of failed /degraded equipment.</p>
	<p>Evaluation of effectiveness of maintenance against procedure/process (based on regular review of maintenance reports/job notes).</p>
	<p>Number or percentage of plant alarms not available/not calibrated at plant start-up.</p>
	<p><b>Intelligent customers</b></p>
<p>Number or percentage of incidents, accidents or root cause investigations in which failures related to outsourcing identified as being a causal factor</p>	<p>Number or percentage of nominated intelligent customer' resources within the organization.</p>
	<p>Number or percentage of defined intelligent customer' competence profiles within the organization.</p>
	<p>Number or percentage of contracts requiring intelligent customer' management.</p>



## E. Risk calculations

Data from QRA:		Small	Medium	Large
Leak frequency	13 a year	8,210526316	4,105263158	0,684210526
Probability of ignition		0,0003	0,01	4-19% cars, 1-2% others
Probability of fire/exp.		0,05	0,05	0,05
Probability of escalation		0,31	0,31	0,31
Fatality contribution: UNKNOWN		1	1	1
1 ESD failure		0,062		ref. QRAen
ESD failure March		0,087		ref. reported data
Gas detection, March figures:		0,001		ref. reported data
Scenario ESD failure given medium gas leak:	9,61E-06			
Increase in the failure rate:	1,35E-05	40,32258065		
ESD:				
Combined with failure rate in the gas detection:	0,063			
	0,088			
New value scenarios:	9,77E-06			
40 % increase	1,36E-05	39,68253968		

shut the ESD valves can be calculated for this node in the following manner:

$$P_{TOT} = P_{ESDV} + P_{ESDL} + (P_{GASDET} * P_{MANDTET}) \quad (Eq. 5.1)$$

where  
 $P_{TOT}$  = probability of failure to shut the ESD valve  
 $P_{ESDV}$  = probability of failure to shut the ESD valve  
 $P_{ESDL}$  = probability of failure to shut the ESD valve  
 $P_{GASDET}$  = probability of gas detection  
 $P_{MANDTET}$  = probability of manual intervention  
 expressed as follow:

$$PLL = \sum_n \sum_j (f_{ni} \times C_{nj}) \quad (Eq. 2.3)$$

where  
 $f_{ni}$  = the annual frequency of accident scenario  $n$  with personnel consequence  $j$ .  
 $C_{nj}$  = expected number of fatalities for accident scenario  $n$  with personnel consequence  $j$ .  
 $N$  = total number of accident scenarios in all event trees  
 $J$  = total number of personnel consequence types, usually immediate,

The annual frequency of an accidental scenario,  $f_{ni}$ , may be expressed as follows, if it assumed that the factors are related:

$$f_{ni} = f_{leak,n} \times P_{ign,n} \times P_{protfail,n} \times P_{escal,n} \times B_{ni} \quad (Eq. 2.4)$$

where  
 $f_{leak,n}$  = frequency of leak  
 $P_{ign,n}$  = conditional probability of ignition, given leak  
 $P_{protfail,n}$  = conditional probability of failure of the safety protective systems, such as ESD,

Medium Gas leak metering station, FAR 0,06 3% of total:						
Given						
Failure rate	F <sub>nj</sub>	F <sub>nj</sub> with dependices	PLL	PLL with dependic	FAR	
0,01	6,36316E-06	6,99947E-06	3,18158E-05	3,49974E-05	0,00276659	
0,02	1,27263E-05	1,36266E-05	6,36316E-05	6,68132E-05	0,005533181	
0,03	1,90895E-05	1,97258E-05	9,54474E-05	9,86289E-05	0,008299771	
0,04	2,54526E-05	2,60889E-05	0,000127263	0,000130445	0,011066362	
0,05	3,18158E-05	3,24521E-05	0,000159079	0,000162261	0,013832952	
0,06	3,81789E-05	3,88153E-05	0,000190895	0,000194076	0,016599542	
0,07	4,45421E-05	4,51784E-05	0,000222711	0,000225892	0,019366133	
0,08	5,09053E-05	5,15416E-05	0,000254526	0,000257708	0,022132723	
0,09	5,72684E-05	5,79047E-05	0,000286342	0,000289524	0,024899314	
0,1	6,36316E-05	6,42679E-05	0,000318158	0,000321339	0,027665904	
0,11	6,99947E-05	7,06311E-05	0,000349974	0,000353155	0,030432494	
0,12	7,63579E-05	7,69942E-05	0,000381789	0,000384971	0,033199085	
0,13	8,27211E-05	8,33574E-05	0,000413605	0,000416787	0,035965675	
0,14	8,90842E-05	8,97205E-05	0,000445421	0,000448603	0,038732265	
0,15	9,54474E-05	9,60837E-05	0,000477237	0,000480418	0,041498856	
0,16	0,000101811	0,000102447	0,000509053	0,000512234	0,044265446	
0,17	0,000108174	0,00010881	0,000540868	0,00054405	0,047032037	
0,18	0,000114537	0,000115173	0,000572684	0,000575866	0,049798627	
0,19	0,0001209	0,000121536	0,000606045	0,000609227	0,052565217	
0,2	0,000127263	0,000127899	0,000636316	0,000639497	0,055331808	
0,21	0,000133626	0,000134263	0,0006668132	0,000670095	0,058098398	
0,22	0,000139989	0,000140626	0,000699947	0,000703129	0,060864989	
0,23	0,000146353	0,000146989	0,000731763	0,000734945	0,063631579	
0,24	0,000152716	0,000153352	0,000763579	0,000766761	0,066398169	
0,25	0,000159079	0,000159715	0,000795395	0,000798576	0,06916476	

