

RELIABILITY ESTIMATION OF PRESSURE SAFETY LOW (PSL) IN OIL AND GAS PRODUCTION

A DISSERTATION

*Submitted in partial fulfillment of the
requirements for the award of the degree*

of

MASTER OF TECHNOLOGY

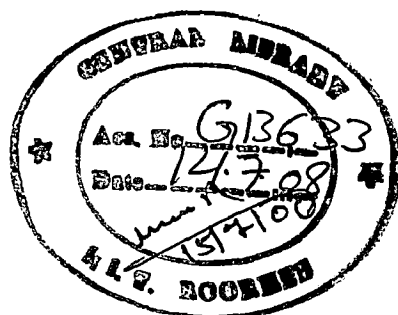
in

CHEMICAL ENGINEERING

(with specialization in Industrial Safety and Hazards Management)

By

HITENDRA KUMAR JAISWAL



**DEPARTMENT OF CHEMICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE -247 667 (INDIA)
JUNE, 2007**

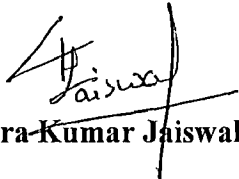
CANDIDATE'S DECLARATION

I hereby declare that the work which is being presented in the dissertation entitled “**Reliability Estimation of Pressure Safety Low (PSL) in Oil And Gas Production**”, in partial fulfillment of the requirement for the award of the degree of Master of Technology with specialization in **Industrial Safety and Hazards Management**, submitted in the department of Chemical Engineering Department, Indian Institute of Technology Roorkee, is an authentic record of my own work carried out during the period from July 2006 to June 2007, under the guidance of Dr. Nidhi Bhandari , Assistant Professor, Chemical Engineering Department, Indian Institute of Technology Roorkee.

The matter embodied in this project work has not been submitted for the award of any other degree.


Date: 29, June, 2007

Place: IIT Roorkee


(Hitendra-Kumar Jaiswal)

CERTIFICATE

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.


27/5Jun/07

Dr. Nidhi Bhandari

Assistant professor

Chemical Engineering Department

Indian Institute of Technology Roorkee

CONTENTS

| | |
|---|-----|
| List of Figures | i |
| List of Tables | iii |
| Acknowledgement | iv |
| Abstract | v |
| | |
| Chapter 1: Reliability Aspects in Leak Detection | 1 |
| 1.1 The Need for Reliability Estimation..... | 1 |
| 1.2 Benefits of Reliability Analysis..... | 2 |
| 1.3 Reliability in Leak Detection..... | 3 |
| 1.4 Offshore Pipelines and Production Facilities..... | 4 |
| 1.5 Offshore Pipeline Leak Detection..... | 8 |
| | |
| Chapter 2: Literature Reviewed | 14 |
| 2.1 Review of Published Literature..... | 14 |
| 2.2 Failure Data Collection and Analysis..... | 16 |
| | |
| Chapter 3: System Overview | 17 |
| 3.1 Pressure Safety Lows (PSL)..... | 17 |
| 3.2 Sensor Operation..... | 17 |
| 3.3 Sensor Manufacturer and Failure Rate..... | 18 |
| 3.4 PSL Location..... | 19 |
| 3.5 Operational Considerations..... | 20 |
| 3.6 Regulatory Aspects of the PSLs..... | 21 |

| | |
|---|-----------|
| 3.7 Methods of Setting PSLs..... | 23 |
| Chapter 4: Failure Analysis of PSL..... | 25 |
| 4.1 Failure Modes of PSLs..... | 25 |
| 4.2 Failure Classification by Cause of Failure..... | 25 |
| 4.3 Classification of Random Hardware Failures by Failure Mode..... | 27 |
| 4.4 Failure Data for PSL..... | 29 |
| | |
| Chapter 5: Reliability Estimation of PSL via Fault Tree Method... .. | 34 |
| 5.1 Fault Tree Analysis..... | 34 |
| 5.2 Fault Tree Symbols..... | 35 |
| 5.3 Why Fault Tree Analysis Method?..... | 36 |
| 5.4 Main characteristics of the FTA method..... | 37 |
| 5.5 Applications of the FTA Method..... | 38 |
| 5.6 Testing of FTA..... | 38 |
| 5.7 Fault Tree Construction..... | 40 |
| 5.8 Structuring Process..... | 42 |
| 5.9 Reliability Theory..... | 42 |
| 5.10 Reliability Analysis of PSLs..... | 44 |
| | |
| Chapter 6: Results and Discussion..... | 59 |
| | |
| Chapter 7: Conclusion and Future Work..... | 61 |
| | |
| References..... | 62 |
| Appendix..... | 67 |
| Abbreviations..... | 70 |

LIST OF FIGURES

| FIGURE | PAGE NO. |
|--|----------|
| Figure 1.1: Subsea Production Facility Tied-back to Host Platform with Flow lines..... | 5 |
| Figure 1.2: Transmission Pipelines | 5 |
| Figure 1.3: Canyon Express Pipeline System..... | 7 |
| Figure 1.4: Relative Scale of Leak Detection..... | 10 |
| Figure 3.1: Pipeline Pressures during PSL Shut-in and Subsequent Recovery | 17 |
| Figure 3.2: Typical Pressure Sensor..... | 18 |
| Figure 3.3: Platforms and Pipeline – Location of Pressure Monitoring..... | 19 |
| Figure 3.4: Details of an Offshore Pipeline..... | 20 |
| Figure 3.5: Example Pipeline Pressure Chart..... | 23 |
| Figure 4.1: Failure classification by cause of failure..... | 25 |
| Figure 4.2: Failure Mode Classification-Component Level..... | 28 |
| Figure 5.1: Fundamental structures of fault tree..... | 41 |
| Figure 5.2: Gaseous Flow – Failure to trip with leak present – PSL only..... | 47 |
| Figure 5.3: Gaseous Flow – False Trip – PSL only..... | 48 |
| Figure 5.4: Gaseous Flow – Failure to trip with leak present - MFS only | 49 |
| Figure 5.5: Gaseous Flows – False Trip – MFS only..... | 50 |
| Figure 5.6: Liquid Flow – Failure to trip with leak present – PSL only..... | 51 |
| Figure 5.7: Liquid Flow – False trip – PSL only..... | 52 |
| Figure 5.8: Liquid Flow – Failure to trip with leak present – MFS only..... | 53 |
| Figure 5.9: Liquid Flow- False trip – MFS only..... | 54 |

| FIGURE | PAGE NO. |
|--|-----------------|
| Figure 5.10: Multiphase Flow- Failure to trip with leak present-PSL only..... | 55 |
| Figure 5.11: Multiphase Flow-False trips- PSL only..... | 56 |
| Figure 5.12: Multiphase Flow – Failure to trip with leak present-MFS only..... | 57 |
| Figure 5.13: Multiphase Flow-False trip- MFS only..... | 58 |
| Figure 6.1: Result for Failure to Trip..... | 59 |
| Figure 6.2: Result for False Trip..... | 60 |

LIST OF TABLES

| TABLE | PAGE NO. |
|---|----------|
| Table 4.1: Failure Causes with Example..... | 26 |
| Table 4.2: Failure Data for PSL..... | 33 |
| Table 5.1: Gate symbols and their description..... | 35 |
| Table 5.2: Event symbols and their description..... | 36 |
| Table 5.3: Matrix of FTA Pipeline Cases..... | 44 |
| Table 5.4: Basic Event Data..... | 46 |
| Table 6.1: Probabilities of Top Events..... | 59 |

ACKNOWLEDGEMENT

Expression of going thanks are just a part of those feeling which are too large for words but shall always remain as memories of the wonderful people with whom I have got the pleasure of working during the completion of project.

College is an organization which trains a lot of technical trainees. They not only train us but also they change entire prospect of our life so I am grateful to Indian Institute of Technology, Roorkee which helped me to do so.


I would like to thank my supervisor, Dr. Nidhi Bhandari for her encouragements and guidance. She has continuously provided me with constructive and insightful feedback on my work. I could always count on her for moral and intellectual support, and I owe her a great deal more than just this report.

I am also grateful to Dr. Shri Chand, HOD, Chemical Engineering Department, Indian Institute of technology Roorkee, for providing me the necessary facilities for the completion of this report.

Furthermore, I would like to extend my gratitude toward my friends particularly Mr. Sukalyan Ghosh, Mr. Raghvendra and Mr. Manoj L. Das for their contributions and for their effort in making the atmosphere as pleasant and inspiring as possible.

Finally, I would like to convey my gratefulness and appreciation to my parents for their support, encouragement and blessing. Also, I would like to express my appreciation to my wife Deep Shikha, not only for their patience but also for her love, endless support and continuous sharing of every moment. I am grateful, as well, to my brothers, sister, and their families, for their love, encouragement and blessing.

In the end, I thank all those who have contributed to my work at least by a word or a thought during this period.


(Hitendra Kumar Jaiswal)

ABSTRACT

The chemical industry as a whole is responsible for preventing major accidents, not only to prevent human fatality and injury, but also to protect the environment and to improve public perception of chemical engineering as a favorable and integral part of society. Especially in oil and gas production facilities safety plays a vital role. There are many safety instrumented systems used in this facility. Pressure Safety Low (PSL) is one of them that is used to detect leak in offshore pipeline based on pressure within the pipeline. PSLs are low-pressure alarms used to monitor oil and gas production facilities. The PSL pipeline alarms are intended to shut-in the production facility in the event of a system leak or catastrophic event. hence the operation of PSL needs to be highly reliable.

This can be assessed by PSL reliability study to address the following questions. When do PSLs function correctly to identify a leak in an offshore pipeline? What conditions may create false alarms with PSLs? Under what conditions do PSLs fail to detect a leak?

As part of loss prevention in the oil and gas production, this dissertation is focused on the probabilistic analysis of safety and reliability over the operating part of the process life cycle of PSL. The methodology developed is data driven with continuous updating of reliability data and models the trade off between safety and economics is plant operation. Then it is continuously quantified and forms the basis for improving design, operation and maintenance strategies. In this dissertation also comparison made between two types of leak detection system first one is the pressure safety low other is mass flow sensor.

Dedicated to My Parents and My Wife Deep Shikha, for their unconditional love and ongoing support, for always being there and believing in me. Thanks for always helping me to remember what is important in life and just hearing me out when I needed it the most.

CHAPTER 1

RELIABILITY ASPECTS IN LEAK DETECTION

1.1 The Need for Reliability Estimation

Microprocessors are increasingly replacing electromechanical relays in safety systems in the process industry. Computer-based fire and gas detection systems, process shutdown systems, and emergency shutdown systems are installed to prevent abnormal operating conditions from developing into an accident. Further, a major increase in the use of this kind of systems is anticipated also in other business sectors such as the public transport industry (air and rail) and the manufacturing industry. The background for this is that there are benefits in terms of cost and manufacturing flexibility, without jeopardizing safety (Lars, 1995)

Computer-based systems may contain hidden errors that may lead to potentially disastrous system failure, perhaps after many years of correct operation. Further, it is hardly possible to construct these systems completely fail-safe. It can not be claimed that all possible failure modes are identified, and thus it can not be assured that a fail-safe response is designed for all the failure modes.

If safety and reliability is addressed in the entire life cycle of the safety systems, significant commercial advantages and reduced commercial risks can be achieved. Some examples are (Bodsberg, 1999):

- ◆ **Access to a larger market:** The operators will demand compliance with the standards and regulations that are emerging. Not addressing these issues is likely to reduce an organization's potential market share. Even where standards are not mandatory and there is no regulation, those who build and operate systems to a recognized standard will have a benefit that should result in increased market share.

- ◆ **Reduced litigation risks:** Systems built and operated in line with recognized practice are less likely to face litigation should an accident occur. Furthermore any costs coming as a result of such litigation may be significantly mitigated.
- ◆ **Reduced direct losses:** System failure can have a direct effect on profitability. Appropriate attention to safety reduces the likelihood of failures and can minimize the consequences of failures.
- ◆ **Reduced bad publicity:** Safety related incidents usually lead to bad publicity.

It should be verified that the safety requirements of safety systems are fulfilled, and here the reliability estimation plays an important role.

1.2 Benefits of Reliability Analysis

The first step towards solving a problem is to fully understand its nature. If we don't, we may draw erroneous conclusions. Reliability analysis may be used as a systematic tool for understanding the system from a safety and production regularity point of view, and thereby understanding how to improve it.

Some main applications of reliability analysis are (SINTEF, 2003):

- ◆ **Reliability assessment:** Verifying that the system fulfils its safety and reliability requirements.
- ◆ **Design optimization:** Balancing the design to get an optimal solution with respect to safety, production regularity and Life Cycle Cost.
- ◆ **Operation planning:** To establish the optimal testing and maintenance strategy.
- ◆ **Modification support:** To verify that planned modifications are legal with respect to the safety and reliability requirements.

Documenting safety, reliability, maintainability and/or production regularity is an important application of reliability analysis. Also, it is becoming increasingly more important to verify the quality of the products and systems in terms of their reliability attributes. IEC 61508 is an example of a standard stating requirements to Safety Instrumented Systems (SIS), and this standard is currently becoming the main standard within the SIS industry. The standard sets

out a generic approach for all safety lifecycle activities for SIS. IEC 61508 is a generic standard common to several industries, and the process industry is currently developing their own sector specific standard for application of SIS, called the IEC 61511. Both these standards present a unified approach to achieve a rational and consistent technical policy for all SIS systems.

The IEC standard focuses on safety unavailability, although when designing safety shutdown systems there is generally a conflict between safety and production regularity.

Although most reliability analyses have been used to gain confidence in the system by assessing the reliability attributes, it is perhaps more interesting to use reliability analysis as a means to achieve reliability, e.g., by design optimization. It would usually be efficient to employ these techniques in the design phase of the system, when less costly changes can be made. Proper analytic tools available during the design process may ensure that an optimal system configuration is installed from the very beginning, thereby reducing overall system cost.

1.3 Reliability in Leak Detection

In the offshore industries, pipelines are the facilities that spill the largest volume of hydrocarbons. Minerals Management Service information indicates that more than 2000 pipeline incidents have been noted since 1969. (MMS, 2001)

From a regulatory standpoint, pipeline leak detection focuses on the use of pressure safety lows (PSLs). PSLs are low-pressure alarms used to monitor oil and gas production facilities. The PSL pipeline alarms are intended to shut-in the producing facility in the event of a system leak or catastrophic event (Health and Safety Executive, 2003).

PSL alarms typically operate with discrete pressure sensors, linked to local controllers, or linked to supervisory, control and data acquisition systems (SCADA). For an offshore pipeline, pressure alarms are placed on the platform immediately upstream of the pipeline junction, and on the fluid receiving facility at the downstream end of the pipeline.

From a leak detection standpoint, three possible outcomes exist:

1. A leak occurs and the PSL alarm is triggered
2. A leak occurs and no PSL alarm is triggered
3. No leak occurs and a PSL alarm is triggered

Case 1 is the outcome expected. Case 2 is of greatest concern, from a regulatory, safety and an environmental standpoint, particularly as operations move into deeper water. Case 3 is a concern to operators because repeated false alarms undermine the trustworthiness of the leak detection method.

It has been observed that many pipeline leaks are not detected by a PSL alarm. Further, operators have reported frequent false alarms if the PSL alarm is set within a narrow margin of the system operating pressure. For these reasons this PSL study to address the following questions:

- ◆ When do PSLs function correctly to identify a leak in an offshore pipeline?
- ◆ What conditions may create false alarms with PSLs?
- ◆ Under what conditions do PSLs fail to detect a leak?

The dissertation addresses these questions by examining the occurrences of PSL alarms, the occurrences of leaks, and the operation of offshore pipelines. PSL reliability is determined based on frequency of occurrence, using probabilistic risk methods and fault tree analysis.

1.4 Offshore Pipelines and Production Facilities

Offshore pipelines can be infield pipelines, gathering lines or transmission lines. Infield lines are typically smaller diameter lines that connect facilities within the same field. For example, infield lines may connect two platforms, a subsea template to a platform, or a production manifold to a production facility. Figure 1.1 illustrates a subsea complex tied back to a host platform.

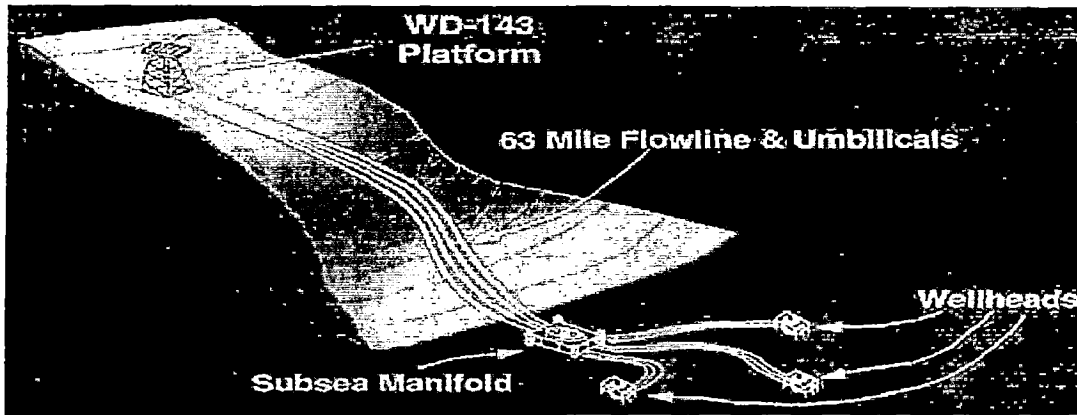


Figure 1.1: Subsea Production Facility Tied-back to Host Platform with Flow lines
(www.offshore-technology.com)

Gathering lines refer to pipelines that connect fluids from multiple facilities, or lines that connect the field production to the major transmission line. Gathering lines may be small to medium diameter.

Transmission lines, or trunk lines, are larger diameter pipelines used to transport production to the processing facility onshore. Transmission lines typically carry combined production from multiple offshore production facilities. The production is most frequently combined through gathering lines that route the fluids to a single platform. The transmission line then transports the fluids from the collection hub to the processing facility on shore. Figure 1.2 illustrates the concept of transmission pipelines.

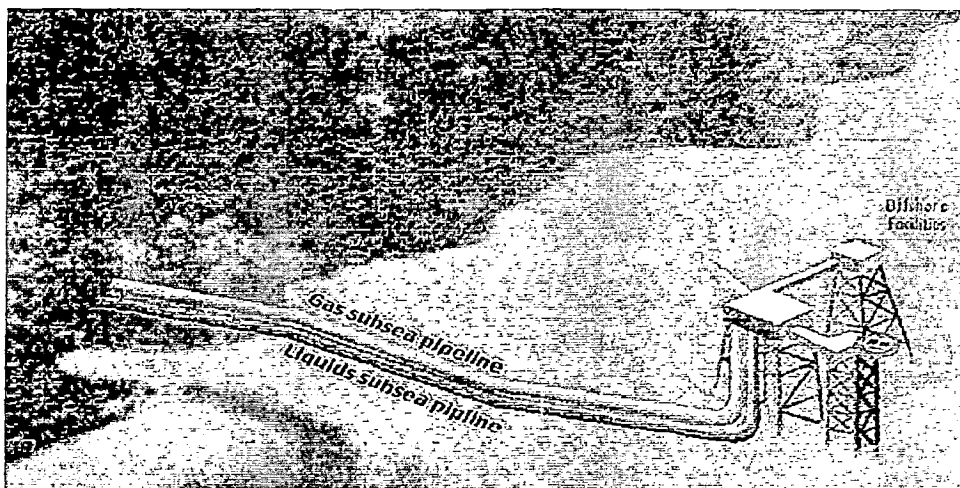


Figure 1.2: Transmission Pipelines (www.offshore-technology.com)

It is common practice to provide a subsea tap for a subsea tie-in along transmission or gathering pipelines. If one pipeline is connected to another pipeline in this manner the fluids are commingled at the point of the subsea tie-in. No pressure or flow measurement is taken subsea at this juncture.

