

RELIABILITY ANALYSIS OF SCADA SYSTEMS
USED IN THE OFFSHORE OIL AND GAS INDUSTRY

by

EGEMEN KEMAL CETINKAYA

A THESIS

Presented to the Faculty of the Graduate School of the

UNIVERSITY OF MISSOURI-ROLLA

In Partial Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

2001

Approved by

Kelvin T. Erickson, Advisor

Eldon K. Stanek

Shari Dunn-Norman

Copyright 2001
by
Egemen Kemal Cetinkaya
All Rights Reserved

ABSTRACT

Reliability studies of systems have been an important area of research within electrical engineering for over a quarter of a century. In this thesis, the reliability analysis of the Supervisory Control And Data Acquisition (SCADA) systems used in offshore petroleum facilities was examined. This thesis presents fault trees for the platform production facilities, subsea control systems, a typical SCADA system, and the human induced fault tree. Software reliability was also studied. The fault trees were developed based on a safety flow chart and Process and Instrumentation Diagrams (P&ID). This work was conducted as a subcontract to the United States Department of the Interior, Mineral Management Service, Technology Assessment & Research Program, Program SOL 1435-01-99-RP-3995 (project no 356) to the University of Missouri-Rolla.

Based on the fault tree diagrams and fault rates, the reliability of the SCADA system used in the offshore facilities was assessed. The failure availability of the SCADA system used in offshore platforms was also found.

ACKNOWLEDGMENTS

The author wishes to thank Dr. Kelvin. T. Erickson for his guidance and assistance not only in the preparation of this work, but also his valuable contributions in M.S. studies.

The author sincerely appreciates the help and encouragement received from Dr. Eldon K. Stanek for the preparation and completion of this project. He was not only my supervisor, but also he was like a father throughout my stay at University of Missouri-Rolla.

The author is thankful to Dr. Shari Dunn-Norman for her help in understanding the process and review of this work. The author also wishes to acknowledge Dr. Ann Miller for her help throughout the project.

Finally, the author would like to dedicate this work to his parents, who may properly consider the completion of this thesis as a success of their own.

TABLE OF CONTENTS

	Page
ABSTRACT	iii
ACKNOWLEDGMENTS	iv
LIST OF ILLUSTRATIONS	vii
LIST OF TABLES	viii
SECTION	
1. INTRODUCTION	1
2. BACKGROUND AND THEORY	4
2.1. INTRODUCTION	4
2.2. FAULT TREE DIAGRAMS	4
2.2.1. Fault Tree Symbols	4
2.2.1.1 Event Symbols	5
2.2.1.2 Gate Symbols	5
2.2.2. Fault Tree Construction	6
2.2.3. Probability Calculation of Fault Trees	6
2.3. RELIABILITY THEORY	6
2.3.1. Reliability Modeling	8
2.3.2. Series and Parallel Reliability	8
2.3.3. Reliability Analysis of a Simple System	9
2.3.4. Fault Tree Analysis Program	11
2.3.5. Conditional Probability	12
3. SCADA SYSTEMS	14
4. RELIABILITY ANALYSIS OF SCADA SYSTEMS	20
4.1. DEVELOPMENT OF THE FAULT TREE FOR OFFSHORE FACILITY	20
4.1.1. Failure Probability for Hardware Components	31
4.1.2. Calculation of the Availability of the Top Event	39
4.2. ANALYSIS OF THE SUBSEA CONTROL SYSTEMS	41
4.2.1. Fault Tree Construction of Subsea Control Systems	41
4.2.2. Failure Probability of Subsea Control Systems	44

4.3. SCADA SYSTEM ANALYSIS	45
4.3.1. Development of the SCADA Fault Tree	45
4.3.2. Failure Probability of the SCADA System	46
4.4. HUMAN ERRORS IN THE SCADA SYSTEM	47
4.5. SOFTWARE RELIABILITY OF THE SCADA SYSTEMS.....	48
5. RESULTS.....	49
6. CONCLUSIONS	51
APPENDICES	
A. PROGRAM REC	53
B. SAFETY DEVICE DESIGNATIONS.....	61
BIBLIOGRAPHY.....	63
VITA.....	66

LIST OF ILLUSTRATIONS

Figure	Page
2.1. Event Symbols	5
2.2. Gate Symbols	5
2.3. Simple Electric Circuit.....	9
2.4. Fault Tree Diagram of Simple System.....	10
3.1. Typical SCADA Components.....	15
3.2. Distributed PLC Architecture	17
3.3. Typical Subsea SCADA Architecture	18
4.1. Safety Flow Chart of Offshore Production Facility	21
4.2. Upper Level Fault Tree Diagram	22
4.3. Fault Tree Diagram of Intermediate State I	24
4.4. Fault Tree Diagram of Overpressure	26
4.5. Fault Tree Diagram of Under pressure	27
4.6. Fault Tree Diagram of Excess Temperature	28
4.7. Fault Tree Diagram of Ignition	29
4.8. Fault Tree Diagram of Excess Fuel	30
4.9. Subsea Control Systems.....	40
4.10. Fault Tree for Subsea Control System	43
4.11. Fault Tree Diagram for a Distributed Platform SCADA System	45
4.12. Human Induced SCADA Fault Tree.....	47

LIST OF TABLES

Table	Page
2.1. Failure Rates of a Simple System	11
4.1. Failure Data for Basic Events in Surface System	38
4.2. Failure Rates and Repair Times for Subsea Failure Modes.....	44
4.3. Failure Data for Basic Events in SCADA Fault Tree	46
4.4. Software-induced Failure Data for Basic Events in SCADA Fault Tree.....	48
5.1. Dependent Event's Failure Availabilities	49
5.2. Summary of Reliability Analysis Results	50

1. INTRODUCTION

The term SCADA stands for, Supervisory Control And Data Acquisition; it is not a full control system, but rather focuses on the supervisory level. Although SCADA implies control at the supervisory level according to [1], in this thesis, the reliability at the device level was also examined, because field devices, such as PLCs, sensors, etc., are components of a SCADA system [2]. SCADA systems are used in production monitoring and control, well monitoring and control, process monitoring and control, unmanned platform monitoring and control, pipeline systems, and drilling for offshore oil and gas in the oil and gas industry [3].

Offshore production systems include producing oil or gas wells, a central production facility, and some means of transporting the oil or gas to shore. In shallower waters (< 1000 ft), wells are located on a conventional steel production platform and a pipeline is used to transport the oil or gas to shore. In water depths over 1000 ft, wells are often located on templates resting on the sea floor. Such systems are referred to as subsea systems, and include not only the subsea wells, but also manifolds, risers, and complex flowline and control systems connecting the various components. Subsea systems are tied back to a central production facility. The central production facility could be a conventional steel platform, but it may also be a compliant or floating structure such as a tension leg platform, guyed tower, spar, or floating production storage and offloading facility (FPSO). This study focuses on production systems including a conventional platform.

Petroleum production systems typically produce oil, gas and water through individual wellbores, wellheads, and tree systems, through flowlines and into a production manifold regardless of their exact configuration. The control of production is at a central facility for offshore production systems. Measurements such as temperatures, pressures, flowrates, injection rates, sand content, and gas leaks are recorded intermittently or continuously for well monitoring purposes [3]. The monitoring and controlling functions in oil and gas processing can be classified as:

- Operational controls

- Shutdown systems
- Fire and gas detection systems
- Fiscal metering systems and reports

The systems and functions were generalized in this thesis for fault tree and reliability analysis. Unmanned platforms were not examined in this thesis. The major trunklines used to connect offshore platforms to terminals on land, or to connect land based processing facilities with refineries or other distribution networks are referred as pipelines [3]. Analysis of pipelines was not addressed in this thesis.

In the 1980s SCADA systems for offshore platforms included modules for production control and monitoring. Event information was on multiple databases with limited time synchronization, making the event analysis difficult. Modern SCADA systems interface with a multitude of input and output points [3].

The importance of reliability analysis of the systems is from the smallest to the largest industrial appliances. Generally, the question that is asked by people is: "Is it reliable?" For a better understanding of the term reliability, the following definition is provided: "Reliability is the probability that a unit will function normally when used according to specified conditions for at least a stated period of time" [4].

Whenever reliability is mentioned, another general term "safety" is also of concern. The safety of human life and the environment is the main concern throughout this study. Therefore, the objective of this thesis is to find the least reliable components, and improve the reliability of the SCADA systems; thereby reducing the risk of loss of lives, and the risk of a polluted environment.

The reliability of the SCADA system was estimated using probabilistic risk assessment (PRA). Several fault trees were constructed to show the effect of contributing events on system-level reliability. It was assumed that the undesirable event(s) such as oil spill and/or personnel injury were consequences of the SCADA failure at the device level.

Probabilistic methods provide a unifying method to assess physical faults, contributing effects, human actions, and other events having a high degree of uncertainty. The probability of various end events, both acceptable and unacceptable, is calculated from the probabilities of the basic initiating failure events.

The outcome of the analysis can be expressed in different reliability indices. The result of this study is expressed as availability, and the mean time between failures is given as well. An effort has been made in this thesis to find the component failure rates, and average repair times for each component.

There is little research on either the reliability of the SCADA systems or the reliability of the petroleum process; however there is a great deal of printed literature dealing with the basic concepts of reliability [4], [5], [6], [7], [8]. The data for the analysis of hardware components of offshore petroleum facilities were found from [9]. The fault rates of the communication networks were supplied from one operator that employs SCADA. The human error probabilities were gathered from [10]. The data for the probability of an accident was found from [11]. Whenever the data were unavailable, they were estimated from historical events. The data to model the system were found from [12] and the Process and Instrumentation Diagrams (P&ID) were supplied from an operator.

Basic explanations about the reliability theory are given in section 2. The SCADA systems used in offshore petroleum platforms are introduced in section 3, while the analysis of the systems are discussed in section 4. Section 5 examines the results. The program to calculate the probability of a top event for a given fault tree is contained in Appendix A. The safety device designations in a safety flow diagram are represented in Appendix B.

2. BACKGROUND AND THEORY

2.1. INTRODUCTION

The first reliability studies came out of the aircraft industry during World War II. In the 1960s, as systems became more complex, new analysis methods were required. H. A. Watson developed the Fault Tree Analysis method in Bell Telephone Laboratories in 1961 for the Minuteman Launch Control System [6]. Later in the 1960s, its use was extended in both nuclear and industrial applications for safety and reliability issues.

Probabilistic Risk Assessment (PRA) is a method to determine the reliability of a system based on the probability of component(s) and/or system(s) failure. Fault Tree Analysis (FTA), which is a part of PRA, provides a method for determining how failures can occur both quantitatively and qualitatively. Fault tree analysis is one of the engineering tools that provides a systematic and descriptive approach to the identification of systems under risk. It also provides a visual aid in understanding the system's behavior [6].

2.2. FAULT TREE DIAGRAMS

Fault tree diagrams provide a means of visualizing all of the possible modes of potential failures, an understanding of the system failure due to component failures and redesign alternatives.

Fault tree diagrams are formed such that an undesired event appears on top of the diagram, called the top event. The causes that lead to the system failure are broken into hierarchical levels until effects of the basic system components that lead to the top failure can be identified. Branches using event statements and logic gates link the basic events, or fault events, that lead to the top event. The failure rate data must be available for those basic events at the lowest hierarchical level. Once the fault tree is formed, the probability of occurrence of the top event can be found [5], [6].

2.2.1. Fault Tree Symbols. Symbols are used to connect basic events to the top event, during fault tree construction. The event symbols are logical representations of the way systems can fail. There are two kinds of fault tree symbols: event symbols, and gate symbols [5], [6].

2.2.1.1. Event Symbols. An event is a dynamic state change of a component due to hardware, software, human and environmental factors. The event symbols are shown in Figure 2.1 [5].

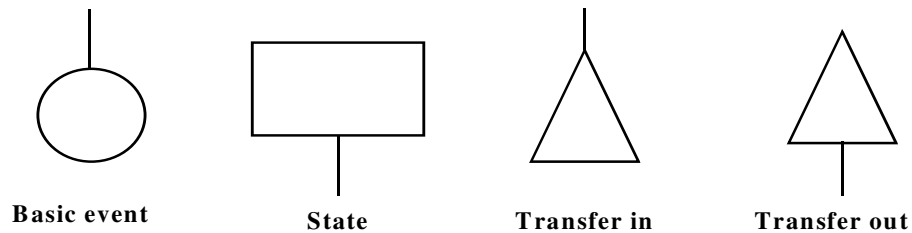


Figure 2.1. Event Symbols

A circle represents a basic component failure. It does not need further development. The reliability data are available for basic events. A rectangle is the symbol to designate an output event. It is also called a state, and used at the output of a logic gate to indicate that other basic events or states are connected to that output. The triangles are used to cross reference two identical pairs of the causal relations. Whenever the fault tree diagrams do not fit a page, triangles are used to show continuity.

2.2.1.2. Gate Symbols. Gate symbols connect basic events and/or states to states according to their causal relation. A gate might have multiple inputs, while its output should be single. The two most common logic gates (“AND” and “OR”) are shown in Figure 2.2 [5].



Figure 2.2. Gate Symbols [5]

The output of an OR gate exists if at least one input to this gate exists. The output existence of an AND gate occurs if all input conditions exist for that gate.

2.2.2. Fault Tree Construction. A fault tree (FT) is constructed such that the undesired event, or top event exists at the highest level in the fault tree. In this study, the top event is “oil spill and/or personal injury”. Basic events and outputs of gates are connected so that they lead to that top event. Basic events and states are at lower levels. “A valve that fails to close” is an example of basic event in this thesis.

Causal relationships can be analyzed in two ways: Backward analysis and forward analysis. Backward analysis starts with a system hazard and traces backward, searching for possible causes. On the other hand forward analysis starts with possible failures that may lead to a potential hazard. Both methods were used to assess the reliability of the system.

2.2.3. Probability Calculations in Fault Trees. One of the major goals of FTA is to calculate the probability of an undesired event. This calculation can be done using the Boolean representation of the system. However, the calculation is lengthy, time consuming and tedious. Therefore a program was written in the C programming language to perform this task. The documentation for it is in Appendix A.

Using the Fault Tree diagrams, and the results obtained from the calculations, which components and systems are safe was assessed.

2.3. RELIABILITY THEORY

Basic concepts about reliability theory must be known to perform analysis of systems. Reliability is the probability of a component or a system under certain conditions and predefined time, to perform its required task. Reliability is characterized by various indices, such as failure rate $\lambda(t)$, Mean Time Between Failures (MTBF), Mean Time To Failure (MTTF), Mean Time To Repair (MTTR), Availability, and Unavailability [5].

Failure rate is the ratio of the number of failures per unit time to the number of components that are exposed to failure. MTTF is the expected value of the time to failure. If the failure rate is constant,

$$MTTF = \frac{1}{\lambda} \quad (1)$$

If a failure occurs in every one million hours for a component, it is said that the component has a failure rate of 1×10^{-6} failures/hour, so the MTTF is reciprocal of failure rate [5]. The failure rates used in this thesis have constant failure rates. If the failure rates have different distributions (e.g. Weibull), then the MTTF is found according to corresponding distribution. The average time to fix a component, MTTR, is expressed as,

$$MTTR = \frac{1}{\mu} \quad (2)$$

where μ is the constant repair rate. If the MTTR is 24 hours for a given component, then there are 365 repairs/year for that component. MTBF is defined as the sum of the MTTF and the MTTR.

$$MTBF = MTTF + MTTR \quad (3)$$

If the repair time is small, then the MTBF is close to the MTTF. Availability and Unavailability are the reliability terms that are derived from MTBF and MTTR. “Availability is the probability of finding the component or system in the operating state at some time in the future” [5]. It can be found as follows:

$$availability = \frac{uptime}{uptime + downtime} = \frac{MTTF}{MTTF + MTTR} = \frac{\mu}{\mu + \lambda} \quad (4)$$

Unavailability is the dual of availability. It is the probability of finding a component or system in the non-operating state at some time in the future [5]. It can be found as follows:

$$unavailability = \frac{downtime}{downtime + uptime} = \frac{MTTR}{MTTR + MTTF} = \frac{\lambda}{\lambda + \mu} \quad (5)$$

These indices will be used in analyzing the SCADA systems, and to express the analysis results.

2.3.1. Reliability Modeling. In reliability theory, mechanical components are assumed to have Poisson distribution, while the reliability of electrical components have exponential distribution. Throughout this study components are assumed to have constant failure rates (λ). Failure rate information needed for most of the elements was found. Whenever the data were unavailable, they are assigned by estimation.