$P_{escal,n}$  = blowdown, deluge, passive fire protection, etc. given that ignition has occurred.  
 $B_{ni}$  = conditional probability of escalation, given ignited leak and failure protective systems response.  
 $B_{ni}$  = fatality contribution of the accident scenario (fraction of scenarios that result in fatalities).

million exposed hours, whereas ALR value is the average number of fatalities per exposed individual. Following equations define how the individual risk expressions are computed [ref].:

$$FAR = \frac{PLL \times 10^6}{Exposed\ hours} \quad (Eq. 2.5)$$

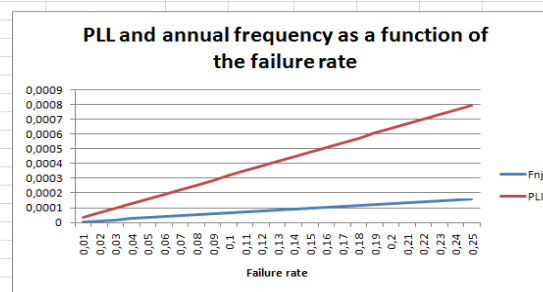


Figure 33: Risk calculations

## Evaluating Gassco's barrier KPI model

ESD valve:					
40 % increase in the failure rate for scenario N gives:					
1	1,4				
1	1,4				
1	1,4				
1	1,4				
1	1,4				
1	1,4				
1	1				
1	1				
1	1				
1	1				
1	1				
1	1				
12	14,4	20 % increase in the PLL value for scenario N			

**Figur 34: Calculations overall % risk change**

Scenario nr	Size and area	Contribution to FAR value from process events			20% increase scenario 7	New FAR	20% increase for all scenarios - new FAR
		Value (FAR)	% of total	PLL			
1	Large leak, Train 100, south	0,51	25	0,005865	0,005865	0,51	0,612
2	Large leak, Train 100, north	0,38	18	0,00437	0,00437	0,38	0,456
3	Large leak, Train 300, south	0,35	17	0,004025	0,004025	0,35	0,42
4	Large leak at the quay	0,19	9	0,002185	0,002185	0,19	0,228
5	Large leak, Train 200, south	0,09	4	0,001035	0,001035	0,09	0,108
6	Large leak at the metering station	0,08	4	0,00092	0,00092	0,08	0,096
7	Medium leak at the metering station	0,06	3	0,00069	0,000828	0,072	0,072
8	Large leak at the gas metering station	0,05	3	0,000575	0,000575	0,05	0,06
9	Medium leak, Train 100, south	0,05	2	0,000575	0,000575	0,05	0,06
10	Medium leak, Train 200, south	0,05	2	0,000575	0,000575	0,05	0,06
11	Large leak, Train 200, north	0,05	2	0,000575	0,000575	0,05	0,06
Sum 11 most important event (in total 45 modelled)		1,84	89	0,02116	0,02116	1,872	2,2464
Total contribution all 45		2				2,032	2,4064
							<b>1,6 % increase in FAR value for in scenario 7</b>
							<b>20,32 % increase in Far value.</b>

Event	FAR-value	% of total	New FAR all 20%	New FAR only scenario 7
Fire and explosion in process and storage area	2	65	2,4064	2,032
Occupational accident	0,6-1,0	32	0,6-1,0	0,6-1,0
BLEVE, tank fracture and explosion inside buildings	4,5 · 10 <sup>-2</sup>	1,5	4,5 · 10 <sup>-2</sup>	4,5 · 10 <sup>-2</sup>
Quay operations (risk only related to vessels)	4 · 10 <sup>-2</sup>	< 1	4 · 10 <sup>-2</sup>	4 · 10 <sup>-2</sup>
Propane filling station	2 · 10 <sup>-4</sup>	< 1	2 · 10 <sup>-4</sup>	2 · 10 <sup>-4</sup>
<b>Total</b>	<b>2,7 - 3,1</b>	<b>100</b>	<b>3,1 - 3,5</b>	<b>2,72 - 3,12</b>