Frequently, the operator of the transmission pipeline is not the operator of the system platforms. This presents a challenge in communications. The platform operators must coordinate their operations with that of the transmission pipeline, and provide information as needed.

Transmission pipelines differ from other offshore lines because the transmission line connects the final production facility to shore. Transmission pipelines are typically either oil or gas pipelines. Multiphase flow introduces complexities in operation and pressure loss and, for this reason, industry has preferred to construct separate oil and gas transmission lines to shore in the shallow outer continental shelf (OCS). Deepwater pipelines may include multiphase flow in the future, but those constructed to date have also been single-phase flow.

Subsea flowlines typically carry multiphase flow (oil, water, gas) because the fluids have not yet reached separation facilities. Subsea wells typically include a pressure sensor at the wellhead, but most subsea systems do not include multi-phase subsea flow monitoring. A notable exception is the Canyon Express pipeline system (US).

The Canyon Express Pipeline System (Figure 1.3) produces three fields, under different operating regimes and varying production rates from multiple zone completions. To accomplish this without any field taking on the performance risk of another field, accurate flow allocation was deemed essential, and subsea multi-phase flow meters were included on each of the subsea wells.

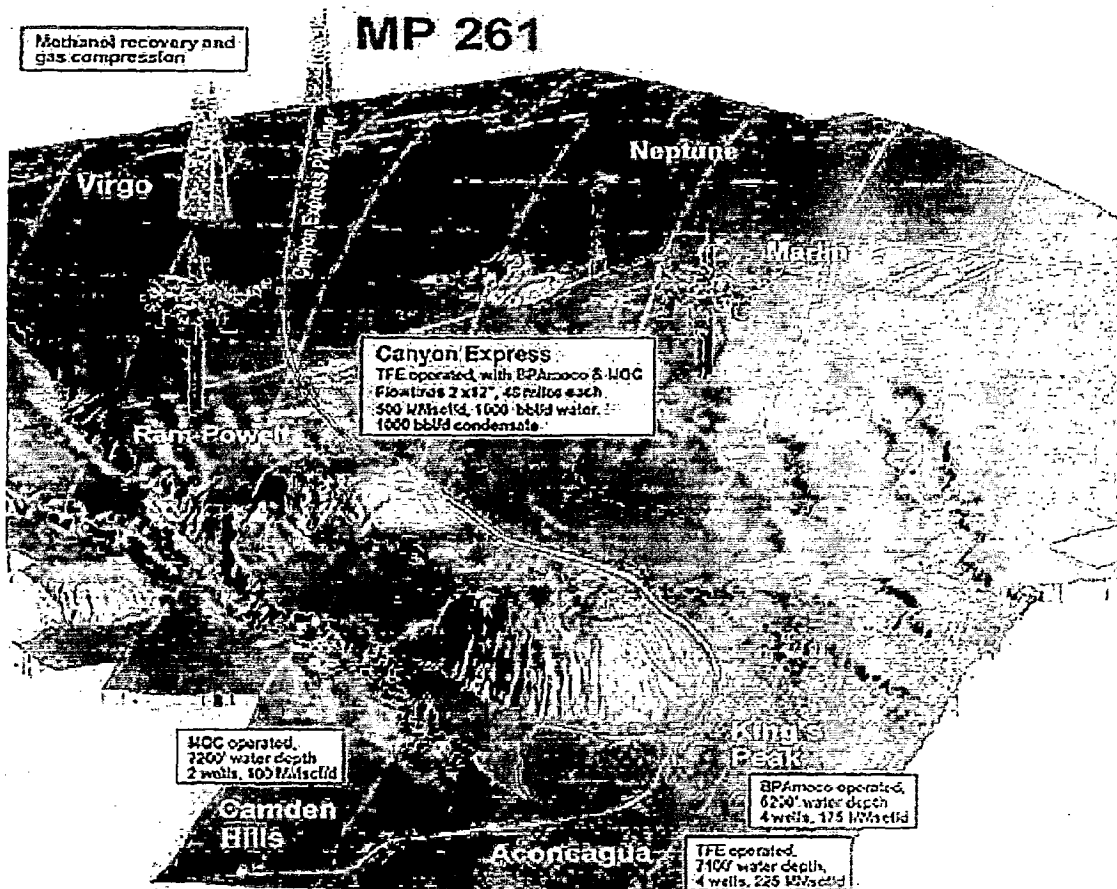


Figure 1.3: Canyon Express Pipeline System (www.offshore-technology.com)

The gas from the three fields will be transported along a gathering system consisting of dual 12-inch pipelines (Figure 1.3).

Supervisory Control and Data Acquisition (SCADA) systems are employed extensively offshore. Gathering pipelines and transmission pipelines are included in such monitoring systems where they exist. Pipeline pressure sensors and flowmeters are linked directly to the platform central processing unit (CPU) via direct connections or through subsea umbilicals.

The existence of SCADA capabilities offshore has implications for offshore leak detection, because certain methods of leak detection require periodic data polling.

1.5 Offshore Pipeline Leak Detection

Multiple methods of leak detection exist and are being applied offshore. The methods frequently applied include visual inspection, pressure monitoring (PSLs), and computational pipeline monitoring. (Health and Safety Executive, 2003)

1.5.1 Visual Inspection

Visual inspection refers to manually looking for a release, by having a helicopter (or a seaplane) fly over the pipeline route and examine the ocean for a hydrocarbon sheen or a similar indication of a release. This method of leak detection is performed routinely, by major pipeline operators (particularly on transmission lines). Many other leaks are seen and reported by offshore personnel, either while flying to a platform or while working on a platform offshore. Remotely operated vehicles (ROVs) may also aid in visual inspection of pipelines.

1.5.2 Pressure Monitoring (PSLs)

Pressure changes are commonly used as a means of leak detection offshore. Pressure sensors are included on the production platform, as the fluids exit the platform into the pipeline or gathering line. A second pressure sensor is located either at the inlet of the next platform, or onshore in the case of a transmission pipeline.

The pressure sensors are set lower than the normal operating pressure of the pipeline. If a leak occurs, then the pipeline pressure drops below the normal operating pressure. If the pressure drops below the level of the PSL and alarm is registered and production is shut-in. Operators who do not employ SCADA monitoring of their production facilities tend to rely on PSLs for their principal leak detection method.

1.5.3 Monitoring Flow Volumes

PSL alarm information can also be combined with monitoring flow volumes to ascertain whether an alarm event is actually a release. In this method, the pipeline operator monitors the volume received into the pipeline over a period of time and checks this against the volumes produced at the pipeline terminus. If the volumes produced are less

than those entering the line, a leak is confirmed. 'Rate of change' in system pressure or flow can also be monitored to yield the same result. This method can work well in liquid filled pipelines provided there is no significant line pack to account for. Simple monitoring of volumes would not be reliable for two phase flow or gas pipelines.

1.5.4 Computational Pipeline Monitoring

Computational pipeline monitoring (CPM) is a term that refers to algorithmic monitoring tools that are used to enhance the abilities of a pipeline controller to recognize anomalies which may be indicative of a release (leak). API publications 1130 (October 1995), 1149 (November 1993) and 1155 (February 1995) summarize various aspects of CPM.

The use of a computational pipeline monitoring system implies that the pipeline operator will employ a SCADA system that polls the pressure sensors and flow meters on a frequent basis. CPM methods cannot be employed unless an operator has this monitoring infrastructure in place.

CPM systems, as well as the other methods of release detection, each have a detection threshold below which commodity release detection cannot be expected. Figure 1.4 indicates that even CPM methods only address commodity releases above some practical detection limit.

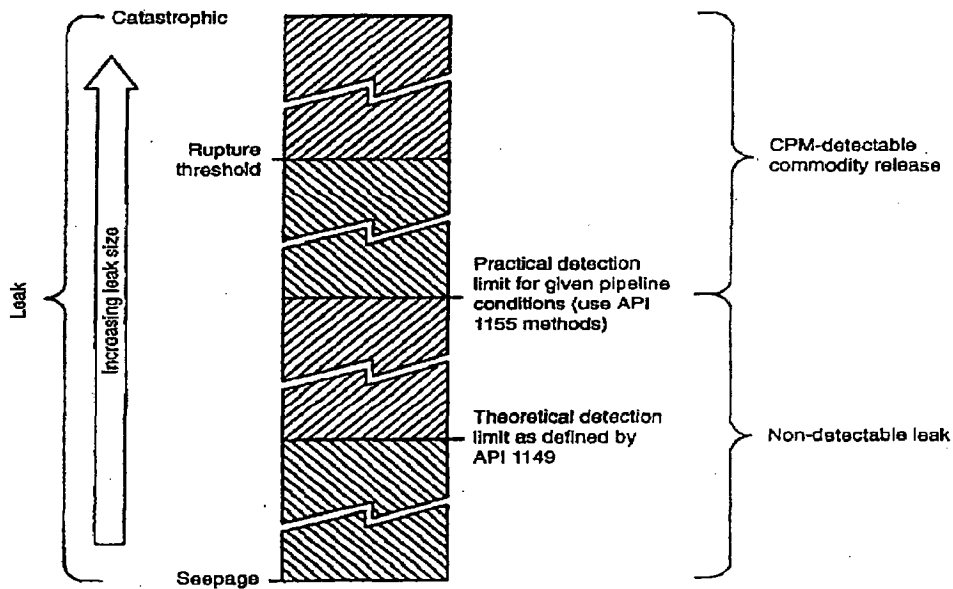


Figure 1.4: Relative Scale of Leak Detection (API 1130)

The following leak detection method descriptions are taken from API 1130.

1.5.6 Line Balance

Line balance is a meter-based method that determines the measurement imbalance between the incoming (receipt) and outgoing (delivery) volumes. The imbalance is compared against a predefined alarm threshold for a select time interval (time window). There is no compensation for the change in pipeline inventory due to pressure, temperature or composition. Imbalance calculations are typically performed from the receipt and delivery meters, but less timely and less accurate volumes can be determined from tank gauging. This method of CPM is the same a manual volume monitoring noted above, but is performed with an algorithm.

1.5.7 Volume Balance

This method is an enhanced line balance technique with limited compensation for changes in pipeline inventory due to temperature and/or pressure. Pipeline inventory correction is accomplished by taking into account the volume increase or decrease in the pipeline inventory due to changes in the system's pressure and/or temperature. It is difficult to manually compensate for changes in pipeline inventory because the

complexity of the imbalance computation. There is usually no correction for the varying inventory density. A representative bulk modulus is used for line pack calculation.

1.5.8 Modified Volume Balance

This is a meter-based enhanced volume balance technique. Line pack correction is accomplished by taking into account the volume change in the pipeline inventory utilizing a dynamic bulk modulus. This modulus is derived from the bulk moduli of the various commodities as a function of their percentage of line fill volume.

1.5.9 Real Time Transient Model

The real time transient model approach is perhaps the most sophisticated CPM method. The fundamental improvement that RTTM provides over the MVB method is that it models all the fluid dynamic characteristics (flow, pressure, temperature). Extensive configuration of physical pipeline parameters (length, diameter, thickness, pipe composition, route topology, internal roughness, pumps, valves, equipment location, etc.) and commodity characteristics (accurate bulk modulus value, viscosity, etc.) are required to design a pipeline specific RTTM. The application software generate a real time transient hydraulic model by this configuration with field inputs from meters, pressure, temperatures, densities and strategic receipt and delivery locations, referred to as software boundary conditions. Fluid dynamic characteristic values are modeled throughout the pipeline, even during system transients.

1.5.10 Pressure/Flow Monitoring

Three approaches to using pressure or flow information can be used. Pressure/flow values that exceed a predetermined alarm threshold are classified as excursion alarms. Initially, excursion thresholds are set out of range of the system operating fluctuations. After the system has reached a steady-state condition, it may be appropriate to set thresholds close to operating values for early anomaly recognition.

Pressure/flow trending is the representation of current and recent historical pressure or flow rate or both. These trends may be represented in a tabular or graphical format on the

control center monitor to enable a controller to be cognizant of these parameter fluctuations. This method can be used to display operating changes that can infer commodity releases.

Rate-of-change (ROC) calculates the variation in a process variable with respect to a defined time interval. The rate at which line pressure or flow or both changes with respect to time are the two most common forms of ROC for pipeline operation. The intent of this approach is to identify rates of change in pressure or flow or both aside from normal operating conditions, thereby inferring a commodity release if operating anomalies cannot be explained.

1.5.11 Acoustic/Negative Pressure Wave

The acoustic/negative pressure wave technique takes advantage of the rarefaction waves produced when the commodity breaches the pipe wall. The release produces a sudden drop in pressure in the pipe at the leak site that generates two negative pressure or rarefaction waves, traveling upstream and downstream. High response rate/moderate accuracy pressure transmitters at select locations on the pipeline continuously measure the fluctuation of the line pressure. A rapid pressure drop and recover will be reported to the central facility. At the central facility, the data from all monitored sites will be used to determine whether to initiate a CPM alarm.

1.5.11 Statistical Analysis

The degree of statistical involvement varies widely with the various methods in this classification. In a simple approach, statistical limits may be applied to a single parameter to indicate an operating anomaly. Conversely, a more sophisticated statistical approach may correlate the averaging of one or more parameters over short and long time intervals in order to identify an anomaly.

The statistical process control (SPC) approach includes statistical analysis on pressure or flow or both. SPC techniques can be applied to generate sensitive CPM alarm threshold from empirical data for a select time window. A particular method of statistical process

control may use line balance 'over/short' data from normal operations to establish upper and lower volume balance imbalance limits. If the volume imbalance for the evaluated time window violates the statistical process control tests, the CPM system will alarm.

All of the API 1130 CPM methods described are applicable only in liquid filled pipelines. Highly volatile liquids, multi-phase, and gas lines are not included in the analysis. However, CPM methods are currently employed in multiphase lines offshore.

Other methods of leak detection, such as clamp on ultrasonic and multi-phase metering are not discussed in this report, because the methods have limited applicability or acceptance offshore. RTTM has been applied to multi-phase flow through subsea flowlines but has not been widely adopted as a leak detection method for multi-phase flow offshore. CPM is the most prevalent method of leak detection, coupled with PSLs.

CHAPTER 2

LITERATURE REVIEWED

Modern technology has developed a tendency to design and manufacture equipment and systems of greater capital cost, sophistication, complexity, and capacity. The disastrous consequences of unreliable behavior of such equipment and systems have led to the desire for higher reliability. The events such as Bhopal, India are prime examples of complex-system failures. As a result, reliability has emerged as one of the vital ingredients in system planning, design, development, and operational phases. The success of reliability engineering in aerospace and military has helped to increase reliability awareness in industries such as nuclear and chemical. In particular, the loss of thousands of human lives and the far-reaching economic, legal, and social implications of the Bhopal accident has further strengthened the reliability consciousness of the chemical industry. In recent years, process plants have grown larger, run at higher temperatures and pressures, and some have become too complex and sophisticated. Factors such as these have led to increase in risks associated with these plants. Therefore, the chemical industry has been increasingly applying reliability engineering principles, especially in instrumentation.

This chapter reviews much of the existing literature on process system reliability. The literature is collected mainly from major journals and conference proceedings. The literature pertaining to chemical process system reliability is concerned with refineries, ammonia plants, chlorine plants, ethylene plants, pressure tanks, boilers, mechanical seals, pumps, valves, protective systems, etc.

2.1 Review of Published Literature

Aird (1982) has assessed the reliability of safety relief valves that perform an essential safety function in the protection of vessels and pipelines. In a subsequent paper (1984) he has provided practical methods for estimating the mean time between failures and its statistical confidence limits. Ansell & Ansell (1987) have developed reliability models for sodium-sulphur cells based on several ceramic degradation mechanisms. The

reliability and hazards analysis of a cumene hydroperoxide plant are developed by Arendt, Casada, and Rooney (1986). Dunglinson and Lambert (1983) described the generation and evaluation of logic models such as fault trees for interval reliability. These concepts were applied to a pressure-tank system and a chlorine vaporizer system.

A new method to test the reliability of operating chemical technological systems was developed by Gaal and Kovacs (1985). Their investigations identified the reliability characteristics of chemical technology systems, demonstrated the characteristics of the time dependence of the breakdown rate, and so on. Gruhn et al. (1983) have studied complex chemical engineering systems. They developed a Markov model for the reliability analysis of a complex piping system. Henley and Gandhi (1975) presented a unified approach for obtaining system reliability and availability parameters from block diagram representations of process systems. Kardos and Lorenz (1987) presented a reduction method for calculating the reliability of complex chemical-systems consisting of processing units and storage tanks.

Reliability in ethylene plants was discussed by Loftus (1970). Margetts (1986) studied the reliability of a dual Programmable Logic Controller system. The reliability analysis of fire protection systems is presented by Miller (1974). Moss & Snaith (1979) discussed practical methods for reliability assessment of chemical plants. The available computer-aided methods for system-reliability assessment are reviewed by Nivolianitou et al. (1986). Ostrander (1971) provided an interesting discussion on spacecraft reliability techniques for industrial plants by illustrating a liquid hydrogen flow system for the Saturn S-II stage. A clear insight into some of the reliability problems at the Puerto Rican refinery is provided by Patterson & Clark (1971). Plant design and its remote location from other industries and equipment suppliers were said to be responsible for initial reliability problems. A reliability analysis of failures pertaining to emergency generators was given by Stevens (1983). Thomas & Zanakis (1974) investigated the reliability of a chemical-process system using simulation. An explanation for improving boiler reliability is provided by Triggs (1978). Williams & Russell (1974) discussed NASA reliability techniques in the chemical industry. A computer model for determining the

reliability of complex integrated process plant systems was developed by Wood et al. (1974). Bloch & Johnson (1985) identified the needed design changes for upgrading of centrifugal pumps by the application of reliability engineering. Seven improvements in the design of medium-duty process pumps could lengthen mean time between failures from 13 months for existing pumps to 25 months. The reliability design in process plants is discussed by Lenz (1970). Rudd (1962) described the concepts of parallel and standby redundancies and applied dynamic programming to determine the optimum design for series processes. Methods are presented for reliability analysis of more complex systems.