In general, the unit for failure rate is given in failures per year or failures per million hours. Assuming a constant failure rate, the reliability of an element is:

$$R(t) = e^{-\lambda t} \quad (6)$$

One of three basic theorems of probability states that $P(q) + P(\bar{q}) = 1$. Similarly the sum of reliability and unreliability is equal to one. Using this theorem, the unreliability of an element can be shown by:

$$Q(t) = 1 - R(t) = 1 - e^{-\lambda t} \quad (7)$$

These concepts match one's intuition. When a product is produced ($t \rightarrow 0$, $R=1$), it is less likely to fail. But as time passes, and its life comes to an end ($t \rightarrow \infty$, $R=0$) it is more likely to fail.

2.3.2. Series and Parallel Reliability. A series system is composed of a group of elements, and if any of these elements fail, the system fails too. If R_i is the reliability of a component, then the overall reliability of the system (R_s), assuming there are n elements in the system, is:

$$R_s = R_1 \times R_2 \times \dots \times R_n = \prod_{i=1}^n R_i \quad (8)$$

In a similar way, unreliability of a series system can be expressed as:

$$Q_s = 1 - \prod_{i=1}^n R_i = 1 - \prod_{i=1}^n (1 - Q_i) \quad (9)$$

Branches form parallel systems. The branches can be composed of single and/or multiple elements. The system fails if some or all of these elements fail to operate depending upon the location of elements. If $Q_i = 1 - R_i$ is the probability that a single element fails, then the probability that whole system fails can be calculated as:

$$Q_p = Q_1 \times Q_2 \times \dots \times Q_n = \prod_{i=1}^n Q_n = \prod_{i=1}^n (1 - R_i) \quad (10)$$

and the reliability of a system is $R_p = 1 - Q_p$, so the reliability of a parallel system is:

$$R_p = 1 - \prod_{i=1}^n (1 - R_i) = 1 - \prod_{i=1}^n Q_i \quad (11)$$

In a series system, system reliability decreases as the number of components increase. On the other hand, the unreliability of a system decreases as the number of parallel components increase in the system [5].

2.3.3. Reliability Analysis of a Simple System. Previously, basic concepts about reliability have been introduced. As an example system, consider the simple circuit shown in Figure 2.3.

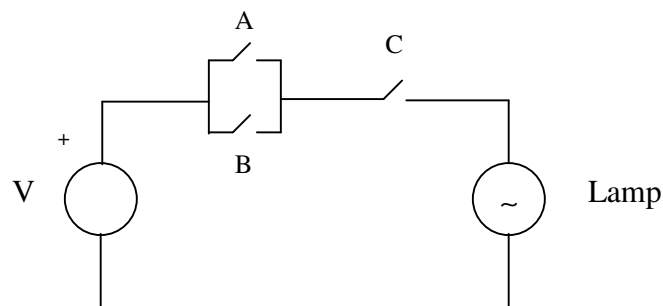


Figure 2.3. Simple Electric Circuit

The FTA method will be used to evaluate the reliability of the system. First, one

must define what could be the top event or undesired event. The purpose of this circuit is to turn on the lamp, so failure of the lamp to lighten could be a top event. It can fail because of failure of the power supply or the combined failure of the switches that might lead to top event. Both A and B switches must fail to close in the parallel path, or only if the switch C fails to close the lamp will not lighten. Now based on FTA method if the fault tree is constructed, the diagram will look as in Figure 2.4. For simplicity, instead of text explanations for the basic causes, numbers are assigned to each basic event, where:

- 1- Failure of power supply.
- 2- Switch A fails to close.
- 3- Switch B fails to close.
- 4- Switch C fails to close.

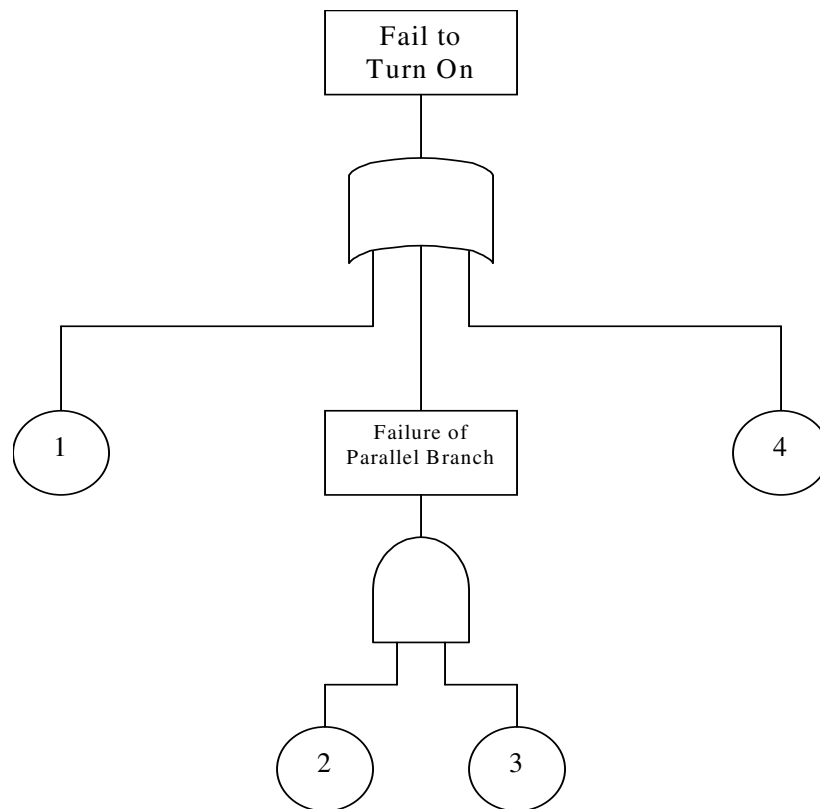


Figure 2.4. Fault Tree Diagram of Simple System

Assume failure probability for each of these basic events is as given in Table 2.1. The numbers were chosen randomly. The probability of the undesired event to occur is:

$$\begin{aligned}
 q_{system} &= (1 - p_1) \times (1 - p_2 \times p_3) \times (1 - p_4) \\
 &= q_1 \times q_2 \times q_4 + q_1 \times q_3 \times q_4 - q_1 \times q_2 \times q_3 \times q_4
 \end{aligned}
 \tag{12}$$

which yields the result 0.0028. As the system becomes more complex, it becomes cumbersome to calculate the probability of the top event. Hence, a computer program is useful to calculate the probability of the top event.

Table 2.1. Failure Rates of a Simple System

Basic events	Probability of failure (q) (unreliability)	Reliability (p) (1-unreliability)
1-Failure of power supply	0.1	0.9
2-A Fails to close	0.1	0.9
3-B Fails to close	0.2	0.8
4-C Fails to close	0.1	0.9

2.3.4. Fault Tree Analysis Program. The fault trees that are constructed in the following chapters are more complex than the one previously shown in Figure 2.4. It would be tedious and prone to error if the calculations were done using calculators. Therefore a program called REC, was written in C programming language using Visual C++ platform to perform these calculations for generic fault trees. The outcome of these calculations is the MTBF. On the other hand using the MTTR values for each basic event, availability and unavailability of system is calculated.

This program is capable of handling 100 gates and 100 basic events. Changing the statements in relevant loops can change these limitations. There can be a maximum number of five events and five states connected to each gate. The number of events and states could also be changed. All states must be designated in ascending order beginning from the top event. Once the events connected to each gate have been defined to the

program, and the data for each event is entered, the program calculates the output.

2.3.5. Conditional Probability. The FTA method is a logical process. First of all, the undesired event is defined and then the fault tree is constructed so that basic events lead to that top event. In the above example, all basic events are independent of each other, which also means, none of the basic events occur in the fault tree more than once. What happens if one or more events occur in the tree more than once?

“When the same event appears several times in the tree, it is called a dependency”, [13]. When the tree contains a dependency, the computational method outlined above cannot be applied. Other steps must be taken. Assume the fault tree has one dependent event called X, and let T be the top event. The well-known Bayes Theorem provides a means of handling dependency.

$$P(T) = P(X) \times P(T / X) + P(\bar{X}) \times P(T / \bar{X}) \quad (13)$$

To compute the conditional probability $P(T / X)$, it is assumed that X has occurred. Hence, by replacing $P(X)$ by the value 1 in each basic event corresponding to the dependency and computing the probability of the top event without change for the other events $P(T / X)$ is found. In the same way, replacing $P(X)$ by 0 allows $P(T / \bar{X})$ to be found. Combining the conditional probabilities with $P(X)$ and $P(\bar{X}) = 1 - P(X)$, the probability of the top event can be found. If the number of dependent events is two, the conditional probability of the top event becomes:

$$\begin{aligned} P(T) = & P(X) \times P(Y) \times P(T / X, Y) + P(X) \times P(\bar{Y}) \times P(T / X, \bar{Y}) \\ & + P(\bar{X}) \times P(Y) \times P(T / \bar{X}, Y) + P(\bar{X}) \times P(\bar{Y}) \times P(T / \bar{X}, \bar{Y}) \end{aligned} \quad (14)$$

As the number of dependent events increases, the number of computations needed also increases in a 2^N mode, where N is the number of dependent events. In later chapters, nine basic events will be encountered, so $2^9 = 512$ computations will be needed! In this case an approximation is needed. When the probability of top event formula is examined, there are a large number of terms that do not contribute to the result significantly. If one

keeps the significant terms in the computation, the result will be a good approximation.

Each term in the summation sign in the above formula has N dependencies. Then only the terms that have maximum of r dependencies equal to 1 are kept. In this way,

$\sum_{i=0}^r C_N^i$ computations are needed instead of 2^N . In this study, r is chosen to be 1, so 10 computations will be performed.

3. SCADA SYSTEMS

In order to perform a reliability analysis of a system, it must be well understood. The Supervisory Control and Data Acquisition (SCADA) system is a combination of telemetry and data acquisition. It consists of collecting information, transferring the information back to a central site, executing necessary analysis and control, and then displaying this information on a number of operator screens. The SCADA system is used to monitor and control a plant or equipment [2].

“Telemetry is usually associated with SCADA systems. It is a technique used in transmitting and receiving information or data over a medium. The information can be measurements, such as voltage, speed or flow. These data are transmitted to another location through a medium such as cable, telephone or radio. Information may come from multiple locations. A way of addressing these different sites is incorporated in the system. Data acquisition refers to the method used to access and control information or data from the equipment being controlled and monitored. The data accessed are then forwarded onto a telemetry system ready for transfer to the different sites. These can be analog and digital information gathered by sensors, such as flowmeter, ammeter, etc. It can also be data to control equipment such as actuators, relays, valves, motors, etc.” [2].

According to ARC Advisory Group (1999) [15], a system is classified as a supervisory control and data acquisition (SCADA) system when

“...the system must monitor and control field devices using remote terminal units (RTUs) at geographically remote sites. The SCADA system typically includes the master stations, application software, remote terminal units and all associated communications equipment to interface the devices. The system must also include the controllers and I/O for the master stations and RTUs and also the system HMI and application software programs. It does not include field devices such as flow, temperature or pressure transmitters that may be wired to the RTU.”

In some respects, Distributed Control Systems (DCS) are similar to the SCADA systems. However, the SCADA system covers larger geographical areas compared to DCS [2]. Human Machine Interfaces (HMI) evolved in the early '80s as windows into the process mainly to replace hardwired control panels full of switches, lights, indicators, and annunciators. Since then, they have been used in all industries wherever process control

is present [14]. The PLCs and the computers used for the Human-Machine Interface are connected via a communication network. The HMI/SCADA software uses the communication network to send commands to the PLCs and to receive information from the PLCs [15]. Typical SCADA system components used in offshore oil and gas industry are shown in Figure 3.1, excerpted from [15]. The major components of a SCADA system are: remote stations, communications network, and SCADA workstations.

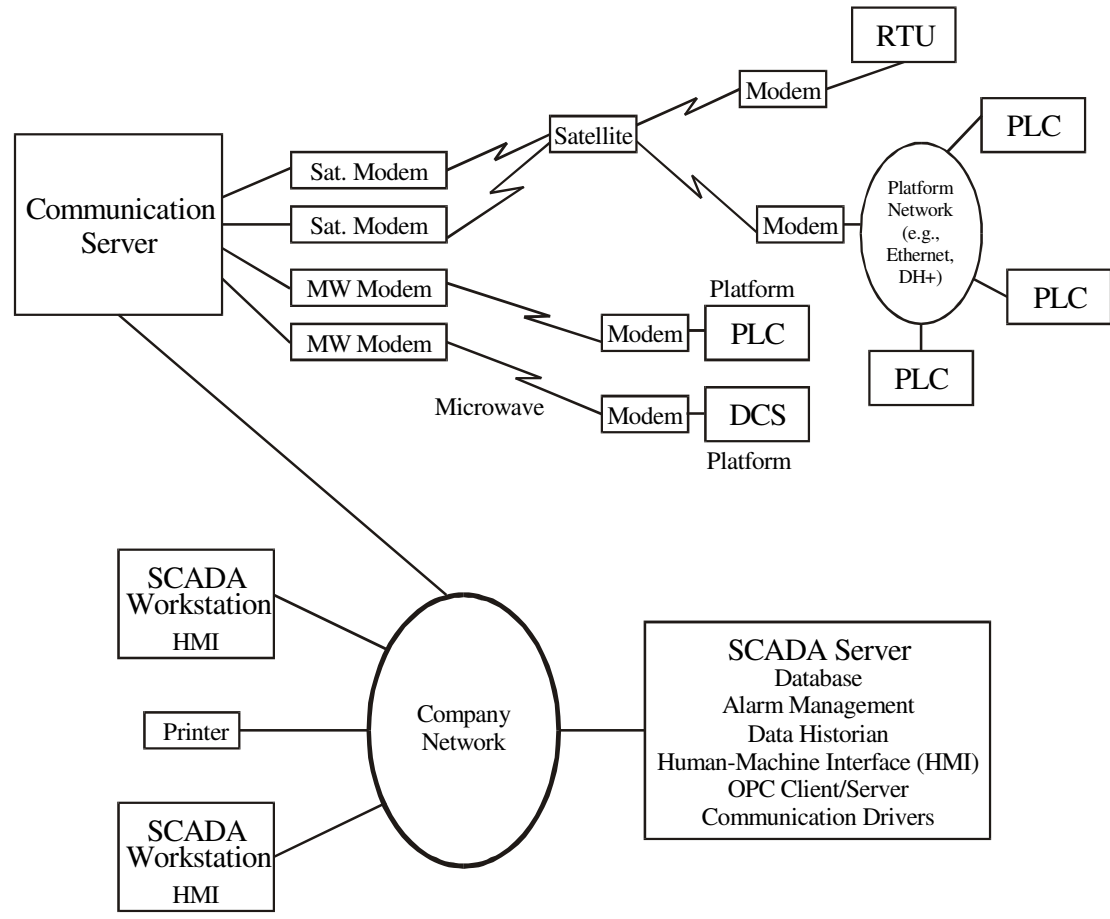


Figure 3.1. Typical SCADA Components

The Remote Station is installed at the remote plant or equipment being monitored and controlled by the central host computer. The Remote Station can be a Remote

Terminal Unit (RTU) or a Programmable Logic Controller (PLC). The Communications Network is the medium for transferring information from one location to another. The SCADA workstation refers to the location of the master or host computer.

One of the major architectures of SCADA systems that are employed on offshore platforms is called distributed PLC. This architecture is typically used in larger conventional platforms, which is shown in Figure 3.2, which has been excerpted from [15].

In a distributed PLC architecture, each major unit of the platform is controlled by a separate PLC. There is a platform communication network that connects the PLCs and the computers used for the HMI. The communication network is primarily used by the HMI/SCADA software to send commands to the PLCs and to receive information from the PLCs. The platform communication network is redundant. If the primary network fails to operate, communication is switched to the secondary network.

There is generally limited information passing between the PLCs. Each major unit normally has a local operator panel to allow personnel to interact with that unit only. In this type of architecture, the safety system is generally handled by one of the PLCs. The platform is monitored from an onshore office by a microwave/radio/satellite link. The onshore office may perform some limited control functions, especially when the platform is evacuated due to bad weather [15].

Each PLC generally works autonomously from the other PLCs and will continue to control even if onshore communication to the PLC is temporarily lost. However, if communication is lost for some significant time, the PLC will shut down the unit [15].

The other architecture is centralized PLC platform. This architecture is more representative of smaller platforms and unmanned platforms. One PLC controls the platform equipment. In this case, the input/output (I/O) modules connected directly to the equipment communicate with the platform PLC over a specialized network, generally called a remote I/O network. Some larger units, e.g., a turbine generator may have a separate PLC, as in the distributed platform architecture. In this architecture, the safety system is generally only monitored by the PLC [15]. The reliability analysis of this type of architecture was not examined in this thesis.