0,740740741 % of total FAR value  
14,81481481 % of total FAR value

**Figure 35: Calculation overall % change in FAR**

# Evaluating Gassco's barrier KPI model

## FORMULAS:

	A	B	C	D	E	F
1						
2	<b>Data from QRA:</b>					
3				Small	Medium	Large
4	Leak frequency	13 a year		= $(12/19)*13$	= $(6/19)*13$	= $(1/19)*13$
5	Probability of igniton			= $3*10^{-4}$	= $10^{-2}$	4-19% cars, 1-2% others
6	Probability of fire/exp.			0,05	0,05	0,05
7	Probability of escalation			0,31	0,31	0,31
8	Fatality contribution: UNKNOWN			1	1	1
9						
10	1 ESD failure			0,062		ref. QRAen
11	ESD failure March			0,087		ref. reported data
12	Gas detection, March figures:			0,001		ref. reported data
13						
14						
15	Scenario ESD failure given meduin		= $SDS10*SE55*SE56*SE57*SE58$			
16	Increase in the failure rate:		= $SDS11*SE55*SE56*SE57*SE58$	= $((C16-C15)/C15)*100$		
17						
18	ESD:					
19	Combined with failure rate in the		= $D10+D12$			
20			= $D11+D12$			
21	New value scenarios:		= $C19*E5*E6*E7*E8$			
22	40 % increase		= $C20*E5*E6*E7*E8$	= $((C22-C21)/C21)*100$		
23						

	A	B	C	D	E	F
24						
25	Medium Gas leak metering station					
26	Given					
27	Failure rate	Fnj	Fnj with dependices	PLL	PLL with dependices	FAR
28	=0,01	= $SA28*SE4*SE55*SE56*SE57*SE58$	= $(SA28+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S828*5$	= $SC28*5$	= $SD28*10^8/(1150000)$
29	0,02	= $SA29*SE4*SE55*SE56*SE57*SE58$	= $(SA29+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S829*5$	= $SC29*5$	= $SD29*10^8/(1150000)$
30	0,03	= $SA30*SE4*SE55*SE56*SE57*SE58$	= $(SA30+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S830*5$	= $SC30*5$	= $SD30*10^8/(1150000)$
31	0,04	= $SA31*SE4*SE55*SE56*SE57*SE58$	= $(SA31+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S831*5$	= $SC31*5$	= $SD31*10^8/(1150000)$
32	0,05	= $SA32*SE4*SE55*SE56*SE57*SE58$	= $(SA32+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S832*5$	= $SC32*5$	= $SD32*10^8/(1150000)$
33	0,06	= $SA33*SE4*SE55*SE56*SE57*SE58$	= $(SA33+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S833*5$	= $SC33*5$	= $SD33*10^8/(1150000)$
34	0,07	= $SA34*SE4*SE55*SE56*SE57*SE58$	= $(SA34+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S834*5$	= $SC34*5$	= $SD34*10^8/(1150000)$
35	0,08	= $SA35*SE4*SE55*SE56*SE57*SE58$	= $(SA35+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S835*5$	= $SC35*5$	= $SD35*10^8/(1150000)$
36	0,09	= $SA36*SE4*SE55*SE56*SE57*SE58$	= $(SA36+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S836*5$	= $SC36*5$	= $SD36*10^8/(1150000)$
37	0,1	= $SA37*SE4*SE55*SE56*SE57*SE58$	= $(SA37+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S837*5$	= $SC37*5$	= $SD37*10^8/(1150000)$
38	0,11	= $SA38*SE4*SE55*SE56*SE57*SE58$	= $(SA38+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S838*5$	= $SC38*5$	= $SD38*10^8/(1150000)$
39	0,12	= $SA39*SE4*SE55*SE56*SE57*SE58$	= $(SA39+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S839*5$	= $SC39*5$	= $SD39*10^8/(1150000)$
40	0,13	= $SA40*SE4*SE55*SE56*SE57*SE58$	= $(SA40+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S840*5$	= $SC40*5$	= $SD40*10^8/(1150000)$
41	0,14	= $SA41*SE4*SE55*SE56*SE57*SE58$	= $(SA41+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S841*5$	= $SC41*5$	= $SD41*10^8/(1150000)$
42	0,15	= $SA42*SE4*SE55*SE56*SE57*SE58$	= $(SA42+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S842*5$	= $SC42*5$	= $SD42*10^8/(1150000)$
43	0,16	= $SA43*SE4*SE55*SE56*SE57*SE58$	= $(SA43+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S843*5$	= $SC43*5$	= $SD43*10^8/(1150000)$
44	0,17	= $SA44*SE4*SE55*SE56*SE57*SE58$	= $(SA44+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S844*5$	= $SC44*5$	= $SD44*10^8/(1150000)$
45	0,18	= $SA45*SE4*SE55*SE56*SE57*SE58$	= $(SA45+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S845*5$	= $SC45*5$	= $SD45*10^8/(1150000)$
46	0,19	= $SA46*SE4*SE55*SE56*SE57*SE58$	= $(SA46+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S846*5$	= $SC46*5$	= $SD46*10^8/(1150000)$
47	0,2	= $SA47*SE4*SE55*SE56*SE57*SE58$	= $(SA47+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S847*5$	= $SC47*5$	= $SD47*10^8/(1150000)$
48	0,21	= $SA48*SE4*SE55*SE56*SE57*SE58$	= $(SA48+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S848*5$	= $SC48*5$	= $SD48*10^8/(1150000)$
49	0,22	= $SA49*SE4*SE55*SE56*SE57*SE58$	= $(SA49+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S849*5$	= $SC49*5$	= $SD49*10^8/(1150000)$
50	0,23	= $SA50*SE4*SE55*SE56*SE57*SE58$	= $(SA50+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S850*5$	= $SC50*5$	= $SD50*10^8/(1150000)$
51	0,24	= $SA51*SE4*SE55*SE56*SE57*SE58$	= $(SA51+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S851*5$	= $SC51*5$	= $SD51*10^8/(1150000)$
52	0,25	= $SA52*SE4*SE55*SE56*SE57*SE58$	= $(SA52+SDS12)*SE4*SE55*SE56*SE57*SE58$	= $S852*5$	= $SC52*5$	= $SD52*10^8/(1150000)$