2.2 Failure Data Collection and Analysis

Anyakora et al. (1971) present instrument failure-rate data obtained from three chemical works and classified these data in terms of the plant environment. Bello & Bobbio (1981) discussed the need for a reliability data-bank in the petrochemical sector and described the criteria for selecting the items to be investigated, the procedures for the event reports collection, and the statistical analysis techniques. Lees (1973) presented data on the failure modes of the major portion of some 9500 instruments. The survey was limited in scope and was concerned primarily with rates rather than modes of failure. In a subsequent paper, Lees (1976) reviewed the instrument failure data. Sherwin (1983) presents a detailed account of a data collection system, ethylene plant data analysis with the aid of Pareto analysis, Frequency analysis, and Weibull analysis.

CHAPTER 3

SYSTEM OVERVIEW

3.1 Pressure Safety Lows (PSL)

The pressure data from an actual PSL event is plotted in Figure 2.1. This line was shut-in due to a PSL trip from an upstream platform. This figure also shows the operating fluctuations in the normal line pressure.

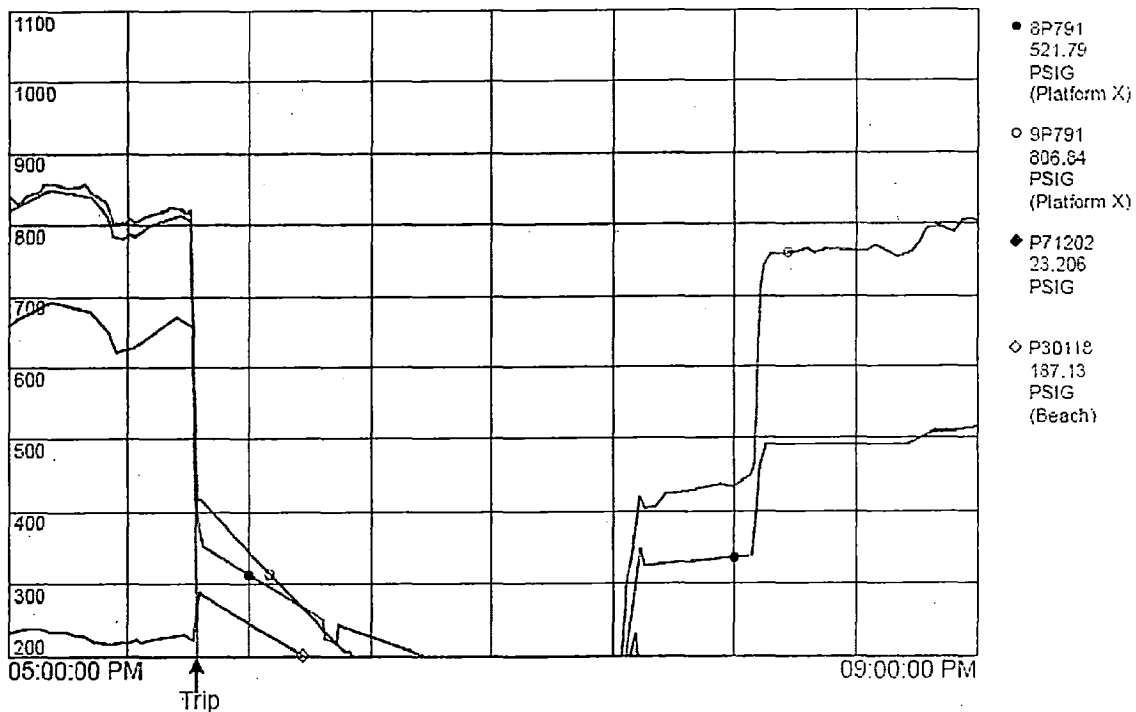


Figure 3.1: Pipeline Pressures during PSL Shut-in and Subsequent Recovery
(www.offshore-technology.com)

3.2 Sensor Operation

A typical pressure sensor and its connection to a gas pipeline are shown in Figure 2.2. The primary sensing element is the differential capacitance between the sensing diaphragm and the two capacitor plates. Both sides of the sensing diaphragm are coupled to isolating diaphragms with oil. One side of the sensing diaphragm is coupled to the low-pressure side, open to the ambient environment, and one side is coupled to the high

pressure side, the pipeline. Often, the electronics package simply converts the differential capacitance to a 4 to 20 mA signal representing the actual pressure over the calibrated range. This 4 to 20 mA signal is transmitted to a distributed control system (DCS) or programmable logic controller (PLC) where the actual pressure alarm is generated. The typical accuracy is $\pm 0.25\%$ of the calibrated span and the response to an abrupt change in pressure has a time constant on the order of 50 to 100 milliseconds. However, some operators have replaced the simple pressure sensor with a microprocessor-based converter that can average the sensor readings. The microprocessor changes the typical accuracy to about $\pm 0.05\%$ of the calibrated span, but adds 50 to 100 milliseconds to the response time. Any averaging of the pressure signal further increases the response time.

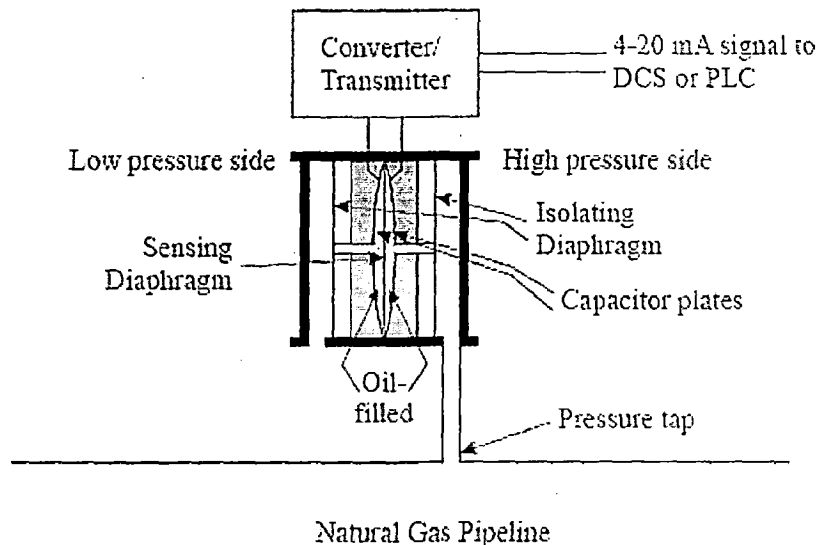


Figure 3.2: Typical Pressure Sensor (www.sensors.com)

3.3 Sensor Manufacturer and Failure Rate

A summary of pressure sensor manufacturers is provided by Erickson et al (2000). No operator questioned in this study indicated particular problems associated with one type of pressure sensor, nor was sensor failure rate indicated as a concern. For these reasons, specific instances of sensor failure data were not collected in this study.

3.4 PSL Location

In the case of gathering lines connecting two platforms, or in the case of a transmission line connecting a production hub to shore, one PSL sensor is located on the platform where the fluid enters the pipeline. A second PSL sensor is located at the point where the pipeline terminates, which is either another platform or a shore facility. This is shown in Figure 3.3.

No operator questioned in the study indicated use of PSL alarms at the point of subsea tie-ins, or at any intermediate point along the pipeline. Similarly, no operator indicated use of intermediate pumps along a pipeline, unless the pipeline was routed over an intermediate small platform.

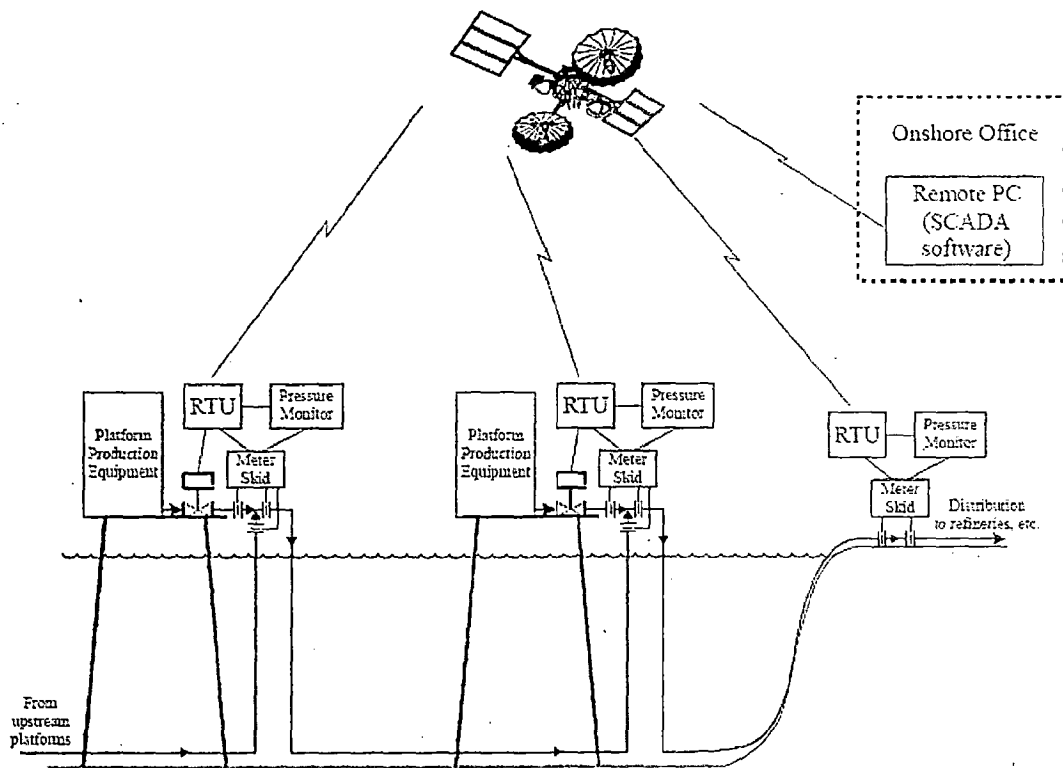


Figure 3.3: Platforms and Pipeline – Location of Pressure Monitoring

(www.offshore-technology.com)

3.5 Operational Considerations

Figure 3.4 details the placement of the PSL sensor relative to the pipeline pumps, valves, and pig launcher. As shown, the PSL is downstream of the pipeline pump.

One operator questioned indicated that a principal difficulty in setting PSL alarms was the nature of the pipeline pump. Offshore pipeline pumps tend to be piston or reciprocating type pumps, which by their nature create more pressure surging in the line. Coupling producing well fluctuations on multiple platforms with the periodic cycling of the pipeline pumps means that the system pressures fluctuate widely.

Once a PSL causes a line to shut-in, if the operator is uncertain as to the cause of the shutdown and/or integrity of the pipeline, an aerial survey of the line is made.

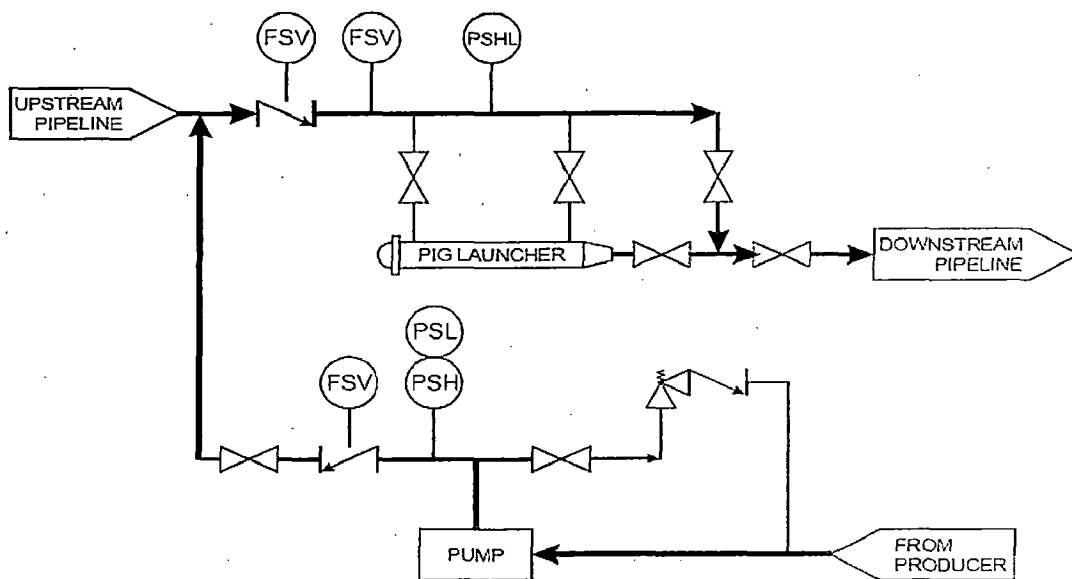


Figure 3.4: Details of an Offshore Pipeline/ Platform Junction Showing Alarm Locations
(www.offshore-technology.com)

Operators surveyed indicated that PSLs on in-field lines do not generally detect leaks. Operators usually notice an oil slick on the water before any PSLs trip.

One operator indicated that rate-of-change (ROC) alarms are an important indication of a leak. However, if a ROC alarm happens, the operators monitor the pipeline pressure at various points to determine the likelihood of a leak.

Another operational consideration is reservoir depletion, and the impact of declining reservoir pressures on pipeline operation. As reservoir pressures decline, pipeline operation pressures must also decrease unless additional pumping equipment is specified. In the older facilities in the shallow OCS, system operating pressures may fall below the hydrostatic pressure of the sea at points along the pipe route. For example, if a pipeline is located in 400 feet of water, and the seawater gradient is 0.465 psi/ft, then the external pressure on the line would be

$$P_{HYDRO} = (0.465 \text{ psi/ft})(400 \text{ ft}) = 186 \text{ psi}$$

If the pipeline operating pressure falls to this level, it is unlikely that the PSL could detect a leak. Several instances of these phenomena were found in the study. This phenomenon has more widespread implications for deepwater operations. For example, if the water depth increases to 6000 ft, the operating pressure of the line must fall below

$$P_{HYDRO} = (0.465 \text{ psi/ft})(6000 \text{ ft}) = 2790 \text{ psi}$$

For a leak to go undetected. This example shows that PSLs on deepwater pipelines will be likely affected by hydrostatic pressure.

3.6 Regulatory Aspects of the PSLs

The regulations concerning pipelines safety equipment and PSLs are as follows:

1. Incoming pipelines boarding to a production platform shall be equipped with an automatic shutdown valve (SDV) immediately upon boarding the platform. The SDV shall be connected to the automatic and remote-emergency shut-in systems.

2. Departing pipelines receiving production from production facilities shall be protected by high and low-pressure sensors (PSHL) to directly or indirectly shut in all production facilities. The PSHL shall be set not to exceed 15 percent above and below the normal operating pressure range. However, high pilots shall not be set above the pipelines MAOP.
3. Crossing pipelines on production or manned non-production platforms which do not receive production from the platform shall be equipped with an SDV immediately upon boarding the platform. The SDV shall be operated by a PSHL on the departing pipelines and connected to the platform automatic- and remote-emergency shut-in system.
4. The Regional Supervisor may require that oil pipelines be equipped with a metering system to provide a continuous volumetric comparison between the input to the line at the structure(s) and the deliveries onshore. The system shall include an alarm system and shall be of adequate sensitivity to detect variations between input and discharge volumes. In lieu of the foregoing, a system capable of detecting leaks in the pipeline may be substituted with the approval of the Regional Supervisor.
5. Pipelines incoming to a subsea tie-in shall be equipped with a block valve and FSV. Bi-directional pipelines connected to a subsea tie-in shall be equipped with only a block valve.
6. Gas-lift or water-injection pipelines on unmanned platforms need only be equipped with an FSV installed immediately upstream of each casing annulus of the first inlet valve on the Christmas tree.
7. Bi-directional pipelines shall be equipped with a PSHL and an SDV immediately upon boarding each platform.

So if the safety equipment is removed or rendered inoperative, it must be replaced by a similar level of protection (MMS, 1990).

3.7 Methods of Setting PSLs

Figure 3.5 is an example pressure chart recorded for an offshore liquids pipeline. In this example the system pressure varies from 300 psi to 1496 psi over a 4 hour period. This wide pressure fluctuation is common in offshore production facilities.

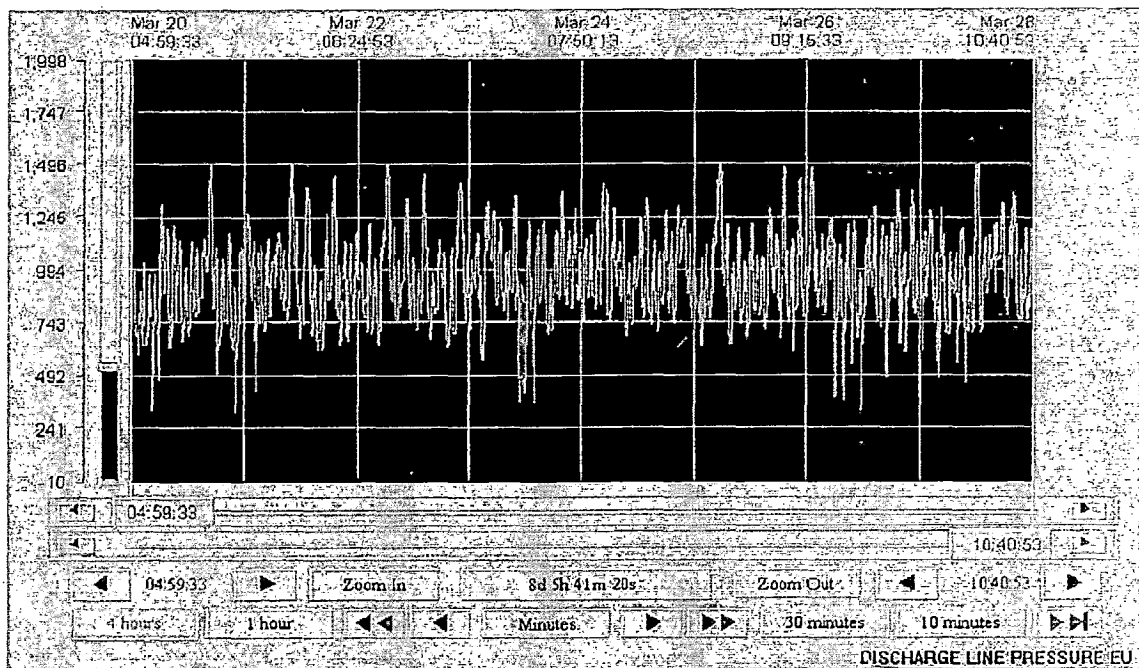


Figure 3.5: Example Pipeline Pressure Chart (www.offshore-technology.com)

The operator must review pressure charts such as the one shown in Figure 3.5, to determine the PSL setting threshold. Federal law prescribes setting PSL alarms on pipelines within 15% of the system operating pressure range, so the PSL can be set 15% below the lowest operating pressure of the pipeline. The federal code does not explicitly detail operational methods for determining what the lowest system operating pressure is.

If operators were asked how they determined their pipeline system operating pressure and set their PSLs. Almost uniformly, their first response was an explanation of the significant pressure fluctuations that occur in an offshore pipeline. Widely varying

operating pressures occur when wells go on and off production, and if entire platforms are shut in. In addition, the operating pressure of the line varies according to the pipeline pumps in operation at the time. The pipeline operator is clearly challenged to determine average pressures across the fluctuations. Typically, operators run charts for 2-3 days, taking the lowest pressure that occurs over a period of time to set the PSL. This is estimated (visually) across the chart.