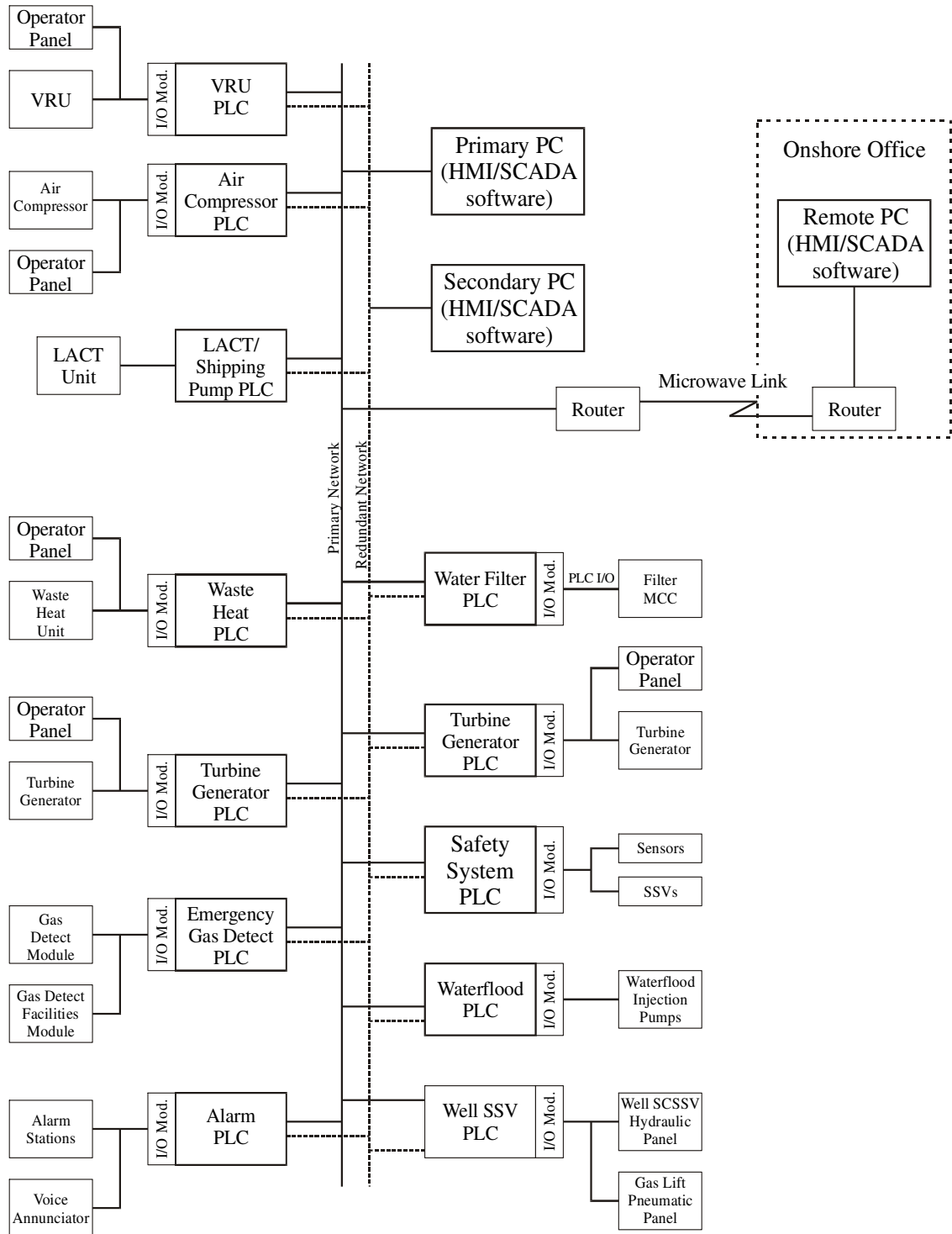
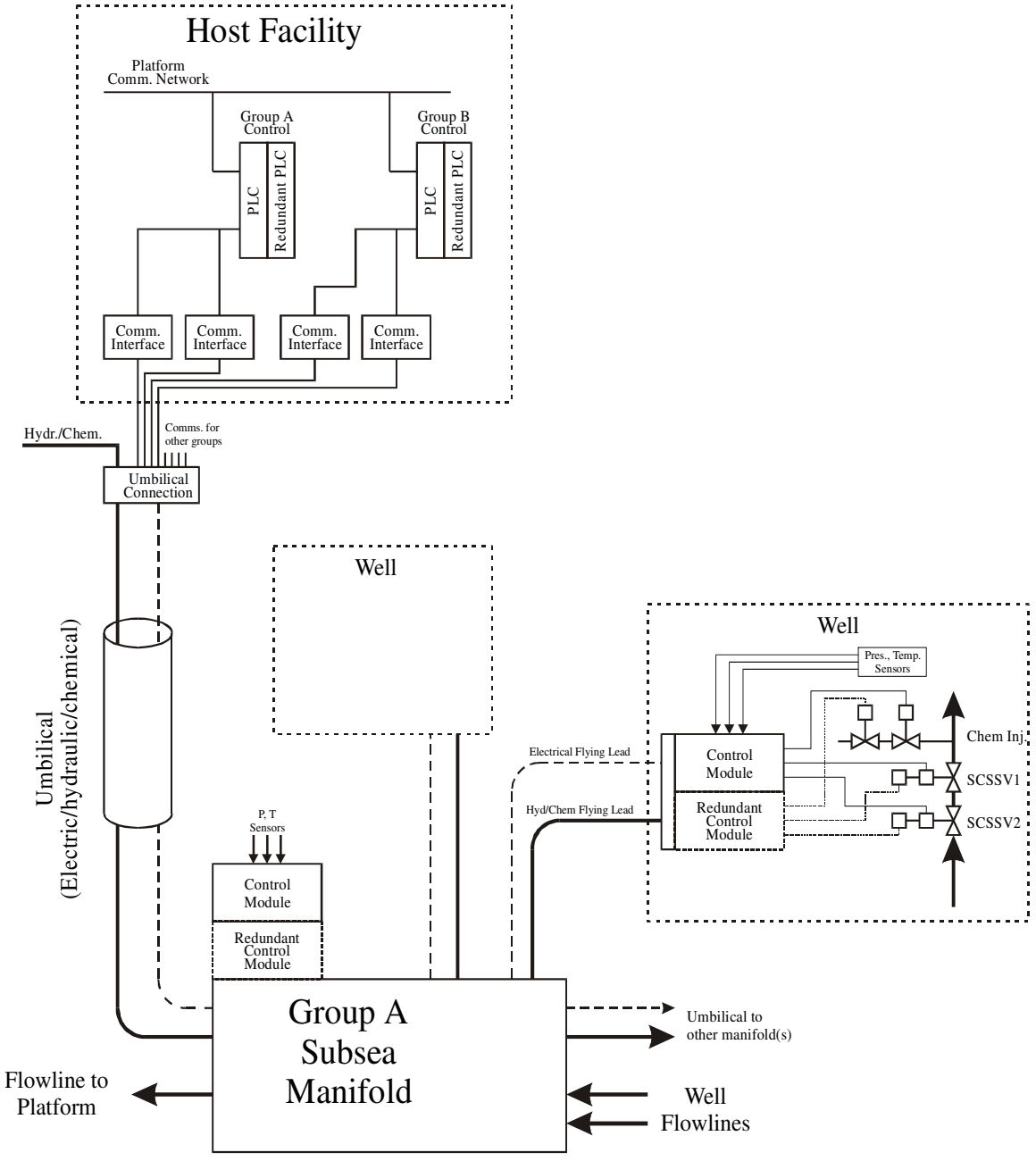


Figure 3.2. Distributed PLC Architecture

Subsea technology has evolved rapidly since the 1980s. The term *subsea systems* refers to clusters of subsea wells, or the combination of subsea wells tied to another host facility. Figure 3.3 depicts a typical arrangement between subsea wells producing to a host facility.



3.3. Typical Subsea SCADA Architecture

The main control for a group of wells sharing a subsea manifold is generally connected to the host facility communication network. The control is handled by a redundant PLC on the host facility, which is connected to a redundant serial communication network to the subsea facilities. An electrical umbilical provides the communication to subsea facilities. Flying leads connect each subsea well to the manifold [15].

A multiplex electrohydraulic control system is used to perform the functions specified. No RTUs or PLCs are located subsea. The multiplex electrohydraulic controls are piloted hydraulic controls with the pilot function replaced by an electrical signal. Individual tree and manifold control is provided by subsea control pods. These modules contain the valving and associated electronic/electric circuits required for routing the hydraulic fluid to the various valve and choke actuators. All monitoring of subsea system status is accomplished in the subsea modules. Individual well control pods also monitor pressure and temperature data, control subsurface safety valves, chemical injection valves and annulus valves. Most subsea systems include redundant control modules [15].

In this section SCADA systems used in offshore oil and gas industry for production monitoring and control, well monitoring and control, process monitoring and control were introduced.

4. RELIABILITY ANALYSIS OF THE SCADA SYSTEMS

To start the reliability analysis of the SCADA systems, the fault tree of the system must be developed. Since the system involves different subsystems (surface, subsea etc.), the approach used in this study is to first develop a fault tree diagram for each subsystem individually, and later to combine all subsystems to find the overall reliability indices.

The system failures were categorized as: offshore facility failure, subsea failure, SCADA failure, human error, and software failure.

4.1. DEVELOPMENT OF THE FAULT TREE FOR OFFSHORE FACILITY

The development of the surface system fault tree was built on the Safety Flow Chart API-14C, 1998, [12] - Offshore Production Facility that appears in Figure 4.1. Abbreviations and symbols used in Figure 4.1 are explained in Appendix B. Figure 4.1 depicts how undesirable events could cause personnel injury and/or facility damage. Figure 4.1 shows where safety devices should be used to prevent the propagation of undesirable events. The release of hydrocarbons is the main factor to lead all top events including facility damage, personal injury, and pollution. The overall objectives of the safety system could be summarized as follows:

- Prevent undesirable events that could lead to hydrocarbon leak.
- Shut the process partially or overall to prevent leak of hydrocarbons and fire.
- Accumulate and recover the released hydrocarbons and gases that escape from the process.

Based on the safety flow chart as shown in Figure 4.1, the fault tree (starting from Figure 4.2 through Figure 4.8) for the surface production facility was constructed.

Elements that are connected in series in Figure 4.1 are connected with an AND gate in the fault tree diagram, and the elements connected parallel in Figure 4.1 are connected with an OR gate in the fault tree diagram. Safety Analysis Tables (SAT) of components were used to find a relationship between undesirable events and causes of the component failures [12]. The upper level of the fault tree diagram is given in Figure 4.2. Fault trees for the undesirable events that lead to the top event were given in Figure 4.3 through Figure 4.8.