Figure 36: Formulas used in figure 27

## Evaluating Gassco`s barrier KPI model

	A	B	C	D	E	F	G	
54	ESD valve:							
55	40 % increase in the failure rate for scenario N gives:							
56								
57	1	1,4						
58	1	1,4						
59	1	1,4						
60	1	1,4						
61	1	1,4						
62	1	1,4						
63	1	1						
64	1	1						
65	1	1						
66	1	1						
67	1	1						
68	1	1						
69	12	14,4	20 % increase in the PLL value for scenario N					

Figure 37: Formulas used in figure 28

## Evaluating Gassco's barrier KPI model

A	B	C	D	E	F	G	H	I	J
71									
72	Sceanrio nr	Size and area	Contribution to FAR value from process event						
73		Value (FAR)	% of total	PLL	20% increase scenario 7	New FAR	20% increase for all scenarios - new FAR		
74	1	Large leak, Train 100, south	25	=C74*1150000/(10^8)	=E74	,51	=G74*1,2		
75	2	Large leak, Train 100, north	18	=C75*1150000/(10^8)	=E75	,38	=G75*1,2		
76	3	Large leak, Train 300, south	17	=C76*1150000/(10^8)	=E76	,35	=G76*1,2		
77	4	Large leak at the quay	9	=C77*1150000/(10^8)	=E77	,19	=G77*1,2		
78	5	Large leak, Train 200, south	4	=C78*1150000/(10^8)	=E78	,09	=G78*1,2		
79	6	Large leak at the metering station	4	=C79*1150000/(10^8)	=E79	,08	=G79*1,2		
80	7	Medium leak at the metering station	3	=C80*1150000/(10^8)	=E80*1,2	{F80*10^8}/1150000	0,072		
81	8	Large leak at the gas metering station	3	=C81*1150000/(10^8)	=E81	,05	=G81*1,2		
82	9	Medium leak, Train 100, south	2	=C82*1150000/(10^8)	=E82	,05	=G82*1,2		
83	10	Medium leak, Train 200, south	2	=C83*1150000/(10^8)	=E83	,05	=G83*1,2		
84	11	Large leak, Train 200, north	2	=C84*1150000/(10^8)	=E84	,05	=G84*1,2		
85	Sum 11 most important event (in t	1,84	89	=C85*1150000/(10^8)	=E85	SUM(G74:G84)	=G85*1,2		
86		Total contribution all 45	2			=C86+(G85-C85)	=H85-C85)+C86		=((G86-C86)/C86)*100 % in
87									=((H86-C86)/C86)*100 % in
88									
89		Event	FAR-value	% of total	New FAR all 20%	New FAR only scenario 7			
90		Fire and explosion in process and storage area	2	65	=H86	=2,032			
91		Occupational accident	0,6-1,0	32	=C91	0,6-1,0			
92		BLEVE, tank fracture and explosion inside buildings	4,5 · 10 <sup>-2</sup>	1,5	=C92	4,5 · 10 <sup>-2</sup>			
93		Quay operations (risk only related to vessels)	4 · 10 <sup>-2</sup>	< 1	=C93	4 · 10 <sup>-2</sup>			
94		Propane filling station	2 · 10 <sup>-4</sup>	< 1	=C94	2 · 10 <sup>-4</sup>			
95		<b>Total</b>	<b>2,7 - 3,1</b>	<b>100</b>	3,1 - 3,5	2,72 - 3,11			
96						=((2,72-2,7)/2,7)*100	% of total FAR value		
97						=((3,1-2,7)/2,7)*100	% of total FAR value		

Figure 38: Formulas used in figure 29

### F. Calculations status

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
2														
3			Values:		$P = [\lambda_1 \times R_1 + \lambda_2 \times R_2 + \dots + \lambda_n \times R_n] \times \frac{1}{\lambda_1 + \lambda_2 + \dots + \lambda_n}$									
4			Green	1	(Exg: C.1)									
5			Yellow	2	$\lambda_i$ : weight factor for system i									
6			Red	4	$R_i$ : rating according to colour on system level (green = 1, yellow = 2, red = 4)									
7	All other indicators (10 stk) green status:													
8			Possible values	ESD valve red							1,30	1,50	1,70	1,90
9				ESD valve green	1,00	1,07	1,13	1,20	1,27	1,37	1,20	1,40	1,60	1,80
10		Indicator weight:		ESD valve yellow		1,10	1,17	1,23	1,30					
11		2	Gas detection	green	green	green	green	green	yellow	green	green	green	green	green
12		3	ESD valve	green	green	green	green	yellow	yellow	yellow	green	green	green	red
13		2	Safety Critical PSD valve	green	green	green	yellow	yellow	yellow	yellow	green	green	red	red
14		2	Ignition source	green	green	yellow	yellow	yellow	yellow	yellow	green	red	red	red
15		2	Deluge valve	green	yellow	yellow	yellow	yellow	yellow	yellow	red	red	red	red
16			Number of combinations		1	5	10	10	5	1	5	10	10	5
17														
18			Possible red status	0	Green value: $1 \leq x < 1.67$									
19			Possible yellow status	43	Yellow value: $1.67 \leq x < 2.33$									
20			Possible green status	205	Red value: $2.33 \leq x < 4$									
21														
22			% red status	0,00										
23			% yellow status	17,34										
24			% green status	82,66										
25				100,00										
26														