One other practice was revealed. An operator had three platforms all operating at different pressures. To set the PSL on the pipeline, the operator used the lowest of the three platform operating pressures as the average system pressure. This practice would almost certainly reduce the effectiveness of leak detection relying strictly on PSL alarms. However, this operator also relied on CPM methods for monitoring the line.

CHAPTER 4

FAILURE ANALYSIS OF PSL

4.1 Failure Modes of PSLs

Failure modes can be classified in several ways. Some important modes are:

- Conditions
- Performance
- Safety, and
- Detection

4.2 Failure Classification by Cause of Failure

Failures can be categorized according to failure cause. IEC splits the failures into random hardware and systematic failures. The FTA method will adopt this classification, but also utilizes a more refined classification, as shown in Figure 3.1.

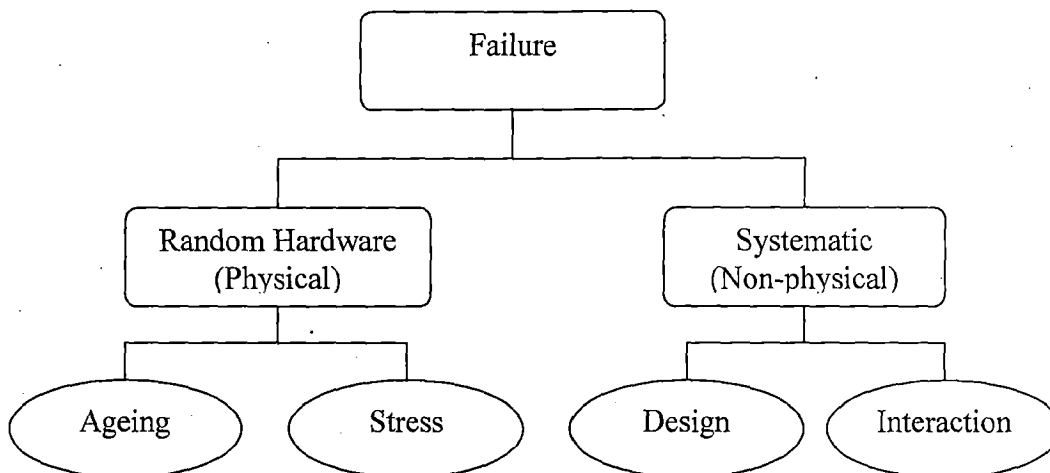


Figure 4.1: Failure classification by cause of failure

Table 4.1: Failure Causes with Example.

| Failure Cause | Example |
|---------------------------|--|
| Ageing | ◆ Natural ageing (within design envelope) |
| Stress | ◆ Sandblasting ◆ High humidity ◆ Overheating |
| Design | ◆ Software error ◆ Sensor does not discriminate true and false demands ◆ Inadequate location of sensor |
| Interaction (Random) | ◆ Scaffolding cover up sensor |
| Interaction (Test/Period) | ◆ Leave in by-pass ◆ Erroneous calibration of sensor |

As seen from Figure the FTA method applies the following failure categories (causes):

- ◆ **Random hardware failures** are **physical failures**, where the delivered service deviates from the specified service due to physical degradation of the module. Random hardware failures are further split into:
 - a) **Ageing** failures, which are failures occurring under conditions within the design envelope of a module.
 - b) **Stress** failures, which occur when excessive stresses are placed on the module. The excessive stresses may be caused either by external causes or by human errors during operation. An example is damage to gas detectors due to inadequate protection during sand blasting.

- ◆ **Systematic failures** are **non-physical failures**, where the delivered service deviates from the specified service without any physical degradation of the module. The failure can only be eliminated by a modification either of e.g. design or manufacturing process, the operating procedures or documentation. Thus, modifications rather than repairs are required in order to remove these failures. The systematic failures are further split into:

- a) **Design** failures, which are initiated during engineering and construction and may be latent from the first day of operation. Examples are software failures, sensors do not discriminate between true and false demands, and erroneous location of e.g. fire/gas detectors.
- b) **Interaction** failures, which are initiated by human errors during operation or maintenance/testing. Examples are loops left in the override position after completion of maintenance, and erroneous calibration of sensors during testing. Scaffolding that cover up a sensor making it impossible to detect an actual demand is another example of an interaction failure.

As a general rule it can be said that stress, interaction and design failures are dependent failures (give rise to common cause failures), while the ageing failures can be denoted independent failures.

In order to avoid a too complex classification, some of the above statements may be somewhat approximate. Not every failure may fit perfectly into the above scheme.

In the FTA method quantitative measures for loss of safety are provided for both random hardware failures and systematic failures. The IEC standard, however, suggests that only the contribution of random hardware failures should be quantified.

The FTA method has a strict focus on the entire safety function, and intend to account for all failures that could compromise this function (i.e. result in "loss of function"). Some of these failures are related to the interface/environment (e.g. "scaffolding cover up sensor"), rather than the safety system itself. However, it is part of the "FTA philosophy" to include such events.

4.3 Classification of Random Hardware Failures by Failure Mode

The IEC standard splits all random hardware failures into:

- ◆ Dangerous Undetected (DU) failures
- ◆ Dangerous Detected (DD) failures

- ◆ Safe Undetected (SU) failures
- ◆ Safe Detected (SD) failures.

Here the safe (S) failures (i.e. SU and SD) apparently include also noncritical failures, i.e. those failures that do not affect any of the two main functions of the module/systems. As a consequence, from this classification it is not possible to derive the rate of spurious trips, which is an integrated part of the FTA approach.

Therefore, the FTA method uses a slightly different notation (see Figure 4.2). The main difference is that in FTA the safe failures are split into noncritical failures (as defined above) and spurious trip failures (i.e. failures where the safety system is activated without a demand). For convenience we assume that all noncritical failures belong to the SU category (and thus none to the category SD).

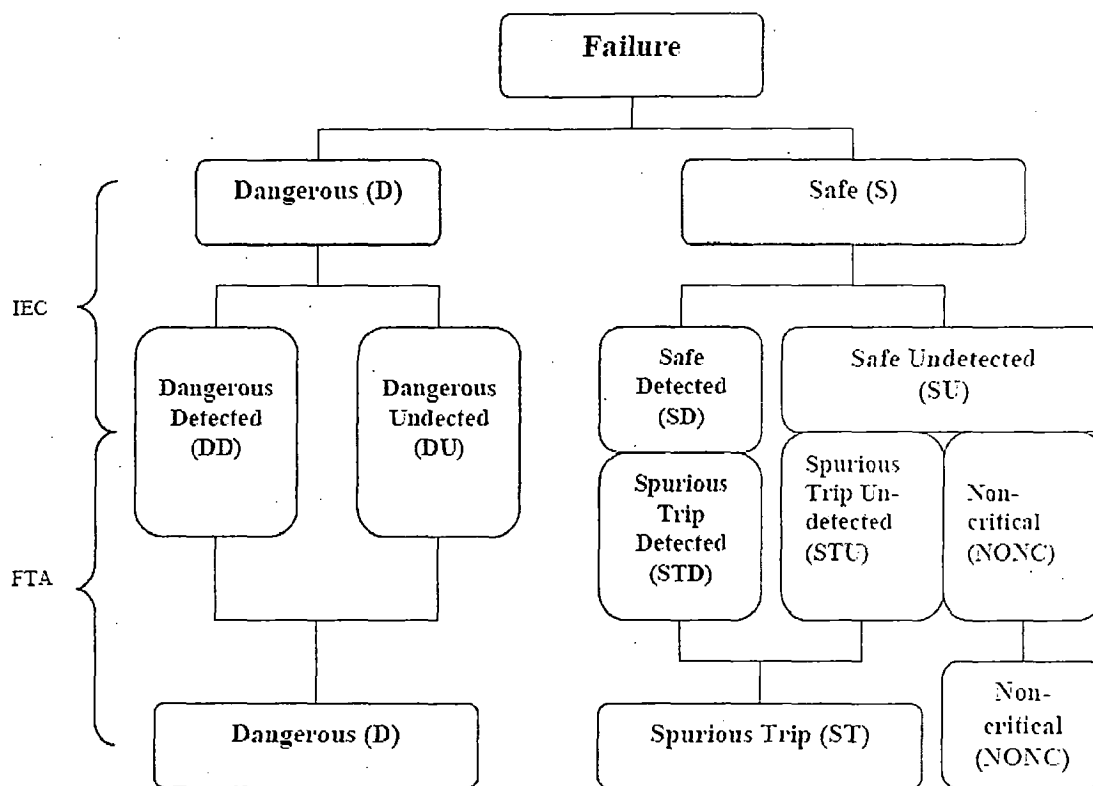


Figure 4.2: Failure Mode Classification-Component Level

Hence, the FTA method considers three failure modes, dangerous, spurious trip and noncritical:

- ◆ **Dangerous (D):** The module does not operate on demand (e.g. sensor stuck upon demand). The Dangerous failures are further split into
 - Dangerous Undetected (DU): Dangerous failures not detected by automatic self-tests (i.e. revealed by a functional test or by demands).
 - Dangerous Detected (DD): Dangerous failures detected by automatic self-test.
- ◆ **Spurious Trip (ST):** The module operates without demand (e.g. sensor provides shut down signal without a true demand - 'false alarm'). These are further split into
 - Spurious Trip Undetected (STU): Spurious trip failures not detected by automatic self-test.
 - Spurious Trip Detected (STD) Spurious trip failures detected by automatic self-test,(depending on configuration, the detection of failure could prevent an actual spurious trip of the system).
- ◆ **Noncritical (NONC):** Main functions are not affected, (e.g. sensor imperfection, which has no direct effect on control path).

The first two of these failure modes, Dangerous (D) and Spurious Trip (ST) are considered "critical", as they affect basic/main functions ("ability to shut down on demand" and "ability to maintain production when safe"). The ST failures are usually revealed instantly upon occurrence, whilst the D failures are "dormant" and can be detected by testing or a true demand.

4.4 Failure Data for PSL

4.4.1 Need for failure Data

The application for reliability techniques creates a demand for data on equipment failure and repair times, on other failure related events and on human error.

These data may be obtained from the literature, from data banks or within the works. Usually it is possible to obtain approximate data fairly readily but the determination of accurate data tends to involve much more effort. It is wasteful, therefore, to seek for greater accuracy in the data than the problem warrants (Funnemark, 1996)

The accuracy required in the data varies considerably between different types of reliability calculation and even between different parts of the same calculation. In general where reliability problem has a structure, as in comparison of a simple equipment with a parallel or a standby system or in a fault tree analysis, less accurate data may often be used, at least in some parts of the calculation. Thus in a fault tree analysis, for example, some branches of the tree may be sensitive to the failure rates used, while others may not be. On the other hand, where the problem is a straight comparison, as between the failure rates of two instruments, the accuracy required is clearly greater.

Often it is sufficient to know that the failure rate lies between certain broad limits for the solution to the reliability problem to be clear. In such cases it may be sufficient to rely on expert judgment or on relative crude failure data rather than on accurate data.

4.4.2 Types of Failure Data:

The failure information required for reliability work includes not only data on (Lees, 1980):

1. Overall failure rate but also data on failure rates in individual failure modes,
2. Variation of failure rates with time and
3. Repair time

4.4.3 Source of Failure Data

Failure data may be obtained from external sources such as the literatures and data banks. Alternatively, they may be collected within the works.

Failure rates depends on many factors, including the function of the equipment in the system and the definition of failure, the process environment and the maintenance

practices, and the types of equipment and its manufacturer. For these reason data obtained in the company's own works are likely to be more applicable than outside data.

On the other hand, the efforts and delay involved in collecting data are often not justifiable. Moreover, if the failures are rare events, internal collection may not be appropriate, since the confidence limits on failure data depend mainly on the number of failure recorded. In most cases use is made of a judicious mixture of data from all these sources.

4.4.4 Failure Data Banks

A number of generic reliability databases are available to the public, of which some are listed below (ISO 2004):

- **OREDA-84:** Offshore Reliability Data 1st Edition, ISBN 82-515-0087-7
- **OREDA-92:** Offshore Reliability Data 2nd Edition, ISBN 82-515-0188-1
- **OREDA-97:** Offshore Reliability Data 3rd Edition, ISBN 82-14-00438-1
- **OREDA-02:** Offshore Reliability Data 4th Edition, ISBN 82-14-02705-5
- **SINTEF:** Reliability Data for Safety Instrumented Systems, PDS Data Handbook, 2003 Edition, ISBN 82-14-02709-8
- **SwedPower:** T-Book, Reliability Data of Components in Nordic Nuclear Power Plants – 5th Edition, ISBN 91-631-0426-1
- **Concawe:** Western European Cross-country oil pipelines, 25-year performance statistics, report no. 2/98.

The OREDA, Offshore Reliability Data, project has been running since the early eighties with a number of major oil companies as participants. The data collected are mainly from the North Sea, but a small amount is from the Gulf of Mexico, the Adriatic and from onshore facilities. The project has issued four handbooks in 1984, 1992, 1997 and 2002 respectively. The 1984 handbook has been withdrawn after a quality assurance process in connection with the 1992 edition selected the data to be included in the new edition. The 1992, 1997 and 2002 handbooks do not contain overlapping data, and the information may thus be merged to produce overall failure rates and repair times.

The OREDA handbooks are considered to contain top quality reliability data in the sense that the data has been collected over a long time, data comprises a wide range of equipment items and that the data collection and quality assurance has been performed according to the ISO standard for such work.

The PDS Forum is a forum of oil companies, vendors of safety equipment, engineering companies and consultants. The forum issued the first version of the PDS Data Handbook in 1998 and a new version, which is used in the present study, in 2003. The data in this handbook is based on the OREDA database which has been supplemented by expert judgments performed by the participants of the PDS Forum. The reliability data covers safety related equipment classes.

The PDS Data Handbook is considered to contain top quality reliability data. Reliability data collection started in Swedish nuclear power plants in the middle of the seventies, and later the Finnish company TVO joined the data collection system. The first edition of the T-book was published in 1982, and the latest version, which is used presently, was published in 2000.

Concawe is the oil companies' European organization for environment, health and safety and has been collecting data on oil spills from cross-country pipelines since the early seventies. It is considered as the best data source for oil pipeline leaks.

The following prioritizations and recommendations for use are given:

- ◆ For equipment classes covered by OREDA this has been considered the most relevant database as it is based on data from the oil and gas industry.
- ◆ For safety related equipment covered by PDS this has been the preferred database as this is also based on data from the oil and gas industry.
- ◆ The T-book has been used for most of the electrical equipment as this is quite poor covered by OREDA and PDS.
- ◆ For pipelines Concawe is the obvious best choice.

4.4.5 Failure Data for PSL Based on OREDA Database

Table 4.2: Failure Data for PSL

| Event | Failure Mode of PSL | MTTF in hrs | Failure Probability |
|-------|---|-------------|---------------------|
| 1 | Pipeline leak due to corrosion | 4.09E+9 | 0.000244 |
| 2 | Pipeline leak due to third party | 5E+9 | 0.00020 |
| 3 | Pipeline leak due to earth movement | 5.6E+9 | 0.00018 |
| 4 | Pipeline leak due to weld failure | 3.31E+9 | 0.00039 |
| 5 | Pipeline leak due to valve failure | 17.52E+9 | 0.00006 |
| 6 | Pipeline leak due to material failure | 2.3E+9 | 0.00043 |
| 7 | Pressure sensors fail to detect low (gas) pressure in pipeline | 87600 | 0.99999 |
| 8 | Communication link failure between PSL and control computer | 9.9E+7 | 0.01 |
| 9 | Safety shut-off valve(SSV) fails to close | 292000 | 0.96744 |
| 10 | Computer fails to trip SSV | 815600 | 0.70656 |
| 11 | Communications link failure between computer and SSV | 9.9E+7 | 0.01 |
| 12 | Pressure sensor signal goes low | 876000 | 0.68068 |
| 13 | Pressure sensor fails to detect low (liquid) pressure in pipeline | 400000 | 0.91792 |
| 14 | Failure of (gas) Mass Flow Sensor -1 (MFS-1) | 768400 | 0.72785 |
| 15 | Failure of (gas) Mass Flow Sensor- 2 (MFS-2) | 768400 | 0.72785 |
| 16 | Communication link failure between MFS-1 and computer | 9.9E+7 | 0.01 |
| 17 | Communication link failure between MFS-2 and computer | 9.9E+7 | 0.01 |
| 18 | Failure of (liquid) mass flow sensor-1 | 768400 | 0.72785 |
| 19 | Failure of (liquid) mass flow sensor-2 | 768400 | 0.72785 |
| 20 | Failure of (multiphase) mass flow sensor-1 | 768400 | 0.72785 |
| 21 | Failure of (multiphase) mass flow sensor-2 | 768400 | 0.72785 |

CHAPTER 5

RELIABILITY ESTIMATION OF PSL VIA FAULT TREE

5.1 Fault Tree Analysis

In the RAMS (reliability, availability, maintainability and safety) domain, fault tree (FT) method is a well known engineering approach. It is one of the most widely used by practitioners. However, because their limited expressive power, FTA cannot be used to assess the exact value of system reliability (Rausand, 2004).

A fault tree analysis is a logical, structured process that can help identify potential causes of system failure before the failures actually occur. It can predict the most likely causes of system failure in the event of system breakdown.

Fault tree methods of analysis are particularly useful in functional paths of high complexity in which the outcome of one or more combinations of noncritical events may produce an undesirable critical event. Typical candidates for fault tree analysis are functional paths or interfaces which could have critical impact on flight safety, munitions handling safety, safety of operating and maintenance personnel, and probability of error free command in automated systems in which a multiplicity of redundant and overlapping outputs may be involved. The fault tree provides a concise and orderly description of the various combinations of possible occurrences within the system which can result in a predetermined critical output event. However, performance of the fault tree analysis does require considerable engineering time and even then the quality of results is only as good as the validity of input data and accuracy of the fault tree logic.

Fault tree methods can be applied beginning in the early design phase, and progressively refined and updated to track the probability of an undesirable event as the design evolves. Initial fault tree diagrams might represent functional blocks (e.g., units, equipments, etc.), becoming more definitive at lower levels as the design materializes in the form of specific parts and materials. Results of the analysis are useful in the following applications (Rausand, 2004):

1. Allocation of critical failure mode probabilities among lower levels of the system breakdown.
2. Comparison of alternative design configurations from a safety point of view.
3. Identification of critical fault paths and design weaknesses for corrective action.
4. Evaluation of alternative corrective action approaches.
5. Development of operational, test, and maintenance procedures to recognize and accommodate unavoidable critical failure modes.

In this study fault tree diagrams have been developed for liquid, gas and multiphase to calculate a probability of failure to trip and false trip. Fault tree diagrams are chosen because of the sensitivity of pressure safety lows. Since any small error in hardware or software leads to failure to trip or false trip, analysis should focus on one particular system failure at a time. Fault tree analysis (FTA) is restricted only to the identification of the system events that lead to one particular undesired failure or accident.

5.2 Fault Tree Symbols

Gate symbols are used to connect events according to their casual relations. A gate may have one or more input events but only one output event. Table 5.1 illustrates different types of gate symbols. Event symbols show specific types of fault and normal events in fault tree analysis. Table 5.2. Summarizes event symbols.