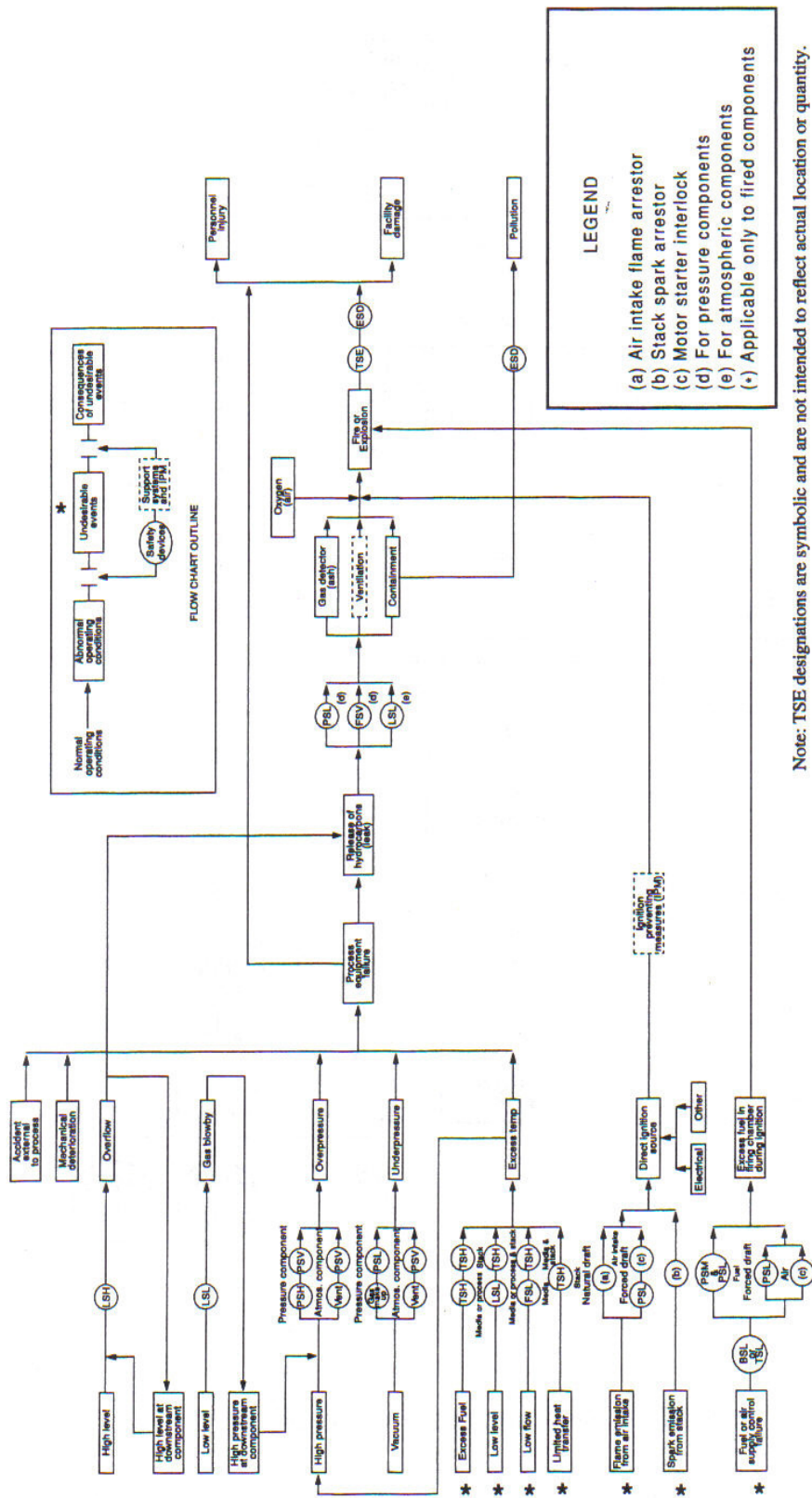


Figure 4.1. Safety Flow Chart of Offshore Production Facility

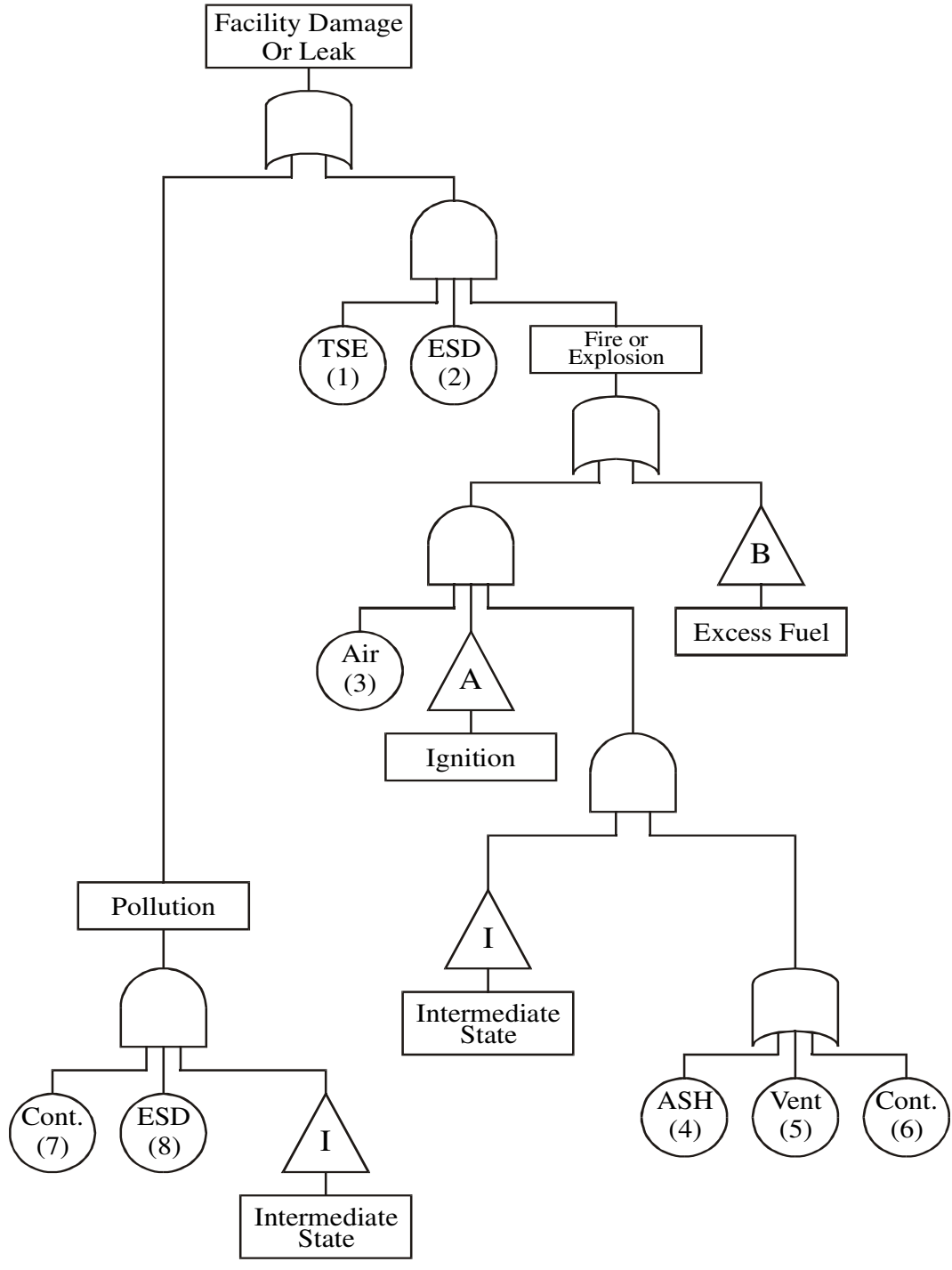


Figure 4.2. Upper Level Fault Tree Diagram

The fault tree diagram in Figure 4.2 was constructed based on the most right part of the safety chart in Figure 4.1. The top event was personnel injury and/or facility damage. The top event for the surface facility is the consequence of a release of hydrocarbons and a failure of the safety devices that may cause fire or explosion. The Intermediate State that is shown in Figure 4.2 is the state of the safety chart after the release of hydrocarbons and three safety devices (PSL, FSV, LSL) that are shown in the middle of Figure 4.1. The pollution is not a cause for the top event, but it appears like an intermediate state that causes the top event. The triangle states that appear in Figure 4.2 are as follows:

I- Intermediate State (Shown in Figure 4.3.)

A-Ignition (Shown in Figure 4.7.)

B-Excess Fuel (Shown in Figure 4.8.)

Safety elements in Figure 4.2 include Temperature Safety Elements (TSE) that were modeled by temperature sensors, and an emergency shutdown system (ESD) that was modeled by valves. Oxygen (air) is assumed to always be in the media. Containment (a system to collect and direct escaped liquid hydrocarbons to a safe location) [12], and gas detector, shown as ASH in the fault tree diagram, are the other safety components. Vent was modeled by a pressure and/or vacuum relief valve.

The fault tree for the intermediate state I is shown in Figure 4.4. This intermediate state occurs because of a release of hydrocarbons and the failure of safety devices: low pressure sensor (PSL), flow safety valve (FSV), low level sensor (LSL). A Release of hydrocarbons is due to an overflow or to process equipment failure. From the SAT, it is found that an overflow happens due to the failure of the level control unit of pressure vessels and failure of the high level sensor. Process equipment failure is due to five factors:

1. Accident
2. O-Overpressure (Shown in Figure 4.4.)
3. Mechanical deterioration of hardware components
4. D-Under pressure (Shown in Figure 4.5.)
5. C-Excess Temperature at Component (Shown in Figure 4.6.)

The capital letters O, D, C in factors two, four, five denotes the name of the triangle states respectively.

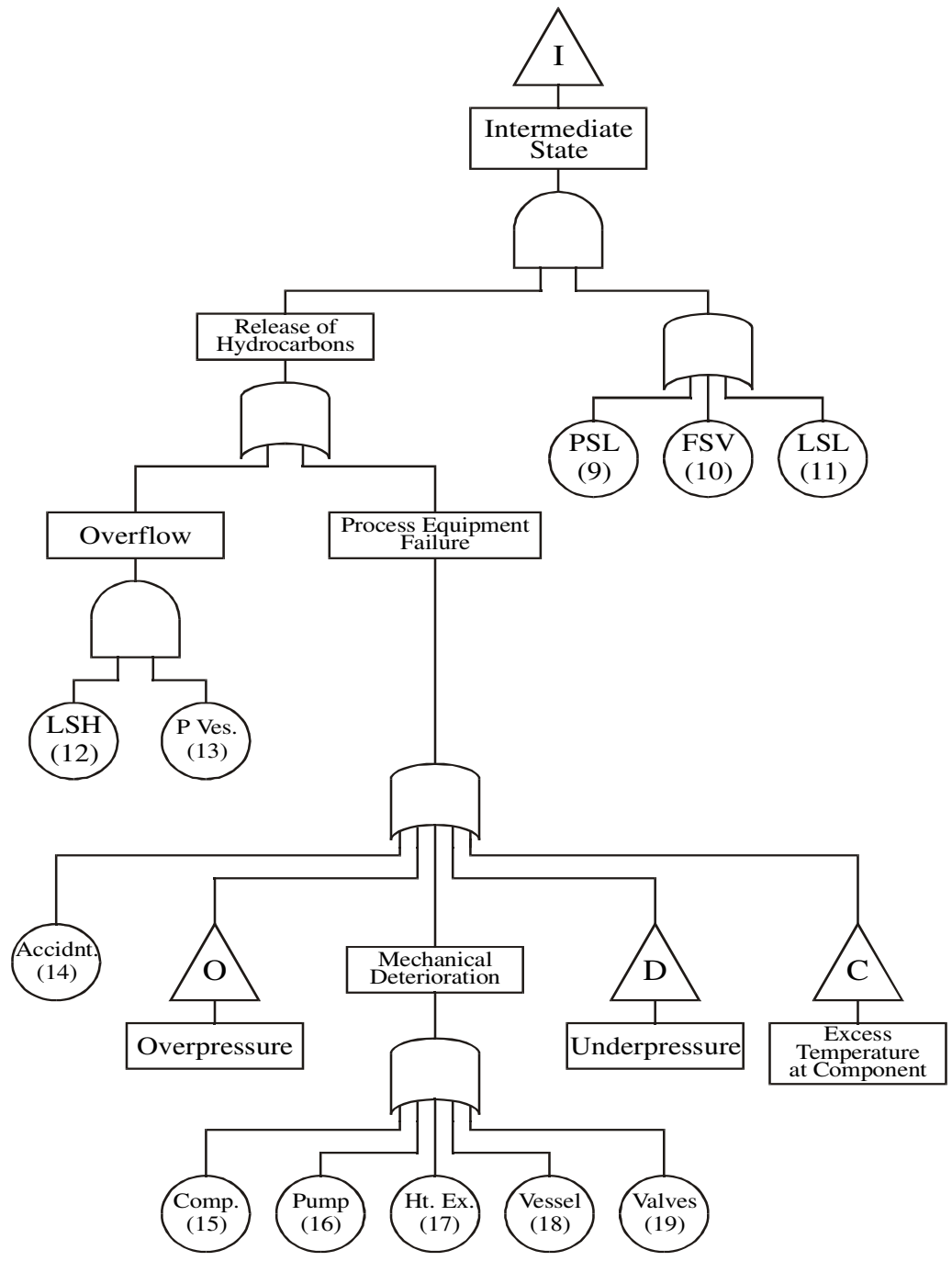


Figure 4.3. Fault Tree Diagram of Intermediate State I

In the refining process, compressors, pumps, heat exchangers, vessels, and valves are the basic mechanical components. So, mechanical deterioration is modeled by the mechanical failures of these components. The accident frequency is estimated from historical data.

Overpressure in a pressure component occurs due to outflow pressure that exceeds inflow pressure. By looking at the safety analysis tables of each component, flow lines, pressure vessels, atmospheric vessels, pumps, compressors, and heat exchangers are found to be basic components for overpressure. The fault tree diagram for the undesirable event, overpressure, is shown in Figure 4.4.

In looking at the safety flow chart as in Figure 4.1, it was assumed that overpressure would occur if high pressure or gas blowby exists and the related safety devices fail. For the pressure component, which was assumed to be a pressure vessel, safety devices used were the high pressure sensor (PSH), and the pressure safety valve (PSV). The vent and the PSV are the safety devices for the atmospheric component.

Gas blowby is the discharge of gas from a process component through a liquid outlet [12]. Undesirable event gas blowby occurs in pressure vessels and atmospheric vessels. It was modeled by the failure of the level control unit of pressure and atmospheric vessels. A low level sensor (LSL) is the safety device used to prevent gas blowby. Failure of the LSL combined with the failure of level control unit of vessels results in gas blowby in the process. The intermediate state for gas blowby is shown as a triangle named as G. The gas blowby triangle state appears twice in the fault tree (Figure 4.4.), but shown only once in detail for simplicity.

The basic events numbered below in the fault tree diagram of overpressure in Figure 4.4 do not appear in the safety flow chart.

- 23- Pump failure that results overpressure.
- 24- Flow line failure that results in overpressure.
- 25- Compressor failure that results in overpressure.
- 26- Heat exchanger failure that results overpressure.

These basic events were added even though they do not appear in the safety chart, because these basic events are included in the safety analysis tables of components that may lead to overpressure.

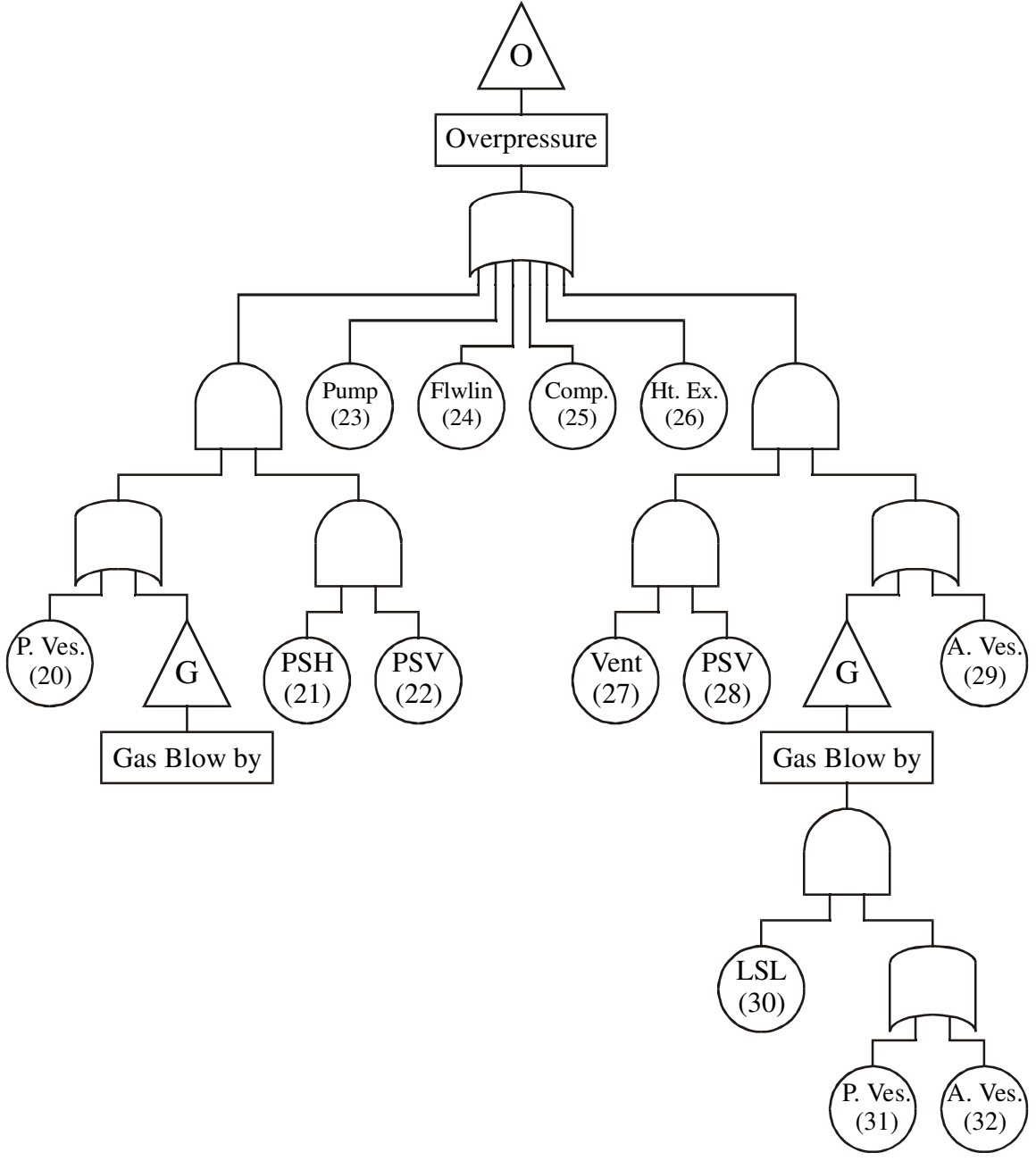


Figure 4.4. Fault Tree Diagram of Overpressure

The failure of the pump, compressor and the heat exchanger was modeled by the failure of the control unit of these components. An outlet valve that fails to open models the failure of the flow line.

The fault tree for the undesirable event underpressure, which is denoted by a triangle named by D, is shown in Figure 4.5. Under pressure can occur in one of the pressure or atmospheric vessels.

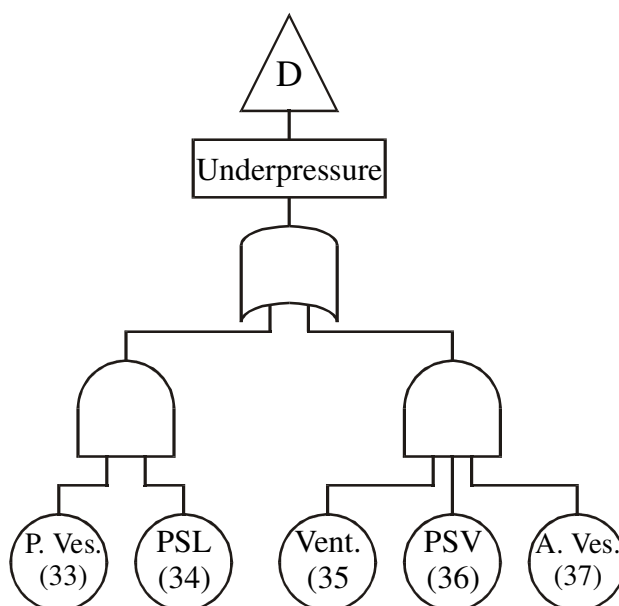


Figure 4.5. Fault Tree Diagram of Underpressure

Underpressure occurs in two ways. It might occur with the combined failure of the safety device for pressure vessels that is the low pressure sensor, and control unit failure of pressure vessels. The other way is a failure of the pressure safety valve and vent with the failure of atmospheric vessels. A vent failure is modeled by the failure of a pressure and/or vacuum relief valve (3 inch ball), peripheral to atmospheric vessel. The related valve is found from the P&ID diagrams of the process that is supplied by an operator.

The fault tree for the triangle intermediate state C, excess temperature at fired and exhaust heated components is shown in Figure 4.6. In looking at the safety flow chart, low flow, low liquid level in a fired component, insufficient flow of heat transfer fluid, or extraneous fuel entering the firing chamber can be counted as causes of the excess

temperature. The main heated component in the process is the reboiler. The low flow sensor (FSL), high temperature sensor (TSH), and low level sensor (LSL) are the main safety devices for prevention from excess temperature.