Figure 39: : Overall status when all other indicators are green



## Evaluating Gassco's barrier KPI model

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
26														
27	<b>Colour interpretation</b>	<b>Reactive indicator:</b>	<b>Weight:</b>	<b>January</b>	<b>February</b>	<b>March</b>								
28	5 Chosen	Gas detection, automatic	2	Green	Green	Green								
29	Others	Ignition Source Control	2	No data input	No data input	No data input								
30		HVAC	1	Green	Green	Green								
31		ESD - Valves	3	Red	Red	Red								
32		ESD - Pushbutton	3	Green	Green	Green								
33		Safety critical PSD valves	2	ESD valve also have PSD function	ESD valve also	ESD valve also have PSD function								
34		Blowdown	3	Green	Green	Green								
35		Fire detection	2	Green	Green	Green								
36		Deluge valve	2	Red	Red	Red								
37		Deluge nozzle	2	Red	Red	Red								
38		Fire Water pumps	2	Red	Yellow	Yellow								
39		PA system	1	Yellow	Green	Green								
40		Emergency power generator	2	Red	Red	Red								
41		UPC capacity	2	Green	Green	Green								
42		Emergency lightning	1	Green	Green	Yellow								
43		Aggregated reactive elements:		Yellow	Yellow	Yellow								
44														
45														
46	<b>All other indicators 50% green status, 50% yellow, highest weight yellow:</b>													
47			Possible values	ESD valve red							1,67	1,87	2,07	2,27
48		ESD valve green		1,37	1,43	1,50	1,57	1,63	1,73	1,57	1,77	1,97	2,17	
49		ESD valve yellow			1,47	1,53	1,60	1,67						
50		Indicator weight:												
51		2	Gas detection	green	green	green	green	green	yellow	green	green	green	green	green
52		3	ESD valve	green	green	green	green	yellow	yellow	green	green	green	red	red
53		2	Safety Critical PSD valve	green	green	green	yellow	yellow	yellow	green	green	red	red	red
54		2	Ignition source	green	green	yellow	yellow	yellow	yellow	green	red	red	red	red
55		2	Deluge valve	green	yellow	yellow	yellow	yellow	yellow	red	red	red	red	red
56			Number of combinations		1	5	10	10	5	1	5	10	10	5

Figure 41: Overall status when all other indicators are 50 % green and 50 % yellow



## Evaluating Gassco`s barrier KPI model

O	P	Q	R	S	T	U	V	W	X	Y	Z	AA
	1,73	1,80	1,87	1,93	1,57	1,67	1,97	2,00	1,93	2,07	2,20	
2,47	1,63	1,70	1,77		1,47	1,67		1,90				
	1,67	1,73	1,80	1,87	1,50	1,70	1,90	1,93	1,87	2,00	2,13	
red	green	green	green	yellow	green	green	yellow	green	yellow	yellow	yellow	
red	green	green	yellow	yellow	green	yellow	red	red	yellow	yellow	yellow	
red	green	yellow	yellow	yellow	yellow	red	red	red	yellow	yellow	red	
red	yellow	yellow	yellow	yellow	red	red	red	yellow	yellow	red	red	
red	red	red	red	red	red	red	red	yellow	red	red	red	
1	20	30	20	5	30	20	5	30	5	10	10	248

Figure 42: Overall status when all other indicators are 50 % green and 50 % yellow – continuing from figure 35

## Evaluating Gassco`s barrier KPI model

	A	B	C	D	E	F	G	H	I	J
57			Possible red status	1						
58			Possible yellow status	177						
59			Possible green status	70						
60										
61										
62			<b>% red status</b>	<b>0,40</b>						
63			<b>% yellow status</b>	<b>71,37</b>						
64			<b>% green status</b>	<b>28,23</b>						
65				<b>100,00</b>						
66										
67										
68	Installation status:									
69	Aggregated values:	green	yellow	red	yellow	green	yellow	yellow	yellow	red
70										
71	Reactive elements	green	yellow	red	green	green	green	yellow	yellow	red
72	Proactive elements	green	yellow	red	yellow	green	green	yellow	yellow	red
73	Management elements	green	yellow	red	red	yellow	red	green	red	green
74	Number of com.	1	1	1	1	1	1	1	1	1
75										
76			Possible red status	2						
77			Possible yellow status	4						
78			Possible green status	2						
79										
80										
81			<b>% red status</b>	<b>25,00</b>		<b>Red on installation level:</b>	<b>0,1</b>			
82			<b>% yellow status</b>	<b>50,00</b>						
83			<b>% green status</b>	<b>25,00</b>						
84				<b>100,00</b>						