Table 5.1: Gate symbols and their description (Rausand, 2004)



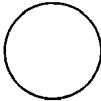

| Fault Tree Symbol | Name | Definition |
|---|----------|--|
|  | AND gate | Output event occurs if all input events occur simultaneously |
|  | OR gate | Output event occurs if any one of the input events occurs |

Table 5.2: Event symbols and their description (Rausand, 2004)

| Fault Tree Symbol | Name | Definition |
|---|-----------|--|
|  | Circle | Basic event an independent elementary representing a basic fault or component. the analysis ends with a basic. |
|  | Rectangle | Resultant event, a fault event resulting from the logical combination of other fault events & usually an output to a logic gate. |

5.3 Why Fault Tree Analysis Method?

Uncritical use of quantitative analyses may weaken the confidence in the value of performing reliability analyses, as extremely ‘good’, but highly unrealistic figures can be obtained, depending on the assumptions and input data used.

The FTA method is, however, considered to be realistic as it accounts for all major factors affecting reliability during system operation, such as:

- ◆ Common cause failures
- ◆ Automatic self-tests
- ◆ Functional (manual) testing
- ◆ Systematic failures (not revealed by functional testing) Complete systems including redundancies and voting
- ◆ All failure categories/causes

Most methods used today do not consider all of these aspects. It should be noted that the FTA method is by no means perfect, but to quote the famous statistician George E. P. Box; “All models are wrong, but some are useful!” It is belief that the FTA method is useful, and that by applying it a large step is taken towards more realistic analyses and trustworthy results.

Although the model is considered realistic, it is still relatively simple. The method is primarily a tool for non-experts in reliability, and should thus contribute to enhance the use of reliability analysis in the engineering disciplines, and to bridging the gap between reliability theory and application.

5.4 Main characteristics of the FTA method

The method gives an integrated approach to hardware, software and human factors. Thus, the FTA accounts for all failure causes:

- ◆ Normal ageing
- ◆ Stress and environmental conditions
- ◆ Human operator interaction errors
- ◆ Design errors

The failure taxonomy is customized to utilizing input data from various data sources,

- ◆ Corrective and preventive maintenance report systems (e.g. SAP)
- ◆ Failure databases (e.g. OREDA)
- ◆ Expert judgments.

Furthermore, the model includes all failure types that may occur, and explicitly accounts for:

- ◆ Dependent (common cause) failures
- ◆ The actual effect of all types of testing (automatic as well as manual).

The main benefit of the FTA taxonomy compared to other taxonomies is the direct relationship between failure cause and the means used to improve safety system performance.

The method is simple and structured:

- ◆ Highlighting the important factors contributing to loss of safety and spurious trip failures

- ◆ Promoting transparency and communication.

As stressed in IEC 61508, it is important to be function oriented, and take into account the performance of the total signal path from the sensors via the control logic and to the actuators. This is a core issue in FTA.

5.5 Applications of the FTA Method

The FTA method has been applied in numerous projects and in many different contexts. The main application, however, has been to computer-based safety systems in the offshore and onshore oil and gas industry. FTA has e.g. been utilized in:

- ◆ A large number of third-party reliability verifications of offshore safety systems.
- ◆ Projects that consider the effects of integrating the process control, process shutdown and emergency shutdown systems.
- ◆ Comparative reliability assessments of different control and safety systems for boiler applications.
- ◆ A study for specifying emergency shutdown (ESD) system requirements on offshore installations.
- ◆ Studies to compare different voting configurations of gas detectors, including different combinations of high/low alarm limits, based on economic and safety assessments.
- ◆ Optimization of the functional testing interval for offshore equipment, considering both safety and maintenance cost.
- ◆ Several HIPPS (High Integrity Pressure Protection System) studies.
- ◆ The evaluation of a new detector design (with increased self test facilities).

5.6 Testing of FTA

The FTA method takes into account the effect of two types of testing: Automatic self-tests Functional testing (.Outfit, 2005). These tests are essentially designed to detect random hardware failures. The method will account for the fact that no test is perfect.

5.6.1 Functional testing

Functional testing is performed manually at defined time intervals, typically 3, 6 or 12 months intervals. The functional test may not be perfect due to:

- ◆ Design failures (present from day 1 of operation) not being detected by functional testing, e.g.:
 - software errors
 - lack of discrimination (sensors)
 - inadequate location (of sensor)
- ◆ Interaction failures occurring during functional testing, e.g.:
 - maintenance crew forgets to test specific sensor
 - test performed erroneously (e.g. wrong calibration or component being damaged)
 - maintenance personnel forgets to reset by-pass of component.

It may also be other shortcomings in the functional testing; e.g. the test demand is not identical to a true demand, and thus some part of the function is not tested.

5.6.2 Automatic self-test

Modules often have built-in automatic self-test to detect random hardware failures. Further, upon discrepancy between redundant modules in the safety system, the system may determine which of the modules have failed. This is considered part of the self-test. But it is never the case that all random hardware failures are detected automatically. A fault coverage factor (Diagnostic coverage, DC) is introduced to quantify the efficiency of the self-test. This factor equals the fraction of failures being detected by the automatic self-test. Note that the actual effect on system performance from a failure that is detected by the automatic self-test will depend on system configuration and operating philosophy; (i.e. the effect depends on the voting logic and whether degraded operation takes place when a failure is detected).

5.6.3 "Random" detection by personnel

In addition, an operator or maintenance crew may detect failures in between tests. For instance, the panel operator may detect a transmitter that is "stuck". He may also detect a sensor left in bypass (systematic failure). The FTA method also aims at incorporating this effect, and defines a coverage factor reflecting detection both by automatic self-test and operator.

Further, a spurious trip failure of a (redundant) detector, giving a pre-alarm, can allow the operator to prevent an automatic activation (trip) to occur, if specified in the operational philosophy; (one should obviously be careful when allowing such a practice). Such failures would then be part of "detected" (and not "undetected") failures.

5.7 Fault Tree Construction

The goal of fault tree construction is to model the system conditions that can result in the undesired event. Before the construction of the fault tree can proceed, the analyst must acquire a thorough understanding of the system. In fact, a system description should be part of the analysis documentation. The analyst must carefully define the undesired event under consideration, called the "top event" (Ebeling, 2000).

The various steps for FTA are as follows:

1. **Develop Function Reliability Block Diagram:** Develop reliability block diagram for the system/equipment functional paths in which the critical failure mode is to be circumvented or eliminated. Define the critical failure mode in terms of the system level mal-performance symptom to be avoided.
2. **Construct the Fault Tree:** Develop the fault tree logic diagram relating all possible sequences of events whose occurrence would produce the undesired events identified in Step 1.
3. **Develop Failure Probability Model:** Develop the mathematical model of the fault tree for manual (or computer) computation of the probability of critical event occurrence on the basis of failure modes identified in the diagram.

4. **Determine Failure Probabilities or Identified Failure Modes:** Determine probability of occurrence (i.e., probability of failure) in each event or failure mode identified in the model.
5. **Identify Critical Fault Paths:** When the probability of an unsafe failure mode at the system level exceeds specification tolerances, identify the critical paths which contribute most significantly to the problem.

A fault tree is structured so that the sequence of events that lead to the undesired event are shown below the top event and are logically related to the undesired event by OR and AND gates. Figure shows how a fault tree grows from the top event to basic events or vice versa. The input events to each logic gate that are also outputs of other logic gates at a lower level are shown as rectangles. These events are developed further until the sequence of events lead to basic causes of interest, called “basic events”. The basic events appear as circles and diamonds on the bottom of the fault tree and represent the limit of resolution of the fault tree.

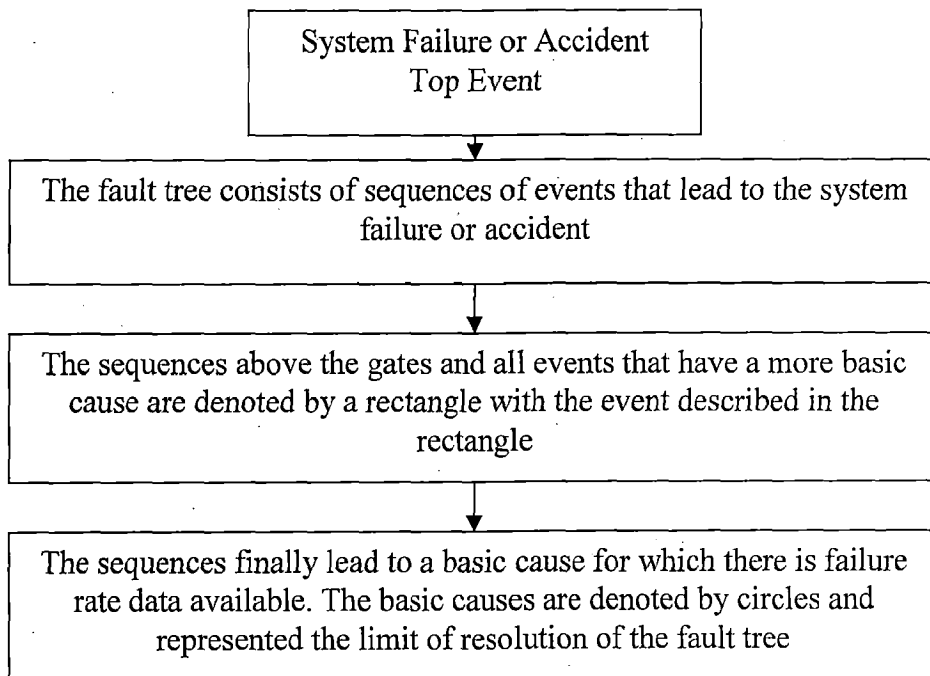


Figure 5.1: Fundamental structures of fault tree

5.8 Structuring Process

The structuring process is used to develop fault flows in a fault tree when a system is examined on a functional basis, i.e., when failures of system elements are considered. At this level, schematics, piping diagrams, process flow sheets, etc., are examined for cause and effect types of relationships to determine the subsystem and component fault states that can contribute to the occurrence of the undesired event.

The structuring process identifies three failure mechanism or causes that can contribute to a component being in a fault state.

1. A primary failure is a failure due to the internal characteristics of the system element under consideration.
2. A secondary failure is a failure due to excessive environmental or operational stress placed on the system element

5.9 Reliability Theory

In performing the reliability analysis of a complex system, it is almost impossible to treat the system in its entirety. The logical approach is to divide the system into functional entities composed of units, subsystems, or components. The subdivision generates a fault tree diagram of system operation. Models are then formulated to fit this logical structure, and the probability theory is used to find the system reliability. Series and parallel structures often occur, and their reliability can be described very simply (Ebeling, 2000).

The random variable T is defined as the failure time of the item in question. Thus, the probability of failure as a function of time is given as

$$P(T \leq t) = F(t) \quad (1)$$

which is simply the definition of failure distribution function. We can define reliability, which is a probability of success in terms of $F(t)$, as

$$R(t) = P_s(t) = 1 - F(t) = P(T \geq t) \quad (2)$$

The simplest and most common reliability function is an exponential,

$$R(t) = e^{-\lambda t} \quad (3)$$

where R stands for system reliability. λ is failure rate defined as the ratio of the number of failures per unit time to the number of components that are exposed to failure.

5.9.1 Series Reliability

Any system in which the system success depends on the success of all its components is a series system. The event signifying the success of n th unit will be x_n and \bar{x}_n will represent the failure of the n th unit. The probability that unit n is successful will be $P(x_n)$. The probability of system success is denoted by P_s . In keeping with definition of reliability, $P_s = R$. The probability of system failure is

$$P_f = 1 - P_s \quad (4)$$

Since the series system requires that all units operate successfully for system success, the event representing system success is intersection of x_1, x_2, \dots, x_n . The reliability of this structure is given by

$$R(t) = P(x_1, x_2, \dots, x_n) = P(x_1)P(x_2 / x_1)P(x_3 / x_1 x_2) \dots P(x_n / x_1 x_2 \dots x_{n-1})$$

If the n items x_1, x_2, \dots, x_n are independent, then

$$R(t) = P(x_1, x_2, \dots, x_n) = \prod_{i=1}^n P(x_i) \quad (6)$$

If each component exhibits a constant hazard, then the appropriate component model is $e^{-\lambda t}$, and Eq. (6) becomes

$$R(t) = \prod_{i=1}^n e^{-\lambda_i t} = \exp\left(-\sum_{i=1}^n \lambda_i t\right) \quad (7)$$

Eq. (3) is the most commonly used and the most elementary system reliability formula.

5.9.2 Parallel Reliability

If the system is such that failure of one or more paths still allows the remaining path to perform properly, the system can be represented by a parallel model. The reliability

expression for a parallel system may be expressed in terms of the probability of success of each component or, more conveniently in terms of probability of failure.

$$R(t) = P(x_1 + x_2 + \dots + x_n) = 1 - P(\overline{x_1 x_2 \dots x_n}) \quad (8)$$

In the case of constant hazard components

$$P_f = P(\overline{x_i}) = 1 - e^{-\lambda t}$$

and Eq. (8) becomes

$$R(t) = 1 - \left[\prod_{i=1}^n (1 - e^{-\lambda t}) \right] \quad (9)$$

In general case, the system reliability function is

$$R(t) = 1 - \left[\prod_{i=1}^n (1 - e^{-\lambda_i t}) \right] \quad (10)$$

5.10 Reliability Analysis of PSLs

Eighteen fault tree analyses (FTA) were performed to predict the probabilities of either a failure to trip a PSL alarm in the presence of a leak or a PSL trip when no leak was present (false alarm). Each case is considered for liquid flow, gas flow and multiphase flow with two possible leak monitoring systems PSL and MFS. Table 5.3 summarizes these cases.

Table 5.3: Matrix of FTA Pipeline Cases

| Monitoring System | Flow Type | | | | | |
|-------------------|-----------------|--------|-------|------------|--------|-------|
| | Gas | Liquid | Multi | Gas | Liquid | Multi |
| PSL | X | X | X | X | X | X |
| MFS | X | X | X | X | X | X |
| Malfunction | Failure to trip | | | False trip | | |

It can be seen that nine cases are examples of failure to trip with a leak present and nine cases are examples of false trips. The three fault tree diagrams for failure to trip will have many similarities. The same can be said of the three fault tree diagrams for false trips.

5.10.1 Basic Events

The eighteen fault tree diagrams will share a great many basic events. It is useful to define all of the basic events before examining the fault tree diagrams. Table 5.4 has a list of the 13 basic events with a definition of the event, the Mean Time to Failure (MTTF) and the Mean Time to Repair (MTTR), the unavailability (q). Fault tree diagram symbols are shown in Tables 5.1 and 5.2 with definitions of each symbol.

Mean time to failure is defined as the expected value of the time to failure. In the case of the exponential distribution this is equal to the reciprocal of the failure rate. If a failure occurs in every one million hours for a component, it is said that the component has a failure of 1E-6 failures/hour. The MTTF is reciprocal of failure rate. The failure rates used in this thesis have constant failure rates. If the failure rates have different distributions, then the MTTF is found according to the corresponding distribution.

$$MTTF = \frac{1}{\lambda}$$

Mean time to repair is the expected value of the time to repair.

$$MTTR = \frac{1}{\mu}$$

Availability is the probability of finding the component/device/system in the operating state at some time in the future.

$$Availability = \frac{MTTF}{MTTF + MTTR} = \frac{\mu}{\mu + \lambda}$$

Unavailability is the probability of finding a component or system in the non-operating state at some time in the future.

$$Unavailability(q) = \frac{MTTR}{MTTR + MTTF} = \frac{\lambda}{\lambda + \mu}$$

Table 5.4: Basic Event Data(OREDA)

| Event | Failure Mode of PSL | MTTF in hrs | Failure Probability |
|-------|---|-------------|---------------------|
| 1 | Pipeline leak due to corrosion | 4.09E+9 | 0.000244 |
| 2 | Pipeline leak due to third party | 5E+9 | 0.00020 |
| 3 | Pipeline leak due to earth movement | 5.6E+9 | 0.00018 |
| 4 | Pipeline leak due to weld failure | 3.31E+9 | 0.00039 |
| 5 | Pipeline leak due to valve failure | 17.52E+9 | 0.00006 |
| 6 | Pipeline leak due to material failure | 2.3E+9 | 0.00043 |
| 7 | Pressure sensors fail to detect low (gas) pressure in pipeline | 87600 | 0.99999 |
| 8 | Communication link failure between PSL and control computer | 9.9E+7 | 0.01 |
| 9 | Safety shut-off valve(SSV) fails to close | 292000 | 0.96744 |
| 10 | Computer fails to trip SSV | 815600 | 0.70656 |
| 11 | Communications link failure between computer and SSV | 9.9E+7 | 0.01 |
| 12 | Pressure sensor signal goes low | 876000 | 0.68068 |
| 13 | Pressure sensor fails to detect low (liquid) pressure in pipeline | 400000 | 0.91792 |
| 14 | Failure of (gas) Mass Flow Sensor -1 (MFS-1) | 768400 | 0.72785 |
| 15 | Failure of (gas) Mass Flow Sensor- 2 (MFS-2) | 768400 | 0.72785 |
| 16 | Communication link failure between MFS-1 and computer | 9.9E+7 | 0.01 |
| 17 | Communication link failure between MFS-2 and computer | 9.9E+7 | 0.01 |
| 18 | Failure of (liquid) mass flow sensor-1 | 768400 | 0.72785 |
| 19 | Failure of (liquid) mass flow sensor-2 | 768400 | 0.72785 |
| 20 | Failure of (multiphase) mass flow sensor-1 | 768400 | 0.72785 |
| 21 | Failure of (multiphase) mass flow sensor-2 | 768400 | 0.72785 |

Table 5.4 gives the basic events that must be considered within the various fault tree diagrams. In this list of failures, events one to six are the various causes for a leak in pipeline. Events 7 and 12 are sensor failures. An event 8 is communications link failures between sensors and the control computer. Events 9, 10 and 11 relate to failure to close safety shut-off valves (SSV's) due to SSV, communications link or computer failures.

5.10.2 Development of the Fault Trees for Gas Flow Pipelines

Fault tree diagrams have been developed for a gas pipeline for PSL and MFS systems. For these systems a pair of fault trees is developed, one for a top event where a leak

occurs but it is not detected, and one for top event where no leak has occurred but a false trip takes place.