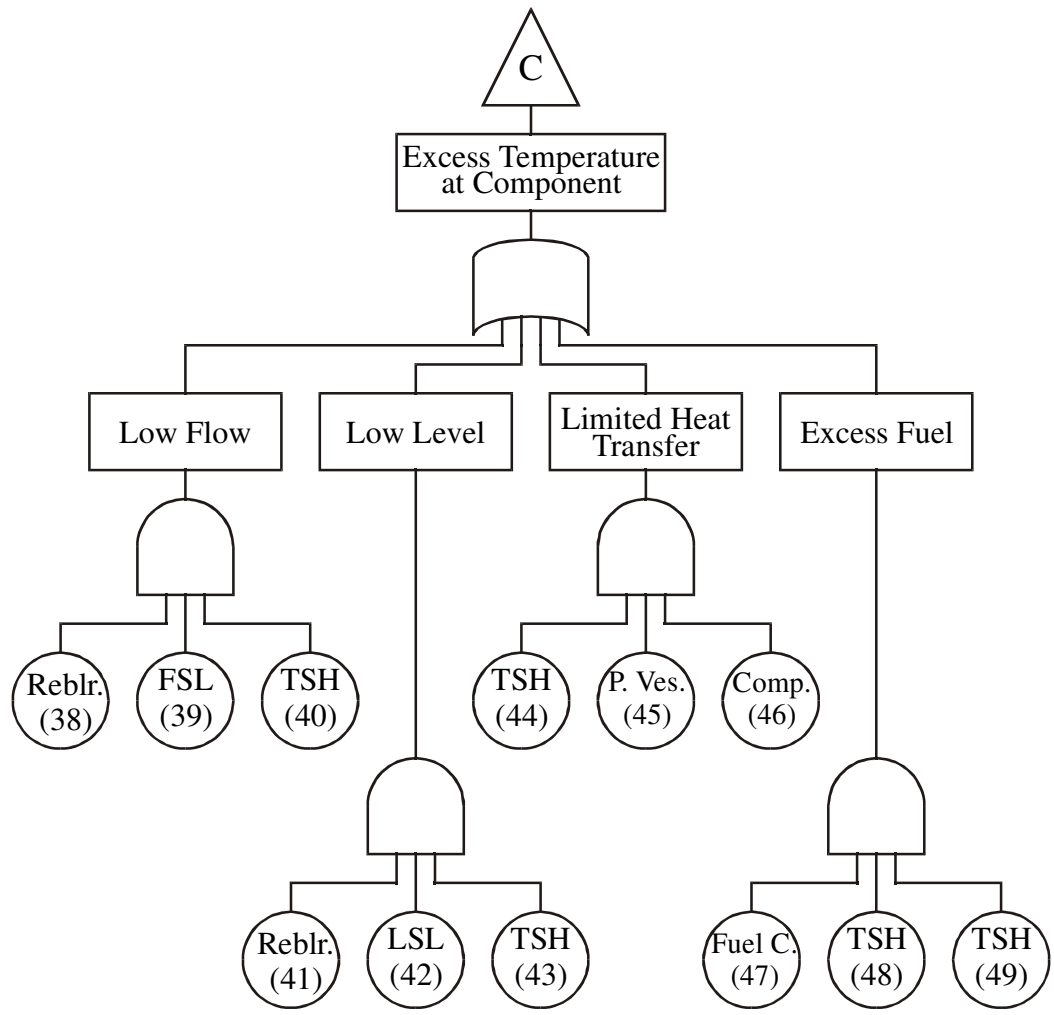


Figure 4.6. Fault Tree Diagram of Excess Temperature

Low flow occurs if the flow control unit of the reboiler fails, and the related safety devices (FSL, TSH) fail to operate. Similarly, a low level occurs if the level control unit of the reboiler and the related safety devices (LSL, TSH) fail. Limited heat transfer occurs if the reboiler, compressor that supplies heat transfer, and the safety device (TSH)

fail. Excess fuel arises if the fuel control element fails. A fuel control element was modeled as a valve. The corresponding safety elements (TSH) must also fail. There are two TSH devices one of which is primary, and the other is a secondary safety device.

The ignition, which is also denoted by a triangle designated by A, occurs in the process if the Ignition Preventing Measures (IPM) fail to operate, and if there is an ignition source in the process. The IPM was modeled via a fire and gas detector. The fault tree diagram for ignition is given in Figure 4.7.

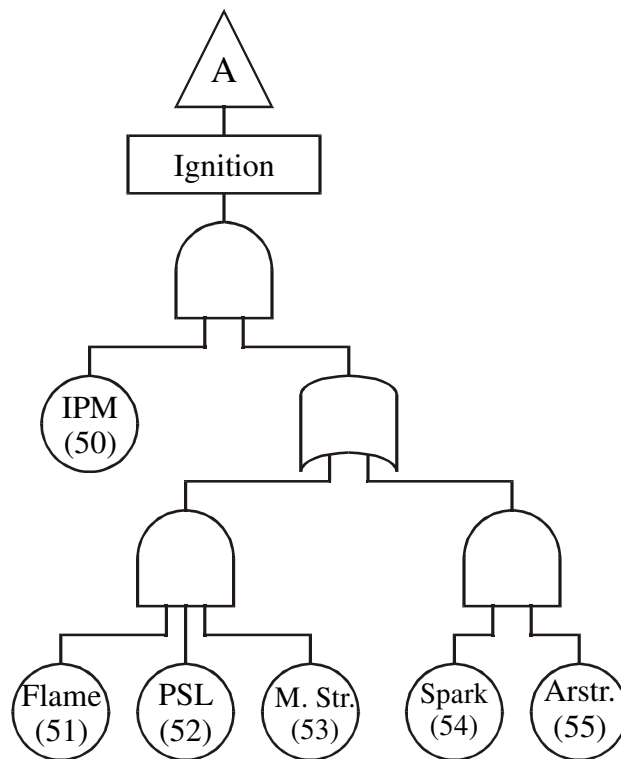


Figure 4.7. Fault Tree Diagram of Ignition

An ignition source could be in the media in two ways: if the flame emission from the air intake arises with the failure of the low pressure sensor (PSL), and motor starter interlock failure, or spark emission from the stack arises with stack spark arrestor failure.

Flame emission from air intake was modeled by a failure of a pump that causes improper fuel usage.

The fault tree diagram for excess fuel in the firing chamber is shown in Figure 4.8. The triangle designated B represents the excess fuel intermediate state. Excess fuel may occur if the fuel is extraneous in the firing chamber and if the safety device, burner safety low (BSL), fails.

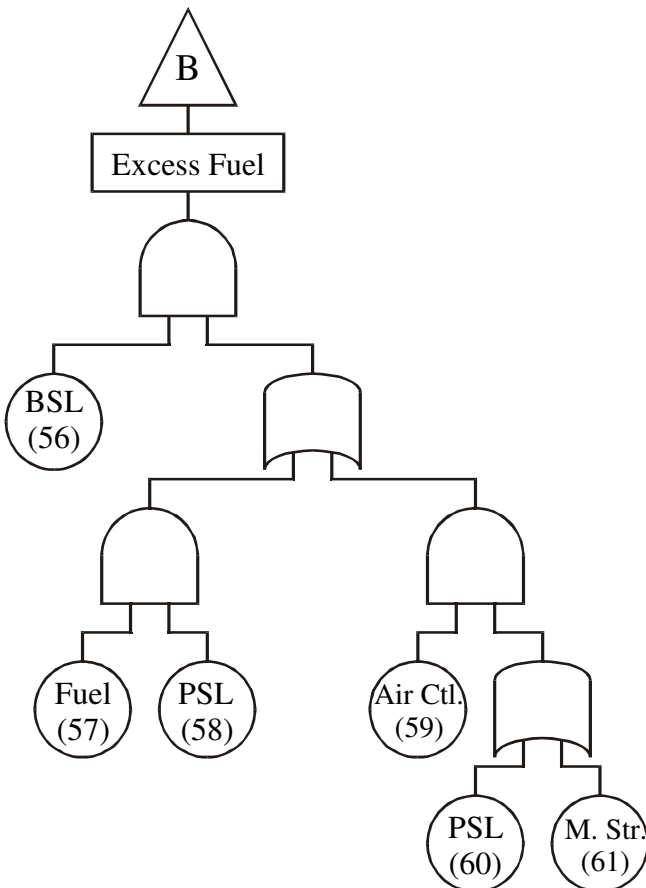


Figure 4.8. Fault Tree Diagram of Excess Fuel

Excess fuel in the firing chamber could occur for two reasons. One of these reasons could be the failure of the fuel supply control (which is modeled by the failure of

the pump control unit), and failure of the low pressure sensor. The other cause is an air supply control failure with the failure of the motor starter interlock and the low pressure sensor (PSL). Air supply control failure is modeled by pump failure.

The fault tree diagrams from Figure 4.2 to 4.8 show the causes for personnel injury and/or facility damage due to sensors, control unit failures of various hardware components (vessels, pumps, compressors etc.). These fault trees are constructed based on the safety flow chart of Figure 4.1. Implementation of a fault tree is a logical process.

4.1.1. Failure Probability for Hardware Components. The data to find the reliability indices were gathered from OREDA, 1997 [9]. Whenever it was unavailable, unknown data (accident frequency, frequency of failure of containment, frequency of spark arrestor) were estimated from historical events. The failure rates, repair times, and calculated availabilities for the surface system are shown in Table 4.1.

The first column in Table 4.1 contains the event numbers (in the circles) that appear in the fault trees. The system component and media (air, accident) that fails, occurs in the second column. The third column has the failure rate, in failures per year. Most of this column is derived from the tables in OREDA, 1997, [9], which have the failure rates in failures per million hours. Simply, the data in failures per million hours is multiplied by a factor of 8760×10^{-6} to find failures per year.

The temperature safety element (TSE), which was modeled as a process temperature sensor, has a failure rate of 7.73 failures per million hours. This number was multiplied by 8760×10^{-6} and the corresponding number in failures per year, as in Table 4.1, was found. The mean time to repair this sensor is 0.2 hours. Dividing this repair time by 8760 and then taking the reciprocal yields the number in Table 4.1 in units of repairs per year.

The emergency shutdown (ESD), which was modeled by ESD type of valves, has a failure rate of 10.51 failures per million hours. This number was multiplied by 8760×10^{-6} and the number in failures per year as in Table 4.1 was found for ESD. The mean time to repair this valve is 33.4 hours. Dividing this repair time by 8760 and then taking the reciprocal yields the number in Table 4.1 in units of repairs per year for the ESD component.

The fourth element in Table 4.1, the gas detector, has a failure rate of 4.81 per million hours, and a repair time of 5.8 hours. The multiplications yield the numbers for the gas detector.

“A vent is a pipe or fitting on a vessel that opens to atmosphere. A vent line might contain a pressure and/or vacuum relief valve” [12]. The vent is modeled by a 3-inch ball valve by looking to P&ID diagrams. The failure rate for that kind of valve is 20.77 failures per million hours, and the average repair time is 12 hours. Multiplication by factors and taking the reciprocals, yield the numbers as in Table 4.1 for the vent.

The containment system failure is 4×10^{-4} failures per year, the same as accident fatality rate [11]. The average repair time was estimated at one week.

The failure rate for low pressure sensor is 1.27 failures per year. From an examination of Example Safety Analysis Flow Diagram of Platform Production Process from API-14C, 1998, [12], it is assumed there are 18 PSL devices. It was assumed that an increase in the number of devices increases the failure rate proportionally, so $1.27 \times 18 = 22.9$ failures per million hours was found. Even though the number of devices is increased, repair times were assumed to be the same.

The average repair time for a PSL is 11.6 hours. The multiplications yield the numbers for the PSL element in Table 4.1. Similarly, it is assumed there are 15 Safety Flow Valves (FSV). The failure rate for a FSV device is 21.5 failures per million hours. Average repair time for a FSV device is 15.1 hours. These valves are assumed to be process control valves. In the process, the number of low level sensors, and high level sensors was assumed to be 19, and the failure rate for level sensors was found as 6.09 failures per million hours, and the average repair time as 7.9 hours. The above calculations yield numbers for level sensors as in Table 4.1.

For pressure vessels: the failure rate for a generic vessel is 17.46 failures per million hours. Failures at a rate of 5.9 % are due to control unit failure of a vessel, so $17.46 \times 5.9 \% = 1.03$ failures per million hours. It is assumed there are seven vessels in the process, so $7 \times 1.03 = 7.21$ failures per million hours because of control unit failure of vessels was found. The failure rate of a separator due to control unit failure is 1 failure per million hours. Three separators were assumed, so there are $3 \times 1 = 3$ failures per million

hours due to the control unit failure of separators. Control unit failure of a scrubber is 1.79 failures per million hours. Seven scrubbers were assumed, so there are $7 \times 1.79 = 12.53$ failures per million hours because of the control unit failure. One contactor was assumed in the refining process. The control unit failure of a contactor is 0.37×10^{-6} . The total failure rate of vessels is (generic vessels, separators, scrubbers, contactor) $7.21 + 3 + 12.53 + 0.37 = 23.11$ failures per million hours. If the result is multiplied by a factor of 8760×10^{-6} , ($23.11 \times 8760 \times 10^{-6} = 0.2$) the result for pressure vessel failures in the table was found. The mean time to repair a generic vessel is 10.4 hours, 10.7 hours for a separator, 6 hours for a scrubber, and 6 hours for a contactor. The average time to repair a pressure vessel was found as follows:

$$\text{average repair time} = \frac{10.4 \times 7 + 10.7 \times 3 + 6 \times 7 + 6 \times 1}{7 + 3 + 7 + 1} = 8.49 \text{ hours}$$

To find the number of repairs per year for pressure vessels, the reciprocal of the average repair time is multiplied by a factor of 8760 ($8760/8.49 = 1031.8$), and the number corresponding to average repairs per year in Table 4.1 is found.

The rate of accidents (collision of a ship to the platform, lightning, etc.) that result in a fatality is 0.0004 per year. The average time to repair of the platforms due to accidents was assumed to be six months.

The events 15, 16, 17, 18, 19 are mechanical deterioration of compressors, pumps, heat exchangers, vessels, and valves, respectively. For simplicity, the failure rates are generalized, the failure rates for different kinds of compressors, vessels, valves were not examined. The generic failure rate for compressors was found to be 539.25 failures per million hours, and 12.38% of these failures are due to material deterioration, and there assumed to be eight compressors in the system, so there are $539.25 \times 12.38\% \times 8 = 534.08$ failures per million hours are due to material deterioration of compressors. The average repair time for a compressor is 56.2 hours.

The generic failure rate for pumps is 106.03 failures per million hours. 15.49% of these failures are due to material deterioration. There are assumed to be 18 pumps in the system, so similar calculations for compressors yield 295.56 failures per million hours for

pumps due to material deterioration. The average time to repair a pump is 40.5 hours. The multiplication by factors, and taking the reciprocals yields the number for pumps as in Table 4.1.

The generic failure rate for heat exchangers was found to be 6.03 failures per million hours. 2.09% of these failures are due to material deterioration, and there are assumed to be three heat exchangers in the system.

The failure rate for heat exchangers due to material deterioration was found to be 0.39 failures per million hours. The average repair time for heat exchangers was found to be 78.3 hours. Similar conversions from failures per million hours to failures per year give the numbers for heat exchangers due to mechanical deterioration as in Table 4.1.

The generic failure rate for vessels is 17.46 hours. 16.01% of these failures are due to mechanical deterioration. There are assumed to be 19 vessels in the system, so 53.2 failures per million hours were found for vessels due to mechanical deterioration. The average repair time for a vessel is 10.4 hours.

The generic failure rate for a valve was found to be 12.39 failures per million hours. 43.53% of these failures are due to material deterioration. There are assumed to be 60 valves in the system. The availability of valves for a year is $12.39 \times 43.53\% \times 60 \times 8760 \div 10^6 = 2.83$. The average repair time to repair a valve is 25.4 hours, so the average repair rate for valves is $8760/25.4 = 344.88$.

The generic failure rate for a valve is 12.39 failures per million hours. There are assumed to be 18 pressure safety valves in the system, so there are $12.39 \times 18 \times 8760 \times 10^{-6} = 1.95$ failures per year for PSV devices. The average repair time for a pressure safety valve is 25.4 hours, so the average repair rate is $8760/25.4 = 344.9$ repairs per year.

The 23rd event, failure of the control unit of pump, is calculated as: There are assumed to be 15 generic pumps (three booster pumps, six pipeline pumps, two 1st stage suction pumps, two glycol pumps, two bad oil tank pumps). The failure rate for a generic pump failure is 106.03 and 8.91% of these failures are due to control unit failure. The generic average repair time for a pump is 40.5 hours. There are two centrifugal pump in the Lease Automation Custody Transfer (LACT) unit, and there is one diaphragm pump peripheral to bad oil tanks. The failure rate for a centrifugal pump is 97.42 failures per million hours. 9.64% of these failures are due to control unit failure. The average repair

time for a centrifugal pump is 42.7 hours. The failure rate for a diaphragm pump is 67.27, and 1.14% of these failures are due to control unit failure. The average repair time for diaphragm pump is 31.4 hours. The overall failure rate for pumps in failures per year is calculated as:

$(106.3 \times 8.91\% \times 15 + 97.42 \times 9.64\% \times 2 + 67.27 \times 1.14\% \times 1) \times 8760 \times 10^{-6} = 1.41$ failures per year.