Figure 43: Calculations installation combinations

# Evaluating Gassco`s barrier KPI model

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	
1																																
2	Checking number of possible combinations:																															
3																																
4	green	yellow	yellow	green	red	red	green	yellow	yellow	green	yellow	green	green	yellow	green	yellow	green	yellow	yellow	green	green	green	green	yellow	yellow	yellow	red	red	red	red	red	
5	green	yellow	yellow	green	green	yellow	yellow	green	green	yellow	yellow	green	yellow	green	yellow	green	yellow	green	green	green	yellow	red	red	red	yellow	red	red	red	green	green	yellow	yellow
6	yellow	green	red	red	green	yellow	green	yellow	green	yellow	green	green	yellow	green	red	red	red	red	red	red	green	yellow	yellow	yellow	green	green	green	yellow	yellow	green	green	
7	yellow	green	green	yellow	yellow	green	yellow	green	yellow	green	green	red	red	red	red	red	red	green	yellow	green	yellow	yellow	green	yellow	green	yellow	green	green	green	yellow	green	
8	red	red	green	yellow	yellow	green	red	red	red	red	red	green	yellow	yellow	green	green	yellow	yellow	green	yellow	green	yellow	yellow	green	green	green	green	yellow	yellow	green	yellow	green
9																																
10																																
11																																
12	Controlling number of combinations:																															
13	green	green	green	red	red	red	green	green	green	yellow	yellow																					
14	green	green	red	yellow	green	red	green	green	yellow	green	green																					
15	green	red	yellow	green	green	green	green	red	green	red	green																					
16	red	yellow	green	green	green	green	green	green	red	green	red																					
17	yellow	green	green	green	yellow	yellow	yellow	green	green	green	green																					
18	Occurring x times:	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
19	green	green	green	yellow	yellow	green	green	green	green	yellow	yellow																					
20	green	green	yellow	yellow	green	yellow	green	yellow	green	yellow	green	green																				
21	green	yellow	yellow	green	green	green	green	yellow	green	yellow	green																					
22	yellow	yellow	green	green	green	green	green	green	yellow	green	green																					
23	yellow	green	green	green	yellow	yellow	yellow	green	green	green	green																					
24	Occurring x times:	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
25	green	green	red	green	yellow	green	red	green	green	green	green	green	yellow	green	green	red																
26	green	green	yellow	red	yellow	yellow	green	yellow	red	red	yellow	green	yellow	yellow	green	yellow	yellow	green														
27	yellow	red	yellow	green	green	green	yellow	red	yellow	yellow	red	green	green	yellow	yellow	red	green	green	yellow	yellow												
28	yellow	yellow	green	yellow	red	yellow	green	green	green	yellow	yellow	red	red	green	yellow																	
29	red	yellow	green	yellow	green	red	red	yellow	yellow	yellow	green	green	yellow	yellow	red	green																
30	Occurring x times:	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	

Figur 44: Quality check - number of possible combinations

## Evaluating Gassco's barrier KPI model

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
8			Possible values	ESD valve red							1,30	1,50	1,70	1,90
9				ESD valve green	1,00	1,07	1,13	1,20	1,27	1,37	1,20	1,40	1,60	1,80
10		Indicator weight:		ESD valve yellow		1,10	1,17	1,23	1,30					
11		2	Gas detection		green	green	green	green	green	yellow	green	green	green	green
12		3	ESD valve		green	green	green	green	yellow	yellow	green	green	green	red
13		2	Safety Critical PSD valve		green	green	green	yellow	yellow	yellow	green	green	red	red
14		2	Ignition source		green	green	yellow	yellow	yellow	yellow	green	red	red	red
15		2	Deluge valve		green	green	yellow	yellow	yellow	yellow	green	red	red	red
16			Number of combinations		1	$= ((\$C\$30*1)+(\$C\$32*1)+(\$C\$34*1)+(\$C\$35*1)+(\$C\$37*1)+(\$C\$38*1)+(\$C\$39*1)+(\$C\$40*1)+(\$C\$41*1)+(\$C\$42*1)+(\$C\$28*1)+(\$C\$29*1)+(\$C\$31*1)+(\$C\$33*1)+(\$C\$36*1))*((1)/((\$C\$30+\$C\$32+\$C\$34+\$C\$35+\$C\$37+\$C\$38+\$C\$39+\$C\$40+\$C\$41+\$C\$42+\$C\$28+\$C\$29+\$C\$31+\$C\$33+\$C\$36)))$								
17			Possible red status		0									
18			Possible yellow status		43									
19			Possible green status		205									
22			% red status		0,00									
23			% yellow status		17,34									
24			% green status		82,66									
25					100,00									
27	Colour interpretation	Reactive indicator:	Weight:	January	February	March								
28	5 Chosen	Gas detection, automatic	2	Green	Green	Green	Green value: $1 \leq x < 1.67$							
29	Others	Ignition Source Control	2	No data input	No data input	No data input	Yellow value: $1.67 \leq x < 2.33$							
30		HVAC	1	Green	Green	Green	Red value: $2.33 \leq x < 4$							
31		ESD - Valves	3	Red	Red	Red								
32		ESD - Pushbutton	3	Green	Green	Green								
33		Safety critical PSD valves	2	ESD valve also have PSD function	ESD valve also have PSD function	ESD valve also have PSD function								
34		Blowdown	3	Green	Green	Green								
35		Fire detection	2	Green	Green	Green								
36		Deluge valve	2	Red	Red	Red								
37		Deluge nozzle	2	Red	Red	Red								