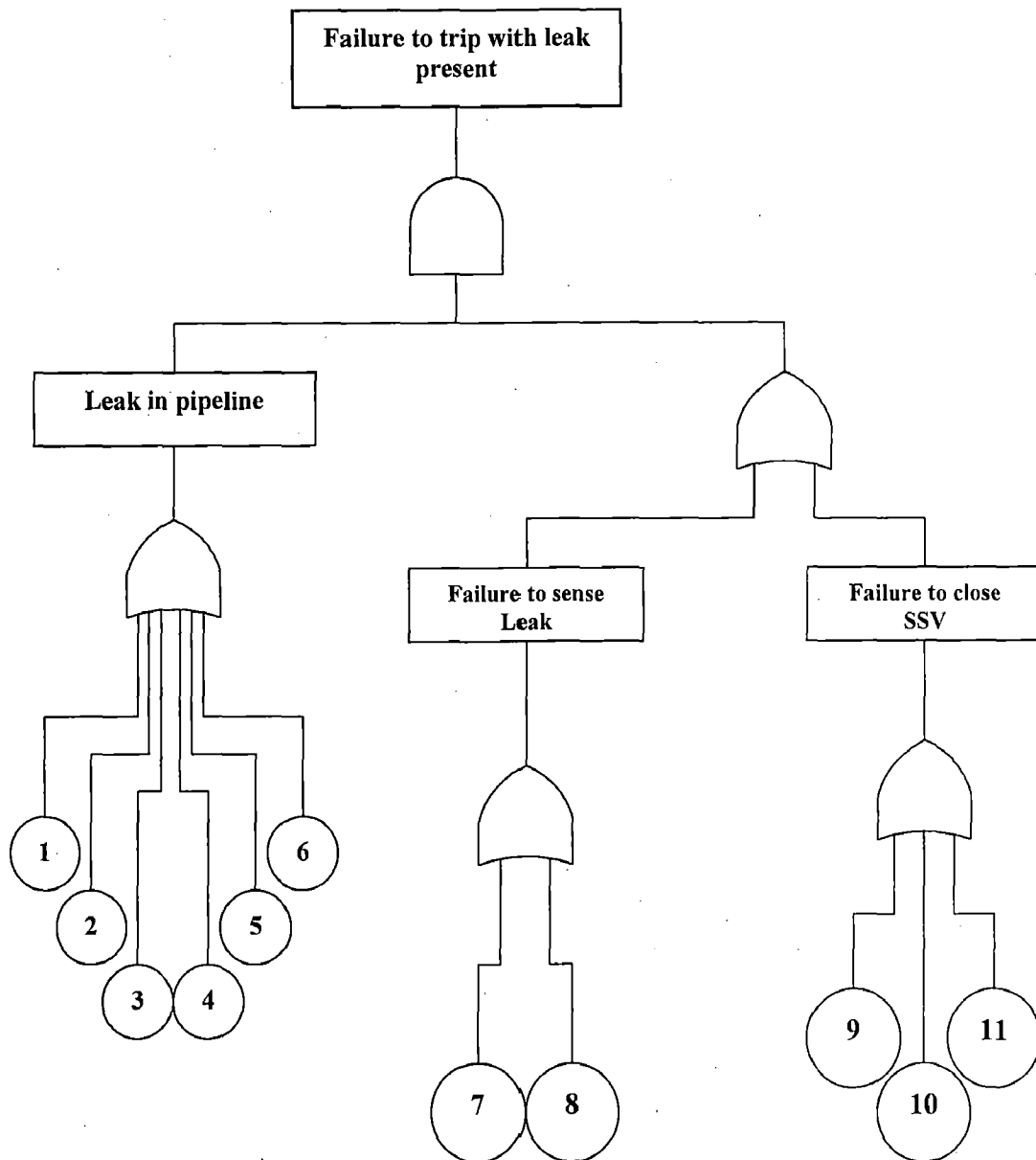


Figure 5.2: Gaseous Flow – Failure to trip with leak present – PSL only

Figure 5.2 shows a fault tree diagram for a gas pipeline protected by a pressure sensor (safety) low (PSL) in which the top event is a failure to trip with a leak present. The top event occurs when there is a leak present AND either the system fails to detect a leak OR the safety shut-off valve(s) fail to close.

The system will fail to sense a leak if the PSL fails to detect low pressure in the pipeline OR the communication link from the PSL to the computer fails in an unsafe mode OR the safety shut-off valves fail to close for one of the reasons outline above. It is assumed that either of these two scenarios can occur in conjunction with a leak in the pipeline to cause the top event.

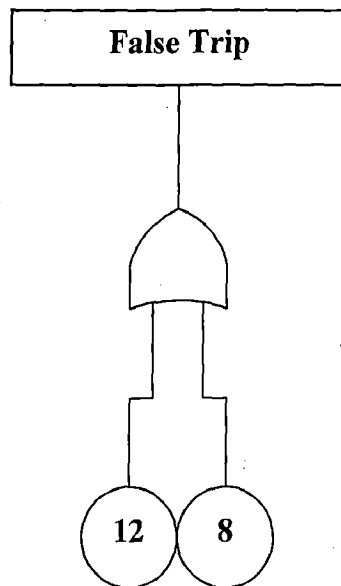


Figure 5.3: Gaseous Flow – False Trip– PSL only

Figure 5.3 shows a fault tree diagram for a gas flow pipeline protected by a pressure sensor low (PSL) system. The top event is a false trip. The top event occurs when either the pressure sensor low OR the communication link between the PSL and the computer fails.

Figure 5.4 shows a fault tree diagram for a gas pipeline protected by a mass flow or line balance system (MFS) in which the top event is a failure to trip with a leak present. The top event occurs when there is a leak AND either the system fails to detect the leak, OR the safety shut- off valves fail to close.

The system will fail to sense a leak if there is a simultaneous loss of mass flow signals either due to sensor failures OR communication links from the computer to the SSV fail to causing the top event.

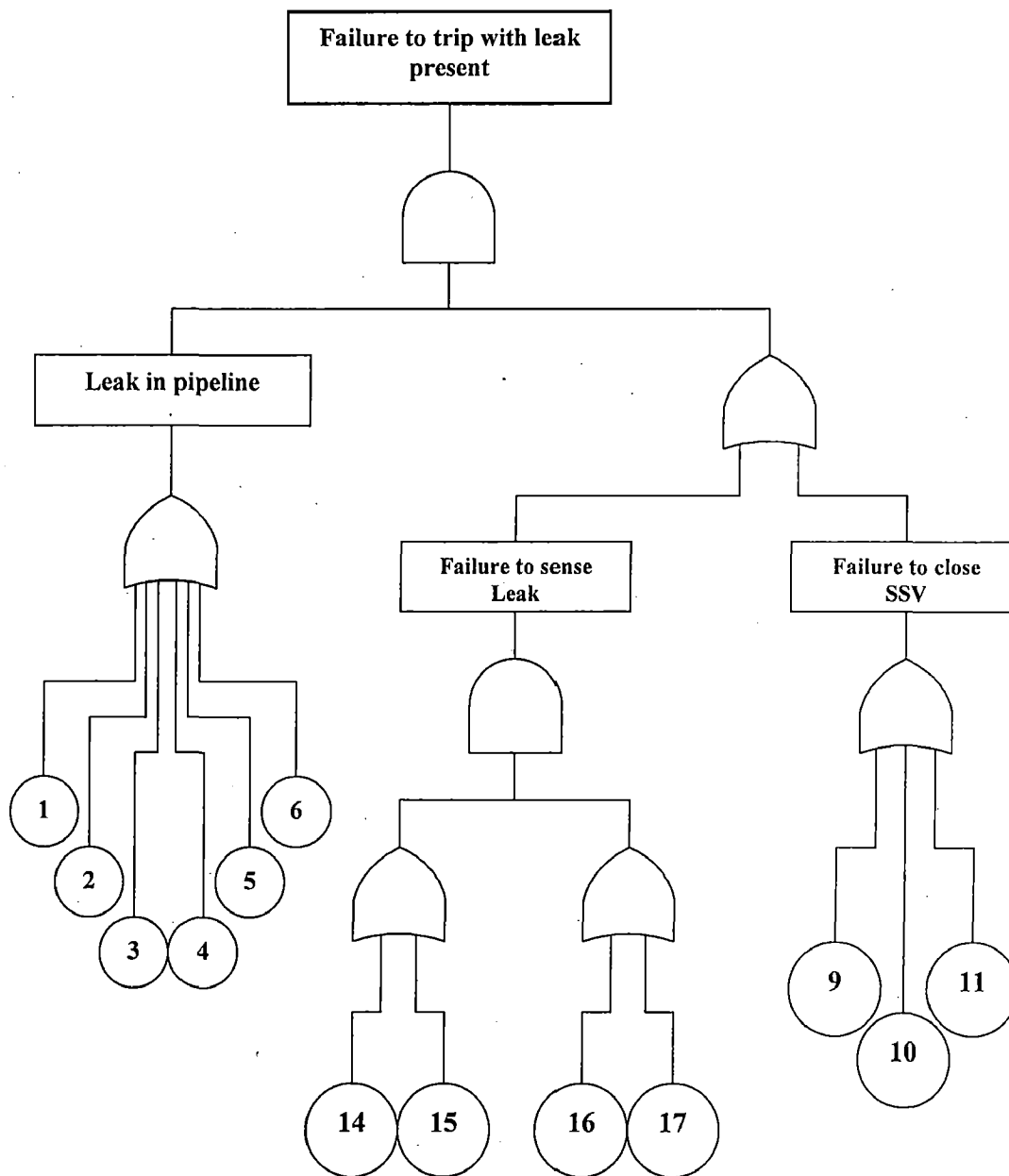


Figure 5.4: Gaseous Flow – Failure to trip with leak present - MFS only

Figure 5.5 shows a fault tree diagram for a gas flow pipeline protected by a mass flow system (MFS). The top event is a false trip. The top event occurs when either mass flow sensor (MFS-1) OR mass flow sensor-2 (MFS-2) OR the communications links between

MFS-1 and the computer OR the communication link between MFS-2 and the computer fails.

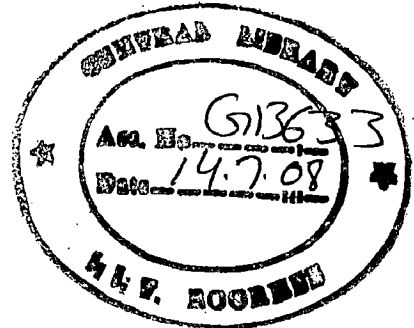
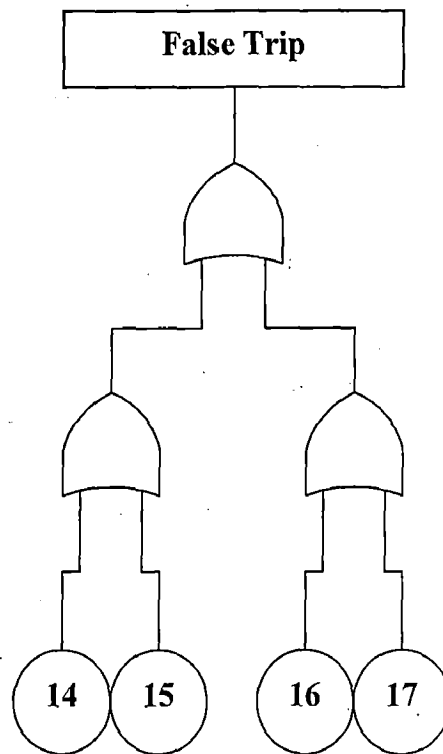


Figure 4.5: Gaseous Flows – False Trip – MFS only

Basic probabilities for each of the failure events will be used to calculate reliability of the top event occurring in Figures 5.2 through 5.5.

5.10.3 Development of the Fault Trees for Liquid Flow Pipelines

Fault tree diagrams have been developed for a liquid flow pipeline for PSL and MFS leak protection. For these type of system a pair of fault trees is developed, one for a top event where a leak occurs but it is not detected, and one for top event where no leak has occurred but a false trip takes place.

Within the various fault tree diagrams, the basic events that must be considered are given in Table 5.4.

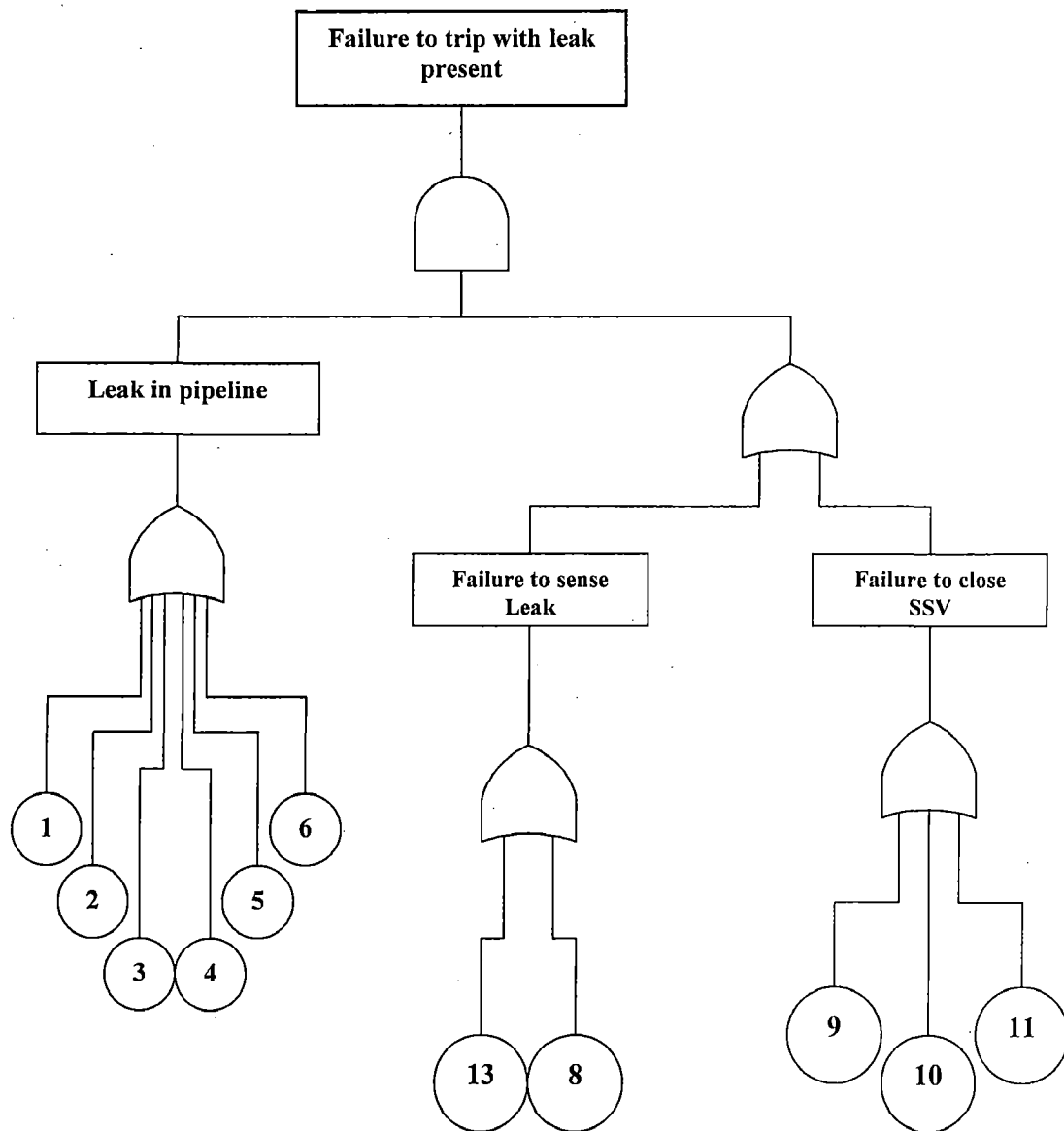


Figure 5.6: Liquid Flow – Failure to trip with leak present – PSL only

Figure 5.6 shows a fault tree diagram for a liquid flow pipeline protected by a pressure sensor (safety) low (PSL) in which the top event is a failure to trip with a leak present. The top event occurs when there is a leak present AND either the system fails to detect a leak OR the safety shut-off valve(s) fail to close.

The system will fail to sense a leak if the PSL fails to detect low pressure in the pipeline OR the communication link from the PSL to the computer fails in an unsafe mode OR the safety shut-off valves fail to close for one of the reasons outline above. It is assumed that

one of these three scenarios can occur in conjunction with a leak in the pipeline to cause the top event.

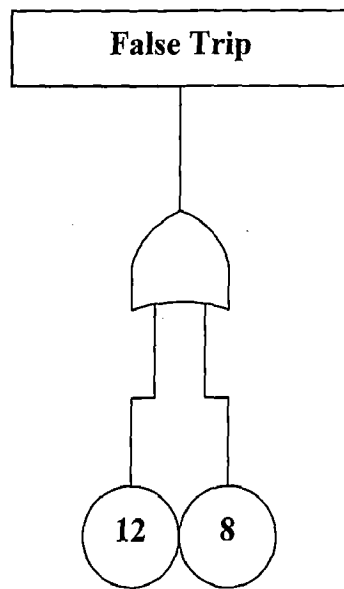


Figure 5.7: Liquid Flow – False trip– PSL only

Figure 5.7 shows a fault tree diagram for a liquid flow pipeline protected by a pressure sensor low (PSL) system. The top event is a false trip. The top event occurs when either the pressure sensor low OR the communication link between the PSL and the computer fails.

Figure 5.8 shows a fault tree diagram for a liquid pipeline protected by a mass flow or line balance system (MFS) in which the top event is a failure to trip with a leak present. The top event occurs when there is a leak AND either the system fails to detect the leak, OR the safety shut- off valves fail to close.

The system will fail to sense a leak if there is a simultaneous loss of mass flow signals either due to sensor failures OR communication link from the computer to the SSV fail, resulting in the top event.

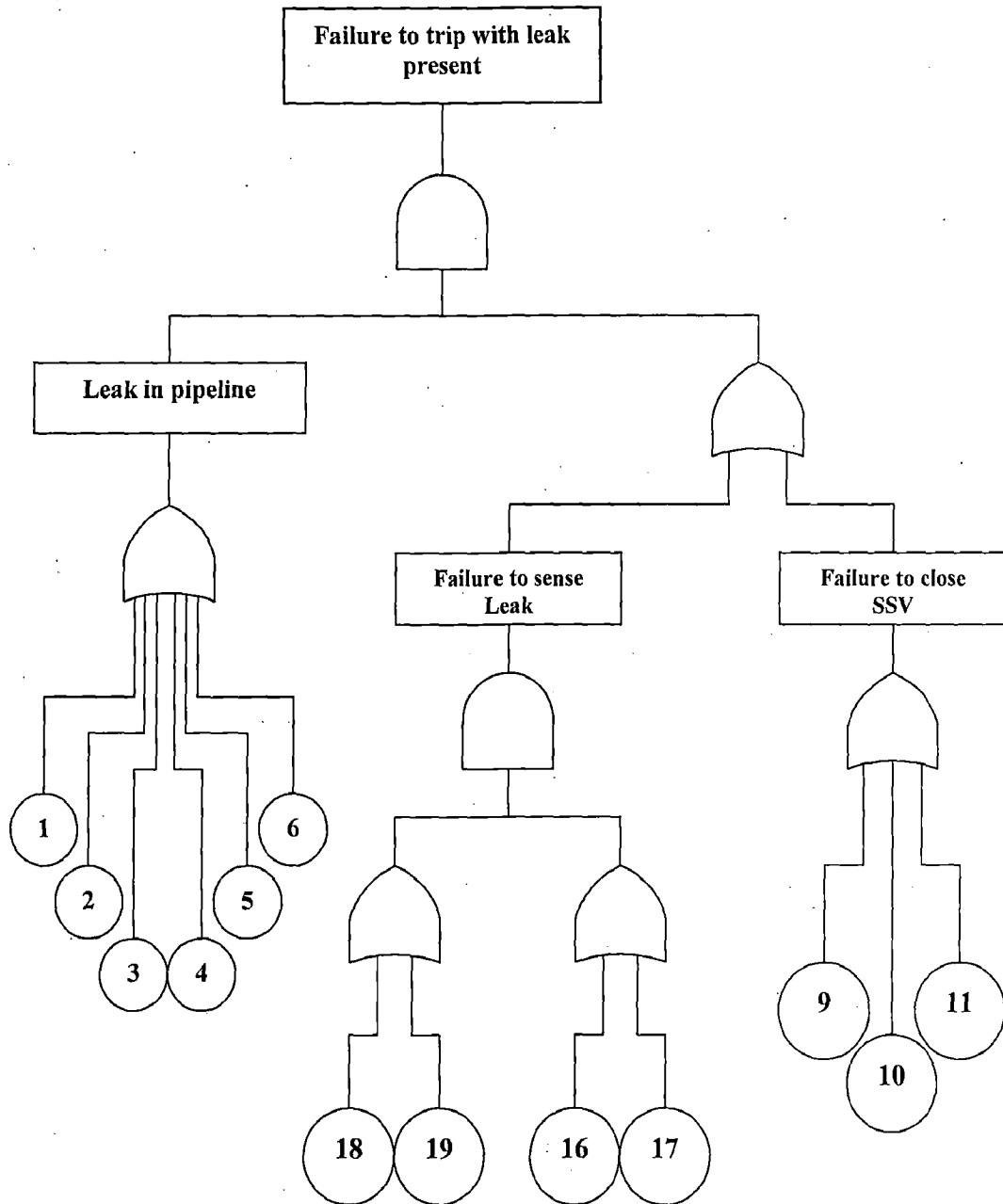


Figure 5.8: Liquid Flow – Failure to trip with leak present – MFS only

Figure 5.9 shows a fault tree diagram for a liquid flow pipeline protected by a mass flow system (MFS). The top event is a false trip. The top event occurs when either mass flow sensor (MFS-1) OR mass flow sensor-2 (MFS-2) OR the communications links between MFS-1 and the computer OR the communication link between MFS-2 and the computer, fails.