The overall average repairs per year is calculated as:

$(15 \times 40.5 + 42.7 \times 2 + 67.27 \times 1) / 18 = 40.24$ hours per repair, $8760 / 40.24 = 217.7$ repairs per year.

The 24th event, failure of the flowline was modeled by a valve that fails to open any flowline. The failure rate for that valve is found to be 0.51 failures per million hours, and the average repair time is 14.3 hours. Multiplying by factors yields the numbers for the flowline as in Table 4.1.

The 25th event, failure of compressors that results in overpressure was modeled by failure of control unit that causes overspeed. There are two centrifugal compressors (4th stage compressors), and there are six reciprocating compressors (2×1st stage, 2×2nd stage, 2×3rd stage). The failure rate for a centrifugal compressor is 393.07 failures per million hours and 9.32% of these failures are due to control unit failure. The failure rate for a reciprocating compressor is 1440.54 failures per million hours and 12.33% of these failures are due to control unit failure. The overall compressor failure rate due to control unit failure is:

$(393.07 \times 9.32\% \times 2 + 1440.54 \times 12.33\% \times 6) \times 8760 \times 10^{-6} = 9.98$ failures per year.

A centrifugal compressor has an average repair time of 47.2 hours, and a reciprocating compressor has an average repair time of 70.7 hours. The required average repairs is found as: $8760 / ((47.2 \times 2 + 70.7 \times 6) / 8) = 135.08$ repairs per year.

For the 26th event, there are two kinds of heat exchangers, gas→glycol/shell and tube, which have 10.24 failures per million hours, and 7.89% of these failures were assumed to be related to overpressure. There is assumed to be one crude oil heater (generic shell and tube), which has 5.93 failures per million hours, and 7.89% of these failures are due to internal leakage that might cause pressure change. The average repair times are 151.5 and 97.4 hours respectively. The failure rate in failures per million hours

is calculated as: $(10.24 \times 7.89\% \times 2 + 5.93 \times 7.89\% \times 1) = 2.09$ failures per million hours. The average repair time for heat exchangers was calculated as: $(151.5 \times 2 + 97.4) / 3 = 133.47$ hours per repair. Conversions from failures per million hours to failures per year, and from hours per year to repairs per year, yields the numbers for the 26th event.

The 29th event, a failure of the control unit of an atmospheric vessel, was found from generic vessel failure rate (17.46 failures per million hours). The 5.9% of these failures are because of control unit failure, and there is assumed to be one atmospheric vessel. The failure rate in terms of failures per year is calculated as:

$$17.46 \times 5.9\% \times 8760 \times 10^{-6} = 0.009.$$

The average repair time is 10.4 hours, so $8760/10.4 = 842.3$ repairs per year is the failure rate.

For the 38th event, control unit failure of the reboiler, there is assumed to be one reboiler, and the numbers are the same as a generic fault rate for a vessel. The 39th event, failure of a flow sensor has a fault rate of 2.76 failures per year and 0.6 hours are required to repair these low flow sensors (FSL). By multiplying 2.76 with 8760×10^{-6} , it is found that FSL devices have a failure rate of 0.024 failures per year. By dividing 8760 into 0.6, it is found that the repair time is 14600 repairs per year.

The 40th event, the failure of a high temperature sensor has a fault rate of 7.73 failures per year, which means $7.73 \times 8760 \times 10^{-6} = 0.068$ failures per year. The average repair time for a high temperature sensor (TSH) is, 0.2 hours, which is $8760/0.2 = 43800$ repairs per year.

The failure rate for a low level sensor (LSL) is 6.09 failures per million hours, which means $6.09 \times 8760 \times 10^{-6} = 0.053$ failures per year. The average time to repair a low level sensor is 7.9 hours, which is 1108.9 repairs per year. The LSL and TSH were assumed to be single devices, peripheral to the heated component (reboiler), so the numbers found were not multiplied by the total number of these devices.

The 46th event is the failure of compressors because of an insufficient flow that causes limited heat transfer in the process. The failure rate for a centrifugal compressor due to insufficient flow is 46.56 failures per million hours, and there are two centrifugal compressors. The failure rate for a reciprocating pump is 100.89, there are six reciprocating compressors in the process, so the overall failure rate becomes

$(46.56 \times 2 + 100.89 \times 6) \times 8760 \times 10^{-6} = 6.1$ failures per year. The average repair time for a centrifugal compressor is 59.9 hours and 32.1 hours for a reciprocating compressor. The average repair time is found to be 39.5 hours, and the average repair rate 221.8 repairs per year.

The 47th event, fuel control failure was modeled by the failure of a generic ball type of valve that controls the fuel injection to the heated component. The failure rate for a ball type of valve is 8.07 failures per million hours, and the average repair time is 10.3 hours. The calculations yield $(8.07 \times 8760 \times 10^{-6} = 0.07$ and $8760/10.3 = 850.5$) the numbers for fuel control as shown in Table 4.1.

The failure of Ignition Preventing Measures (IPM) was modeled as failure of a fire & gas detector. The generic failure rate for a fire & gas detector is 4.81 failures per million hours, and the average repair time is 5.8 hours. Multiplying 4.81 with 8760×10^{-6} yields 0.042 failures per year, and multiplication of the reciprocal of 5.8 with 8760 gives the result $(8760/5.8 = 1510.34)$ for IPM as repairs per year.

Flame emission is modeled by the control unit failure of a pump that fails. The generic failure rate for a pump is 106.03 failures per million hours, and 8.91% of these failures are due to a control unit failure, which yields $106.03 \times 8.91 = 9.45$ failures due to a control unit failure of that pump. The conversion from failures per million hours to failures per year yields 0.083 as in Table 4.1. The average repair time for a pump is 40.5 hours; so the average repair rate is 216.3 repairs per year.

The low pressure sensor failure (52nd event) was modeled just for a reboiler, where the previous PSL numbers are for the whole system. The failure rate for a pressure sensor is 1.27 failures per million hours, and the average repair time is 11.6 hours. Multiplying by coefficients yield the fault rates in units of failures per year, and repairs per year.

The failure rate for the 53rd event, failure of the motor starter interlock was found to be 15 failures per million hours [11]. It was assumed that the average repair time is 40.5 hours [9]. The 54th event, spark emission from stack, was assumed to happen with a probability of 10^{-3} per hour, and it was assumed it takes one hour to repair the consequences. The 55th event, failure of stack spark arrestor, was assumed to happen once in every million hours. It was assumed to require one day of repair time. The 56th

event, failure of burner safety low sensor, was assumed to be a flame detector with a failure rate 7.82 per million hours, and with an average repair time of 6.5 hours. Air supply control failure was modeled with a failure of a pump.

Table 4.1. Failure Data for Basic Events in Surface System

No.	Basic Failure Rates	Failure Rates of Basic Events (Failures per Year)	Repair Times for Basic Events (Repairs per Year)	Availability of Failure
1	TSE (Temp. Safety Element)	0.068	43800	0.0000016
2	ESD (Emerg. Shut Down)	0.092	262.3	0.00035
3	Air			1
4	ASH (Gas Detector)	0.042	1510.34	0.000028
5	Vent	0.18	730	0.00025
6	Containment	0.0004	52.14	0.0000077
7	Containment	0.0004	52.14	0.0000077
8	ESD (Emerg. Shut Down)	0.092	262.3	0.00035
9	PSL (Pressure Safety Low)	0.2	755.2	0.00026
10	FSV (Flow Safety Valve)	2.8	580.13	0.0048
11	LSL (Level Safety Low)	1.01	1108.9	0.00091
12	LSH (Level Safety High)	1.01	1108.9	0.00091
13	Pressure Vessel	0.2	1031.8	0.00019
14	Accident	0.0004	2	0.00005
15	Compressor	4.7	155.87	0.029
16	Pump	2.6	216.3	0.012
17	Heat Exchanger	0.0034	111.88	0.00003
18	Vessel	0.47	842.31	0.00056
19	Valves	2.83	344.88	0.0081
20	Pressure Vessel	0.2	1031.8	0.00019
21	PSH (Pressure Safety High)	0.2	755.2	0.00026
22	PSV (Pressure Safety Valve)	1.95	344.9	0.0056
23	Pump	1.41	217.7	0.0064
24	Flowline	0.0045	612.6	0.0000073
25	Compressor	9.98	135.08	0.069
26	Heat Exchanger	0.018	65.6	0.00027
27	Ventilation	0.18	730	0.00025
28	PSV (Pressure Safety Valve)	1.95	344.9	0.0056
29	Atmospheric Vessel	0.009	842.3	0.000011
30	LSL (Level Safety Low)	1.01	1108.9	0.00091
31	Pressure Vessel	0.2	1031.8	0.00019
32	Atmospheric Vessel	0.009	842.3	0.000011
33	Pressure Vessel	0.2	1031.8	0.00019
34	PSL (Pressure Safety Low)	0.2	755.17	0.00026
35	Ventilation	0.18	730	0.00025
36	PSV (Pressure Safety Valve)	1.95	344.9	0.0035

Table 4.1. Failure Data for Basic Events in Surface System (cont.)

37	Atmospheric Vessel	0.009	842.3	0.000011
38	Reboiler	0.009	842.3	0.000011
39	FSL (Flow Safety Low)	0.024	14600	0.0000016
40	TSH (Temp. Safety High)	0.068	43800	0.0000016
41	Reboiler	0.009	842.3	0.000011
42	LSL (Level Safety Low)	0.053	1108.9	0.000048
43	TSH (Temp. Safety High)	0.068	43800	0.0000016
44	TSH (Temp. Safety High)	0.068	43800	0.0000016
45	Pressure Vessel	0.2	1031.8	0.00019
46	Compressor	6.1	221.8	0.027
47	Fuel Control	0.07	850.5	0.000082
48	TSH (Temp. Safety High)	0.068	43800	0.0000016
49	TSH (Temp. Safety High)	0.068	43800	0.0000016
50	IPM (Ignition Prev. Measures)	0.042	1510.34	0.000028
51	Flame Emission	0.083	216.3	0.00038
52	PSL (Pressure Safety Low)	0.011	755.17	0.000015
53	Motor Starter Interlock	0.13	216.3	0.0006
54	Spark Emission	8.76	8760	0.001
55	Arrestor	0.0088	365	0.000024
56	BSL (Burner Safety Low)	0.069	1347.7	0.000051
57	Fuel Gas Supply	0.07	850.5	0.000082
58	PSL (Pressure Safety Low)	0.011	755.17	0.000015
59	Air Supply Control	0.083	216.3	0.00038
60	PSL (Pressure Safety Low)	0.011	755.17	0.000015
61	Motor Starter Interlock	0.13	216.3	0.0006

4.1.2. Calculation of the Availability of the Top Event. The fault tree method is a well- established process to calculate the availabilities of component failures through a series of AND/OR gates. The availability of the top event is the fraction of time a system of components with repair will be in an unsuccessful or failed state. The fault tree for the surface system has nine basic events that are repeated. They are failure of:

- Pressure safety valve (PSV); 28,36
- Pressure vessel; 13, 20, 31*, 33, 45
- Level safety low (LSL); 11, 30*
- Atmospheric vessel; 29, 32*, 37
- Ventilation; 5, 27, 35
- Pressure safety low (PSL); 52, 58, 60

- Temperature safety high (TSH); 40, 43, 48
- Motor Starter Interlock; 53, 61
- Containment; 6,7

Event 28 and 36 are components peripheral to the atmospheric vessel, so the 28th and the 36th events are dependent. The PSV is also the 22nd event, but it is related to pressure vessels. Events 13, 20, 31*, 33, 45 are failures of the control unit of pressure vessels. An asterisk denotes that failure of a pressure vessel occurs in gas blowby twice, but is not shown in Figure 4.4. The failure of a LSL occurs three times in the fault tree, but the one in the event of gas blowby is not shown in Figure 4.4. The 42nd event is also LSL, but this sensor is connected to the reboiler, and its failure data is different. The control unit failure of atmospheric vessels occurs four times in the diagrams. The failure of a vent appears three times in the fault tree diagrams. The failure of a low pressure sensor (PSL) appears five times in the fault tree. Three of them are dependent; they are assumed to be peripheral to the heated component. Event nine, a failure of PSL is assumed to be a generic component, and event 34 is assumed to be relevant to pressure vessels. Another dependent event is the high temperature sensor failure. It appears three times in the fault tree diagrams. The 44th event is assumed to be peripheral to pressure vessels. The 49th event, or second temperature sensor, was assumed to be a redundant sensor, which is another high temperature sensor independent of 40, 43, and 48. The failure of the motor starter interlock appears twice in the fault tree diagrams. The failure of the containment system appears twice in the fault tree diagrams (Figure 4.2).

These particular basic events occur at more than one point in the fault tree. This complicates the calculation because if the basic event occurs at one input with availability of failure, q_i , then it must occur at all other locations with availability of 1. Similarly, if it does not occur at one input with availability $1 - q_i$, then it does not occur at all other locations with availability of 0.

Consider a fault tree with one basic event, q_1 , which is repeated. The availability of the top event can be found using Bayes Theorem as:

$$A(\text{top event}) = q_1 \times A(\text{top event} | q_1 \text{ occurs}) + (1 - q_1) \times A(\text{top event} | q_1 \text{ doesn't occur})$$

The term $A(\text{top event} | q_1 \text{ occurs})$ can be found by forcing $q_1 = 1$ and calculating the unavailability of the top event using the fault tree program. In a similar fashion $A(\text{top event} | q_1 \text{ doesn't occur})$ can be found by forcing $q_1 = 0$ and using the fault tree program [14].

When nine repeated basic events occur, the situation is somewhat more complicated. Now one must consider all combinations of these nine events. Since each event can occur or not occur, there are $2^9 = 512$ combinations. In theory, the program should be run 512 times. In reality, one can get a very good approximation by considering only ten of the 512 states. These ten states are the following:

State 1: No basic event failures exist or $q_i = 0, i = 1, 9$

State 2 → 10: One and only one basic event failure exists or

$$\begin{aligned} q_1 = 1; q_i = 0, i = 1, 9 \text{ and } i \neq 1 \\ q_2 = 1; q_i = 0, i = 1, 9 \text{ and } i \neq 2 \\ \text{etc.} \end{aligned}$$

Then, the availability of the top event will be

$$\begin{aligned} A(\text{top event}) = \prod_{i=1}^9 (1 - q_i) A(\text{top event} | \text{all } q_i = 0) \\ + \sum_{i=1}^9 q_i \left[\prod_{\substack{j=1 \\ j \neq i}}^9 (1 - q_j) A(\text{top event} | \text{all } q_j = 0 \text{ except } q_i = 1) \right] \end{aligned}$$

The terms that are neglected all have more than one factor of q_i . Since these terms are small, the product of two or more of these terms is negligibly small.

When the preceding calculation was done for the surface system, a very small availability of the top event resulted (7.6×10^{-13}). This is logical since any path through the fault tree from basic events to top event involves at least four or five failures with availabilities in the 10^{-3} or 10^{-4} range. When these are processed through AND gates, the result is $(10^{-3} \text{ or } 10^{-4})^m$ where m is 3 or 4 [15].

4.2. ANALYSIS OF THE SUBSEA CONTROL SYSTEMS

4.2.1. Fault Tree Construction of Subsea Control Systems. The subsea portion of the fault tree was developed using the generalized subsea architecture shown in Figure 3.3. The control systems controlling single satellite wells, and more complex subsea production facilities such as multi-well manifold template systems, can be broken into subsystems as shown in Figure 4.9 [16].