Figure 45: Formula used when calculating possible values

Formula B.1 is used to calculate all values in the colour table.

### G. Calculations moving average

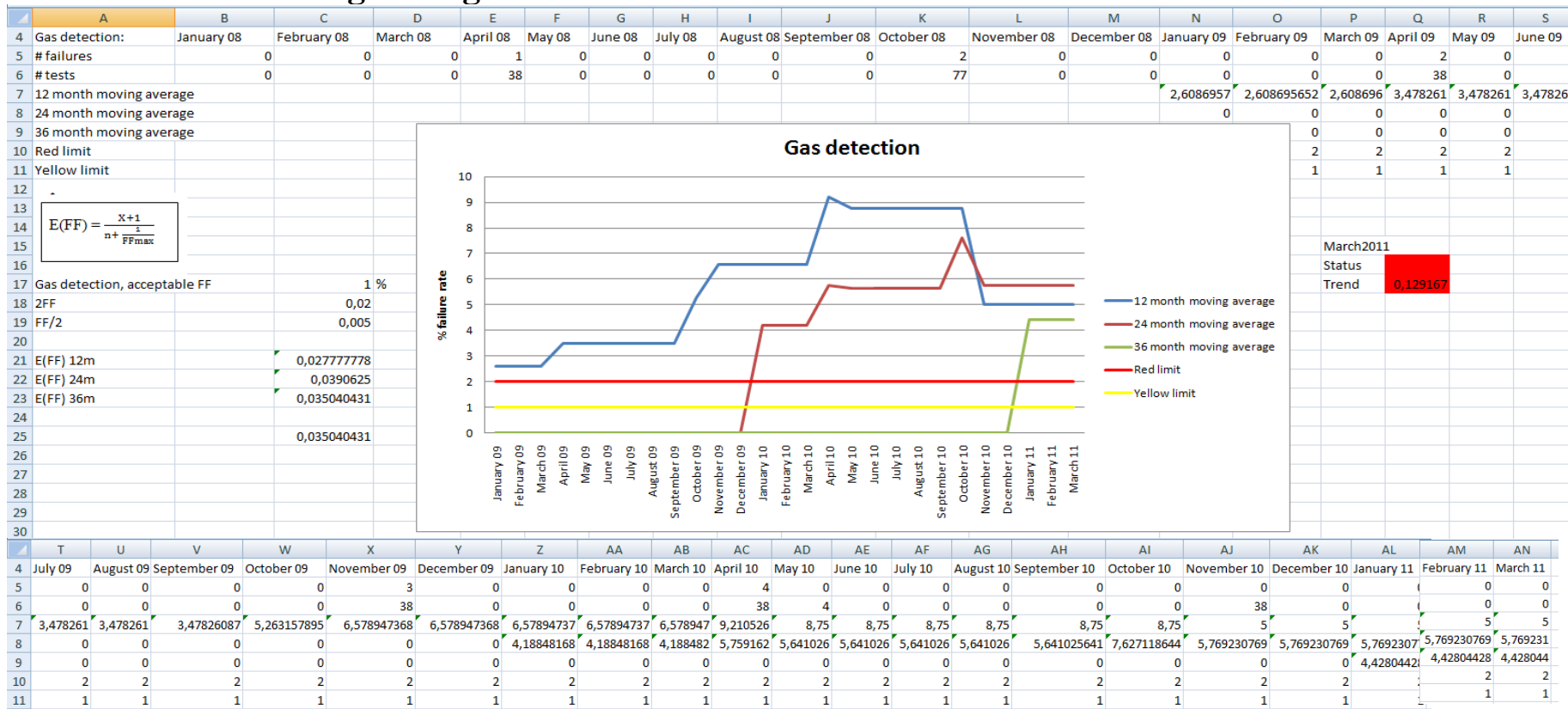


Figure 46: Calculations moving average and FF gas detection

## Evaluating Gassco`s barrier KPI model



Figure 47: Calculations moving average, aggregated and FF gas detection

## Evaluating Gassco's barrier KPI model

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
29																
30		January 10	February 10	March 10	April 10	May 10	June 10	July 10	August 10	September 10	October 10	November10	December10	January 11	February 11	March 11
31	24 month moving average	4,188481675		4,188481675	4,188481675	5,759162	5,641026	5,641026	5,641026	5,641026	5,641025641	7,627118644	5,769230769	5,769230769	5,769230769	5,769231
32	Aggregated value	0,814479638		0,814479638	0,814479638	1,137358	1,133391	1,133391	1,133391	1,133391	1,133391456	1,133391456	1,097046414	1,097046414	1,0970464	1,097046
33	% different	80,55429864		80,55429864	80,55429864	80,25133	79,90806	79,90806	79,90806	79,90806	79,90806055	85,13997869	80,98452883	80,98452883	80,984529	80,98452883
34	Status															
35	Trend															