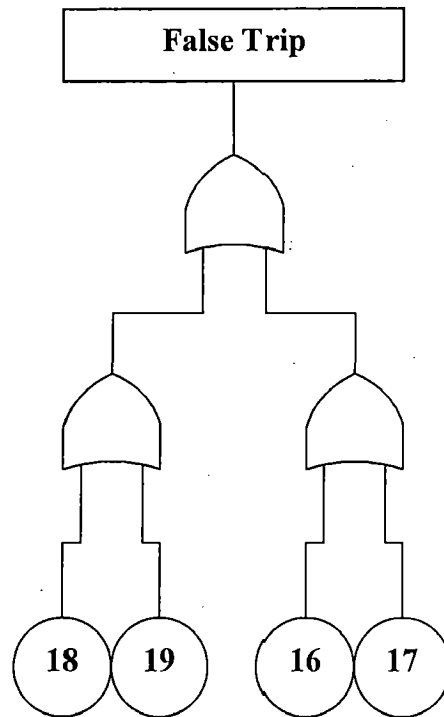


Figure 5.9: Liquid Flow- False trip – MFS only

Basic probabilities for each of the failure events will be used to calculate probability of the top event occurring in Figures 5.6 through 5.9.

5.10.4 Development of the Fault Trees for Multiphase Flow Pipelines

Fault tree diagrams have been developed for PSL and MFS leak protection. For these type of system a pair of fault trees is developed, one for a top event where a leak occurs but it is not detected, and one for top event where no leak has occurred but a false trip takes place.

Within the various fault tree diagrams, the basic events that must be considered are given in Table 5.4.

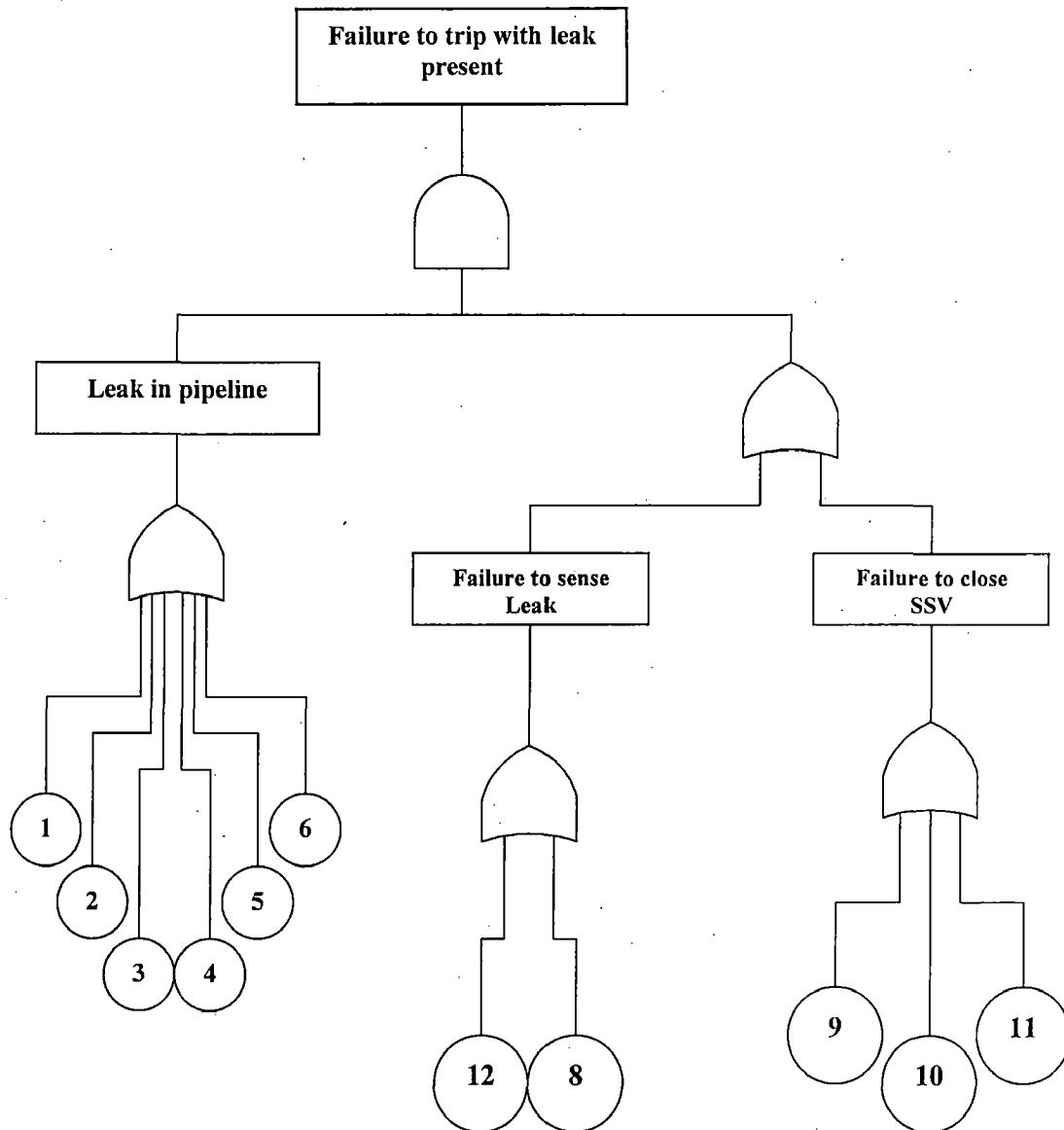


Figure 5.10: Multiphase Flow- Failure to trip with leak present– PSL only

Figure 5.10 shows a fault tree diagram for a multiphase flow pipeline protected by a PSL in which the top event is a failure to trip with a leak present. The top event occurs when there is a leak present AND either the system fails to detect a leak OR the safety shut-off valve(s) fail to close.

The system will fail if the PSL fails to detect low pressure in the pipeline OR the communication link from the PSL to the computer fails in an unsafe mode OR the safety

shut-off valves fail to close for one of the reasons outline above. It is assumed that one of these three scenarios can occur in conjunction with a leak in the pipeline to cause the top event.

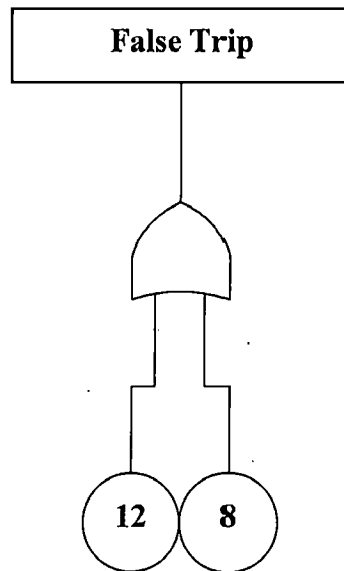


Figure 5.11: Multiphase Flow-False trips– PSL only

Figure 5.11 shows a fault tree diagram for a multiphase flow pipeline protected by a pressure sensor low (PSL) system. The top event is a false trip. The top event occurs when either the pressure sensor low OR the communication link between the PSL and the computer, fails.

Figure 5.12 shows a fault tree diagram for a liquid pipeline protected by a mass flow or line balance system (MFS) in which the top event is a failure to trip with a leak present. The top event occurs when there is a leak AND either the system fails to detect the leak, OR the safety shut- off valves fail to close.

The system will fail to sense a leak if there is a simultaneous loss of mass flow signals either due to sensor failures OR communication link from the computer to the SSV fail, resulting in the top event.

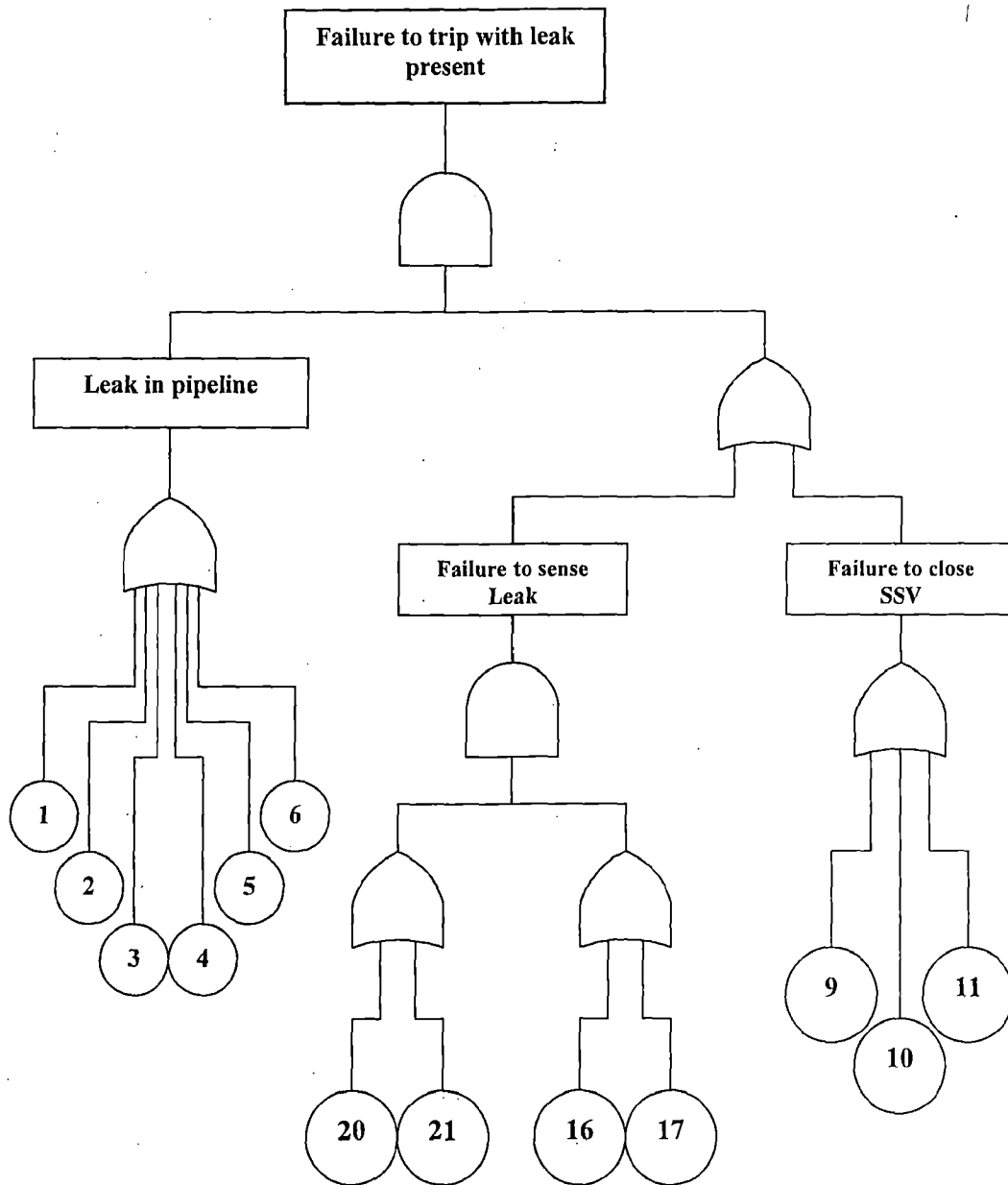


Figure 5.12: Multiphase Flow – Failure to trip with leak present – MFS only

Figure 5.13 shows a fault tree diagram for a multiphase flow pipeline protected by a mass flow system (MFS). The top event is a false trip. The top event occurs when either mass flow sensor (MFS-1) OR mass flow sensor-2 (MFS-2) OR the communications links between MFS-1 and the computer OR the communication link between MFS-2 and the computer fails.

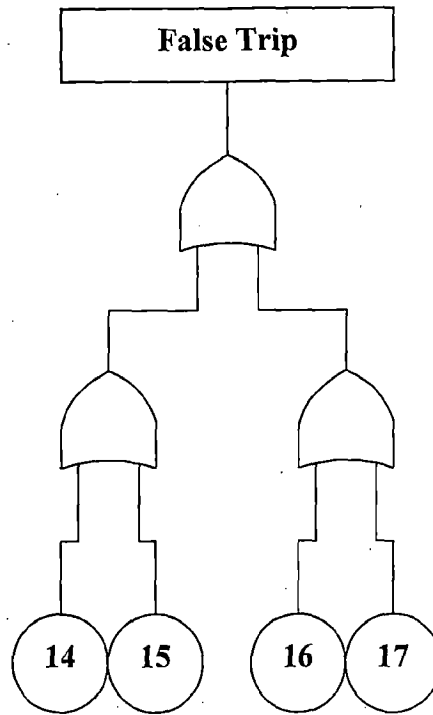


Figure 5.13: Multiphase Flow-False trip- MFS only

Basic probabilities for each of the failure events will be used to calculate probability of the top event occurring in Figures 5.10 through 5.13.

CHAPTER 6

RESULTS AND DISCUSSION

Table 6.1 summarizes the reliability of the top events for the twelve pipeline cases considered.

Table 6.1: Reliability of Top Events

| Monitoring System | Flow Type | | | | | |
|-------------------|-----------------|---------|---------|------------|---------|---------|
| | Gas | Liquid | Multi | Gas | Liquid | Multi |
| PSL | 0.99850 | 0.99923 | 0.99850 | 0.31613 | 0.31613 | 0.31613 |
| MFS | 0.99851 | 0.99851 | 0.99851 | 0.07259 | 0.07259 | 0.07259 |
| Malfunction | Failure to trip | | | False trip | | |

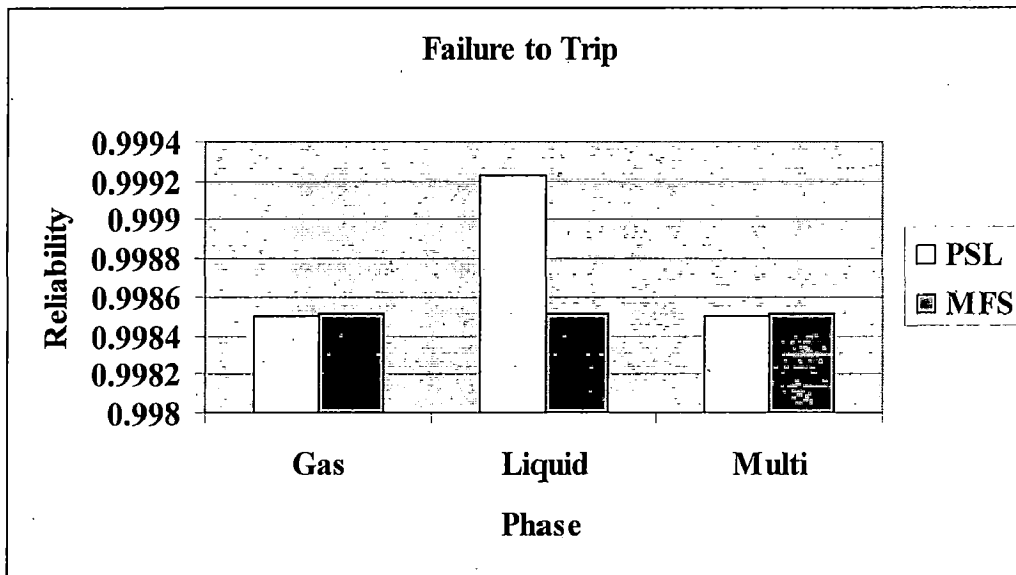


Figure 6.1: Result of FTA for three cases considering Failure to Trip

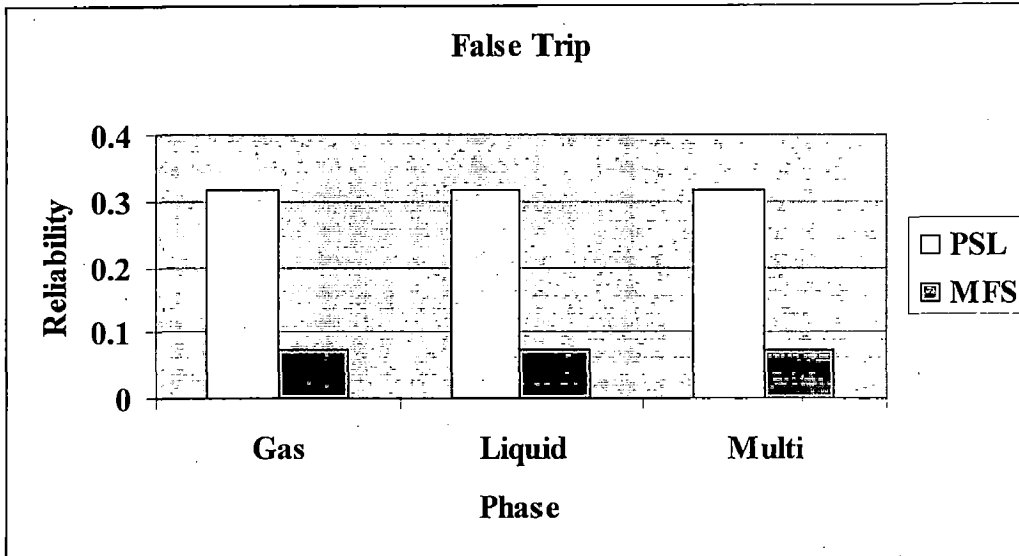


Figure 6.2: Result of FTA for three cases considering False Trip

As shown, the monitoring system using PSL has the highest values of reliability for failure to trip for but consistence values of false trip for all phase. This is typical of redundant monitoring systems.