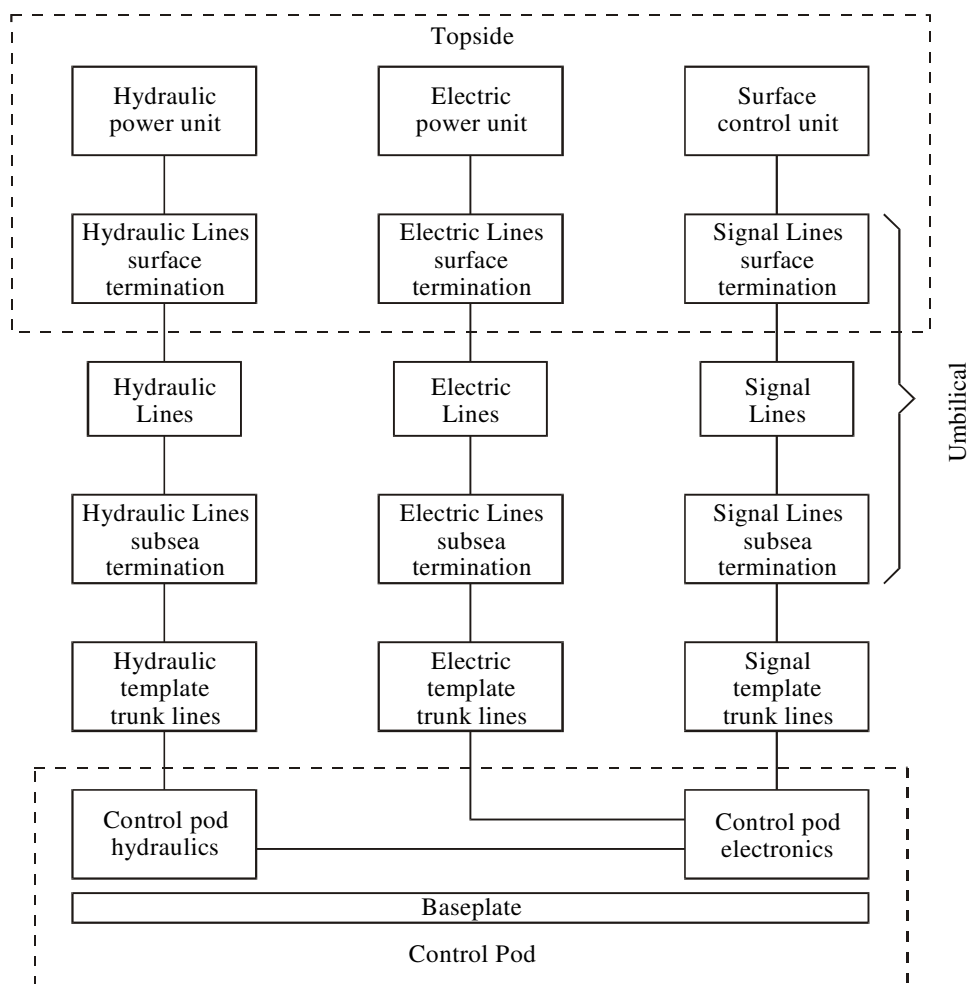


Figure 4.9. Subsea Control Subsystems

Failure modes for the subsystems shown in Figure 4.9 include:

- Electrical Power Failure - Pod (EFP)
- Hydraulic Power Failure - Connector (HFC)

- Hydraulic Power Failure - Line (HFL)
- Hydraulic Power Failure - Pod (HFP)
- Signal Transmission Failure - Connector (SFC)
- Signal Transmission Failure - Line (SFL)
- Signal Transmission Failure - Pod (SFP)
- Signal Transmission Failure - Surface (SFS)

These failure modes are independent events, represented as “OR” gates on a fault tree. Ultimately, however, these “OR” gates are combined because any one fault causes complete system failure.

The block diagram of the subsea control subsystems shown in Figure 4.9 illustrates the flow of electrical power, hydraulic and communications signals that could lead to a critical failure. It should be noted that this is essentially a series system from a reliability point of view (any failure leads to system failure). There are two areas where redundancy occurs; (1) the redundant subsea control modules at either the well or the subsea manifold, and (2) the redundant PLCs at the host facility. In both cases, the failure of the redundant set is considered the basic event and the failure rate is selected accordingly. With these assumptions, the fault tree will consist of only basic events, “OR” gates and derived states, including the top event.

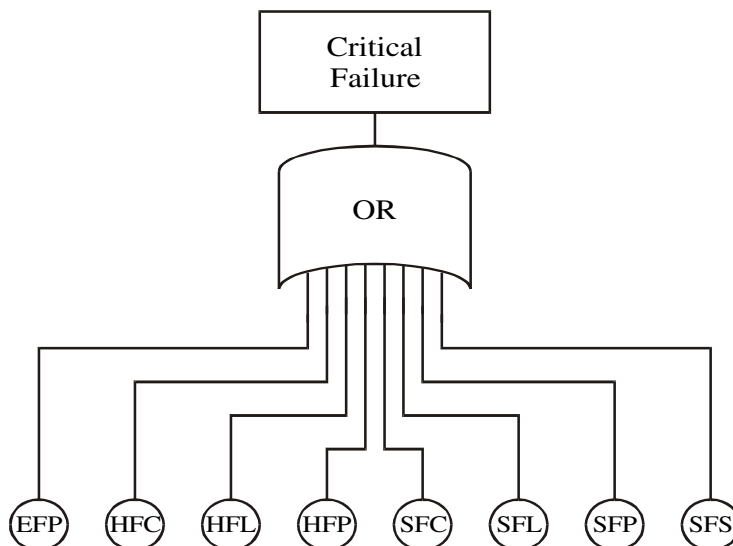


Figure 4.10. Fault Tree for Subsea Control System

It should also be noted that three basic events are actually combinations of two or more fundamental events: (1) the electrical power failure of the pod (EFP) could be either a short circuit at the pod connector or a generic electric failure in the subsea control unit; (2) the signal transmission failure in the line (SFL) could be either a blocked or plugged sensor or a faulty signal line; (3) the signal transmission failure at the pod (SFP) could be either a pilot valve control failure or a subsystem faulty signal.

Using the block diagram in Figure 4.9, the fault tree diagram in Figure 4.10 can be drawn. In this fault tree diagram, hydraulic failures (HFC, HFL or HFP) and signal failures (SFP, SFC or SFL) can occur for any of the n satellite wells. In addition, signal failures on the surface (SFS) can occur for any of the m group controls. Once again, the failure rates used account for this fact (Effective failure rate equals n or m times component failure rate) Dunn-Norman, et al., 2000, [16].

4.2.2. Failure Probability of Subsea Control Systems. Based on the data from OREDA, 1997, [9], the following fault rates are used in Table 4.2 for the basic events in the fault tree, where all fault rates are in failures per million hours. It is easily seen that the electric power failure at the pod (EFP), and the signal transmission failure - line (SFL) are the dominant failure modes. The overall failure rate for critical failures is 132.93 failures per million hours or about 1.16 failures per year. This corresponds to a mean time to failure of about 0.86 years. The average time to repair the subsea control system was found to be 47 hours. The availability of the failure of subsea control systems was found 0.00618.

Table 4.2. Failure Rates and Repair Times for Subsea Failure Modes

Failure Modes Multiplexed electro hydraulic	Failure Rates of Failure Modes (Failures per Million Hours)	Repair Times for Failure Modes (Mean Time to Repair-Hours)
EFP	42.8	7.8
HFC	3.81	109.9
HFL	7.62	144
HFP	1.9	109.9
SFC	1.9	1
SFL	57.4	1
SFP	3.81	1
SFS	13.69	1

4.3. SCADA SYSTEM ANALYSIS

4.3.1. Development of The SCADA Fault Tree. The fault trees for the surface facilities on a typical offshore platform were shown through Figure 4.2 to 4.8. The previous fault tree diagrams were constructed mainly for initiating events, sensor failures, and control unit failure of main hardware components (pumps, vessels, etc.), which were assumed to be PLCs. Using the typical SCADA system as shown in Figure 3.2, the fault tree was constructed as shown in Figure 4.11. The SCADA fault tree constructed in this section is at the supervisory level that includes PCs, PLCs, and communication links.

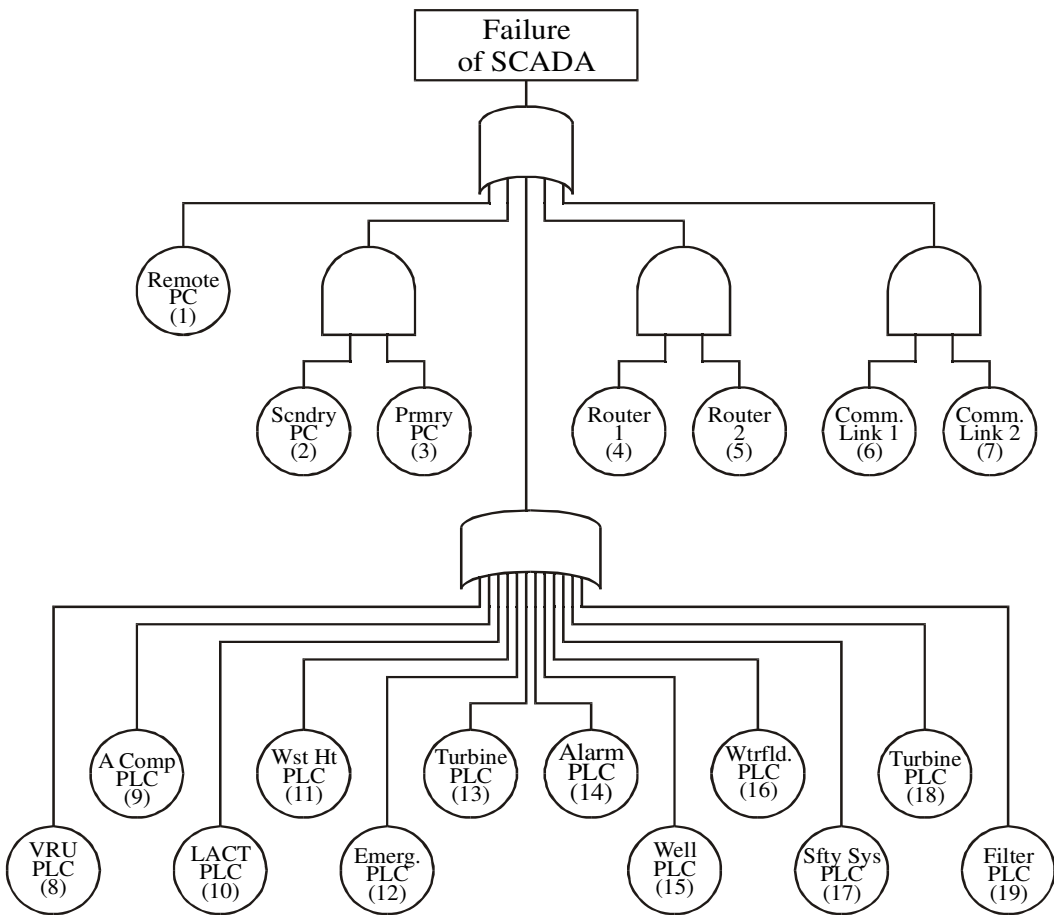


Figure 4.11. The Fault Tree Diagram for a Distributed Platform SCADA System

SCADA failure occurs, in the case of one remote PC failure, primary and secondary PC failures, any PLC failure, both routers failure, or both communication links failure. The PLCs used in the process are: Vapor Recovery Unit (VRU) PLC, air compressor PLC, LACT PLC, waste heat PLC, emergency PLC, turbine generator PLC, alarm PLC, well PLC, waterflood PLC, safety system PLC, and water filter PLC. In the event of a SCADA system failure, redundancy is another issue of concern. There are two communication networks. The system fails if both of the communication links fail.

4.3.2. Failure Probability of the SCADA Systems. A PC's failure rate is found to be 122.66 failures per million hours. Average repair time for a PC is 4.1 hours. These values are converted to failures per year and repairs per year. Similarly, the failure rate for a PLC is found to be 134.83 failures per million hours, and a PLC requires 1.1 hour to be repaired. The communication network availability of 0.99 was supplied from one operator. Assuming one hour of repair for the communication network, failure rate was found as in Table 4.3. The router failure rate was estimated to be 3 failures per million hours, and the repair time for the router was estimated to be five minutes. The router failure rate was estimated from switch failure rate [11].

The availability of the top event (failure of the SCADA system) can be found by analyzing the fault tree diagram with the basic event data of Table 4.3. Calculating this value results in the availability of the top event (SCADA system failed) equal to 1.2×10^{-2} . The average time to repair of the SCADA system was calculated using the average repair times. This calculation yielded an average of 1.6 hours to fix any problem due to SCADA failure. The failure rate is dominated by the communication network.

Table 4.3. Failure Data for Basic Events in SCADA Fault Tree

No	Basic Events	Failure Rates of Basic Events (Failures per Year)	Repair Times for Basic Events (Repairs per Year)	Availability of Failure
1	Remote PC	1.075	2136.6	0.0005
2, 3	PC	1.075	2136.6	0.0005
4, 5	Router	0.027	73000	0.0000004
6, 7	Comm. Link	109.1	8760	0.01
8-19	PLC	1.18	7963.6	0.00015

4.4. HUMAN ERRORS IN THE SCADA SYSTEM

One of the most difficult tasks in a reliability study is to assess the relative importance of human error versus component failures. Data exist on the frequency of human error in common tasks found in an industrial environment (Henley and Kumamoto, 1992, [6]; Shooman, 1968, [7]). The fact that there is a high degree of automation in the operation should minimize the chance of human error.

For the SCADA systems used in offshore facilities, there is not much need for human actions. The SCADA system can fail because of incorrect human action at the remote PC and one of the PLC's, shown as the fault tree in Figure 4.12.

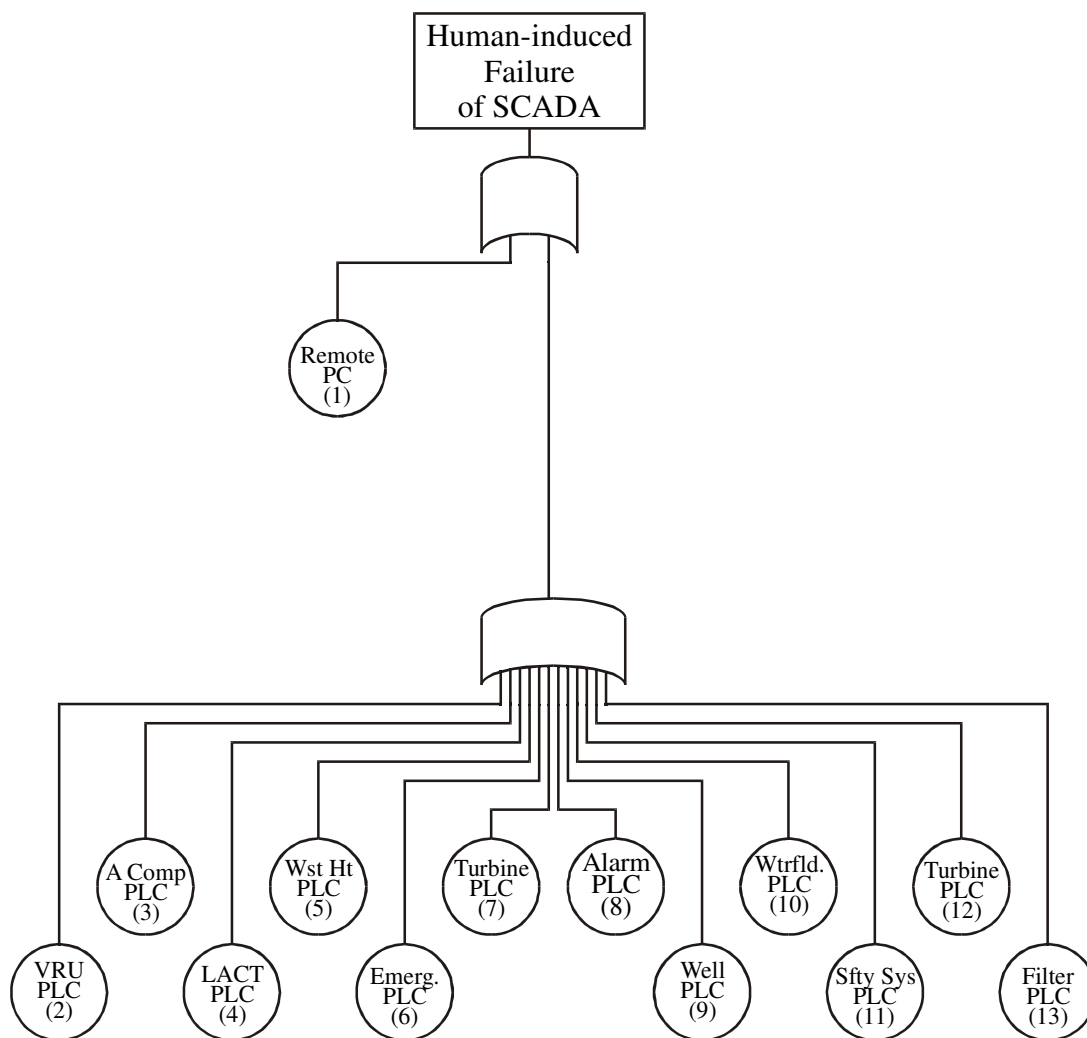


Figure 4.12. Human-induced SCADA Failure Fault Tree

For each PLC, the probability of checking the wrong indicator lamp on the local operator panel is 0.003 (Henley and Kumamoto, 1985, [10]). For the PC, the probability of wrongly reading an indicator is 0.001 (Henley and Kumamoto, 1985, [10]). Using these numbers, the human reliability in the SCADA system is 0.999964. The probability of human error that could result in the failure of the SCADA system is $1 - 0.999964 = 3.54 \times 10^{-5}$.