Figure 48: Calculations different status/trend when using method suggested in chapter 5.4

Formulas used in figure 46 and 47:

	A	B	AL	AM	AN
1			January 11	February 11	March 11
2			0	0	0
3			0	0	0
4	Gas detection:	January 08	February 08		
5	# failures	0	0		
6	# tests	0	0		
7	12 month moving average		$=\frac{\text{SUM}(\text{AA5}:\text{AL5})}{\text{SUM}(\text{AA6}:\text{AL6})} * 100$	$=\frac{\text{SUM}(\text{AB5}:\text{AM5})}{\text{SUM}(\text{AB6}:\text{AM6})} * 100$	$=\frac{\text{SUM}(\text{AC5}:\text{AN5})}{\text{SUM}(\text{AC6}:\text{AN6})} * 100$
8	24 month moving average		$=\frac{\text{SUM}(\text{O5}:\text{AL5})}{\text{SUM}(\text{O6}:\text{AL6})} * 100$	$=\frac{\text{SUM}(\text{P5}:\text{AM5})}{\text{SUM}(\text{P6}:\text{AM6})} * 100$	$=\frac{\text{SUM}(\text{Q5}:\text{AN5})}{\text{SUM}(\text{Q6}:\text{AN6})} * 100$
9	36 month moving average		$=\frac{\text{SUM}(\text{C5}:\text{AL5})}{\text{SUM}(\text{C6}:\text{AL6})} * 100$	$=\frac{\text{SUM}(\text{D5}:\text{AM5})}{\text{SUM}(\text{D6}:\text{AM6})} * 100$	$=\frac{\text{SUM}(\text{E5}:\text{AN5})}{\text{SUM}(\text{E6}:\text{AN6})} * 100$
10	Red limit		2	2	2
11	Yellow limit		1	1	1
12					
13					
14	$E(\text{FF}) = \frac{X+1}{n + \frac{1}{\text{FFmax}}}$				
15					
16					
17	Gas detection, acceptable FF		1		
18	2FF		=0,01*2		
19	FF/2		=0,01/2		
20					
21	E(FF) 12m		$=\frac{\text{SUM}(\text{AA5}:\text{AL5})+1}{\text{SUM}(\text{AA6}:\text{AL6})+(1/0,01)}$		
22	E(FF) 24m		$=\frac{\text{SUM}(\text{O5}:\text{AL5})+1}{\text{SUM}(\text{O6}:\text{AL6})+(1/0,01)}$		
23	E(FF) 36m		$=\frac{\text{SUM}(\text{C5}:\text{AL5})+1}{\text{SUM}(\text{C6}:\text{AL6})+(1/0,01)}$		
24					
25			$=\frac{12+1}{271+100}$		

All average values are calculated by using this type of formula

Figure 49: Formulas used when calculating moving average and FF

## Evaluating Gassco's barrier KPI model

	A	B	C	AL	AM
3					
4	Gas detection:	January 08	February 08	March 08	
5	# failures	0	0	0	
6	# tests	0	0	0	January 11
7	12 month moving average			0	February 11
8	24 month moving average			0	0
9	36 month moving average			0	0
10	Aggregated data since 2001			0	0
11	Red limit			1	1
12	Yellow limit			2	2
13					
14	$E(FF) = \frac{x+1}{n + \frac{1}{FF_{max}}}$				
15					
16					
17					
18					
19	Gas detection, acceptable FF		1	%	
20	2FF		=0,01*2		
21	FF/2		=0,01/2		
22					
23	E(FF) 12m		= (SUM(AA5:AL5)+1)/(SUM(AA6:AL6)+(1/0,01))		
24	E(FF) 24m		= (SUM(O5:AL5)+1)/(SUM(O6:AL6)+(1/0,01))		
25	E(FF) 36m		= ((SUM(C5:AL5)+1)/((SUM(C6:AL6)+(1/0,01))		
26					
27	E(FF) aggregated		= (SUM(\$C\$5:AN5)+1)/((SUM(\$C6:AN6)+864)+(1/0,02))		

All average values are calculated by using this type of formula

Figure 50: Formulas used when calculating aggregated values and FF

	A	B	C	D	E
29					
30		January 10	February 10	March 10	April 10
31	24 month moving average	4,18848167539267	4,18848167539267	4,18848167539267	5,75916230366492
32	Aggregated value	0,81447963800905	0,81447963800905	0,81447963800905	1,13735783027122
33	% different	=((B31-B32)/B31)*100	=((C31-C32)/C31)*100	=((D31-D32)/D31)*100	=((E31-E32)/E31)*100
34	Status				
35	Trend				
36					

Figure 51: Formulas used when calculating different status/trend using method suggested in chapter 5.4