The PSL system has not consistent values of reliability for failure to trip regardless of flow type. The reason for this is that the PSL system is capable of accurately sensing leakages for any type of flow and it has the same propensity to false trip for all types of flow. Generally, it can be seen that false tripping is the predominant failure mode, usually by three or four orders of magnitude.

CHAPTER 7

CONCLUSIONS AND FUTURE WORK

The principal conclusions of this study are

1. PSLs can detect leaks of a certain size in both liquid and gas pipe flow. Liquid data suggests leaks above a critical size can be detected at a significant distance from the PSL sensor, provided the PSL is set high (with respect to pipeline operating pressure) and the leak is large.
2. PSLs can be triggered when no leak is present. Operators are less likely to register, analyze and remember false alarms unless they occur repeatedly, for example, when a new leak system is installed or an existing system is recalibrated.
3. PSLs cannot protect pipeline systems where the hydrostatic head of the seawater exceeds the PSL trip pressure, or the operating pressure of the line. This is a concern in deepwater, but may also be a concern in shallow water. Mature reservoirs in the shallow OCS have declining reservoir pressures, which translate to lower pipeline operating pressures.
4. Gas pipelines cannot rely on PSLs for leak detection due to gas compressibility. The data collected indicate that unless the leak is on the riser (very near the PSL alarm) it cannot be detected on a gas pipeline.
5. The use of PSLs as the principal regulatory mechanism for pipeline leak detection should be reviewed. Sufficient data indicate that PSLs, alone, simply cannot function reliably to detect even large leaks in many pipelines.

This study uses the exact probability value of various system components, in future this can be done by the use of exploratory data analysis. Also modeling can be done for each component considering the failure rate. One more major outcome of this study is PSL in case failure to trip not gives a consistent reliability. This can be achieved by arranging the PSL and MFS in parallel. This gives higher reliability to the emergency shutdown system.

REFERENCES

1. Aird, R. J. "The application of reliability engineering to process plant maintenance", *The Chemical Engineer*, 1980 May, pp 301-305, 311.
2. Aird, R. J. "Reliability assessment of safety relief valves", *Trans. Institute of Chemical Engineers*, vol 60, 1982, pp 3 14-3 18.
3. Aird, A. J. "Practical estimation of reliability parameters for process equipment", *Reliability Engineering*, vol 7, 1984, pp 77-87.
4. Ansell, J.I. and M.J.Phillips, "Practical reliability data analysis", *Reliability Engineering and System Safety*, Vol. 28, 1990, pp337-356.
5. Ansell, R.O., J. I. Ansell, "Modeling the reliability of sodium sulphur cells", *Reliability Engineering*, vol 17, 1987, pp 127-137.
6. Arendt, J. S., M. L. Casada, J. J. Rooney, "Reliability and hazards analysis of a cumene hydroperoxide plant", *Plant/Operations Progress*, vol 5, Apr 1986, pp 97-102.
7. Anyakora, S. N., G. F. Angel, F. P. Lees, "Some data on the reliability of instruments in the chemical plant environment", *The Chemical Engineer*, Nov 1971, pp 396-402.
8. Bello, G. A. Bobbio, "A reliability data bank in the petrochemical sector", *Terotechnica*, vol 2, 1981, pp167-174.
9. Bendell, Tony "An Overview of Collection, Analysis, and Application of Reliability Data in the Process Industries", *IEEE Transactions on Reliability*, Vol. 37, No. 2, 1988.
10. Bloch, H. P., D. A. Johnson, "Downtime prompts upgrading of centrifugal pumps", *Chemical Engineering*, 1985 Nov 25, pp 3541.
11. Bullock, B. C., "The practical application of reliability engineering techniques", *American Institute of Chemical Engineering*, Loss Prevention Symposium, Washington, DC, 1974.
12. Caceres, S., E. J. Henley, "Process failure analysis by block diagrams and fault trees", *Industrial and Engineering Chemistry Fundamentals*, vol 15, No 2, 1976, pp 128-134.

13. Centre for Chemical process Safety of the American Institute of Chemical Engineers, *Guidelines for Chemical Process Quantitative Risk Analysis*, New York, 1989.
14. Delia, Montoro-Cazorla, Rafael Pérez-Ocón, "Reliability of a system under two types of failures using a Markovian arrival process", *Operations Research Letters* 34, 2006, pp 525 – 530.
15. Dhillon, Balbir S., K. Ugwu, "Bibliography of Literature on Chemical Systems Reliability", *Microelectronics. Reliability*, Vol. 24, No. 6, 1984, pp. 1087-1093.
16. Dhillon, Balbir S., Subramanyam Naidu Rayapati, "Chemical-System Reliability: A Review", *IEEE Transactions on Reliability*, Vol. 37, No. 2, 1988.
17. Duglinson, C., H. Lambert, "Interval reliability for initiating and enabling events", *IEEE Trans. Reliability*, vol R-32, Jun 1983, pp 150-163.
18. Ebeling, Charles E, "*An Introduction to Reliability and Maintainability Engineering*", Tata McGraw Hill, New Delhi, 2000.
19. Farit, M. Akhmedjanov, "Reliability Databases: State-of-the-Art and Perspectives", *Risk National Laboratory*, Roskilde, August 2001.
20. Freshwater, D. C., B. A. Buffham, "Reliability engineering for the process plant industries", *The Chemical Engineer*, Oct 1969, pp 367-369.
21. Funnemark, Espen, Jan Erik Eldor and Gerd Petra Haugom, "Identification and Review of Databases for Reliability Data", *WP4 HyApproval*, Version 1.0, 2006.
22. Gaal, Z., Z. Kovacs, "Reliability of chemical technological systems II", *Hungarian J. Industrial Chemistry*, vol 13, 1985, pp 271-286.
23. Gibson, S. B., "Reliability engineering applied to the safety of new projects", *The Chemical Engineer*, Feb 1976, pp105-106.
24. Gruhn, G., W. Neumann, R. Seidel, "Reliability analysis of complex chemical engineering systems", *Hungarian J. Industrial Chemistry*, vol 11, 1983, pp 275-282.
25. Henley, E. J. ,S. L. Gandhi, "Process reliability analysis", *American Institute of Chemical Engineering Journal*, vol 21, Jul 1975, pp 677-686.
26. ISO, "*Petroleum and natural gas industries- Collection and Exchange of reliability and maintenance data for equipment*", Research report, International Organization for Standardization, 2004.

27. John, R. Mastandrea, J. Wesley Miller, David M. Clare, "*Rapid Leak Detection for Sea Floor Pipeline*", Minerals Management Service CA, Technical Report, 1990.
28. Kardos, J., K. Lorenz, "Reliability analysis and optimization of chemical engineering systems", *Hungarian J. Industrial Chemistry*, vol 15, 1987, pp 29-38.
29. Lars, Bodsberg, Per Hokstad, "A System Approach to Reliability and Life Cycle Cost Of Process Safety Systems", *IEEE Transactions on Reliability*, Vol-44, No-2, 1995.
30. Lees, F. P., "Some data on the failure modes of instruments in the chemical plant environment", *The Chemical Engineer*, Sep 1973, pp 418-421.
31. Lees, F. P., "A review of instrument failure data", *Institute of Chemical Engineers Symposium Series*, 1976, No 47, 73.
32. Lees, F. P., "*Loss Prevention in the Process Industries*", Butterworths, Vol-1&2, London, 1980.
33. Lenz, R. E., "Reliability design in process plants", *Chemical Engineering Progress*, vol 66, Dec 1970, pp 42-44.
34. Loftus, J., "Reliability in ethylene plants", *Chemical Engineering Progress*, vol 66, Dec 1970, pp 53-58.
35. Margetts, T., "PLCs for alarm and shutdown systems", *The Chemical Engineer*, Jul/Aug 1986, pp 36-37.
36. Miller, M. J., "Reliability of fire protection systems", *Chemical Engineering Progress*, vol 70, Apr 1974, pp62-67
37. Modarres, Mohammad, Mark Kaminskiy, Vasilii Krivtsov, "*Reliability Engineering and Risk Analysis- A Practical Guide*", Marcel Dekker, New York, 1999.
38. Moss, T.R., "Uncertainties in reliability statistics", *Reliability Engineering and System Safety*, Vol. 34, 1991, pp. 79-90.
39. Moss, T. R. , E. R. Snaith, "Practical methods for reliability assessment of chemical plants", *Institute of Chemical Engineers*, North West Branch, 1979, pp 6.
40. Nivolianitou, Z., A. Amendola, G. Reina, "Reliability analysis of chemical processes by the DYLAM approach", *Reliability Engineering*, vol 14, 1986, pp 163-182.

41. Office of Safety and Mission Assurance, NASA Headquarter, “*Probabilistic Risk Assessment Procedure Guide for NASA Managers and Practitioners*”, Version 1.1, Washington, 2002.
42. Ostrander, V. P., “Spacecraft reliability techniques for industrial plants”, *Chemical Engineering Progress*, vol 67, Jan 1971, pp 49-53.
43. Outfit, Y., A. Rauzy “Approximate estimation of system reliability via fault trees”, *Reliability Engineering and System Safety*, Vol. 87 2005, pp 163–172.
44. Palmer, A. C. and R. A. King, "*Subsea Pipeline Engineering*", Pennwell Corporation, Tulsa, Oklahoma, 2004.
45. Patterson, L. W., J. M. Clark, "Process plant reliability in Puerto Rico", *Chemical Engineering Progress*, vol 67, Jan 1971, pp 54-56.
46. Per, Hokstad, Kjell Corneliussen, “*Reliability Prediction Method for Safety Instrumented Systems*”, SINTEF Industrial Management, Trondheim, Norway, 2003.
47. Peters, John, “*Assessment of valve failures in the offshore oil & gas sector*”, Research Report, Health and Safety Executive, UK, 2003.
48. Rausand, Marvin, “*System Reliability Theory*”, 2nd ed Wiley 2004.
49. Rudd, D. F., “Reliability theory in chemical system design”, *Industrial and Engineering Chemistry Fundamentals*, vol 1, May 1962, pp 138-143.
50. Saleh, J.H. K. Marais, “Reliability: How much is it worth? Beyond its estimation or prediction, the (net) present value of reliability”, *Reliability Engineering and System Safety* 91, 2006, pp 665–673.
51. Sherwin, D. J., “Failure and maintenance data analysis at a petrochemical plant”, *Reliability Engineering*, vol 5, 1983, pp 197-215.
52. SINTEF, 1997, *OREDA - Offshore Reliability Data*, 3rd Edition, SINTEF Industrial Management, Trondheim, Norway.
53. Skelton, Bob, “*Process Safety Analysis – An Introduction*”, Gulf Publishing, Houston, 1997.
54. Stevens, R., “Emergency generators: A reliability study based on an analysis of failures”, *Plant/Operations Progress*, vol 2, Oct 1983, pp 203-208.

55. Tarek, Elsayed, Bob Bea, "*PIMPIS: Knowledge-Based Pipeline Inspection, Maintenance and Performance Information System*", Progress Report, Marin Technology and management Group, Civil and Environment Department, CA, 1997.
56. Thomas, J. C., S. H. Zanakis, "Reliability of a chemical process system: A simulation approach", *Winter Simulation Conf. Annual Proceedings*, Washington DC, 1974 Jan14-16, vol 1, pp 198-209.
57. Triggs, L. E., "Improving boiler reliability", *Chemical Engineering Progress*, Oct 1978, pp 53-58.
58. US Department of Defence, "*MIL-HDBK-338B*", Washington, October 1998.
59. US Department of Defence, "*Reliability Prediction of Electronic Equipment*", Washington, 1991.
60. Wasserman, Garry S., "*Reliability Verification Testing and Analysis in Engineering Design*", Marcel Dekker, New York, 1999.
61. Williams, H. L., B. H. Russell, "NASA reliability techniques in the chemical industry", *Chemical Engineering Progress*, vol 66, Dec 1970, pp 45-49.
62. Wood, D. R., E. J. Muehl, A. E. Lyon, "Determining process plant reliability", *Chemical Engineering Progress*, vol70, Oct 1974, pp 62-66.

Website Resources

1. Offshore technology (<http://www.offshore-technology.com>)
2. Sensors (<http://www.sensors.com>)
3. Regularity of PSL (<http://www.access.gpo.gov/nara/cfr/index.html>)
4. Health and Safety Executive (<http://www.hse.gov.uk>)
5. Reliability Analysis Centre (<http://rac.iitri.org>)

APPENDIX

For The Fault Tree Calculation

It is considered here that every failure occurs in every one million hours for a component.

So

$$\text{Total life } t = 1E+6 \text{ hrs}$$

Now consider for each failure mode

P_1 = Probability of failure of Event 1

P_2 = Probability of failure of Event 2

P_3 = Probability of failure of Event 3

P_4 = Probability of failure of Event 4

P_5 = Probability of failure of Event 5

P_6 = Probability of failure of Event 6

P_7 = Probability of failure of Event 7

P_8 = Probability of failure of Event 8

P_9 = Probability of failure of Event 9

P_{10} = Probability of failure of Event 10

P_{11} = Probability of failure of Event 11

P_{12} = Probability of failure of Event 12

P_{13} = Probability of failure of Event 13

P_{14} = Probability of failure of Event 14

P_{15} = Probability of failure of Event 15

P_{16} = Probability of failure of Event 16

P_{17} = Probability of failure of Event 17

P_{18} = Probability of failure of Event 18

P_{19} = Probability of failure of Event 19

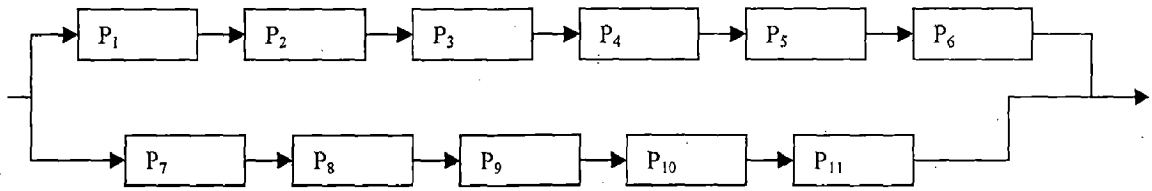
P_{20} = Probability of failure of Event 20

P_{21} = Probability of failure of Event 21

And distribution considered in calculation is exponential with constant failure rate

$$P = 1 - \exp(-\lambda t)$$

For Figure 4.2



Reliability Block Diagram for Figure 4.2

Top Event Reliability

$$= 1 - [\{ 1 - (1 - P_1) * (1 - P_2) * (1 - P_3) * (1 - P_4) * (1 - P_5) * (1 - P_6) \} \{ 1 - (1 - P_7) * (1 - P_8) * (1 - P_9) * (1 - P_{10}) * (1 - P_{11}) \}]$$

For Figure 4.3

Top Event Reliability

$$= (1 - P_{12}) * (1 - P_8)$$

For Figure 4.4

Top Event Reliability

$$= 1 - [1 - \{ (1 - P_1) * (1 - P_2) * (1 - P_3) * (1 - P_4) * (1 - P_5) * (1 - P_6) \}] * [1 - \{ (1 - P_9) * (1 - P_{10}) * (1 - P_{11}) \} * \{ 1 - (1 - (1 - P_{14}) * (1 - P_{15})) * (1 - (1 - P_{16}) * (1 - P_{17})) \}]]$$

For Figure 4.5

Top Event Reliability

$$= (1 - P_{14}) * (1 - P_{15}) * (1 - P_{16}) * (1 - P_{17})$$

For Figure 4.6

Top Event Reliability

$$= 1 - [\{ 1 - (1 - P_1) * (1 - P_2) * (1 - P_3) * (1 - P_4) * (1 - P_5) * (1 - P_6) \} \{ 1 - (1 - P_8) * (1 - P_9) * (1 - P_{10}) * (1 - P_{11}) * (1 - P_{13}) \}]$$

For Figure 4.7

Top Event Reliability
 $= (1 - P_{12}) * (1 - P_8)$

For Figure 4.8

Top Event Reliability
 $= 1 - [1 - \{ (1 - P_1) * (1 - P_2) * (1 - P_3) * (1 - P_4) * (1 - P_5) * (1 - P_6) \}] * [1 - \{ (1 - P_9) * (1 - P_{10}) * (1 - P_{11}) \}] * \{ 1 - (1 - (1 - P_{18}) * (1 - P_{19})) * (1 - (1 - P_{16}) * (1 - P_{17})) \}]$

For Figure 4.9

Top Event Reliability
 $= (1 - P_{18}) * (1 - P_{19}) * (1 - P_{16}) * (1 - P_{17})$

For Figure 4.10

Top Event Reliability
 $= 1 - [\{ 1 - (1 - P_1) * (1 - P_2) * (1 - P_3) * (1 - P_4) * (1 - P_5) * (1 - P_6) \} \{ 1 - (1 - P_{12}) * (1 - P_8) * (1 - P_9) * (1 - P_{10}) * (1 - P_{11}) \}]$

For Figure 4.11

Top Event Reliability
 $= (1 - P_{12}) * (1 - P_8)$

For Figure 4.12

Top Event Reliability
 $= 1 - [1 - \{ (1 - P_1) * (1 - P_2) * (1 - P_3) * (1 - P_4) * (1 - P_5) * (1 - P_6) \}] * [1 - \{ (1 - P_9) * (1 - P_{10}) * (1 - P_{11}) \}] * \{ 1 - (1 - (1 - P_{20}) * (1 - P_{21})) * (1 - (1 - P_{16}) * (1 - P_{17})) \}]$

For Figure 4.13

Top Event Reliability $= (1 - P_{14}) * (1 - P_{15}) * (1 - P_{16}) * (1 - P_{17})$

ABBREVIATIONS

| | |
|-------|---|
| API | American Institute Of Petroleum |
| CPM | Computational Pipeline Monitoring |
| CPU | Central Processing Unit |
| D | Dangerous |
| DD | Danger Detected |
| DU | Dangerous Undetected |
| DCS | Distributed Control System |
| FTA | Fault Tree Analysis |
| MFS | Mass Flow Sensor |
| MMS | Mineral Management Service |
| MAOP | Maximum Allowable Operating Pressure |
| MTTF | Mean Time To Failure |
| MTTR | Mean Time To Repair |
| NONC | Noncritical |
| OCS | Outer Continental Shelf |
| OREDA | Offshore Reliability Equipment Data |
| PDS | Probabilistic Distribution Study |
| PLC | Programmable Logic Control |
| PSL | Pressure Safety Low |
| PSHL | Protected By High And Low Pressure Sensor |
| ROC | Rate Of Change |
| ROV | Remotely Operated Vehicle |

| | |
|-------|--|
| RTTM | Real Time Transient Model |
| SD | Safe Detected |
| SU | Safe Undetected |
| ST | Spurious Trip |
| SDV | Shutdown Valve |
| SIS | Safety Instrumented System |
| SPC | Statistical Process Control |
| STD | Spurious Trip Detected |
| STU | Spurious Trip Undetected |
| SCADA | Supervisory, Control And Data Acquisition System |