4.5. SOFTWARE RELIABILITY OF THE SCADA SYSTEMS

The software reliability was approached in a manner similar to that of the overall SCADA system. The fault tree is the same as for the SCADA system (Figure 4.11), but with the failure information shown in Table 4.4.

For each PC in the SCADA system there are 122.66 failures per 10^6 hours. According to [9], 5.61% of these failures are due to software failures. Thus, one can calculate 6.88 ($122.66 \times 5.61\% = 6.88$) failures per 10^6 hours. The MTTR for PC's is 4.1 hours. From this information, the software availability is calculated as 0.99997.

For each PLC, there are 134.83 failures per 10^6 hours. Assuming 5.61% of these failures are due to software failures, there are 7.56 ($134.83 \times 5.61\% = 7.56$) failures per million hours. The MTTR for a PLC is 1.1 hours. From this information, the calculated software availability for a PLC is 0.99999.

For the routers, the assumption is that 5.61% of the failures are software failures. Communication link availability is assumed to be the same as for the analysis of the entire SCADA system.

The overall availability of the software for the system is 0.9906. As with the previous SCADA system analysis, communication links dominate the calculations.

Table 4.4. Software-induced Failure Data for Basic Events in SCADA Fault Tree

No	Basic Events	Failure Rates of Basic Events (Failures per Year)	Repair Times for Basic Events (Repairs per Year)	Availability of Failure
1	Remote PC	0.060	2136.6	0.00003
2, 3	PC	0.060	2136.6	0.00003
4, 5	Router	0.0015	73000	0.00000002
6, 7	Comm. Link	109.1	8760	0.01
8-19	PLC	0.066	7963.6	0.00001

5. RESULTS

The reliability of the SCADA systems used in the offshore oil and gas industry has been investigated using a probabilistic risk assessment method. The fault tree analysis method provides identification of system potential failure modes. The fault tree analysis method can be thought as an art. Different implementations of the fault tree diagrams are possible. The analysis results are discussed in this section.

In looking at the surface subsystem, the availability of failure is found to be 7.6×10^{-13} . Using an average of 1.6 hours to fix a problem in the SCADA system, it was found that the MTTF is 2.5×10^8 years. Even though this number seems high, it is logical because the fault tree has four to five layers, in which every layer has a small probability to fail. Other fact is that human errors were not considered to assess surface availability. Human factors were considered separately. While doing the calculations it was found that the containment system has significant effect on the offshore facilities' availability. It could be concluded that if the containment system fails, it is more likely that a release of hydrocarbons will occur. The results of dependent event failure availability, given that the rest of the dependent events have occurred, are given in Table 5.1.

Table 5.1. Dependent Event's Failure Availabilities

Dependent Events	Availability of Failure of The Dependent Event Given The Rest of The Dependent Events Occurred
Vent	2.37×10^{-25}
Containment	2.21×10^{-7}
LSL	6.62×10^{-30}
Pres. Vessel	6.71×10^{-30}
Atm. Vessel	6.62×10^{-30}
PSV	6.62×10^{-30}
TSH	6.62×10^{-30}
PSL	1.32×10^{-17}
Motor Starter Int.	1.08×10^{-17}

In looking at the subsea portion of the analysis, it can be concluded that the hydraulic components are the main reason for the failure. This is concluded from Table

4.2. On the other hand, because one cannot eliminate hydraulic components in the system, the repair times should be decreased to increase the availability of the subsea control systems.

The SCADA portion of the system seems reliable compared to the digital controllers in the nuclear industry. The software unavailability is 1.1×10^{-5} failures per demand for a specific brand of software that is used in nuclear industry [17]. Assuming 1 hour of average repair time, the failure rate would be 11 failures per million hours. The assumption to repair the system was made to reboot the system, not to fix the operating system crashes. Looking at the SCADA systems used in offshore platform facilities, system unavailability was found to be 8.3×10^{-4} as in Table 5.2. By looking at the individual components in the SCADA system, PLCs and PCs have an approximate failure rate of 100 failures per million hours. The availability for the communication network is 99%, which compared to the other components (PLC, PC, etc.), indicates that it should be a candidate for improvement.

The results of the reliability analysis of SCADA systems used in offshore facilities are summarized in Table 5.2. In the first column the subsystems and combined subsystems are shown. In the second column the MTBF in per year for those systems are given. The MTTR of the SCADA system is low compared to the MTTF of the system, so the MTBF is used instead of the MTTF to show the failure rates per year. In the last column the failure availability for each system is given.

Table 5.2. Summary of Reliability Analysis Results

System	MTBF (years)	Failure Availability
Surface	2.5×10^8	7.6×10^{-13}
Subsea Control	0.86	0.00618
Surface/Subsea	0.86	0.00618
SCADA	0.09	0.012
Surface/SCADA	0.09	0.012
Surface/Subsea/SCADA	1.4	0.00083
Human Error Probability		0.000035
Software	0.0095	0.0094

6. CONCLUSIONS

This chapter concludes the thesis, presents conclusions that are drawn from this work and makes suggestions for future work. To speak about the reliability of a system, the numbers gathered are compared relatively.

1. Reliability analysis of the surface facilities shows that mechanical components, pumps and compressors, have higher failure rates compared to other mechanical components e.g. vessels, valves.
2. Final safety systems e.g. containment, ESD should be working properly in order to impede a release of hydrocarbons.
3. The failure rate of the hydraulic components in the subsea is higher than electrical components, and those hydraulic components are the main reason for low availability. If the repair times for those hydraulic components are decreased, availability of the subsea systems would increase.
4. The failure rate for subsea control systems may seem high but, in this context, a “critical failure” means loss of automatic control. Oil spills will also require a simultaneous leak in a critical valve component. This aspect of the reliability study has not been addressed.
5. The main reason for the SCADA failure is the communication network failure. PLCs and PCs have low failure rates compared to communication network. The availability of the communication network should be increased for a more reliable SCADA system.
6. The importance of human factors when incorporating in safety critical systems is crucial. Since the SCADA system is highly automated, the probability of a human error causing a hydrocarbon leak is small. On the other hand, a wrong decision at the wrong time may directly cause catastrophic consequences. The performance of human actions depends on different factors. These factors (motivation, work hours, hunger etc.) are explained in [10]. The performance is best when there is moderate stress on human operators [6].

7. Control software and HMI software are the products that are used in the SCADA software. The reliability of the software can be increased at the design stage, instead of development stage. If the errors in a program are discovered and corrected through testing, the cost to improve the reliability after design would be higher [18]. The software development should be standardized to increase the reliability of software. The standardization process in the software product cycle will reduce the time to train new personnel, and reduce the cost [15], [18].
8. There should be sharing of failure data in commercial industries.

APPENDIX A.
PROGRAM REC

```
// REC.cpp : Defines the entry point for the console application.
//
//This is a program to find the probability and failure rate
//of the top event, for a general type of fault tree model.
//
//In this fault tree, it is assumed that all the states are designated
//in the ascending order, starting from the top event.
//Also it is assumed that a maximum number of five basic events and
//five states are allowed as inputs to any state.
//
//The information needed is: the total number of states,
//total number of basic events, failure rates of all the
//basic events, and the topology of the fault tree.
//
//The variables used in this program are as follows:
//
//User supplied variables:
//
//M: Number of basic events
//N: Number of states
//IS: Information of inputs from other gates
//IB: Information of inputs from basic events
//C: Type of gate(1= "AND" gate, 0= "OR" gate)
//B: Failure rates of the basic events
//
//Internal variables:
//
//SSAVE: Temporary storage for the values of the intermediate states
//BSAVE: Temporary storage for the values of the intermediate states
//SAVE: Temporary storage for the values of (i) basic events while
//executing OR function
```

```

//MS:Counter to check the number of states
//MB:Counter to check the number of basic events
//MT:Total number of inputs to the OR gate
//NP:Vaule of the highest designated selected state
//IX:Temporary storage for the values of either intermediate states
//or basic events
//x:A variable used in calculations of probabilities of different states
//
//Output variables:
//
//P:Probabilities of the basic events
//A[NP]:Probability of intermediate states
//A[1]:Probability of the top event

#include <iostream.h>
#include <math.h>
#include <stdio.h>

int main(int argc, char* argv[])
{
    double B[100], P[100], SSAVE[5], BSAVE[5], A[100],SAVE[100],x;
    int M,N,NP,IS[100][5],IB[100][5],C[100],MS,MB,IX,MT;
    int i,j,k;
    float a=0;

    /*read in data*/

    printf("\n Enter number of basic events and intermediate states : ");
    scanf("%d %d", &M, &N);

```



```

for(i=0;i<M;i++)
{
    printf("\n Enter failure rate for the %d.th event : ",i);
    scanf("%f", &a);
    B[i]=a;
}

for(i=0;i<N;i++)
{
    for(j=0;j<5;j++)
    {
        printf("\n Enter gate numbers for %d.th state IS[%d][%d]: ", i,i,j);
        scanf("%d",&IS[i][j]);
    }
}

for(i=0;i<N;i++)
{
    for(j=0;j<5;j++)
    {
        printf("\n Enter event numbers for %d.th state IB[%d][%d]: ",
i,i,j);
        scanf("%d",&IB[i][j]);
    }
}

for (i=0;i<N;i++)
{
    printf("\n Enter gate type for %d.th gate : ",i);
    scanf("%d",&C[i]);
}

```

```
/* Convert failure rates into corresponding probabilities */
```

```
for(i=0;i<M;i++)  
{  
    P[i]=B[i];  
}
```

```
/* Select the highest designated state (NP) */
```

```
for (k=0;k<N;k++)  
{  
    NP=N-k-1;  
    MS=0;
```

```
    /* Set each SSAVE[j] & BSAVE[j]=1 */
```

```
    for(j=0;j<5;j++)  
    {  
        SSAVE[j]=1;  
        BSAVE[j]=1;  
    }
```

```
/* Fetch states that are connected as inputs to state NP */
```

```
for(j=0;j<5;j++)  
{  
    IX=IS[NP][j];
```

```
/* Test whether any states are connected as inputs to state NP */
```

```

        if(IX>=0)
        {
            SSAVE[MS]=A[IX];
            MS=MS+1;
        }
    }
    MB=0;

```

/* Fetch basic events that are connected as inputs at state NP */

```

for(j=0;j<5;j++)
{
    IX=IB[NP][j];

```

/* Test for the presence of basic event to state NP */

```

        if(IX>=0)
        {
            BSAVE[MB]=P[IX];
            MB=MB+1;
        }
    }

```

/* Test for the type of gate */

```

if(C[NP]==1)
{
    x=1;

    for(j=0;j<5;j++)
    {

```

```
        x=x*SSAVE[j]*BSAVE[j];
    }

    A[NP]=x;

}

else

{

    /* Test if any states are connected as inputs to state NP */

    if(MS>0)
    {
        for(i=0;i<MS;i++)
        {
            SAVE[i]=SSAVE[i];
        }
    }

    /* Test if any basic events are connected as inputs to state NP */

    if(MB>0)
    {
        for(i=0;i<MB;i++)
        {
            SAVE[MS+i]=BSAVE[i];
        }
    }
}
```

```
/* Total number of inputs to state NP */

MT=MS+MB;
x=SAVE[0];
MT=MT-1;

/* Test if total inputs to state NP is zero */

if(MT>0)
{
    for(i=0;i<MT;i++)
    {

        /* Execute the two input "OR" Gate */

        x=(x+SAVE[i+1])-(x*SAVE[i+1]);

    }
}

A[NP]=x;
}

}

/* Print the probability of the top event */
printf("\n A[0]=%e",A[0]);

return 0;

}
```

APPENDIX B.
SAFETY DEVICE DESIGNATIONS

Safety Device Designations

VARIABLE	SAFETY DEVICE DESIGNATION		Abbreviation
	Common	Instrumentation Society of America (ISA)	
Backflow	Check valve	Flow Safety Valve	FSV
Burner flame	Burner flame detector	Burner Safety Low	BSL
Flow	High flow sensor	Flow Safety High	FSH
	Low flow sensor	Flow Safety Low	FSL
Level	High level sensor	Level Safety High	LSH
	Low level sensor	Level Safety Low	LSL
Pressure	High pressure sensor	Pressure Safety High	PSH
	Low pressure sensor	Pressure Safety Low	PSL
	Pressure relief or safety valve	Pressure Safety Valve	PSV
Temperature	High temperature sensor	Temperature Safety High	TSH
	Low temperature sensor	Temperature Safety Low	TSL
Fire	Heat detector	Temperature Safety High	TSH
	Fusible material	Temperature Safety Element	TSE

BIBLIOGRAPHY

1. <http://ref.cern.ch/CERN/CNL/2000/003/scada/>
2. <http://www.micrologic-systems.com/primers/scada.htm>
3. Kelvin T. Erickson, Ann Miller and E. Keith Stanek, Shari Dunn-Norman. "Survey of SCADA System Technology and Reliability in the Offshore Oil and Gas Industry." Proposal to United States Department of Interior, Mineral Management Service, Technology Assessment & Research Program. University of Missouri – Rolla, 2000.
4. Dhillon, B. S. and Reiche, H. 1985. *Reliability and Maintainability Management*, Van Nostrand Reinhold Company Inc.
5. Billinton, R. and R.N. Allan. 1992. *Reliability Evaluation of Engineering Systems: Concepts and Techniques*, 2nd Ed., New York: Plenum Press
6. Henley, E.J. and H. Kumamoto. 1992. *Probabilistic Risk Assessment*, New York: IEEE Press.
7. Shooman, Martin L., *Probabilistic Reliability: An Engineering Approach*, McGraw-Hill, New York, 1968.
8. Henley, E.J. and H. Kumamoto. 1981. *Reliability engineering and risk assessment*, Prentice-Hall, Inc.
9. SINTEF, 1997, *OREDA - Offshore Reliability Data*, 3rd Edition, SINTEF Industrial Management, Trondheim, Norway.

10. Henley, E.J. and H. Kumamoto. 1985. *Designing for Reliability and Safety Control*, New Jersey: Prentice-Hall Inc.
11. Smith, David J., *Reliability and Maintainability in Perspective*, Second Edition, New York: John Wiley & Sons, 1985
12. API, 1998. *Recommended Practice 14C*, sixth edition, March 1998; Recommended Practice for Analysis, Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms.
13. Apostolakis, G., Garriba, S., Volta, G. 1978. *Synthesis and Analysis Methods for Safety and Reliability Studies*, Plenum Press.
14. <http://www.kenonic.com/techexp/humach.htm>
15. Kelvin T. Erickson, Ann Miller and E. Keith Stanek, Shari Dunn-Norman. 2000. Survey of SCADA System Technology and Reliability in the Offshore Oil and Gas Industry
16. Dunn-Norman, S., Erickson, K. T., Cetinkaya, E. K., Stanek, E.K. and Miller, A., "SCADA System Trends In Deepwater Developments" Rio Oil & Gas Expo and Conference, October 2000
17. USNRC. 1997. *Digital Instrumentation and Control Systems in Nuclear Power Plants*, NUREG/CR-6101, Washington, D.C.: USNRC.
18. Yates III, Wilson D. The Application of Reliability Engineering Concepts to Software Development. Thesis. University of Missouri-Rolla, 1990. Rolla: UMR. 1990. T6044.
19. Musa J.D., A. Iannino, and K. Okumoto. *Software Reliability: Measurement, Prediction, Application*, McGraw-Hill, 1987

20. Stanek, Keith E. 1980. EE 403: Power System Reliability. Produced and directed by Michigan Technical University. 20 Videocassettes.

21. Gupta, Gopal B. Safety Analysis of Mine Electrical Power Systems Using Reliability Techniques. Thesis. Michigan Technical University, 1982.

VITA

Egemen Kemal Cetinkaya was born on August 2, 1977, in Izmir, Turkey. He received his primary education in Malatya, Turkey. He received his secondary education from Malatya Science High School in Malatya, Turkey. He received his Bachelor of Science degree in Electronics Engineering from Uludag University, Bursa, Turkey in June 1999.

He has been enrolled in the Graduate School of the University of Missouri-Rolla since January 2000. During his studies, he worked as a graduate research assistant at the Electrical Engineering department at UMR.